Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

EDITORIAL
MAR ABIERTO

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE INFORMACIÓN

Análisis y comparación con las otras Autoridades Portuarias del Ecuador

Jéssica Ostaiza Macías
Carlos Manosalvas García
Danny Aguaiza Tenelema
Ulises Carofilis Moreira

Colección
T.I.C.

Esquema gubernamental de seguridad de información

Análisis y comparación con las otras Autoridades Portuarias del Ecuador

Jéssica Ostaiza Macías
Carlos Manosalvas García
Danny Aguaiza Tenelema
Ulises Carofilis Moreira

EDITORIAL MAR ABIERTO

Universidad Laica Eloy Alfaro de Manabí
Ciudadela universitaria vía circunvalación (Manta)
www.uleam.edu.ec

Autoridades:
Miguel Camino Solórzano, Rector
Iliana Fernández, Vicerrectora Académica
Doris Cevallos Zambrano, Vicerrectora Administrativa

Esquema gubernamental de seguridad de información
Análisis y comparación con las otras Autoridades Portuarias del Ecuador

Revisión pares académicos:
Nombre: Benigno Javier Alcívar Martínez
Institución: Espam
Tiempo completo
Teléfono: 0990547811
Email: balcivar@espam.edu.ec

Nombre: Edgar Xavier Salazar Ojeda
Institución: Universidad Politécnica Salesiana
Tiempo completo
Teléfono: 0998274381

Email: esalazar@ups.edu.ec

Consejo Editorial: Universidad Laica Eloy Alfaro de Manabí
Director Editorial: Hernán Murillo Bustillos
Diseño de cubierta: José Márquez
Diseño y diagramación: José Márquez
Estilo, corrección y edición: Alexis Cuzme (DEPU)

ISBN: 978-9942-775-01-6
Edición: Primera. Octubre 2017

Departamento de Edición y Publicación Universitaria (DEPU)
Editorial Mar Abierto
2 623 026 Ext. 255
www.marabierto.uleam.edu.ec
www.depu.uleam.blogspot.com
www.editorialmarabierto.blogspot.com
Manta - Manabí – Ecuador

ÍNDICE GENERAL

RESUMEN

El Esquema Gubernamental de Seguridad de la Información, está conformado básicamente por dominios, directrices y controles de la Norma ISO 27002, eliminando controles que no tienen que ver con actividades de las empresas públicas. Los demás controles del EGSI involucran áreas de las instituciones como Administrativo, Seguridad, Talento Humano y de manera primordial Tecnología de la Información.

Validar qué resultados se obtuvo por la implementación del Esquema Gubernamental de Seguridad de la Información, dispuesto por Decreto Ministerial, en la Autoridad Portuaria de Manta, es el objetivo clave de este libro, comparando resultados con otras Autoridades portuarias a nivel Nacional, de igual forma, comparar resultados obtenidos enfocados en la seguridad de la información, con puertos internacionales que aplican Norma ISO 27002 y como el Esquema basado en la Norma ISO, apoyo en la infraestructura tecnológica y de seguridad de la institución.

Se analizaron normas, estándares, relacionados con la seguridad de la información y con seguridades en instalaciones portuarias, ya que el giro del negocio de la institución a investigar, es el de brindar los servicios portuarios. Adicional se comparó la implementación del Esquema Gubernamental de Seguridad de la Información con otras instalaciones portuarias del país, utilizando mecanismos como cuestionarios para la recopilación de datos y un benchmarking de los resultados obtenidos entre las Autoridades portuarias, ya que el país no cuenta con muchas instituciones que tengan el mismo giro de negocio, solo se pudo comparar los resultados obtenidos entre las cuatro autoridades portuarias del país.

Palabras Claves: información, portuaria, seguridad.

PRÓLOGO

Con el transcurrir de los tiempos y la evolución de los ataques informáticos, los cuales se han dado a conocer a nivel mundial siendo los afectados desde un simple usuario de hogar hasta grandes empresas, lo cual ha podido mostrar, que la seguridad de la información es un punto débil y de poco interés en las empresas en especial para los altos directivos. En el año 2011, en Ecuador, se presentó una ola de ataques informáticos a empresas públicas y privadas, lo cual se fue expandiendo a otros países vecinos (Operación Cóndor, por el grupo Anonymous), donde se pudo observar la fragilidad de los sistemas informáticos y sus seguridades, ante ataques como la denegación de servicio, *phishing, facing*, entre otros, notando que la seguridad informática no era un punto principal en la agenda de los Directores de Tecnología de estas empresas.

No solo los ataques informáticos antes mencionados, han demostrado que la seguridad de la información es frágil, la fuga o robo de información dentro de las empresas públicas por funcionarios o por terceros, es otro ejemplo. Esta información de las empresas que fue usurpada la utilizaron para dar inicio a acusaciones, demostrar problemas internos en la institución, relacionados con corrupción, deficiencias en las instituciones, o simplemente para desinformar, hizo que el Gobierno Central tome acciones pertinentes para proteger, controlar y asegurar la información dentro de las instituciones públicas, en especial las que tienen una dependencia directa con la Presidencia de la República. En el 2013, sale a la luz un decreto ejecutivo que obliga a las instituciones públicas, implementar un Esquema Gubernamental de Seguridad de la Información, para normalizar y regular a todas las Entidades que dependen del Estado, a manejar procesos y políticas básicos enfocados en la seguridad de la información, basándose en la Norma ISO 27002.

La implementación del EGSI, se lo realiza con el objetivo de resguardar y proteger la información, cumpliendo con los principios de la seguridad de la información, los cuales son la **Confidencialidad**,

Disponibilidad e **Integridad**, adicional para que la ciudadanía tenga confianza en la información que es procesada en las entidades del Estado. Este Esquema Gubernamental, es de carácter obligatorio su implementación, para las empresas que dependen del Gobierno Central el cual tiene un límite de tiempo (25 de marzo de 2015) y deberá cumplir con todos los reglamentos y procedimientos indicados en el Acuerdo Ministerial No. 166, dando inicio con la FASE I, que tiene determinado 126 controles agrupados por Dominio y denominados prioritarios por el ente regulador que es la Secretaría Nacional de Administración Pública (SNAP).

El órgano regulador SNAP, por medio de la Sub Secretaría de Gobierno Electrónico, quien apoya, guía y controla la implementación del EGSI a más 100 empresas, las cuales se comprometen primero en conformar un Comité de Seguridad de la Información, luego en nombrar un Oficial de Seguridad de la Información, que será la contraparte de la SNAP en la empresa Pública y que es la persona encargada de ejecutar la implementación de dicho Esquema. Todas estas instituciones están obligadas a reportar mensualmente los avances de la implementación en el sistema de Gobierno por Resultados (GPR).

CAPÍTULO 1

1.1.1 LA INFORMACIÓN

La información en una institución, es un activo valioso, sea este tangible o no (físico o digital), por este motivo requiere de un control y protección del medio o mecanismo por el que se vaya a transmitir. La interconexión global aumenta el rango de amenazas y vulnerabilidades hacia la información.

En la actualidad la información está vinculada directamente al buen funcionamiento de una institución, proteger la disponibilidad, la confidencialidad e integridad es ahora un reto y compromiso de las instituciones.

1.1.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información hace referencia al control, y protección enfocadas en dar continuidad a las operaciones de la institución, protegiendo de la gran cantidad de amenazas y riesgos que pueden generarse, permitiendo reducir los daños y problemas que causarían dichas amenazas.

Esta seguridad de la información se la obtiene implementando controles, como políticas, mejores prácticas, manuales y procedimientos, hardware y software en especial para la protección de la información digital. Dichos controles deben de seguir un proceso hasta cumplir con el objetivo de la seguridad por el cual se lo está implementando, permitiendo lograr una madurez en dicho control.

1.1.3 PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

- Integridad
- Disponibilidad
- Confidencialidad

1.1.4 ISO

"La *International Organization for Standardization* o simplemente Organización para la Estandarización Internacional, surge de la unión de dos organismos creados previamente dedicados a la estandarización. Estos organismos estaban formados por asociaciones nacionales dedicados a la creación de estándares." (ISO 9001 CALIDAD PARA TODOS, 2012)

"Tiene como función principal la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional." (LOGISMAN, 2011)

1.1.5 SERIE DE NORMAS ISO/IEC 27000

La información es el principal activo de las organizaciones, esta reside en la infraestructura tecnológica y físicamente en papeles, utilizada por los usuarios, la cual garantiza el éxito y continuidad en los mercados de las empresas.

Por este motivo que las altas autoridades le dan o deberían darle un enfoque especial a la protección de la información y sus sistemas informáticos que administran toda la información de su negocio.

La gestión de seguridad de la información en las organizaciones, en la actualidad está tomando un enfoque primordial para las instituciones, requiriendo que este sistema cubra los objetivos de seguridad de la institución y genere como resultado una correcta evaluación de los riesgos que podría tener la información de la institución.

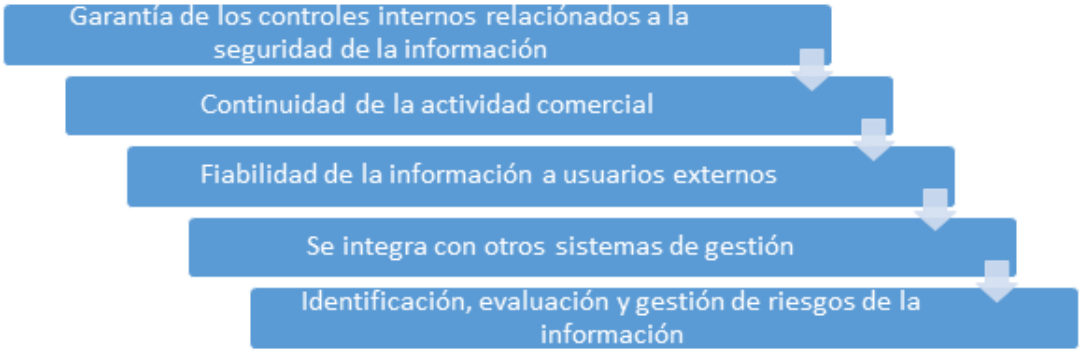

Figura 1: Beneficios que sobresalen de la norma, cuando las empresas lo implementan.

1.1.6 HISTORIA DE ISO/IEC 27000

Sus orígenes se dan desde 1901 por una entidad de normalización a nivel mundial llamada BSI (*British Standards Institution*) la cual fue responsable de algunas Publicaciones como:

- BS 5750, publicada en 1979, la cual ahora es ISO 9001
- BS 7750, publicada en 1992, la cual ahora es ISO 14001
- BS 8800, publicada en 1996, la cual ahora es OHSAS 18001

La norma BS 7799, fue publicada en 1995, con la finalidad de dar los lineamientos y conjunto de mejores prácticas para la gestión de seguridad de la información, para cualquier empresa británica o no británica. La ISO/IEC 27000, fue publicada en mayo de 2009, revisada con una segunda edición en diciembre de 2012 y una tercera edición a inicios de 2014.

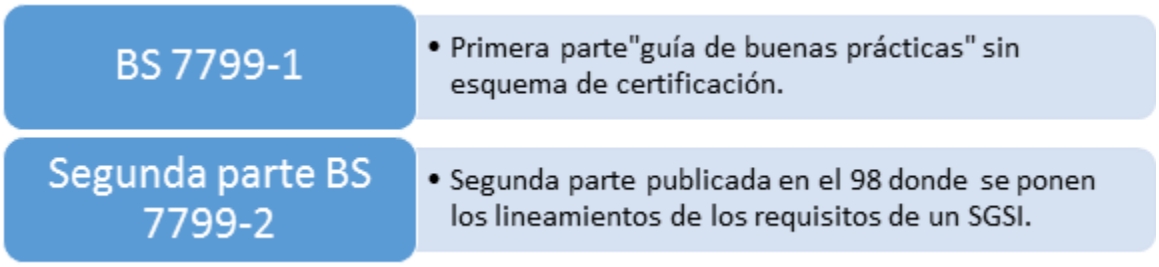

Figura 2: Partes por la cual se conforma la Norma.

En 1999 fue revisada la primera parte de la norma y adoptada por ISO en el año 2000, como ISO 17799, mientras que en el 2002 la segunda parte se adecuo para la ISO de sistema de gestión. En el 2005 la segunda parte de la norma se publicó como ISO 27001 y la primera parte se la renombra como ISO 27002:2005 en el año del 2007.(ISO 27000.ES EL PORTAL DE ISO 27001 EN ESPAÑOL, 2012)

A continuación, se detalla en la gráfica los acontecimientos más importantes de la historia de la norma ISO relacionado a la seguridad de la información.

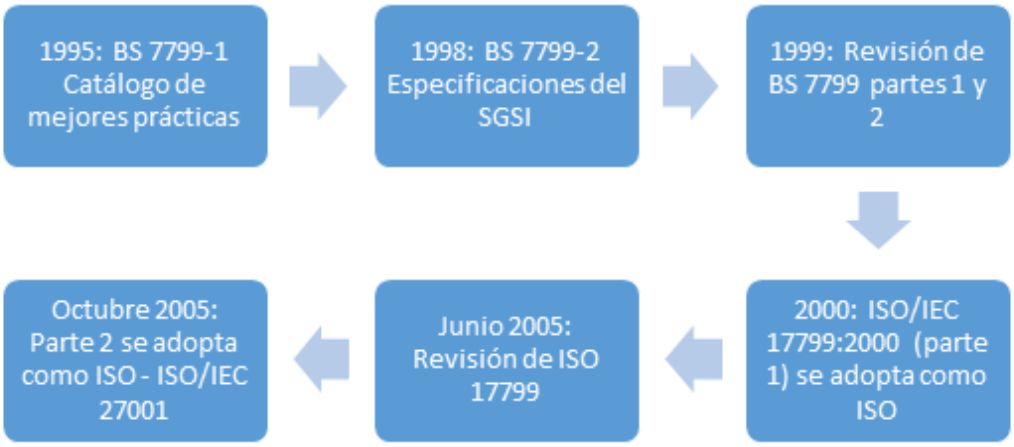

Figura 3: Historia resumida de la norma ISO en seguridad de la información.

1.1.7 SERIE DE ESTÁNDARES DE LA ISO 27000

A diferencia de otras normas, ISO 27000 agrupa varios estándares relacionados con la protección y seguridad de la información, los cuales han sido elaborados por la Organización Internacional para la Estandarización y la Comisión Electrónica Internacional.

Estas series incorporan las prácticas para la implementación de los Sistemas de Gestión de Seguridad de la Información. La ISO reservó ciertos rangos de numeración para la serie 27000, tal como se muestra a continuación:

Figura 4: Normas de la Serie ISO 27000.

ISO 27000: Actualmente está en una fase de desarrollo, es un estándar para el Sistema de Gestión de Seguridad de la Información. Contendrá los términos y definiciones para toda la serie ISO 27000, ya que se necesita de un vocabulario claramente definido.

ISO 27001: Certificación para organizaciones, norma que indica los lineamientos para implementar un Sistema de Gestión de Seguridad de la Información. Publicada en octubre de 2005, de la familia de estándares ISO 27000, relacionada con la gestión de riesgos y la mejora continua de procesos.

ISO 27002: Remplazo de nombre a la ISO 17799:2005 en julio de 2005. Este estándar es una guía de las buenas prácticas recomendables en cuanto a los controles de seguridad de la información. Está conformado por 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Figura 5: Distribución de los dominios de la norma ISO 27002. (INTECO - Instituto Nacional de Tecnologías de la Comunicación, 2014)

ISO 27003: Este estándar fue publicado en febrero de 2010, no está actualmente certificada, pero incluyen las directrices para la implementación de un SGSI e información sobre el modelo PDCA (Plan – Do – Check – Act) con los requisitos en cada fase. (INSTITUTO URUGUAYO DE NORMAS TÉCNICAS, 2014)

ISO 27004: Publicada en diciembre del 2009, estándar que proporciona las métricas para la gestión de seguridad de la información. En él se incluyen las recomendaciones:

- QUIÉN realiza las mediaciones de seguridad de la información.
- CUÁNDO realizar las mediaciones de seguridad de la información.
- CÓMO realiza las mediaciones de seguridad de la información.

Estas métricas de medición están enfocadas en la fase DO del modelo PDCA, las cuales ayudarán la eficacia del SGSI.

ISO 27005: Fue publicada en junio de 2008, define los lineamientos para la gestión del riesgo de seguridad de la información. Enfocada para la implementación en instituciones de cualquier tipo, público, privado, basado a la gestión de riesgos.(ISO 27000.ES, 2014)

ISO 27006: Este estándar indica los requisitos necesarios para acreditar como entidades auditoras y certificadoras del SGSI. Publicada en febrero de 2007.(ISO 27000.ES, 2014)

ISO 27007: Este estándar es una guía ya que indica los pasos para auditar un Sistema de Gestión de Seguridad de la Información, actualmente está en construcción.

ISO 27011: Estándar que contiene los lineamientos de gestión de seguridad de la información, enfocados específicamente en las telecomunicaciones. Está basada en la ISO 27002 y fue elaborada en conjunto con la ITU. (Unión Internacional de Telecomunicaciones)

ISO 27031: Consiste de un estándar que incluye una guía de continuidad de negocio enfocado en las TIC de una organización. El documento está basado en el estándar BS 25777, actualmente está en desarrollo. (ISO 27000.ES, 2014)

ISO 27032: Estándar enfocado en la ciberseguridad, actualmente está en fase de desarrollo.

Figura 6: Dominios de seguridad enfocados en el ISO 27032 (CIIP).

ISO 27033: Dedicada a la seguridad en las redes de datos de la institución, continúa en etapa de construcción, la cual se encuentra dividida en las siguientes secciones:

27033-1	•conceptos generales
27033-2	•directrices en redes y seguridad
27033-3	•escenarios redes
27033-4	•seguridad en las comunicaciones redes
27033-5	•seguridad en las VPNs
27033-6	•convergencia IP
27033-7	•redes inalámbricas

Figura 7: Secciones de la ISO 27033.

ISO 27034: Guía dedicada a la seguridad en las aplicaciones informáticas. Parcialmente desarrollada y conformado por seis partes:

PARTES – NORMA ISO
27034-1 - Detalle: Conceptos
27034-2 - Detalle: Marco
27034-3 - Detalle: Procesos de aplicaciones
27034-4 - Detalle: Validación de aplicaciones
27034-5 - Detalle: Estructura de datos y aplicaciones.
27034-6 - Detalle: Guías.

Tabla 1: Secciones de la ISO 27034.

ISO 27799: Estándar para la gestión de la salud informática, actualmente es la ISO 27002.

NORMA	EDICIÓN	DETALLE
27799	2008	"Esta norma ISO hace referencia a un conjunto de controles y directrices de buenas prácticas para la seguridad de la información, apropiado para las organizaciones que van a mantener: - Confidencialidad - Integridad - disponibilidad de la información Sea cual fuera el medio utilizado, digital, impreso, y sea cual sea el medio por el que se transmitirá, ya que la información siempre debe estar adecuadamente protegida." (ISO 27000.ES, 2014)

Tabla 2: Detalle de la Norma ISO 27799.

1.2 TÉRMINOS Y ABREVIATURAS

Activo: en esta investigación hacemos referencia a la información y demás componentes que sean de valor para la institución.

Amenaza: en lo relacionado a tecnología es un evento interno o externo que puede generar inconvenientes a los sistemas informáticos.

Ataque: considerado como un evento que atenta al performance de un sistema informático.

Auditoría: es el proceso de examinar sistemas o actividades para validar la integridad de la información.

Hacker: persona con un alto conocimiento que intenta vulnerar las seguridades informáticas para lograr un objetivo específico, como puede ser el de robar información, paralizar algún servicio, infectar equipos, etc.

IEC: Comisión Electrotécnica Internacional o en inglés International Electrotechnical Commission.

ISO: Organización Internacional de Estandarización o en inglés International Organization for Standardization.

Políticas: son un conjunto de reglas o controles que va dirigido a los usuarios de una institución para su respectivo cumplimiento.

Riesgo: considerado como la probabilidad de una amenaza.

Seguridad de la Información: son un grupo de directrices enfocado en la protección de la información.

SPAM: correos maliciosos enviados de forma masiva mediante el internet.

Usuario: sujeto de la institución o externo que acceden a datos o recursos informáticos en esta investigación.

Virus: es el más conocido del grupo de los ataques informáticos, el cual incluye un código malicioso y se copia dentro de los programas para reducir el performance del equipo informático.

1.3 MODELOS DE SEGURIDAD DE LA INFORMACIÓN PARA PUERTOS MARÍTIMOS

1.3.1 ANTECEDENTES DE SEGURIDAD EN LOS PUERTOS MARÍTIMOS

"Después de los atentados terroristas surgidos en Nueva York – EE.UU. el 11 de Septiembre de 2001, surgió una iniciativa de implementar mejoras en la seguridad en los distintos puntos de ingreso a los países incluyendo los puertos marítimos." (ISO 27000.ES, 2014)

Basado en un análisis de seguridad portuaria surge que la falta de controles es un problema que involucra a todo ente relacionado a los puertos marítimos, este motivo generó gran preocupación lo cual ha llevado al incremento de medidas orientadas a la seguridad portuaria.

"En la conferencia realizada en diciembre de 2012, del convenio SOLAS donde intervienen los Gobiernos Contratantes de dicho Convenio Internacional, por iniciativa de la Organización Marítima, en Londres, se generaron una serie de medidas entre ellas la de modificar el Convenio SOLAS para incrementar la seguridad marítima y la protección de los puertos e instalaciones portuarias". (Universidad Nacional del Noreste, 2004)

1.3.2 CÓDIGOS, NORMAS Y ESTÁNDARES INTERNACIONALES PARA LA SEGURIDAD EN LOS PUERTOS MARÍTIMOS

Código PBIP: es un Código Internacional con una función principal, que es la de implementar un marco para la Protección de las Instalaciones Portuarias, por ende este código incluye directrices de control para detectar amenazas e implementar medidas preventivas en las instalaciones de los puertos marítimos.

El código PBIP, no se enfoca en la protección de la información, pero como este código da los lineamientos para la seguridad en los puertos marítimos, la información que se procesa deberá ser protegida en base a los estándares de seguridad de la información.

Es el principal código de seguridad que utilizan o implementan todos los puertos marítimos del Ecuador.

Figura 8: Logo o imagen que identifica al código PBIP o sus siglas en inglés ISPS.

Este código PBIP consta de dos partes principales, las cuales se detallan en la figura a continuación:

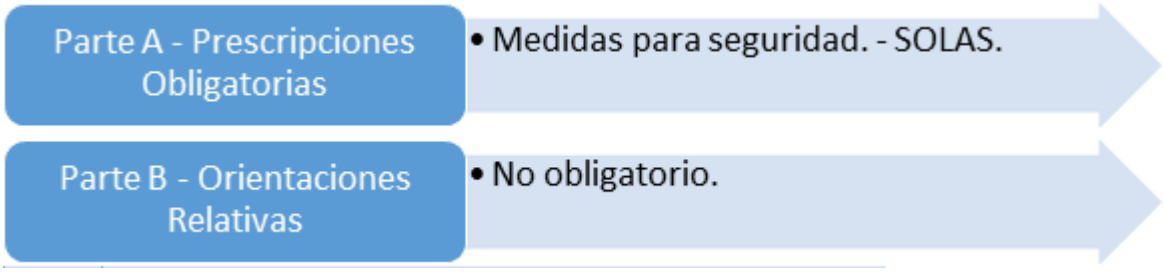

Figura 9: Partes que conforman el código PBIP.

Si una instalación portuaria desea implementar el código PBIP deberá realizar los siguientes pasos:

"1 Gobierno contratante representado por el Jefe de Estado.
2 Autoridad nacional de mando designada.
3 Funcionario encargado de la seguridad portuaria.
4 Organizaciones y expertos de seguridad reconocidos.

5 Evaluación de la seguridad de las instalaciones portuarias.

6 Planes de seguridad de las instalaciones portuarias.

7 Implementación de los planes de seguridad de las instalaciones portuarias" (Autoridad Portuaria Nacional de Perú, 2014)

En el contenido del PBIP, se presentan algunas definiciones de niveles de protección, tales como:

NIVEL	DETALLE
NIVEL DE PROTECCIÓN 1	Se deberá mantener medidas de protección en todo momento, las mínimas recomendadas.
NIVEL DE PROTECCIÓN 2	Se deberá mantener medidas de protección durante un periodo de tiempo, como resultado de un aumento del riesgo de que ocurra un suceso que afecte a la protección marítima.
NIVEL DE PROTECCIÓN 3	Se deberá mantener más medidas concretas de protección durante un periodo de tiempo limitado cuando sea inminente un suceso que afecte a la protección marítima.

Tabla 3: Niveles de Protección del Código PBIP (PREFECTURA NAVAL ARGENTINA, 2002)

El código PBIP, emite unos lineamientos para un plan de protección de la instalación portuaria, entre otros temas relacionados, pero lo más importante son los aspectos que deben tomarse en cuenta para la protección:

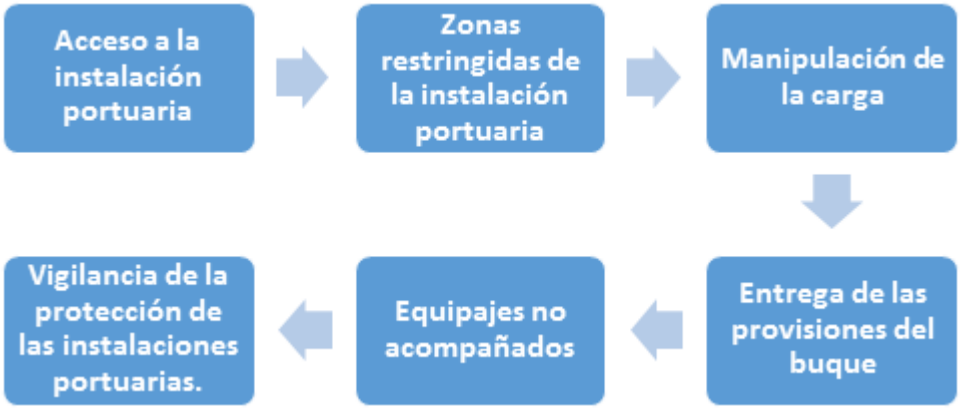

Figura 10: Directrices de seguridad PBIP. (ACADEMIA MARITIMA DE SEGURIDAD INTEGRAL ASI LTDA., 2014)

Cada uno de estos aspectos en la actualidad, en los puertos marítimos están automatizados por medio de la tecnología, siendo la información procesada en los sistemas informáticos, lo cual conlleva a una protección y custodia de la información, en base a estándares especializados para la seguridad informática, ya que en el código PBIP no se detalla en ninguna parte de su contenido la protección de la información. El Plan de Protección de las Instalaciones Portuarias conocido como el PPIP, es responsabilidad principal de Oficial de Protección de la Instalación Portuaria (OPIP). Todo Plan de Protección de las Instalaciones Portuarias debe de tener como mínimo lo siguiente:

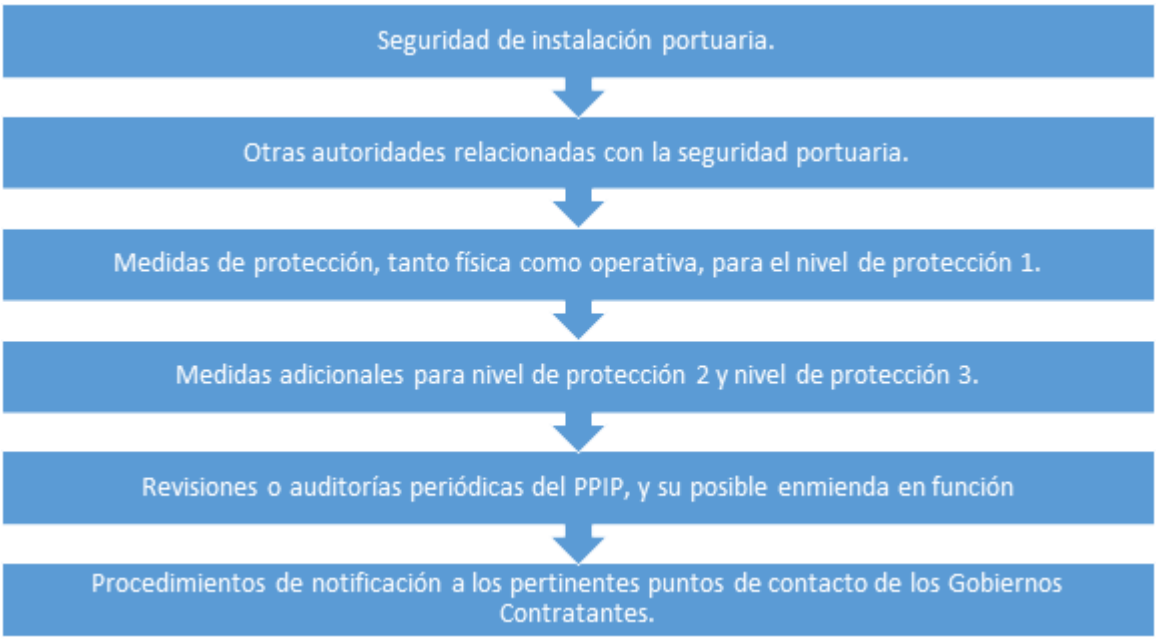

Figura 11: Requerimientos del Plan de Protección PPIP.

Norma BASC: *Business Alliance for Secure Commerce*, se enfoca en promover un comercio seguro por medio de una alianza a nivel internacional gracias a la cooperación de gobiernos y otros organismos internacionales, que dan cabida a dicha alianza.

"La denominación *World BASC Organization* tiene como misión generar una cultura de seguridad a través de la cadena de suministro, la cual es liderada por el sector empresarial."(World BASC Organization, 2015)

Figura 12: Logotipo o imagen que identifica a la norma BASC.

“La **misión** y **visión** de BASC es generar una cultura de seguridad a través de la cadena de suministro, mediante la implementación de sistemas de gestión e instrumentos aplicables al comercio internacional y ser en el año 2017 un referente internacional de comercio seguro que permita la sostenibilidad del comercio en beneficio de la sociedad.”(World BASC Organization, 2015)

Las instituciones a nivel mundial deberían apuntar como objetivo principal la implementación de Gestión Control y Seguridad basado en altos estándares, con la importancia igual o mayor que dan a otros aspectos de sus actividades empresariales, lo cual implica incorporar mecanismos de seguridad en las actividades de comercio internacional que se ejecutan cuando interactúan con otras entidades, en especial con los puertos marítimos.

BASC está elaborado y enfocado para mejorar la fusión del Control de Gestión y la Seguridad Integral de una institución, basándose en las mejores prácticas.

La norma BASC indica lineamientos y da información sobre:

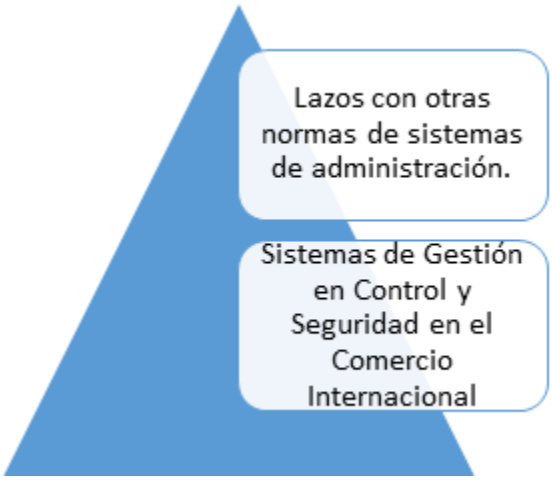

Figura 13: Lineamientos norma BASC.(BASC, 2014)

Los mecanismos de ataque cada día se incorporan más en las organizaciones, por lo que BASC recomienda en esta nueva versión la implementación y el manejo de un Sistema de Gestión en Control y Seguridad (SGSC).

En esta nueva versión BASC 4, hace hincapié y reforzar las directrices de un Sistema de Gestión en Control y Seguridad el cual se complementa de manera directa con estándares internacionales de seguridad BASC – C-TPAT, creados para los sectores que participan de forma directa o indirecta en la cadena de suministro y las actividades relacionadas con el comercio internacional.

Todo sistema de gestión, por más robusto que sea puede ser ineficiente si no se toman en cuenta el factor humano, cultura, políticas, etc., dentro de las organizaciones ya que deben ser considerados cuidadosamente al implementar BASC.

Al implementar un Sistema de Gestión en Control y Seguridad, se debe tener en cuenta los requisitos de orden legal aplicable en los países donde los puertos marítimos tienen sede, sobre los criterios de normas y estándares, por tanto ningún requisito puede implementarse incumpliendo la normativa legal vigente en el país. (Business Alliance for Secure Commerce, 2014)

BASC como norma internacional fue concebida para implementar y administrar un Sistema de Gestión en Seguridad y Control, de tal forma que puede ser integrada con otras Publicaciones o normativas, tal como se muestra en la figura a continuación.

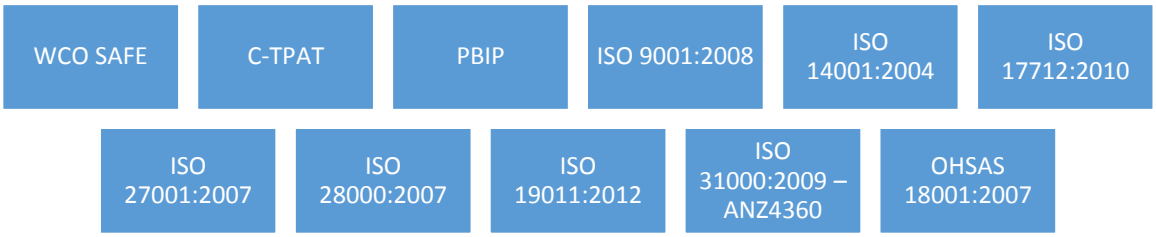

Figura 14: Normativas y/o Estándares relacionados con la seguridad de puertos marítimos y la seguridad de la información.

El sistema de Gestión en Seguridad y Control, propuesto por BASC, en esta nueva versión 4, está conformada por Normas y Estándares. La Norma está estructurada de la siguiente forma:

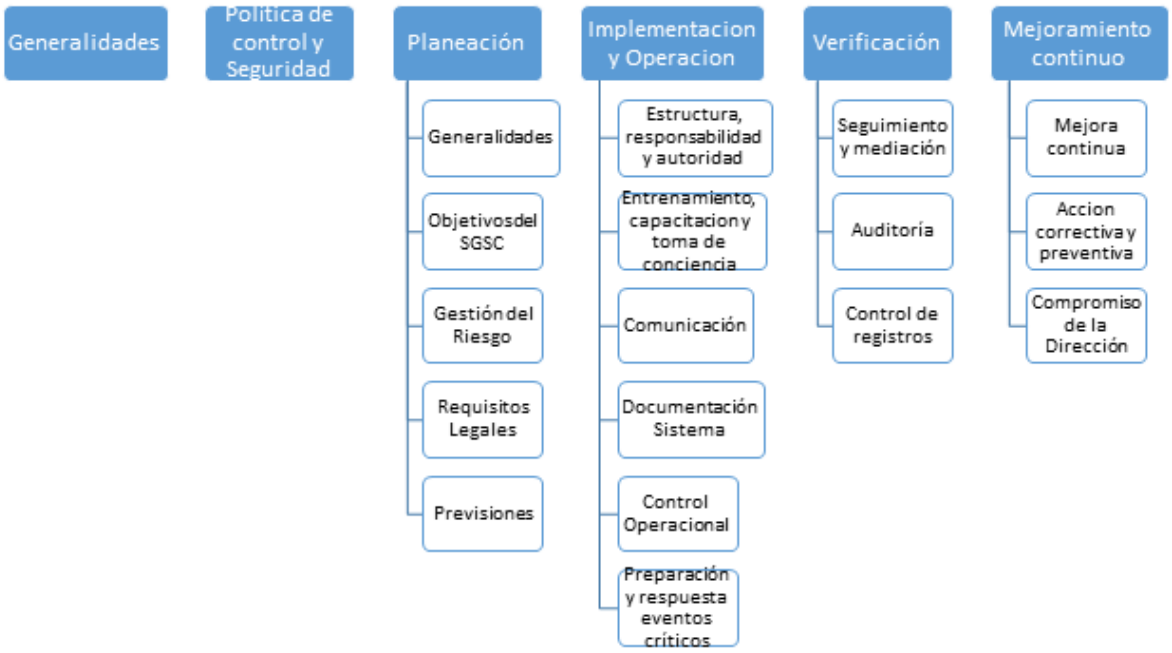

Figura 15: Estructura de la Norma para el SGSC.

Esta norma internacional se basa en la metodología conocida como PLANEAR-HACER-VERIFICAR-ACTUAR o sus siglas en ingles PDCA (Plan Do Check Act).

Figura 16: Relación de las Normas con la metodología P-H-V-A.

Y la otra parte que conforma el Sistema de Gestión en Control y Seguridad, son los Estándares BASC, que se describen en la figura a continuación.

Figura 17: Listado de Estándares de BASC distribuido por capítulos.

Y entre las instituciones que deben de cumplir con estos estándares internaciones, tenemos:

Figura 18: Listado de instituciones que pueden aplicar a la certificación BASC.

En la actualidad existe un sin número de instituciones que se encuentran certificadas y otras que ya se encuentran inscritas para la certificación, ya que en la actualidad los puertos marítimos del Ecuador, en especial el Puerto de Manta, por medio de la Autoridad Portuaria de Manta, exige que todas las empresas con las que se relaciona laboralmente, o las que necesiten interactuar por trabajo deben estar certificadas con la norma BASC. (BASC GUAYAQUIL, 2014) (BASC Pichincha, 2014)

A diferencia del código PBIP, BASC tiene un estándar enfocado en la seguridad de la información, como lo es seguridad en las tecnologías de la información, donde se hace referencia a muchos aspectos tecnológicos, y este estándar se relaciona con los demás estándares cuando estos involucran a la tecnología para el respectivo cumplimiento de lo indicado por BASC.

CAPÍTULO 2

2. ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1 ESTADO DEL MODELO DE LA SEGURIDAD DE LA INFORMACIÓN

2.1.1 DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

"La seguridad de la información es un término general que se lo puede relacionar con el de Seguridad IT, que se enfocan en la seguridad de la información debido a la naturaleza y el valor de los datos dentro de dicha institución, por ser un activo valioso deben estos especialistas mantenerla a salvo de ataques cibernéticos maliciosos para manipular los sistemas internos." (CENTRO DE ARTIGOS, 2014)

Las áreas de especialización de la seguridad de la información, la podemos resumir a continuación, basado en el crecimiento y evolución que ha tenido en los últimos años:

Figura 19: Áreas de especialización de la seguridad de la información.

Definiendo un concepto más aterrizado al término de Seguridad de la Información, podemos decir:

TÉRMINO	CONCEPTO
SEGURIDAD DE LA INFORMACIÓN	No debe de ser confundida con Seguridad Informática, ya que este solo se encarga de la información que se encuentra en el medio informático, pero la seguridad de la información, abarca otros medios, ya que la información no solo se encuentra en una institución, en medios como discos, memorias, unidas de almacenamiento, etc.

Tabla 4: Conceptos de Seguridad de la Información.

2.1.2 PRINCIPIOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los principios básicos de la seguridad de la Información hacen referencia a tres términos importantes: Confidencialidad, Integridad y Disponibilidad conocida como la Triada CIA en inglés.

TÉRMINOS	DETALLE
CONFIDENCIALIDAD	"Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" (INTECO - Instituto Nacional de Tecnologías de la Comunicación, 2014)
INTEGRIDAD	"Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas" (INTECO - Instituto Nacional de Tecnologías de la Comunicación, 2014)
DISPONIBILIDAD	"La disponibilidad es la característica de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones" (INTECO - Instituto Nacional de Tecnologías de la Comunicación, 2014)

Tabla 5: Detalle de las piedras angulares de la seguridad de la Información.

La seguridad de la información tiene como objetivo proteger a la información de las amenazas enfocadas a personas, equipos, procesos, que manejan información, donde estas identifican oportunidades para una violación de la seguridad en los ámbitos antes mencionados.

Las amenazas o ataques informáticos tienen cuatro categorías generales, las cuales son:

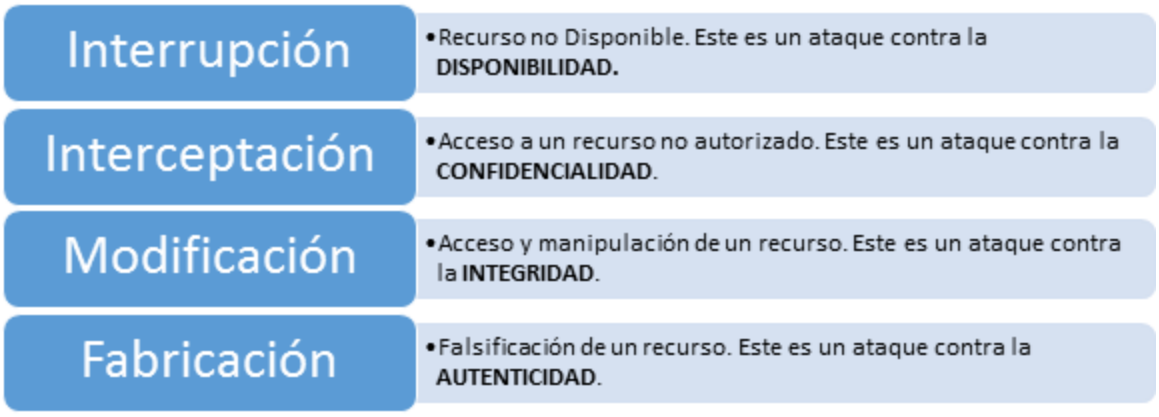

Figura 20: Categorías generales de las amenazas. (Instituto Nacional de Estadísticas Informáticas, 2000)

2.1.3 LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DEL ECUADOR

Las empresas privadas en su gran mayoría sí han tomado en cuenta el tema de proteger su información, en especial las empresas grandes, ya que saben que la información es un activo valioso para la institución.

En el sector privado, las empresas han trabajado en la seguridad de la información, creando áreas o contratando personal especializado en la seguridad de la información.

Sus altas autoridades han presionado y dado apoyo con políticas institucionales relacionadas con la seguridad de la información.

Y otras instituciones privadas, han ido un poco más y han invertido en la implementación de un Sistema de Gestión de Seguridad de la Información, para la protección de la misma, a tal punto que

estos procesos internos son certificados con normas ISO relacionadas a la seguridad de la información.

Existen también empresas que brindan el servicio de auditorías, para realizar revisiones de los procesos así estos no sean certificados, pero desean que se esté realizando lo correcto para la protección del activo más valioso en las instituciones que es ahora la información.

Empresas privadas en sectores como las telecomunicaciones, financiero, petrolero, son los que más importancia le han dado al ámbito de seguridad de la información y los que han realizado inversiones para proteger la información que manejan internamente y con sus clientes y/o proveedores.

La seguridad de la información en las instituciones públicas en el Ecuador no ha sido uno de los puntos fuertes donde se enfocan las altas autoridades, esto se puede evidenciar de forma clara porque las empresas públicas, no cuentan en su gran mayoría con un área de seguridad de la información o por lo menos una persona relacionada con estas tareas.

2.2 ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN PROPUESTO POR EL GOBIERNO

La Presidencia de la República, por medio de la Secretaría Nacional de Administración Pública (SNAP), decretó la implementación de un Esquema Gubernamental para mantener la seguridad en la información de todas las instituciones que dependen de la Función Ejecutiva. Este Esquema Gubernamental está conformado por normas, procesos, procedimientos enfocados principalmente en la seguridad de la información. Este Esquema Gubernamental se especifica en el Acuerdo Ministerial N° 166, Publicado en el Registro Oficial, suplemento 88, el 25 de septiembre de 2013.

Figura 21: Entidades que conforman la comisión de seguridad informática. (Secretaría Nacional de Planificación y Desarrollo, 2013)

Esta comisión tiene como atribución establecer mecanismos de seguridad informática, para proteger la información que reside en las entidades de la Administración Pública Central e Institucional.

El EGSI fue basado en la norma ISO 27002, para que todas las instituciones públicas, implementen dicho esquema y den inicio a prácticas básicas de seguridad de la información el cual es de implementación obligatoria para las entidades públicas que están relacionadas con la Función Ejecutiva.

Dichas Entidades están obligadas a implementar el Esquema, el cual lo deberán realizar en un máximo de dieciocho (18) meses, una vez que se publicó el Acuerdo Ministerial, pero en un máximo de seis (6) meses se deberá dar cumplimiento con 126 directrices prioritarias llamadas HITOS que se detallan en el Esquema. (DELOITTE, 2014)

En este Esquema Gubernamental, otra obligatoriedad es que toda entidad pública cuente con una persona que haga de Oficial de Seguridad de la Información, para que se haga cargo de dar seguimiento y hacer cumplir dicho Esquema Gubernamental, ya que esta persona, es la contraparte

de la Secretaría Nacional de Administración Pública. (Secretaría Nacional de Planificación y Desarrollo, 2013)

Otro punto importante del EGSI es la designación formal de un responsable de Seguridad del Área de Tecnología y la conformación de un Comité de Seguridad de la Información donde sus integrantes deberán ser:

Figura 22: Integrantes del Comité de Seguridad de la Información de una entidad pública, de acuerdo al EGSI. (Secretaría Nacional de Planificación y Desarrollo, 2013)

La Secretaría Nacional de Administración Pública, realizará de forma ordinaria una revisión anual del cumplimiento del Esquema Gubernamental en conformidad a lo que indica la Norma ISO 27002 y de forma extraordinaria cuando las circunstancias lo ameriten, adicional se deberá evaluar los riesgos en base a la Norma ISO 27005 Gestión de Riesgo en la Seguridad de la Información. (Secretaría Nacional de Planificación y Desarrollo, 2013)

2.2.1 CONTENIDO DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Una vez explicado el origen del Esquema Gubernamental de Seguridad de la Información (EGSI), se detallará cómo está constituido dicho Esquema Gubernamental.

Este Esquema de Seguridad de la Información, está conformado por 11 Dominios, los cuales a su vez tiene 38 Objetivos de Control o sub dominios, detallado en 119 Controles, lo cual da como resultado 126 HITOS Prioritarios y 582 HITOS no Prioritarios.

Figura 23: Dominios que conforman el EGSI, propuesto por la SNAP.

Todos los objetivos de control hacen referencia a la Norma ISO 27002:2005, pero en el EGSI, no se hace referencia a uno de ellos, el cual es servicios de comercio electrónico, que se encuentra dentro del dominio de Gestión de Comunicaciones y Operaciones. (ISO 27000, 2011)

El Oficial de Seguridad de la Información, es el responsable de reportar los avances a un sistema llamado Gobierno por Resultados (GPR), donde se encuentra el proyecto para el cumplimiento del EGSI, siendo considerado un proyecto de Gasto Corriente por todas las instituciones.

El Oficial de Seguridad de la Información, adicional deberá de tener dicha información en su poder, ya que la SNAP, por medio de la Subsecretaría de Gobierno Electrónico, podrán auditar y pedir la documentación que avale los avances reportados en el sistema GPR. El tiempo máximo para dar cumplimiento con todos los HITOS, es hasta marzo del 2015, una vez concluida esta fecha, el Oficial de Seguridad de la Información, cambia su tarea a dar seguimiento y que se dé cumplimiento a lo ya implementado por el Esquema Gubernamental de Seguridad de la Información en la institución.

2.3 NORMATIVAS LEGALES

Existen varias normativas legales, que giran alrededor de este Esquema Gubernamental de Seguridad de la Información, de los cuales se puede hacer referencia a los más importantes:

NORMATIVAS LEGALES	DETALLE
Acuerdo Ministerial 804	Crea la comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, expedido por la Secretaría Nacional de administración Pública el 29 de Julio de 2011 y Publicado en el Registro Oficial No. 511 del 11 de agosto de 2011.
Acuerdo Ministerial 166	Se dispone a las instituciones públicas, la implementación del EGSI, en su primera fase, basado en las Normas Técnicas ISO/IEC 27000.
Decreto Ejecutivo 149	La Secretaría Nacional de la Administración Pública emite un Plan Nacional de Gobierno Electrónico para la Función Ejecutiva, expedido por la Presidencia de la República el 20 de Noviembre de 2013 y Publicado en el Registro Oficial.

Decreto Ejecutivo 1014	Se establece como política gubernamental el uso de Software Libre en la Administración Pública Central. Expedido por la Presidencia de la República el 10 de Abril de 2008 y Publicado en el Registro Oficial No. 322 del 23 de Abril de 2008.

Tabla 6: Listado de Normativas Legales relacionados con la implementación del EGSI. (Secretaria Nacional de Administracion Publica, 2014)

2.4 ANÁLISIS DE LA AUTORIDAD PORTUARIA DE MANTA

2.4.1 RESEÑA HISTÓRICA

Autoridad Portuaria de Manta, institución emblemática de la ciudad, se creó el 24 de octubre de 1966, a través del Decreto Ejecutivo N° 1373. Su primer Directorio inició funciones el 12 de noviembre del mismo año y con él, la libérrima provincia de Manabí, tiene la invaluable realidad del Puerto de Manta. El 20 de febrero de 1968 se acoderó a los muelles de Manta el buque de bandera colombiana "Ciudad de Buenaventura", inaugurando así los nuevos servicios portuarios. El 1 de febrero del 2007 Autoridad Portuaria de Manta, por delegación del Estado a través de la modalidad de concesión, se otorgó a una compañía internacional privada el uso de las facilidades y de la prestación de servicios portuarios. El 1 de abril de 2010 Autoridad Portuaria de Manta retomo con bríos el liderazgo y control absoluto en la operatividad, administración y desarrollo del Puerto, una vez que el Directorio, en sesión efectuada el 9 de marzo de 2010, resolviera la terminación unilateral del contrato de concesión. (Autoridad Portuaria de Manta, 2015)

2.4.2 MISIÓN Y VISIÓN

MISIÓN	Ser reconocidos en el ámbito nacional e internacional como el Puerto de Aguas Profundas del Ecuador: Puerto Gateway y Multipropósito de tercera generación con opción de trasbordo para la Costa Oeste del Pacífico Sur.

VISIÓN	Oferta de servicios portuarios que contribuyen a la competitividad del Comercio Exterior del Ecuador.

2.4.3 SITUACIÓN ACTUAL

La Autoridad Portuaria de Manta se encuentra localizada en la provincia de Manabí, a 25 millas de la ruta internacional y su acceso es directo. El área donde se encuentran los muelles está protegida por un rompeolas de abrigo, de siete metros de ancho y aproximadamente 1.600 metros de longitud, que sirve además de calzada para el tráfico de vehículos.

Autoridad Portuaria de Manta en la actualidad, cuenta con un aproximado de doscientos (200) empleados, enfocados en cumplir con los objetivos de la institución, los cuales son el brindar los servicios portuarios que son de competencia de la institución.

2.4.4 ESTRUCTURA ORGANIZACIONAL DE LA INSTITUCIÓN

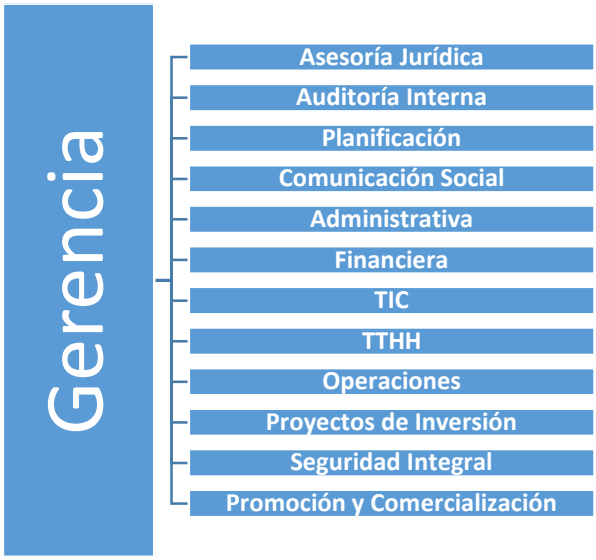

Figura 24: Estructura Organizacional de la Autoridad Portuaria de Manta.

2.4.5 ESTRUCTURA ORGANIZACIONAL DE LA DIRECCIÓN DE TIC

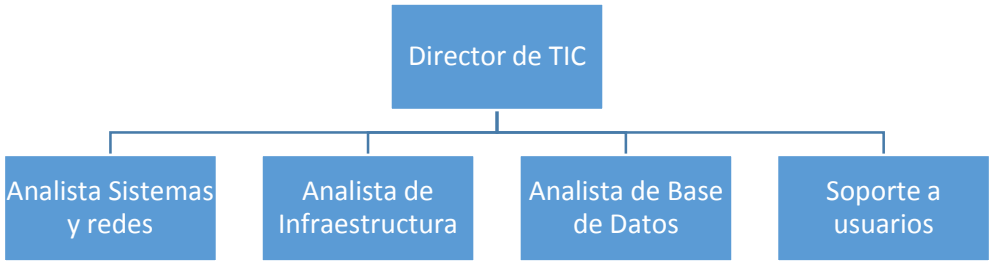

Figura 25: Estructura interna de la Dirección de TIC de la Autoridad Portuaria de Manta.

Esta estructura organizacional de la Dirección de TIC, denota que no existía persona alguna o área enfocada en el ámbito de seguridad de la información, la cual debió encargarse de salvaguardar la información procesada en la institución.

Días después de la firma del Acuerdo Ministerial, donde se dispone la implementación del EGSI en las instituciones Públicas, la Autoridad Portuaria de Manta, crea un puesto, el cual tiene el nombre de Oficial de Seguridad de la Información, que reporte a Gerencia y trabaje de la mano con el Comité de Seguridad de la Información, los cuales lo conforman Directores de área de la institución, los cuales cumplen con funciones específicas tal como lo detalla el EGSI.

2.4.6 ESTADO ACTUAL DE LA INFRAESTRUCTURA TECNOLÓGICA

En la parte de Tecnología de la Información la Autoridad Portuaria de Manta cuenta actualmente con dos (2) centros de cómputo, el principal y el secundario, los cuales se encuentran ubicados en las oficinas de la Dirección de TIC en el edificio Administrativo y el Edificio de Operaciones respectivamente.

La Dirección de Tecnología de la Información de la Autoridad Portuaria de Manta, fue creada como un área de apoyo, la cual es responsable de brindar servicios informáticos, la disponibilidad de los sistemas y el soporte a los usuarios.

2.4.7 INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA

La infraestructura tecnológica de la Autoridad Portuaria de Manta tiene un cambio radical en lo relacionado a la Seguridad Informática, al momento que se da inicio a la implementación del EGSI en la institución, ya que gracias al apoyo de la Gerencia y las gestiones del comité de seguridad de la Información, se procedió a adquirir hardware y software solicitado por el Oficial de Seguridad, los mismos que estaban enfocados en la protección y control de la información, para dar cumplimiento a los HITOS del EGSI.

Diferenciando el antes y después del EGSI en la Autoridad Portuaria de Manta, podemos detallar los equipos y sistemas informáticos enfocados en la seguridad de la información:

HARDWARE Y SOFTWARE DESTINADOS PARA LA SEGURIDAD DE LA INFORMACIÓN – ANTES DEL EGSI		
HARDWARE – SOFTWARE	**DESCRIPCIÓN**	**CANTIDAD**
FIREWALL PERIMETRAL	UTM que apoya en la protección de la información que llega desde el internet, con funcionalidades como: - antispam - antivirus - web filtering	1
ANTIVIRUS	Software instalado en cada PC del funcionario para la protección de virus y otros ataques informáticos. Se lo administra de manera centralizada su instalación y actualización.	1
SERVIDORES	Un solo servidor para la instalación del Antivirus.	1

Tabla 7: Listado de soluciones tecnológicas de la Autoridad Portuaria de Manta, antes de la implementación del EGSI.

Una vez realizada la inspección de la infraestructura tecnológica de la Autoridad Portuaria de Manta, el Oficial de Seguridad de la Información, emitió un informe donde indica las falencias y necesidades, que pueden ser cubiertas con la adquisición de herramientas tecnológicas, las cuales fueron adquiridas en el 2014 y los primeros meses de 2015, para dar cumplimiento a los HITOS de la FASE I, las cuales se detallan a continuación:

HARDWARE Y SOFTWARE ADQUIRIDOS PARA LA SEGURIDAD DE LA INFORMACIÓN – DESPUES DEL EGSI		
HARDWARE – SOFTWARE	**DESCRIPCIÓN**	**CANTIDAD**
SISTEMA DE MESA DE AYUDA	Solución que permite reportar los incidentes tecnológicos y de seguridad de la información, por medio de una página web o correo electrónico. Lo cual permite un mayor control de los incidentes, toma de decisiones, registro de los incidentes, etc.	1
SISTEMA DE PROTECCIÓN DE ACCESO A LA RED DE DATOS	Solución que protege el acceso a la red de datos de equipos que no son de la institución, esto es controlado en la red alámbrica e inalámbrica.	1
SOLUCIÓN DE WIFI CONTROLADO	Permite tener en la institución dos tipos de acceso al WiFi, uno libre para visitantes y otro para funcionarios, los cuales son controlados por la dirección MAC del equipo.	1
SISTEMA DE RESPALDO DE LA INFORMACIÓN Y SISTEMAS INFORMÁTICOS	Se adquirió una solución automatizada que respalda los datos de los sistemas informáticos y de las bases de datos transaccionales. Adicional respalda la información de un servidor donde los funcionarios centralizan todos los documentos.	1

SISTEMA DE MONITOREO AVANZADO DE LA RED Y SERVIDORES	Solución para identificar cuellos de botella en la red de datos, puertos con mayores conexiones, detectar tráfico anormal, lo cual conlleva a determinar si existe algún ataque informático.	1
SISTEMA DE ACTUALIZACIÓN AUTOMÁTICA DE LOS PCS Y SERVIDORES DE LA INSTITUCIÓN	Solución que permite actualizar las computadoras, para que estén con los últimos parches del sistema operativo, del navegador de internet y los sistemas de Ofimática. Esta solución ayuda en el ahorro del consumo de ancho de banda, ya que descarga las actualizaciones por medio de una técnica avanzada y este a su vez lo distribuye a cada PC.	1
SISTEMA PARA LA CENTRALIZACIÓN DE DOCUMENTOS	Herramienta que permite centralizar los documentos importantes de la institución y con eso permitir la colaboración y mejoras en la comunicación de la información entre funcionarios.	1
SISTEMA PARA LA CENTRALIZACIÓN DE LOS CORREOS ELECTRÓNICOS	Configuración que se realizó en el correo electrónico de los funcionarios para que puedan acceder a todos los correos desde afuera, al momento de centralizar los mismos en el servidor.	1
SISTEMA DE AUTENTICACIÓN ALTERNA POR MEDIO DE TOKENS CON HUELLA DIGITAL	Permite a funcionarios que manejan información crítica a tener doble autenticación por medio de un token con identificador de huella.	1
SISTEMA DE AUDITORÍA PARA LOS SISTEMAS INFORMÁTICOS	Solución para identificar cambios, en los sistemas y las bases de datos, adicional en las políticas de control de las cuentas de usuario y buzones de correo.	1

SERVIDORES	Servidores para la instalación de las soluciones antes mencionadas.	2
UNIDAD DE ALMACENAMIENTO MASIVO	Sistema de almacenamiento masivo (NAS) para guardar los datos de los sistemas informáticos antes mencionados.	1

Tabla 8: Listado de soluciones tecnológicas de la Autoridad Portuaria de Manta, adquiridas para la implementación del EGSI.

Todas estas soluciones informáticas, han permitido dar cumplimiento en su gran mayoría a los controles que solicita el EGSI en la fase inicial, los demás controles fueron completados por medio de Políticas y procedimientos de la Dirección de TIC.

La implementación de estas soluciones informáticas generó un cambio institucional en la forma de trabajo de los funcionarios, primero de oposición al cambio, pero por parte de Gerencia se impulsó la utilización de las herramientas para un mejor control de la información, lo cual generó nuevas políticas y procedimientos para la seguridad de los datos.

CAPÍTULO 3

3.2 DESCRIPCIÓN DE LA ENTIDAD A EVALUAR

AUTORIDAD PORTUARIA DE MANTA

ANTECEDENTES:

Autoridad Portuaria de Manta, institución emblemática de la ciudad, se creó el 24 de octubre de 1966, a través del Decreto Ejecutivo N° 1373. Su primer Directorio inició funciones el 12 de noviembre del mismo año y con él, la libérrima provincia de Manabí, tiene la invaluable realidad del Puerto de Manta. El 20 de febrero de 1968 se acoderó a los muelles de Manta el buque de bandera colombiana "Ciudad de Buenaventura", inaugurando así los nuevos servicios portuarios. El 1 de febrero de 2007 Autoridad Portuaria de Manta, por delegación del Estado a través de la modalidad de concesión, se otorgó a una compañía internacional privada el uso de las facilidades y de la prestación de servicios portuarios. El 1 de abril de 2010 Autoridad Portuaria de Manta retomó con bríos el liderazgo y control absoluto en la operatividad, administración y desarrollo del Puerto, una vez que el Directorio, en sesión efectuada el 9 de marzo de 2010, resolviera la terminación unilateral del contrato de concesión."(Autoridad Portuaria de Manta, 2015)

LOGO


Figura 26: Logotipo de la Autoridad Portuaria de Manta.

SITIO WEB, CORREO Y REDES SOCIALES	
Sitio web	www.puertodemanta.gob.ec
Correo Electrónico	**info@apmanta.gob.ec**
Facebook	**Autoridad Portuaria de Manta**
Twitter	**@APortuariaManta**

Tabla 9: Listado de contactos de Autoridad Portuaria de Manta.

IMÁGENES DE LAS INSTALACIONES

Instalaciones Portuarias –Muelle Internacional

 Edificio Administrativo
 Acceso al Muelle Internacional

Tabla 10: Imágenes de las instalaciones de Autoridad Portuaria de Manta.

3.3 DESCRIPCIÓN DE LAS ENTIDADES LOCALES A COMPARAR SOBRE LA IMPLEMENTACIÓN DEL EGSI

AUTORIDAD PORTUARIA DE GUAYAQUIL

ANTECEDENTES:

"Guayaquil es el puerto principal de la República del Ecuador, a través del cual se moviliza el 70% del comercio exterior que maneja el Sistema Portuario Nacional. Fue construido durante el periodo 1959 - 1963. La ubicación privilegiada del puerto constituye un incentivo para la captación de tráficos de las rutas del lejano oriente y del continente americano,

especialmente los relativos a la costa del Pacífico. Asimismo, esta resulta altamente conveniente para la concentración de cargas latinoamericanas destinadas a cruzar el canal de Panamá con destino a la costa este del continente o hacia Europa y África. El marco legal sobre el que desarrolla sus actividades, permite a las empresas privadas ejercer sin limitaciones la actividad portuaria. El Ecuador se encuentra inmerso en una exitosa acción de modernización tanto de puertos como de aduanas, generando un alto grado de confiabilidad para las inversiones que se realizan en el país."(Autoridad Portuaria de Guayaquil, 2015)

MISIÓN	Constituirse en la entidad portuaria más eficiente de la región, procurando que los servicios portuarios se presten con tecnología, seguridad y competitividad en beneficio del comercio exterior.
VISIÓN	Organizar y planificar el desarrollo de AUTORIDAD PORTUARIA DE GUAYAQUIL, así como dirigir y controlar que los servicios portuarios se provean competitivamente de manera sustentable y sostenible, con la racionalización de los recursos para lograr el desarrollo del comercio exterior.
LOGO	
	

Figura 27: Logotipo de la Autoridad Portuaria de Guayaquil.

SITIO WEB, CORREO Y REDES SOCIALES	
Sitio web	www.apg.gob.ec
Correo Electrónico	**info@apg.gob.ec**

Facebook	**N/A**
Twitter	**N/A**

Tabla 11: Listado de contactos de Autoridad Portuaria de Guayaquil.

IMÁGENES DE LAS INSTALACIONES

Instalaciones Portuarias – Administradas por Concesionaria

Edificio Administrativo

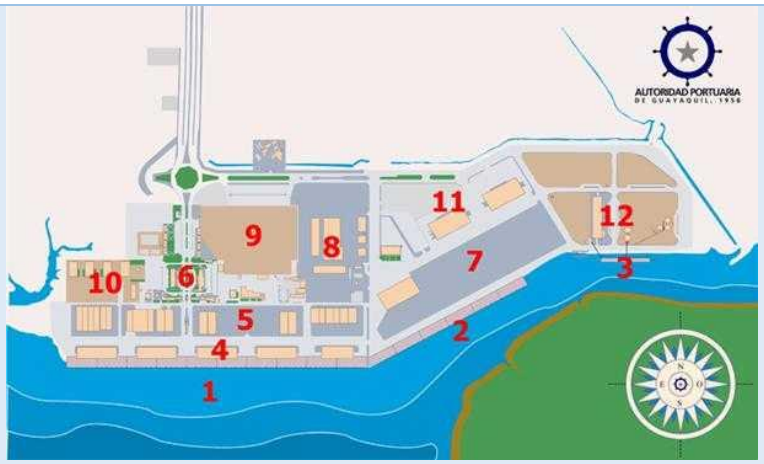

Diagrama de Autoridad Portuaria de Guayaquil

Tabla 12: Imágenes de las instalaciones de Autoridad Portuaria de Guayaquil.

AUTORIDAD PORTUARIA DE ESMERALDAS

ANTECEDENTES:

"Autoridad Portuaria de Esmeraldas fue creada el 28 de diciembre de 1970 mediante Decreto Ejecutivo número 1043, es una entidad estatal, con autonomía de gestión y patrimonio propio, que a través del Puerto Comercial de Esmeraldas, realiza enlace entre el transporte marítimo y terrestre de manera segura, eficiente y económica, apoyando de esta manera al desarrollo del comercio exterior del país. El Puerto de Esmeraldas cuenta con una dársena (área marítima), protegida de la agitación del mar por un rompeolas; en las dársenas los buques se acoderan a tres muelles para efectuar las actividades de carga y descarga de mercaderías. Autoridad Portuaria de Esmeraldas les invita a ser parte de su positiva gestión, que aporta positivamente al desarrollo y progreso del Ecuador." (Autoridad Portuaria de Esmeraldas, 2015)

GENERALIDADES:

El puerto de Esmeraldas es de tipo multipropósito y en la actualidad presta los servicios mediante tres muelles, uno de los cuales tiene un calado de 11,5 metros, con acceso directo desde mar abierto, lo cual permite una gran maniobrabilidad y atraques de las buques, brindando también servicio de remolque y el servicio profesional de practicaje. (Autoridad Portuaria de Esmeraldas, 2015)

LOGO
AUTORIDAD PORTUARIA DE ESMERALDAS

Figura 28: Logotipo de la Autoridad Portuaria de Esmeraldas.

SITIO WEB, CORREO Y REDES SOCIALES	
Sitio web	www.puertoesmeraldas.gob.ec
Correo Electrónico	**N/A**
Facebook	**Puerto de Esmeraldas**
Twitter	**@redSocialApe**

Tabla 13: Listado de contactos de Autoridad Portuaria de Esmeraldas.

IMÁGENES DE LAS INSTALACIONES
 Instalaciones portuarias
 Patio de contenedores y autos
 Vista panorámica de las instalaciones portuarias

Tabla 14: Imágenes de las instalaciones de Autoridad Portuaria de Esmeraldas.

AUTORIDAD PORTUARIA DE PUERTO BOLIVAR

ANTECEDENTES:

> “La historia relata la primera utilización del estero llamado Puerto Pilo, después Puerto Machala (1783-1860) que sirvió como antiguo atracadero de embarcaciones y fue el eslabón para los primeros comerciantes entre Machala y Guayaquil. Ante el auge cacaotero y por la sedimentación de Puerto Pilo, "el desarrollo portuario de Machala era una necesidad imperiosa" pues sus autoridades consideraron buscar otro lugar para un nuevo puerto que brindara mejores facilidades para el embarque y desembarque de pasajeros y mercancías desde y hacia la Isla Puná y Guayaquil. El Cabildo Machaleño resolvió formar un nuevo Puerto frente a la Isla Jambelí (1861-1883) Puerto Huaylá como se denominó al nuevo Puerto. En 1879 el Concejo de Machala decide construir un muelle en el Puerto de Huaylá.” (Autoridad Portuaria de Puerto Bolivar, 2015)

GENERALIDADES:

“En la actualidad Puerto Bolívar pone a proa al progreso con la construcción de su moderno terminal multipropósito de 240 metros por 100 de plataforma, estructura que contará con todas las facilidades en equipos de grúas de pórtico y que permitirán el arribo de naves de hasta 14,00 metros en la más baja marea.” (Autoridad Portuaria de Puerto Bolivar, 2015)

LOGO


Figura 29: Logotipo de la Autoridad Portuaria de Puerto Bolivar.

SITIO WEB, CORREO Y REDES SOCIALES	
Sitio web	www.puertobolivar.gob.ec
Correo Electrónico	**appb@appb.gob.ec**
Facebook	**N/A**
Twitter	**N/A**

Tabla 15: Listado de contactos de Autoridad Portuaria de Puerto Bolivar.

IMÁGENES DE LAS INSTALACIONES

Instalaciones Portuarias

 Área de contenedores y maquinarias
 Construcción de nuevo puerto

Tabla 16: Imágenes de las instalaciones de Autoridad Portuaria de Puerto Bolívar.

3.4 PUERTOS MARÍTIMOS INTERNACIONALES QUE HAN IMPLEMENTADO NORMAS ISO 27001

En base a la investigación realizada por internet, no se obtuvo información sobre puertos en América Latina que hayan implementado Normas ISO 27000, lo cual llevó a investigar en otros continentes, teniendo resultados de puertos marítimos de países como India, Malasia, Emiratos Árabes Unidos y Australia, los que han implementado Normas ISO 27001, pero específicamente a procesos relacionados con los servicios portuarios.

JOHOR PORT BERHAD (JPB)

Situado en el extremo más meridional de la península de Malasia, Johor Port está estratégicamente situado en el corazón de la extensa 8,000 acres Pasir Gudang Industrial Estate. El área es el hogar de una amplia gama de industrias especializadas en la petroquímica, ingeniería, muebles, telecomunicaciones, productos electrónicos y productos alimenticios, entre otros. Johor Port está vinculada a importantes centros comerciales e industriales en Malasia, así como otros puertos y países vecinos. Esta red se apoya en las conexiones de infraestructura vial y ferroviaria de la nación.

Terminal de Gráneles Líquidos ofrece servicios especializados para atender a las cargas líquidas y petroquímica comestibles. La terminal también se nutre de la utilización de una red de tuberías con múltiples brazos de alta capacidad de carga para permitir la carga a transportar directamente a patios de tanques a altas velocidades de transferencia.

El 4 de Enero de 2013, JPB, obtiene la certificación ISO/IEC 27001:2005, siendo la primer terminal multipropósito de Malasia en obtener dicha certificación.

Figura 30: Certificados de acreditación Normas ISO 27001.

Logotipo	Sitio web
	http://www.johorport.com.my

Figura 31: Logotipo y web site del puerto internacional Johor Port Berhad.

DP WORLD – JEBEL ALI PORT

DP World tiene una cartera de más de 65 terminales marítimas a través de seis continentes (1), incluyendo nuevos desarrollos en curso en la India, África, Europa y Oriente Medio. Manejo de contenedores es el negocio principal de la empresa y genera más de tres cuartas partes de sus ingresos. En 2014, *DP World* manejó 60 millones de TEUs (veinte pies unidades de contenedores equivalentes). Con su línea de compromiso de los desarrollos y ampliaciones, se espera que la capacidad aumente a más de 100 millones de TEUs en 2020, en línea con la demanda del mercado. *DP World* tiene un equipo dedicado, experimentado y profesional de más de 36.000 personas que sirven a sus clientes en todo el mundo, y la empresa invierte constantemente en terminales de infraestructura, las instalaciones y las personas para proporcionar servicios de calidad, hoy y mañana, cuando y donde los clientes los necesitan. Al adoptar este enfoque centrado en el cliente, *DP World* está construyendo sobre las relaciones establecidas y el nivel superior de servicio demostrado en su buque insignia instalación Jebel Ali en Dubái, que ha sido votado como "Mejor Seaport en el Medio Oriente" durante 20 años consecutivos.

La estrategia describe el plan para maximizar el valor para los accionistas mediante el aprovechamiento de la cartera de activos de infraestructura de clase mundial, para fortalecer las cadenas de suministro globales y generar un crecimiento económico sostenible. Con el objetivo comprometido sobre la Seguridad y la Seguridad, Jebel Ali se convirtió en el primer

puerto del mundo en alcanzar la norma ISO 27001: 2005 para sus Sistemas de Gestión de Seguridad de la Información (SGSI) excepcionales. También fue el primer puerto del mundo en recibir la Fundación Europea para la Gestión de la Calidad (EFQM) certificación 5 Estrellas. Otras áreas claves en las que el puerto del buque insignia ha obtenido la certificación internacional incluyen, del Sistema de Gestión de Calidad, Sistema de Gestión de la satisfacción del cliente, y el Sistema de Gestión Ambiental. A medida que se evoluciona y vive en un mundo más integrado, hay que adaptarse constantemente a los cambios del entorno y las necesidades de los clientes. Por tanto, esta estrategia tiene que ser flexible para la dinámica cambiante, mientras que proporciona una orientación clara sobre cómo alcanzar la visión. En 2013, se introdujo el concepto del marco de cuadro de mando integral para comunicar la estrategia de *DP World*, con el objetivo de comunicar una visión clara, coherente y compartida de *DP World* para un futuro sostenible. El marco proporciona orientación y objetivos de *DP World* en el mediano y largo plazo medibles, y utiliza indicadores clave de rendimiento (KPI) para medir la aplicación de la estrategia a través de la cartera.

Figura 32: Certificado de acreditación Normas ISO 27001 para DP WORLD.

Logotipo	Sitio web
	http://web.dpworld.com/

Figura 33: Logotipo y web site del puerto JEBEL ALI – DP WORLD.

En Dubái el 11 de marzo de 2009 el buque insignia de operador de terminal marítima global *DP World* puerto de Jebel Ali se ha convertido en el primer puerto del mundo para ganar la norma ISO 27001: 2005 la certificación de *Lloyds Register Quality Assurance* (LRQA) para su Sistema de Gestión de Seguridad de la Información (SGSI). Esto viene como parte de un mayor enfoque de la compañía en asegurar la gestión de la seguridad en sus terminales.

LRQA con sede en Londres, reconocido internacionalmente por sus certificaciones de sistemas de gestión, llevó a cabo una evaluación detallada del sistema de gestión de seguridad de la información reciente aplicación del puerto de Jebel Ali y certificado de que cumple con los más altos estándares de excelencia en términos de eficiencia operativa a largo plazo. Mohammed Al Muallem, Vicepresidente Senior y Director General de *DP World*, Emiratos Árabes Unidos Región, dijo: "La norma ISO 27001: 2005 añade otra pluma a la tapa de todos los logros redondos de Jebel Ali Port. Nos hemos comprometido a poner en marcha los sistemas más eficaces de gestión de seguridad de la información para asegurar la excelencia en esta área. El reconocimiento ISO subraya el éxito en nuestros esfuerzos y nos inspira a continuar nuestra unidad para mantener la posición del puerto de Jebel Ali como el eje principal de envío de la región en todos los aspectos". ISO 27001: 2005 es el estándar internacional para el SGSI. Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema documentado que satisface las necesidades de control de seguridad de la empresa.

El Departamento de Tecnología de la Información de DP World, Emiratos Árabes Unidos Región, desarrolló el SGSI, lo puso a través de una gestión rigurosa y revisiones técnicas y puso en marcha después de la capacitación especializada para el personal.

DP World ha invertido fuertemente en todas las áreas de gestión de la seguridad a través de su red de terminales en todo el mundo, que ya ha ganado el reconocimiento internacional. Es el primer operador de la terminal marítima para lograr la certificación ISO28000 por sus normas de gestión de la seguridad. *DP World* es también un miembro del programa de la agencia de Aduanas Protección Fronteriza de Asociación Comercial Aduanera contra el Terrorismo (C-TPAT).

LEMBAGA PELABUHAN KUANTAN

Kuantan puerto es un puerto comercial ubicado en Tanjung Gelang (Latitud 3 ° 58'N, longitud 103 ° 26'E), en la intersección de las rutas de transporte marítimo internacional en el Mar del Sur de China. Se encuentra a unos 25 kilómetros de la ciudad capital del estado de Kuantan, Pahang. Kuantan puerto es una importante puerta de entrada para el comercio en la región Asia-Pacífico y Oriente Región Económica costa de la península de Malasia.

El objetivo del puerto de Kuantan, es el de actuar como regulador y facilitador para hacer como centro de comercio marítimo brindando instalaciones y servicios óptimos y de calidad para el beneficio de los usuarios del puerto y garantizar el funcionamiento, el desarrollo y el éxito del puerto en general.

Entre los servicios que ofrece el puerto de Kuantan, tenemos:

- Servicios de Carga
    - Ruptura granel
    - Carga seca al granel

- Granel Líquido
- Carga Peligrosa

- Servicios Marítimos
  - Pilotaje
  - Dilación
  - Amarre-litera
  - Control de puertos y navegación

- Servicios de Soporte

Logotipo	Sitio web
PELABUHAN KUANTAN MALAYSIA	http://www.lpktn.gov.my

Figura 34: Logotipo y web site del puerto KUANTAN.

Sobre el tema de la certificación ISO, KPA obtuvo de manera exitosa el ISO Sistema de Gestión de Seguridad de la Información (SGSI) IEC 27001 /: 2013 certificación del SIRIM QAS Internacional Sdn Bhd en 2014, donde la validez de la certificación es de 19 de diciembre 2014 hasta el 26 de diciembre de 2016. El alcance de la certificación del Ejército Popular de Corea fue "Sistema de Gestión de Seguridad de la Información (SGSI) enfocándose en el proceso de la notificación electrónica de Pre ingreso al Sistema de protección del buque (e-PENS) a Kuantan Puerto "y que está estrechamente relacionado con la función del Ejército Popular de Corea como un regulador de Kuantan Puerto."

CERTIFICATE

SIRIM QAS International hereby certifies that

LEMBAGA PELABUHAN KUANTAN
TANJUNG GELANG
25720 KUANTAN
PAHANG DARUL MAKMUR
MALAYSIA

has implemented an Information Security Management System complying with

ISO/IEC 27001:2013
Information Technology – Security Techniques – Information Security Management Systems – Requirements

Scope of Certification

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR ELECTRONIC PRE-ENTRY NOTIFICATION SHIP SECURITY SYSTEM (e-PENS) AT KUANTAN PORT.

THIS IS IN ACCORDANCE TO STATEMENT OF APPLICABILITY: VERSION 1.0, 01 JULY 2014

Issue date : 19 December 2014
Validity period : 19 December 2014 - 26 December 2016
Certification No. : AR 6032

Khalidah Mustafa
Managing Director
SIRIM QAS International Sdn. Bhd

Figura 35: Certificado ISO 27001:2013 del puerto de KUANTAN, obtenida el 19 de diciembre de 2014.

3.5 COMITÉ DE EVALUACIÓN SOBRE LA IMPLEMENTACIÓN DEL EGSI EN AUTORIDADES PORTUARIAS DEL ECUADOR

Para poder evaluar los niveles de seguridad, relacionados a la información de las Instituciones de Autoridades Portuarias del Ecuador, se conformó un grupo de personas, quienes ayudaron mediante cuestionarios a verificar el estado de los controles que se indican en el Esquema Gubernamental de Seguridad de la Información, enfocados en la FASE I, por lo que se ocuparon los hitos prioritarios.

Las personas seleccionadas para conformar este comité son:

#	Nombre de Evaluador	Cargo	Empresa
1	Ing. César Cedeño Cedeño	Director de TIC	Autoridad Portuaria de Manta
2	T.C. Patricio Camacho Alarcón	Analista TIC	Autoridad Portuaria de Manta

3	Ing. Daniel Navas R.	Director de Seguridad Integral	Autoridad Portuaria de Manta
4	Ing. Auxiliadora Palma	Directora de Talento Humano	Autoridad Portuaria de Manta
5	Ec. Jessenia Velásquez	Directora Administrativa	Autoridad Portuaria de Manta
6	Director de TIC Director de Seguridad Director de Talento Humano Director Administrativo		Autoridad Portuaria de Guayaquil
7	Director de TIC Director de Seguridad Director de Talento Humano Director Administrativo		Autoridad Portuaria de Esmeraldas
8	Director de TIC Director de Seguridad Director de Talento Humano Director Administrativo		Autoridad Portuaria de Puerto Bolívar

Tabla 17: Listado de directivos de la Autoridad Portuaria de Manta que conforman comité de evaluación.

3.6 NIVELES DE EVALUACIÓN DE LA IMPLEMENTACIÓN DE EGSI EN LAS AUTORIDADES PORTUARIAS DEL ECUADOR

A continuación se detallan los niveles que se utilizará para la evaluación en el cuestionario relacionado a las directrices de los controles del Esquema Gubernamental de Seguridad de la Información.

- Nivel 0: No se tiene implementada la directriz prioritaria en la institución, de manera automatizada ni manual.
- Nivel 1: Se tiene implementada la directriz prioritaria que se está evaluando en la institución, pero de manera manual, lo cual no incluye ningún tipo de tecnología.
- Nivel 2: La directriz prioritaria evaluada está implementada de manera básica con algún tipo de tecnología, pero se necesita de procesos manuales para la obtención de resultados.
- Nivel 3: El control evaluado está implementado de manera avanzada por medio de tecnología y genera resultados de forma automática o sistematizada.

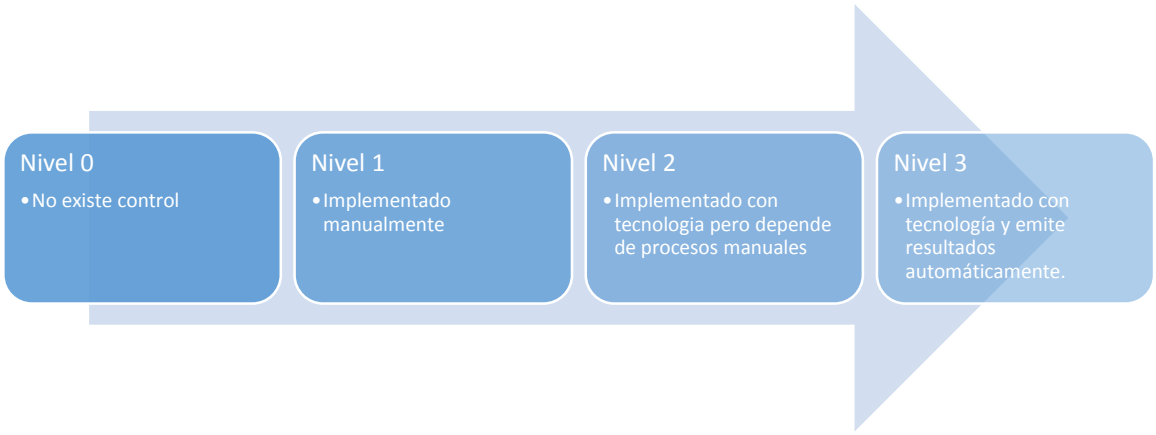

Figura 36: Niveles de evaluación para los controles del EGSI en el cuestionario.

3.7 DESCRIPCIÓN DE LOS DOMINIOS, CONTROLES Y DIRECTRICES A EVALUAR

El Esquema Gubernamental de Seguridad de la Información, elaborado por la Subsecretaría de Gobierno Electrónico y que es controlado por la Secretaría Nacional de Administración Pública, está basado en la NORMA ISO/IEC 27002, por lo que los Dominios, Controles y Directrices que se definió en la FASE I, son:

3.7.1 DOMINIO 1: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1 Documento de la Política de Seguridad de la Información.	
1.1.1 Disponer la implementación del EGSI en la institución por la máxima autoridad.	1.1.2 Difundir la política de seguridad de la información de referencia o propia de la institución.

Tabla 18: Listado de Control y Directrices del Dominio 1 del EGSI. (DERECHO ECUADOR, 2014)

3.7.2 DOMINIO 2: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

2.1 Compromiso de la máxima autoridad de la institución con la seguridad de la información realizada.		
2.1.1 Realizar el seguimiento de la puesta en marcha de las normas de este documento.	2.1.2 Disponer la difusión, capacitación y sensibilización del contenido de este documento.	2.1.3 Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a los integrantes.

2.2 Coordinación de la Gestión de la Seguridad de la Información.	
2.2.1.1 Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CSI.	2.2.1.2 Designar formalmente al responsable de seguridad del área de Tecnologías de la Información.

2.5 Acuerdos sobre Confidencialidad.				
2.5.1 Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.	2.5.2 Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción.	2.5.3 Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos.	2.5.4 Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.	2.5.5 Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros.

Tabla 19: Listado de Control y Directrices del Dominio 2 del EGSI. (DERECHO ECUADOR, 2014)

3.7.3 DOMINIO 3: GESTIÓN DE LOS ACTIVOS

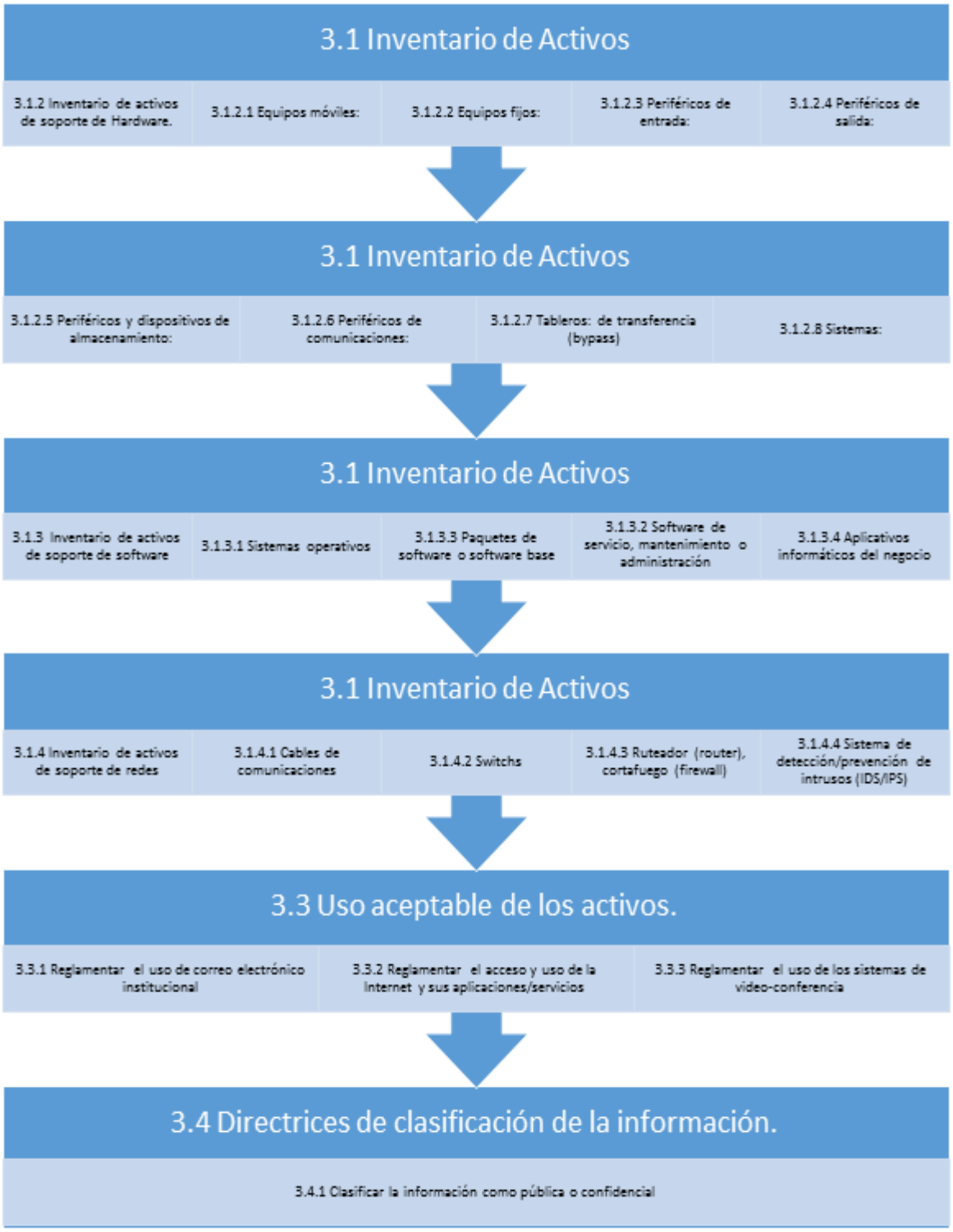

Tabla 20: Listado de Control y Directrices del Dominio 3 del EGSI. (DERECHO ECUADOR, 2014)

3.7.4 DOMINIO 4: SEGURIDAD DE LOS RECURSOS HUMANOS

Tabla 21: Listado de Control y Directrices del Dominio 4 del EGSI. (DERECHO ECUADOR, 2014)

3.7.5 DOMINIO 5: SEGURIDAD FÍSICA Y DEL ENTORNO

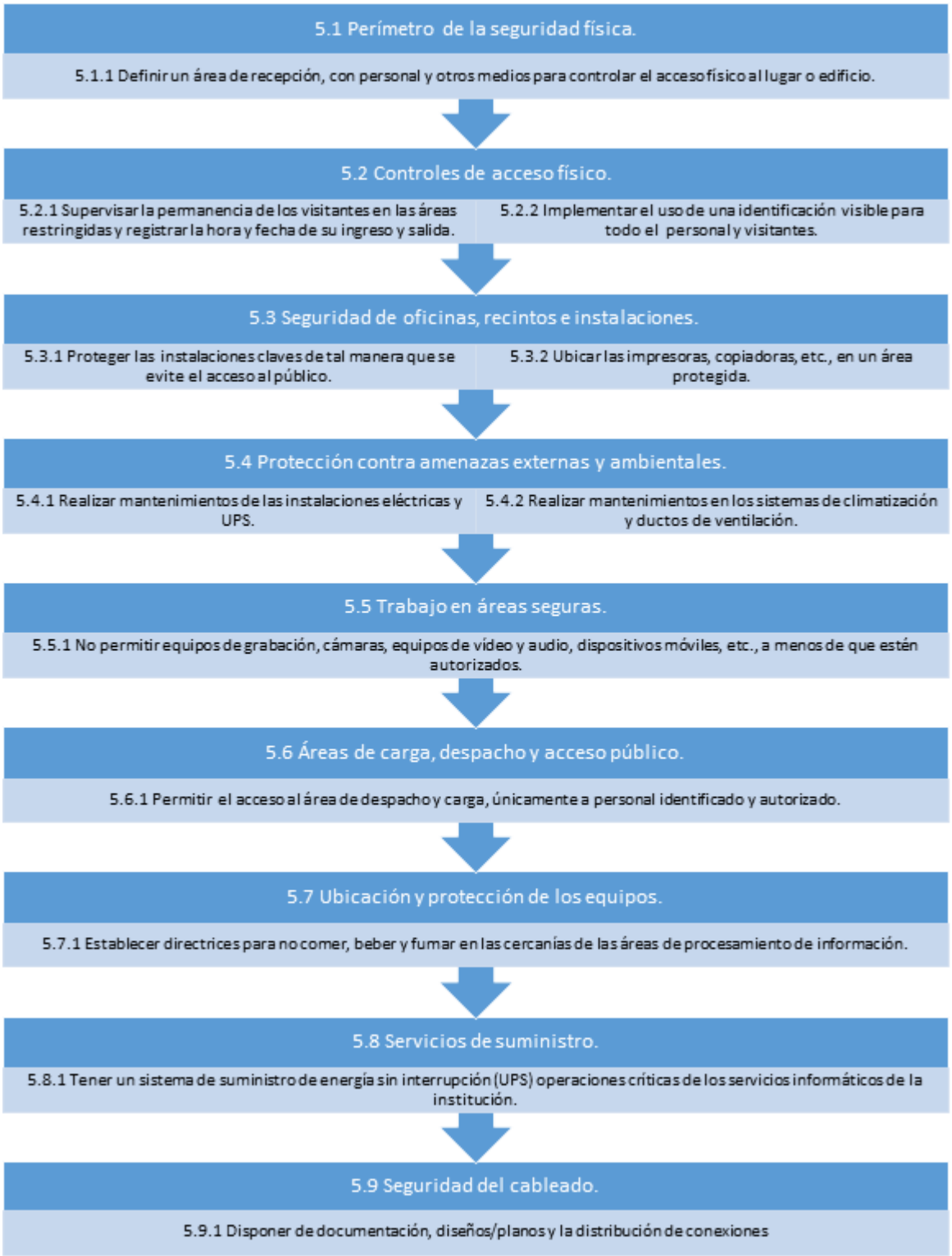

Tabla 22: Listado de Control y Directrices del Dominio 5 del EGSI. (DERECHO ECUADOR, 2014)

3.7.6 DOMINIO 6: GESTIÓN DE COMUNICACIONES Y OPERACIONES

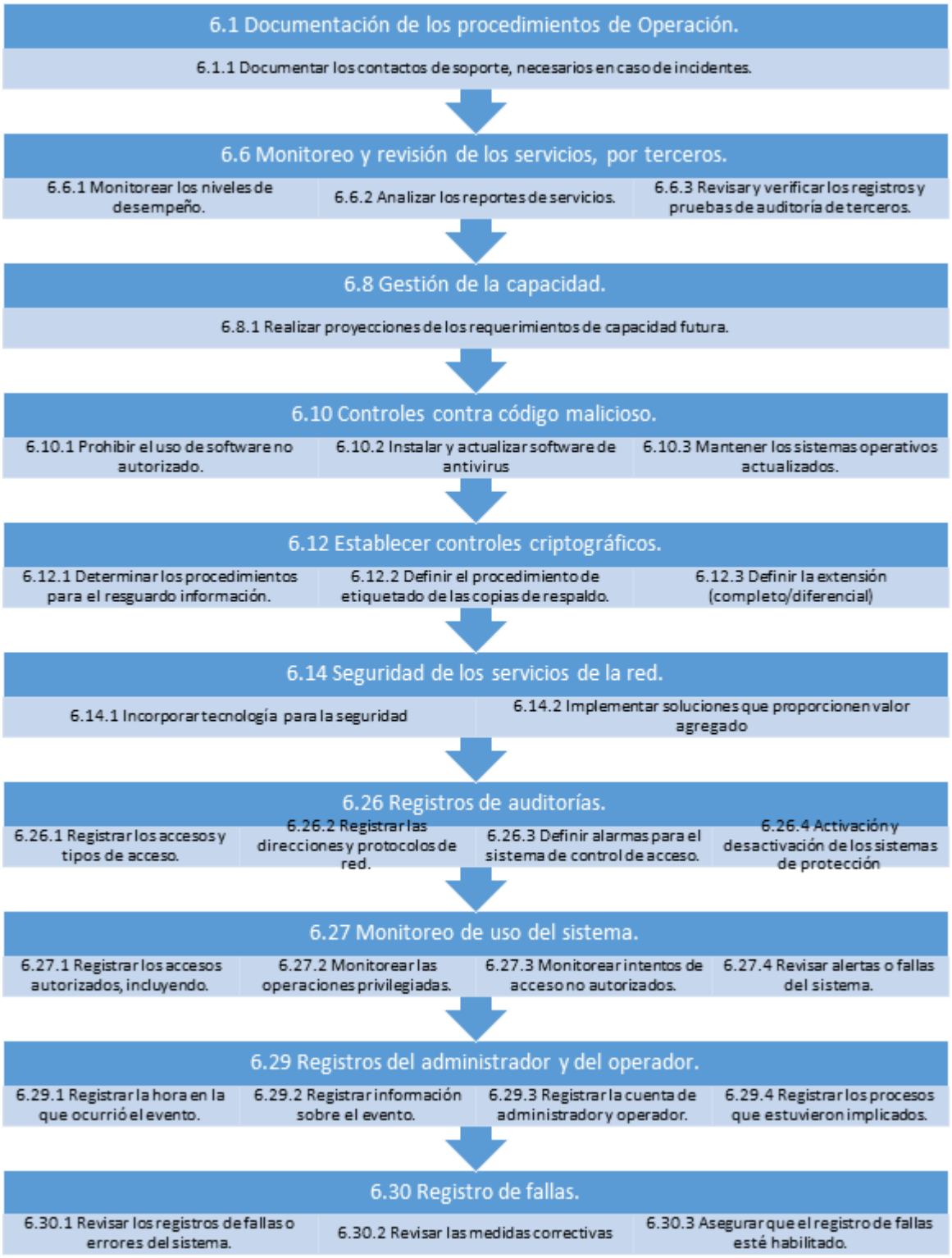

Tabla 23: Listado de Control y Directrices del Dominio 6 del EGSI. (DERECHO ECUADOR, 2014)

3.7.7 DOMINIO 7: CONTROL DE ACCESO

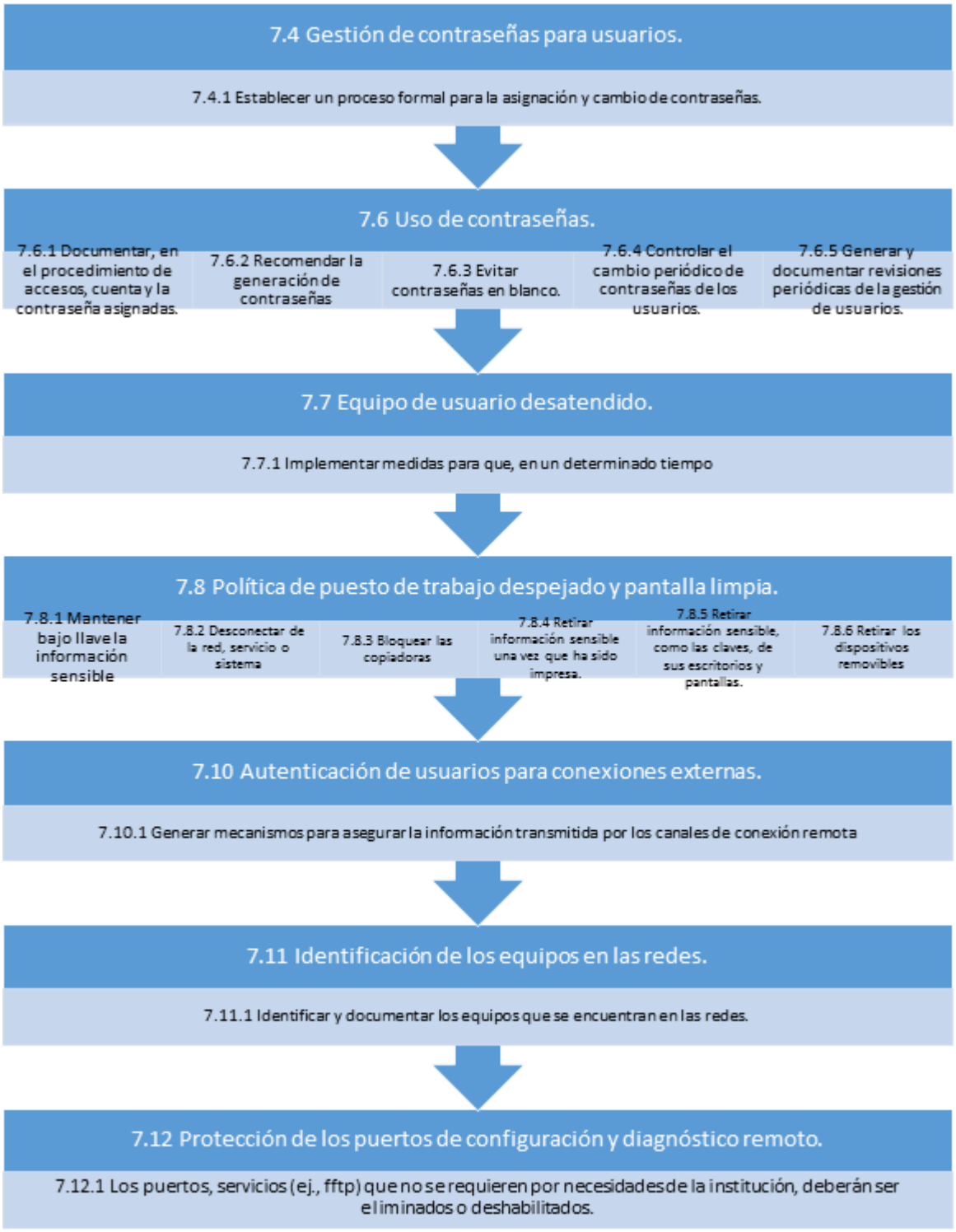

Tabla 24: Listado de Control y Directrices del Dominio 7 del EGSI. (DERECHO ECUADOR, 2014)

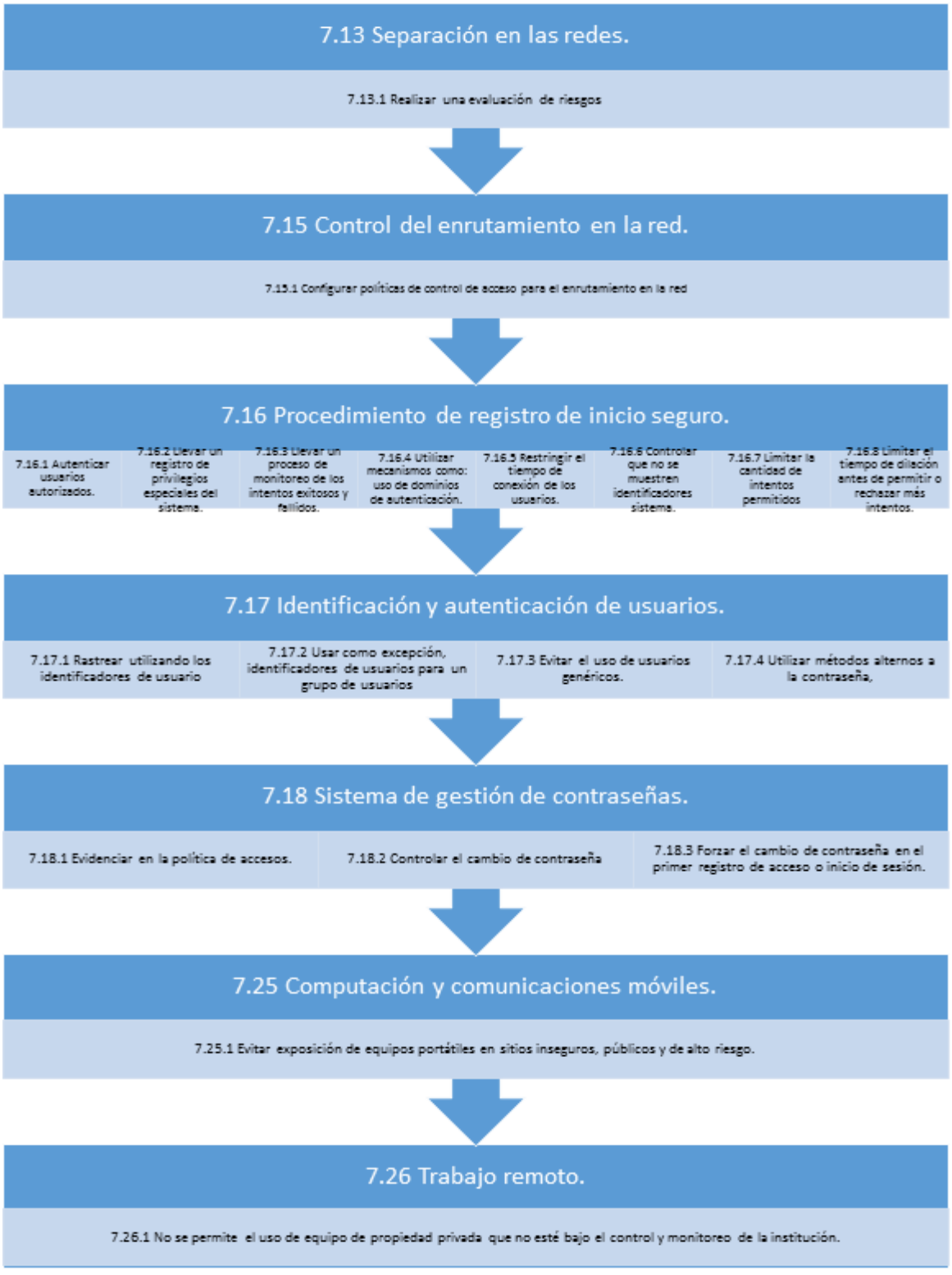

Tabla 25: Continuación de Control y Directrices del Dominio 7 del EGSI. (DERECHO ECUADOR, 2014)

3.7.8 DOMINIO 8: ADQUISICIÓN, DESARROLLO, Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.1 Análisis y especificaciones de los requerimientos de seguridad.	
8.1.1 Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.	8.1.2 Definir los controles apropiados, tanto automatizados como manuales.

Tabla 26: Listado de Control y Directrices del Dominio 8 del EGSI. (DERECHO ECUADOR, 2014)

3.7.9 DOMINIO 9: GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN.

9.1 Reporte sobre los eventos de seguridad de la información					
9.1.1 Instaurar un procedimiento formal9.1.2 Cuando un incidente se produzca	9.1.2.1 Identificar el incidente.	9.1.2.2 Registrar el incidente en una bitácora de incidentes	9.1.2.3 Notificar al Oficial de Seguridad de la Información.	9.1.2.4 Clasificar el incidente	9.1.2.5 Asignar una prioridad de atención al incidente

9.1 Reporte sobre los eventos de seguridad de la información				
9.1.2.6 Realizar un diagnóstico inicial,	9.1.2.7 Escalar el incidente	9.1.2.8 Investigar las causas por las cuales se produjo el incidente.	9.1.2.9 Resolver y restaurar el servicio afectado.	9.1.2.10 Cerrar el incidente.

Tabla 27: Listado de Control y Directrices del Dominio 9 del EGSI. (DERECHO ECUADOR, 2014)

3.8 MECANISMO DE EVALUACIÓN DE LA IMPLEMENTACIÓN DEL EGSI

El mecanismo para realizar la evaluación, fue por medio de CUESTIONARIOS, el cual es un mecanismo para investigar por medio de preguntas y respuestas, con el afán de recopilar los resultados por medio de dichas preguntas a las personas que serán evaluadas.

Para esta investigación se elaborara *cuestionarios por el rol* del funcionario a evaluar, por lo que se agruparán las directrices en base a las funciones que cumplen cada Director dentro de la institución.

Las preguntas del *cuestionario*, no serán nada más que las directrices que están denominadas como hitos prioritarios dentro del Esquema Gubernamental de Seguridad de la Información, en su FASE I, que fue que se tomó para esta investigación.

3.8.1 FORMATO DE LOS CUESTIONARIOS

Los formatos de cuestionario que se utilizarán para la evaluación, están elaborados por Directrices de acuerdo a las funciones de los encuestados. Como los encuestados cumplen en su gran mayoría funciones distintas en cada institución, se deberá agrupar las directrices para que estas sean evaluadas de mejor forma por los Directores de Área.

Por este motivo se tendrán los siguientes cuestionarios:

- CUESTIONARIO enfocado en actividades de TALENTO HUMANO
- CUESTIONARIO enfocado en actividades de TECNOLOGÍA DE LA INFORMACIÓN
- CUESTIONARIO enfocado en actividades de SEGURIDAD
- CUESTIONARIO enfocado en actividades de ADMINISTRACIÓN

3.9 BENCHMARKING

Consiste en recopilar información relacionada para el mejoramiento de un proceso dentro de una institución.

La información puede ser obtenida comparando los procesos de una empresa ejemplo con los de la institución que se está evaluando, por ende este método no significa copiar las mejores prácticas de una empresa, sino aprender de estas empresas que están realizando de manera correcta la ejecución de sus procesos, identificando donde se encuentra actualmente un proceso y saber hacia dónde lo quiero proyectar en el futuro.

Por todo lo antes mencionado, se puede decir que *benchmarking* es una técnica o herramienta de gestión que permite la comparación de una empresa que gestiona las mejores prácticas, en lo relacionado a productos, procesos, servicios u otros, con el propósito de adquirir dichas experiencias.

Por este motivo se escogió a *BENCHMARKING* como la herramienta para evaluar el Esquema Gubernamental de Seguridad de la Información, su correcta implementación en la Autoridad Portuaria de Manta y comparación con otros puertos marítimos del país, para verificar el estado de madurez operacional de dichas instituciones y como este Esquema Gubernamental, apoya en la evolución de la seguridad de la información dentro de la institución.

3.10 RESULTADOS DE LAS DIRECTRICES AGRUPADAS POR FUNCIONES RELACIONADAS CON LAS DIRECCIONES INSTITUCIONALES.

3.10.1 DIRECTRICES RELACIONADAS CON LA DIRECCIÓN ADMINISTRATIVA

#	DIRECTRICES RELACIONADAS CON ADMINISTRATIVO	AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	2.5.5 Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros.	1	2	1	1
2	3.1.2.7 Tableros de transferencia (bypass) de la unidad no interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.	1	2	0	2
3	5.4.1 Realizar mantenimientos de las instalaciones eléctricas y UPS	1	2	1	1
4	5.4.2 Realizar mantenimientos en los sistemas de climatización y ductos de ventilación	1	2	1	1
5	5.8.1 Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios	1	2	0	1

Tabla 28: Controles relacionadas con la Dirección Administrativa.

Figura 37: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección Administrativa.

Estos resultados indican que el Área Administrativa de la Autoridad Portuaria de Guayaquil cuenta con una mayor madurez operacional, sobre las Directrices de la seguridad de la información, por lo que los procesos en su gran mayoría se manejan de forma sistematizada, basados en la tecnología de la información pero con apoyos o procesos manuales para la obtención de los resultados.

Cabe indicar que las demás entidades portuarias, cuentan en su gran mayoría con procesos manuales, para el cumplimiento de dichas directrices.

3.10.2 DIRECTRICES RELACIONADAS CON LA DIRECCIÓN DE TALENTO HUMANO

#	DIRECTRICES RELACIONADAS CON TALENTO HUMANO	AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	2.5.2 Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción	1	2	1	1
2	2.5.3 Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos	1	2	1	2
3	2.5.4 Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción	1	2	1	2
4	4.1.1 Verificar a los candidatos, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida	1	2	1	1
5	4.1.2 Entregar formalmente a los funcionarios sus funciones y responsabilidades	1	2	0	0

Tabla 29: Controles relacionadas con la Dirección de Talento Humano.

Figura 38: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de Talento Humano.

Los resultados del gráfico y tabla anterior hacen referencia a la madurez operacional de las Directrices relacionadas con el Área de Talento Humano, indicando que en su gran mayoría estos controles de la Seguridad de la Información, se manejan con sistemas informáticos y procesos manuales para la obtención o control de la información.

La institución que logra una mayor madurez operacional es la Autoridad Portuaria de Guayaquil, en base a los cuestionarios, indicando también de forma gráfica que el resto de autoridades portuarias, tienen los controles de las directrices de forma manual.

3.10.3 DIRECTRICES RELACIONADAS CON LA DIRECCIÓN DE SEGURIDAD INTEGRAL

#	DIRECTRICES RELACIONADAS CON SEGURIDAD FISICA O INTEGRAL	AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	5.1.1 Definir una área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio	1	2	1	1
2	5.2.1 Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida	1	1	1	2
3	5.2.2 Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas	2	2	1	2
4	5.3.1 Proteger las instalaciones claves de tal manera que se evite el acceso al público	2	2	2	2
5	5.5.1 No permitir equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles, etc., a menos de que estén autorizados	0	1	0	0
6	5.6.1 Permitir el acceso al área de despacho y carga, únicamente a personal identificado y autorizado	2	2	1	2
7	5.7.1 Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información	1	1	0	0

Tabla 30: Controles relacionadas con la Dirección de Seguridad.

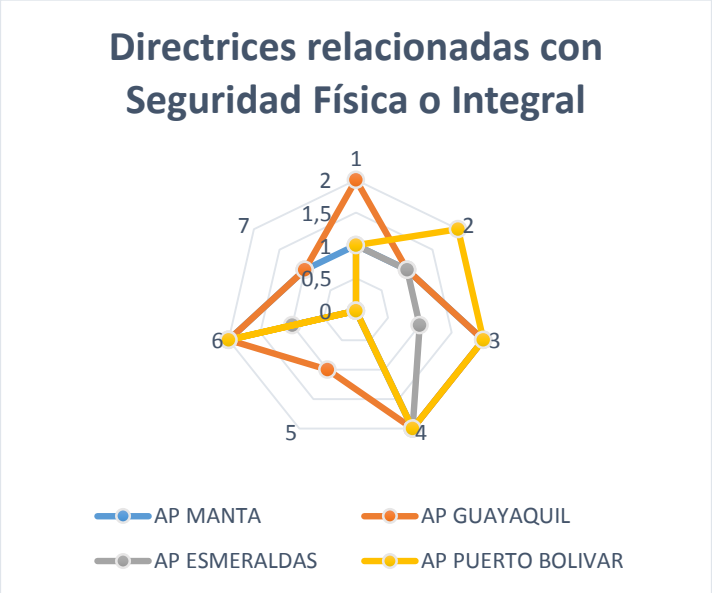

Figura 39: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de Seguridad.

Estos resultados mostrados gráficamente, indican que la Autoridad Portuaria de Guayaquil, continúa siendo una de las mejores en madurez operacional de seguridad de la información, con los controles relacionados a la Seguridad Física o Integral, pero cabe recalcar que estas seguridades que fueron evaluadas en la APG, se relacionan también con las seguridades de la empresa CONTECON S.A., ya que como es de conocimiento público, el Puerto de Guayaquil esta concesionado a dicha empresa.

3.10.4 DIRECTRICES RELACIONADAS CON LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

A continuación se mostrarán los resultados de las Directrices evaluadas por Dominios, ya que la mayoría de los HITOS del EGSI, están enfocados en Tecnología de la Información.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 2 "ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	2.5.1 Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI	1	1	2	1	1

Tabla 31: Controles relacionadas con la Dirección de TIC vs. Dominio 2 del EGSI.

Figura 40: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 2 del EGSI.

El gráfico y la tabla anterior, muestran los resultados de la evaluación a los Directores de TIC, dando a la Autoridad Portuaria de Guayaquil, como la entidad que mayor madurez operacional tiene, y las demás instituciones portuarias solo cumplen con el control a dichas directrices pero de forma manual.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 3 "GESTION DE LOS ACTIVOS"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	APG UAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.	1	1	3	1	1
2	Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.	2	1	2	2	1
3	Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.	2	2	3	2	1
4	Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plóter, máquina de fax, etc.	2	2	3	2	1
5	Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.	2	1	2	1	1
6	Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc	2	1	2	0	1
7	Sistemas de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc	2	2	2	2	2
8	Sistemas operativos		1	3	1	2
9	Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc	2	1	3	1	2
10	Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc	2	2	3	1	2
11	Aplicativos informáticos del negocio	2	2	3	1	2
12	Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ,interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc	1	0	0	0	2
13	Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, etc.).	2	0	2	1	2
14	Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc	2	1	2	1	2
15	Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc	2	1	2	2	2

Tabla 32: Controles relacionadas con la Dirección de TIC vs. Dominio 3 del EGSI.

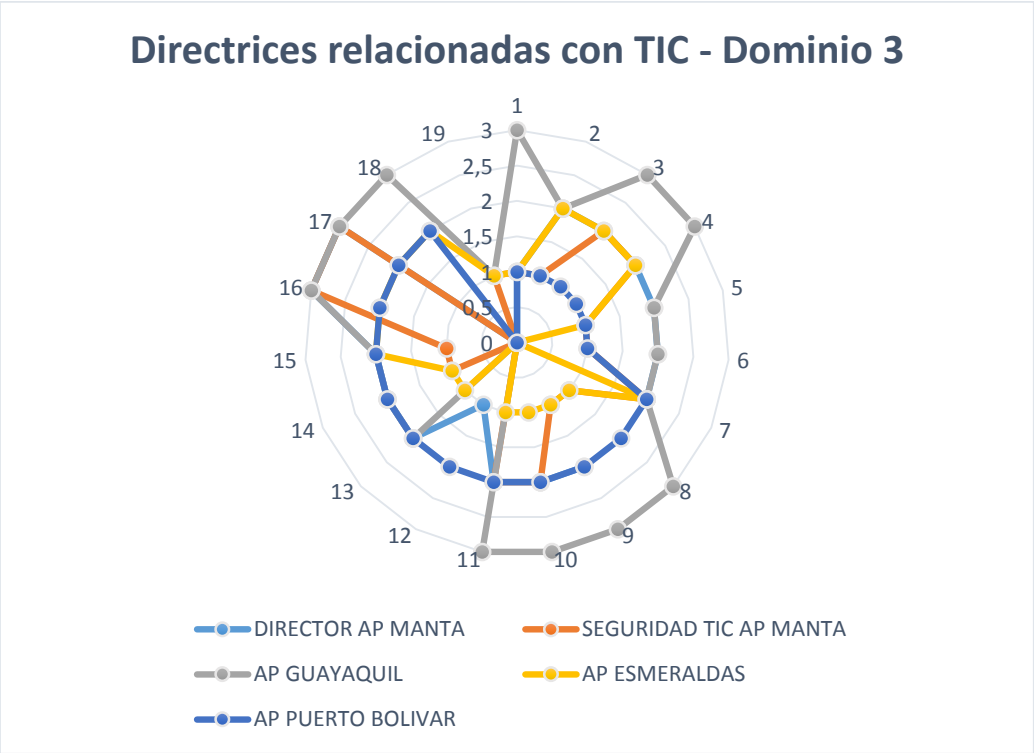

Figura 41: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 3 del EGSI.

En este Dominio, relacionado con la Gestión de los Activos, la Autoridad Portuaria de Guayaquil, tiene sistemas informáticos que ayudan de manera automática en la obtención de los resultados, teniendo una mayor madurez operacional en relación a las demás instituciones portuarias.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 4 "SEGURIDAD DE LOS RECURSOS HUMANOS"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	*Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles*	0	1	1	0	0

Tabla 33: Controles relacionadas con la Dirección de TIC vs. Dominio 4 del EGSI.

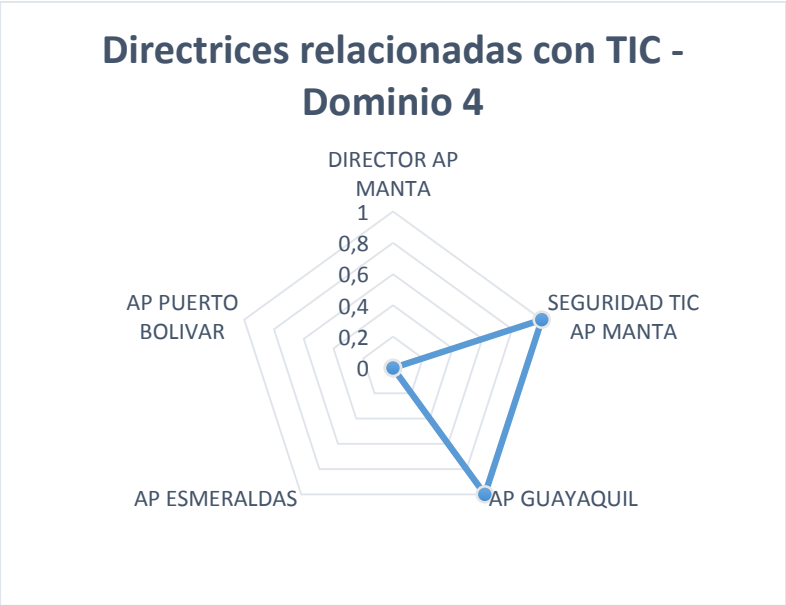

Figura 42: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 4 del EGSI.

Estos resultados indican que ninguna institución portuaria controla dichas directrices de forma sistematizada, la única forma es de manera manual y solo dos de las cuatro entidades portuarias lo controlan.

Esta directriz evaluada tenía una particularidad en especial ya que en ninguna de las instituciones no se definía si era tarea del área de Talento Humano o de TICs, se puede entender que por ese motivo no ha sido automatizada aún.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 5 "SEGURIDAD FISICA Y DEL ENTORNO"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	*Ubicar las impresoras, copiadoras, etc., en un área protegida*	0	1	1	0	0
2	*Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc*	0	1	2	0	0

Tabla 34: Controles relacionadas con la Dirección de TIC vs. Dominio 5 del EGSI.

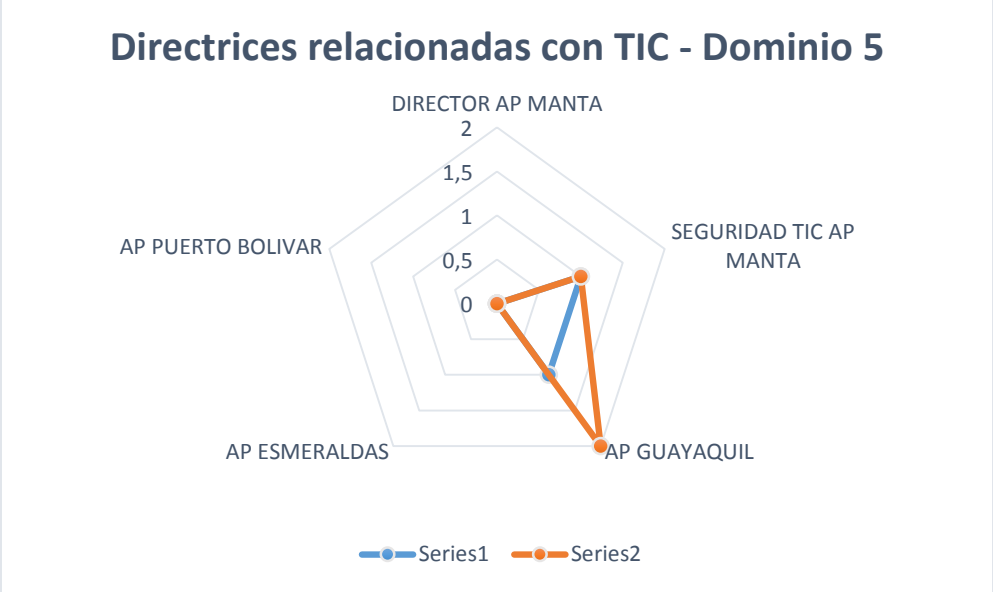

Figura 43: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 5 del EGSI.

Los resultados del gráfico y tabla anterior, permiten interpretar que dos instituciones portuarias tienen estas directrices controladas de forma manual y una institución como la Autoridad Portuaria de Guayaquil, lo tiene con un proceso sistematizado, pero que dependen de procesos manuales, mientras que las otras dos instituciones no ejecutan dicho control.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 6 "GESTION DE COMUNICACIONES Y OPERACIONES"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	*Documentar los contactos de soporte, necesarios en caso de incidentes*	0	1	2	1	0
2	*Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos*	0	0	2	1	0
3	*Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos*	0	0	2	1	0
4	*Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado*	0	0	2	1	0
5	*Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos*	2	1	3	1	1
6	*Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado*	1	1	2	1	1
7	*Instalar y actualizar periódicamente software de antivirus y contra código malicioso*	2	3	3	2	2
8	*Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles*	2	3	3	2	2
9	*Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.*	1	1	2	1	1
10	*Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención*	2	2	3	1	1
11	*Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución*	2	2	3	1	1
12	*Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red*	2	2	2	1	1
13	*Implementar soluciones que proporcionen valor agregado a los conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.*	2	2	3	2	1
14	*Registrar los accesos y tipos de acceso*	2	2	3	1	1
15	*Registrar las direcciones y protocolos de red*	2	2	3	1	1
16	*Definir alarmas originadas por el sistema de control de acceso*	0	0	3	1	0
17	*Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS)*	1	2	3	1	0

Tabla 35: Controles relacionadas con la Dirección de TIC vs. Dominio 6 del EGSI.

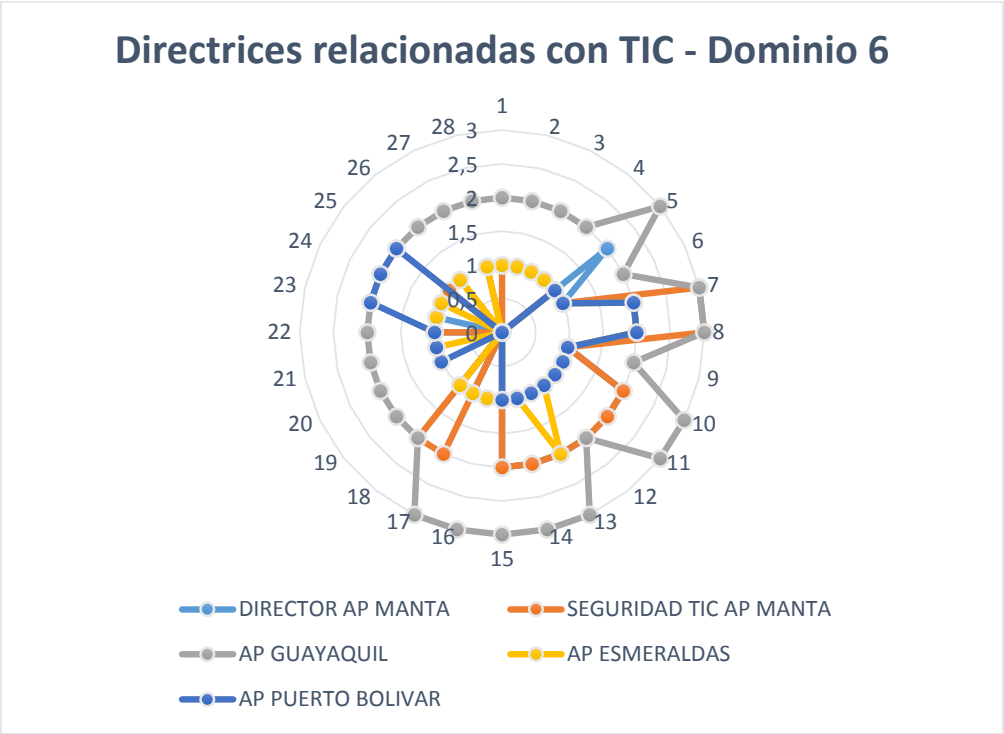

Figura 44: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 6 del EGSI.

La Autoridad Portuaria de Guayaquil, tiene en este Dominio Gestión de Comunicación y Operaciones, la mayor madurez operacional, en base a las otras instituciones portuarias, teniendo en su gran mayoría controles sistematizados de forma automática y otros con el apoyo de proceso manuales para la obtención de resultados, de igual forma la Autoridad Portuaria de Manta, mas no las otras instituciones que manejan sus procesos en su gran mayoría de forma manual.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 7 "CONTROL DE ACCESO"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	Establecer un proceso formal para la asignación y cambio de contraseñas	3	2	2	1	0
2	Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados	0	0	1	0	0
3	Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta	2	2	2	1	1
4	Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables	3	2	2	1	2
5	Controlar el cambio periódico de contraseñas de los usuarios	3	2	2	1	2
6	Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información	0	2	2	1	2
7	Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave	3	2	2	1	2
8	Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no estén en uso y no se encuentre personal en la oficina	1	1	1	0	0
9	Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave	0	0	3	0	0
10	Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas	0	0	2	0	0
11	Retirar información sensible una vez que he sido impresa	1	1	1	1	0
12	Retirar información sensible, como las claves, de sus escritorios y pantallas	1	1	1	1	0
13	Retirar los dispositivos removibles una vez que se hayan dejado de utilizar	1	0	2	1	0
14	Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes	0	2	3	0	0

Tabla 36: Controles relacionados con la Dirección de TIC vs. Dominio 7 del EGSI.

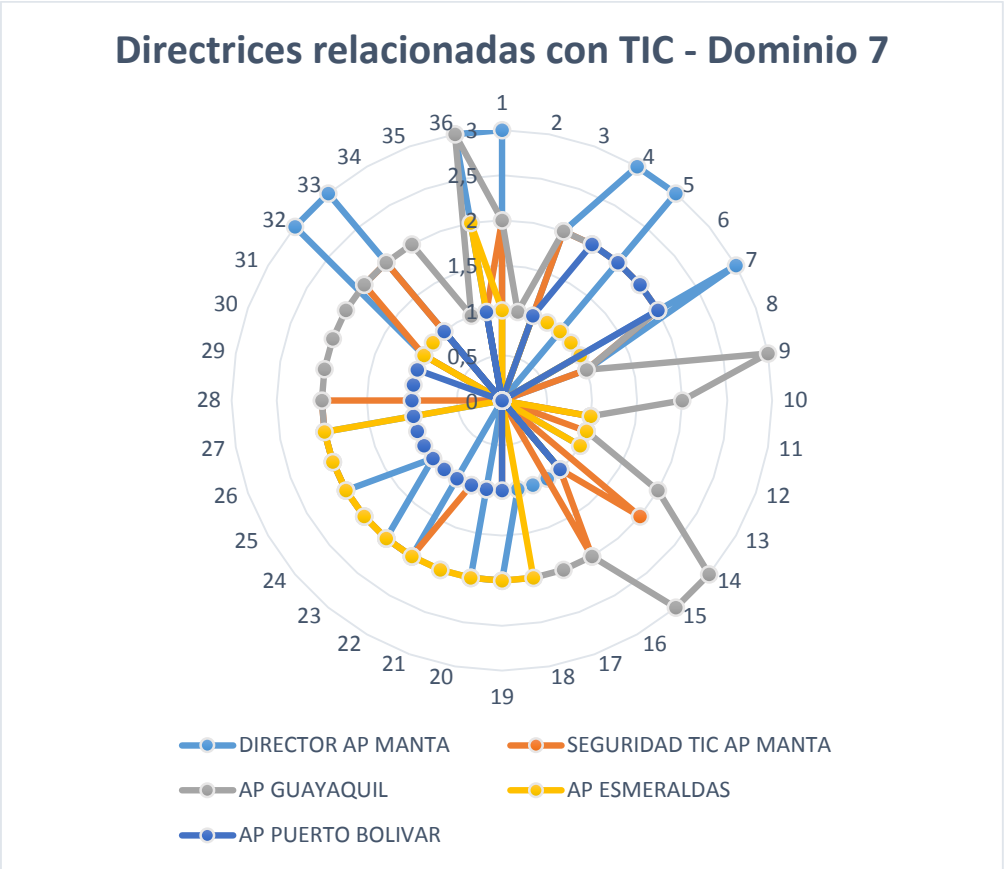

Figura 45: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 7 del EGSI.

En los resultados relacionados a las directrices del dominio de control de acceso se puede evidenciar que la mayoría de controles es manejada por todas las instituciones portuarias de forma manual y también de forma sistematizada, pero no en su totalidad. No existe ningún proceso o directriz que se maneje de forma sistematizada automáticamente, por lo que el modelo de madurez operacional no está en su mejor performance por ninguna de las instituciones evaluadas.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 8 "ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN"	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.	0	0	2	0	1
2	Definir los controles apropiados, tanto automatizados como manuales	0	0	2	0	1

Tabla 37: Controles relacionadas con la Dirección de TIC vs. Dominio 8 del EGSI.

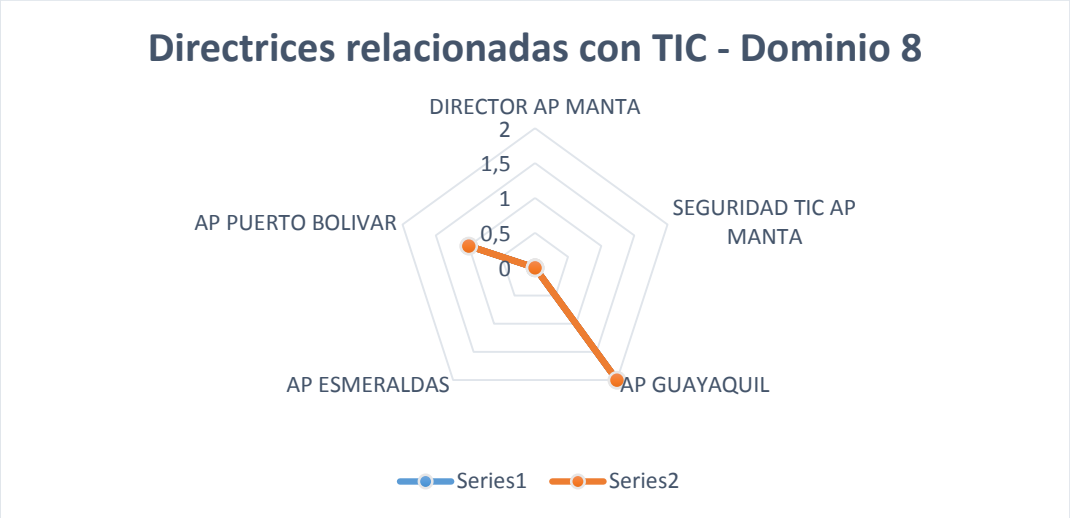

Figura 46: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 8 del EGSI.

Lo que permite evidenciar estos resultados es que las instituciones evaluadas en esta investigación, determina que no realizan o no controlan los procesos para la adquisición o mantenimiento de software, de manera manual o sistematizada, lo que da a entender es que no existe una planificación al momento de adquirir o dar mantenimiento a un sistema, sino que se adquieren por necesidad o para cumplir con algún requerimiento especifico que se solicite al área de TIC.

#	DIRECTRICES RELACIONADAS CON TIC DOMINIO 9	DIRECTOR AP MANTA	SEGURIDAD TIC AP MANTA	AP GUAYAQUIL	AP ESMERALDAS	AP PUERTO BOLIVAR
1	Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información	2	2	3	1	0
2	Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden	3	2	3	1	1
3	Identificar el incidente	3	2	3	1	1
4	Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente	3	2	3	1	1
5	Notificar al Oficial de Seguridad de la Información de la institución	2	2	2	1	1
6	Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad	3	2	3	1	1
7	Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultanea	3	2	3	1	1
8	Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas	3	2	3	1	1
9	Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado	3	2	3	1	1
10	Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente	3	2	3	1	1
11	Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes	2	2	3	1	1
12	Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a “Resuelto”. Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto	2	2	2	1	0

Tabla 38: Controles relacionadas con la Dirección de TIC vs. Dominio 9 del EGSI.

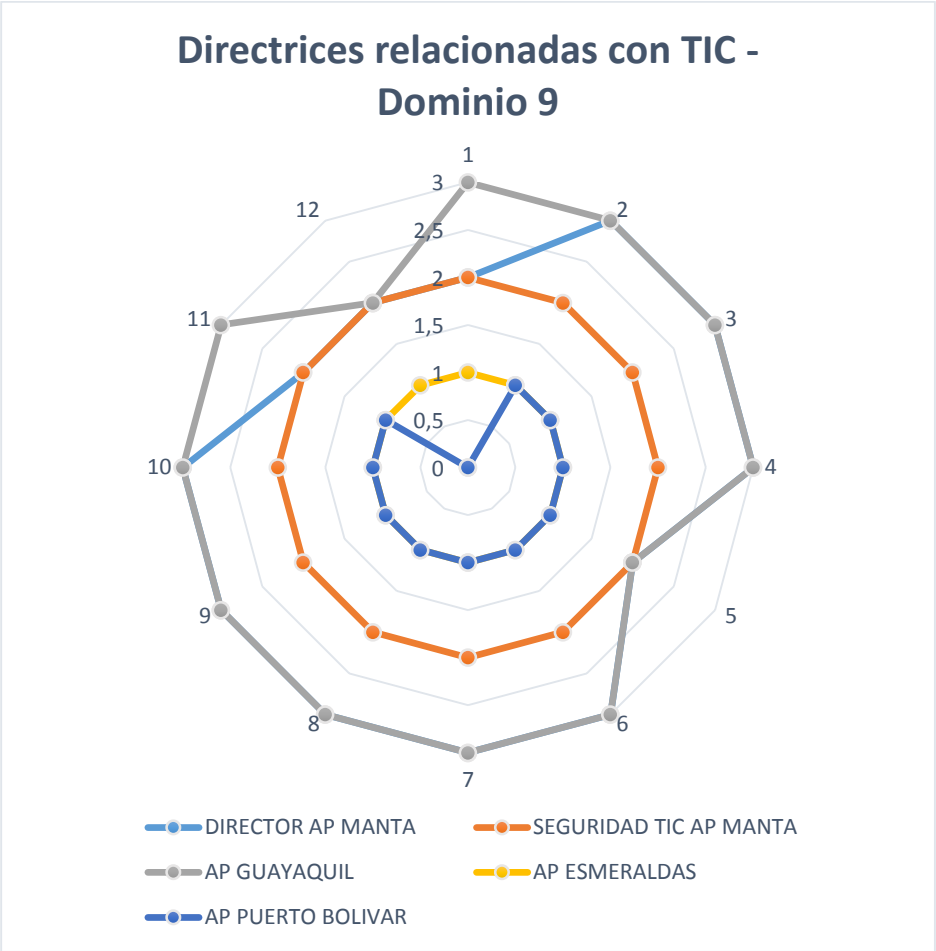

Figura 47: Gráfico Estadístico sobre niveles de cumplimiento relacionados con la Dirección de TIC versus el Dominio 9 del EGSI.

Y en este último gráfico y tabla, que indican los resultados de la evaluación de los controles del Dominio 9, se puede notar que la Autoridad Portuaria de Guayaquil junto con la de Manta, son las que tienen una madurez operacional avanzada en relación a las otras entidades portuarias. Recalcando que la APG, tiene en su gran mayoría un sistema que permite manejar los incidentes tecnológicos y de seguridad de forma automática e integrada con los sistemas de la institución.

3.11 RESULTADOS DE LAS DIRECTRICES AGRUPADAS POR INSTITUCIÓN Y SU NIVEL DE MADUREZ OPERACIONAL.

En el siguiente gráfico se muestra de manera general los niveles de madurez de la implementación del Esquema Gubernamental en las Autoridades Portuarias del País, comparado con las cantidades de HITOS o Controles del EGSI:

	MADUREZ OPERACIONAL			
AUTORIDADES PORTUARIAS	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3
ESMERALDAS	17	55	9	0
GUAYAQUIL	1	9	52	19
MANTA	14	26	27	14
PUERTO BOLIVAR	24	38	19	0

Tabla 39: Cuadro comparativo de los niveles de madurez operacional en las Autoridades Portuarias del País en relación al EGSI.

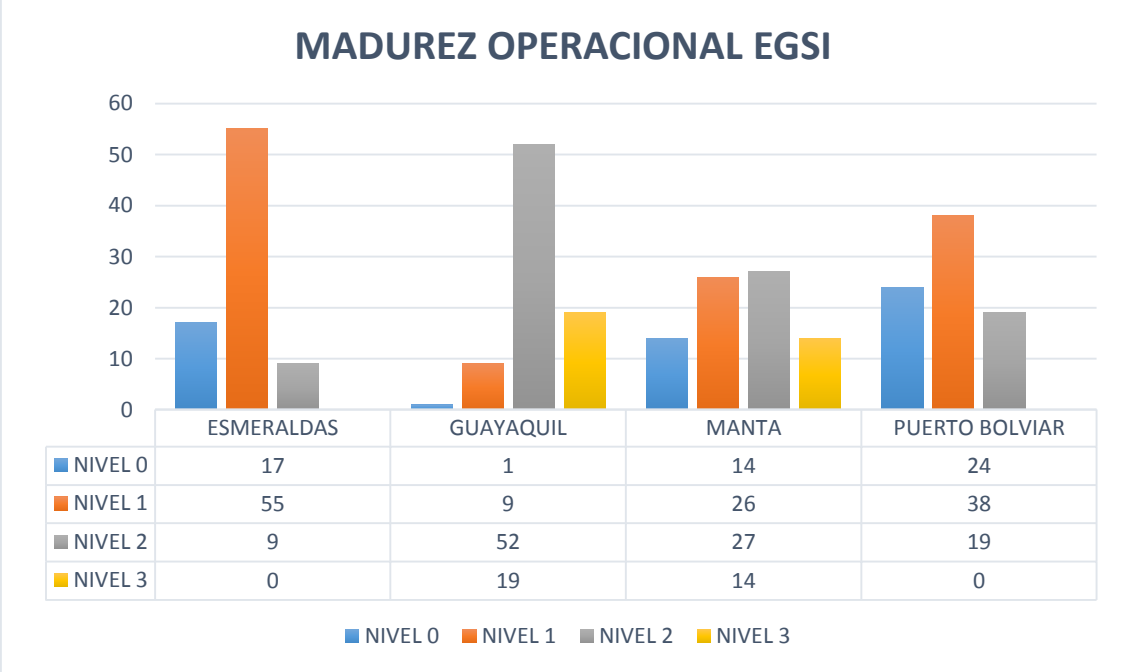

Figura 48: Gráfico Estadístico sobre los niveles de madurez operacional de las Autoridades Portuairas sobre la implementación del EGSI.

3.11 COMPARACIÓN DEL EGSI IMPLEMENTADO EN AUTORIDAD PORTUARIA DE MANTA CON PUERTOS INTERNACIONALES QUE IMPLEMENTARON NORMA ISO 27001

En esta investigación se intentó primero buscar puertos marítimos de países vecinos que hayan implementado la Norma ISO 27002, del cual está basado el Esquema Gubernamental de Seguridad de la Información (EGSI), lo cual no se obtuvo ninguna información.

Ampliando el abanico en la investigación, se procedió a buscar en países de primer mundo en lo relacionado a puertos marítimos, identificando países como Malasia y Emiratos Árabes Unidos, donde tienen puertos marítimos que han optado desde hace varios años implementar la Norma ISO 27001, la cual está enfocada en gestionar la seguridad de la información de la empresa.

Esta Norma ISO 27001, tiene como primera revisión en el año 2005, publicada en el mismo año, la versión más reciente es la de 2013.

Entre los puertos marítimos internacionales que han implementado esta Norma ISO tenemos:

Puerto Marítimo	País	Año Certificación ISO 27001
JOHOR PORT BERHAD (JPB)	**Malasia**	**2013**
DP WORLD – JEBEL ALI PORT	**EAU - Dubai**	**2014**
LEMBAGA PELABUHAN KUANTAN	**Malasia**	**2014**

Tabla 40: Puertos Internacionales con certificaciones Norma ISO 27001.

Por este motivo no se puede realizar una comparación directa entre los controles de seguridad implementados en los puertos marítimos, ya que el EGSI está basado en la Norma ISO 27002, pero entrando a detalle en la Norma ISO 27001, se identificaron controles que cumple la misma función en las Normas ISO 27001 y 27002, las cuales se detalla en el siguiente cuadro comparativo, donde

solo se mostrarán los controles que está dando cumplimiento la Autoridad Portuaria de Manta (APM):

#	CONTROL ISO 27001	DOMINIO – ISO 27001	DOMINIO – EGSI (ISO 27002)
1	Documento de la política de seguridad de la información	A.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
2	Revisión de la política de seguridad de la información	A.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3	Coordinación de la seguridad de la información	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
4	Asignación de responsabilidades para la seguridad de la información	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
5	Acuerdos sobre confidencialidad	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
6	Inventario de activos	A.7 GESTIÓN DE LOS ACTIVOS	3 GESTIÓN DE LOS ACTIVOS
7	Uso aceptable de los activos	A.7 GESTIÓN DE LOS ACTIVOS	3 GESTIÓN DE LOS ACTIVOS

8	Directrices de clasificación	A.7 GESTIÓN DE LOS ACTIVOS	3 GESTIÓN DE LOS ACTIVOS
9	Roles y responsabilidades	A.8 SEGURIDAD DE LOS RECURSOS HUMANOS	4 SEGURIDAD DE LOS RECURSOS HUMANOS
10	Perímetro de seguridad física	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
11	Controles de acceso físico	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
12	Seguridad de oficinas, recintos e instalaciones	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
13	Protección contra amenazas externas y ambientales	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
14	Trabajo en áreas seguras	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
15	Áreas de carga, despacho y acceso público	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
16	Ubicación y protección de los equipos	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
17	Servicios de suministro	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO
18	Seguridad del cableado	A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	5 SEGURIDAD FÍSICA Y DEL ENTORNO

19	Documentación de los procedimientos de operación	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
20	Monitoreo y revisión de los servicios por terceras partes	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
21	Controles contra códigos maliciosos	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
22	Seguridad de los servicios de la red	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
23	Registro de auditorías	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
24	Monitoreo del uso del sistema	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
25	Registros del administrador y del Operador	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES
26	Registro de fallas	A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

27	Gestión de contraseñas para usuarios	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
28	Uso de contraseñas	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
29	Equipo de usuario desatendido	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
30	Política de escritorio despejado y de pantalla despejada	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
31	Autenticación de usuarios para conexiones externas	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
32	Identificación de los equipos en las redes	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
33	Protección de los puertos de configuración y diagnóstico remoto	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
34	Separación en las redes	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
35	Control de enrutamiento en la red	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
36	Procedimientos de ingreso Seguros	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
37	Identificación y autenticación de usuarios	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
38	Sistema de gestión de contraseñas	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
39	Computación y comunicaciones móviles	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
40	Trabajo remoto	A.11 CONTROL DE ACCESO	7 CONTROL DE ACCESO
41	Análisis y especificación de los requisitos de seguridad	A.12 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
42	Reporte sobre los eventos de seguridad de la información	A.13 GESTIÓN DE LOS INCIDENTES DE LA	9 GESTIÓN DE LOS INCIDENTES DE LA

		SEGURIDAD DE LA INFORMACIÓN	SEGURIDAD DE LA INFORMACIÓN

Tabla 41: Listado de controles implementados por APM del EGSI con la Norma ISO 27001.

La Norma ISO 27001, la cual han implementado los puertos marítimos internacionales antes mencionados, tienen un total de 133 controles, de los cuales solo 42 controles se están cumpliendo en lo relacionado al EGSI en los controles prioritarios u obligatorios, lo que podemos representarlo gráficamente de la siguiente forma:

DOMINIOS	CONTROLES ISO 27001	CONTROLES EGSI CUMPLIDO POR APM
1	2	1
2	11	3
3	5	3
4	9	2
5	13	9
6	32	10
7	25	14
8	16	1
9	5	1
10	5	0
11	10	0
Total	**133**	**44**

Tabla 42: Tabla comparativa de controles de la Norma ISO 27001 versus el EGSI.

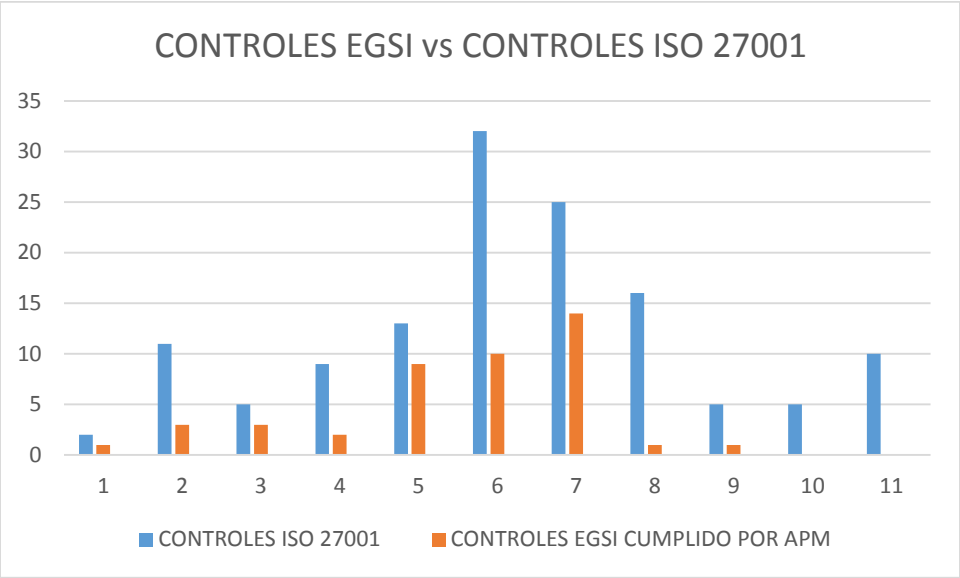

Figura 49: Gráfico de comparación de controles implementados en el EGSI versus ISO 27001.

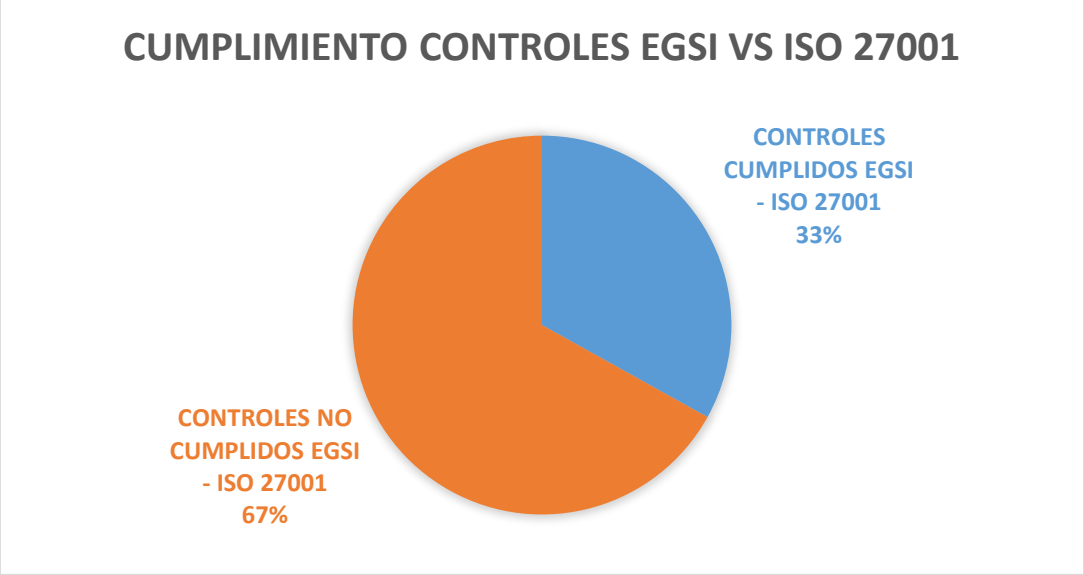

Figura 50: Gráfico de cumplimiento de los controles EGSI en relación a la ISO 27001.

3.12 CAMBIOS EN LA SEGURIDAD DE LA INFORMACIÓN DESPUÉS DE LA IMPLEMENTACIÓN DEL EGSI EN LA AUTORIDAD PORTUARIA DE MANTA

Una vez dado inicio a la implementación del EGSI en la Autoridad Portuaria de Manta, se pudo notar cambios significantes en relación a la seguridad de la información, gracias al apoyo de la máxima

autoridad y al comité de seguridad de la información, se dio inicio a un sin número de tareas las cuales debieron ser acatadas por parte de los funcionarios y jefes de área.

Al inicio el oficial de seguridad de la información debió clasificar los controles y directrices por área para solicitar a cada jefe el apoyo para el respectivo cumplimiento, teniendo como resultados hasta el transcurso de esta investigación los siguientes avances:

- **Difusión de la política de seguridad de la información:** En la actualidad la Autoridad Portuaria de Manta, tiene como procedimiento el difundir, socializar y capacitar a todo el personal de la institución sobre el Esquema Gubernamental de Seguridad de la Información dos (2) veces por año.

Número de difusiones de la Política de Seguridad de la Información (EGSI)	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
0	3

Tabla 43: Comparación de capacitaciones seguridad de la información antes y después del EGSI.

- **Acuerdos de Confidencialidad:** En la actualidad la Autoridad Portuaria de Manta, tiene en el procedimiento de vinculación de personal, que todo funcionario que ingresa a laborar a la institución firme el acuerdo de confidencialidad. También se les exige a los proveedores realizar la misma firma de acuerdo de confidencialidad al momento de que se los contrata para brindar un servicio a la institución.

Acuerdos de Confidencialidad Funcionarios	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
150	TODOS los funcionarios (208) a la fecha

Tabla 44: Comparación de acuerdos de confidencialidad de funcionarios antes y después del EGSI.

Acuerdos de Confidencialidad Proveedores	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
Ninguno	TODOS los proveedores

Tabla 45: Comparación de acuerdos de confidencialidad de proveedores antes y después del EGSI.

- **Inventario de Activos Tecnológicos:** La Autoridad Portuaria de Manta, en especial la Dirección de TIC, realiza de manera trimestral su inventario de activos tecnológicos, procedimiento que no se lo realizaba de manera continua, sino cuando alguien de la institución lo solicitaba. Con las nuevas herramientas adquiridas, facilitan la generación de los activos tecnológicos.

Inventario de Activos Tecnológicos	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
Rara vez se realizaba el inventario	4 veces hasta la fecha

Tabla 46: Comparación de elaboración de inventarios tecnológicos antes y después del EGSI.

- **Reglamentar el uso del correo electrónico:** En especial en las cuentas de correo, se estandarizó el formato de las cuentas de correo y se eliminó la creación de cuentas genéricas, lo que no permitía saber qué persona manejaba esa cuenta. Anteriormente la Autoridad Portuaria de Manta, en puestos rotativos se creaban cuentas genéricas, o a personal se les creaban cuentas de correo en función del puesto o cargo que se le asignaba.

Cuentas de correo electrónico genéricas	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
34	2 Solo la del Gerente y el Director de Operaciones

Tabla 47: Comparación de cuentas de correo electrónico genéricas antes y después del EGSI.

- **Reglamentar el uso del internet:** En la actualidad, la Autoridad Portuaria de Manta cuenta con políticas de navegación de acuerdo a las tareas del funcionario, impuestas por el Jefe de Área, antes no existía dicho control.

Políticas de navegación de internet para funcionarios y visitantes	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
0	5 Políticas para funcionarios y 1 para Visitantes

Tabla 48: Comparación de políticas de navegación de internet antes y después del EGSI.

- **Controles contra código malicioso:** la Autoridad Portuaria de Manta, antes y ahora cuenta con antivirus y firewall perimetral, lo cual ha significado que los virus no han sido un gran problema en la institución, pero con la implementación del EGSI y la capacitación sobre las políticas de seguridad de la información, ha permitido reducir en su gran mayoría los equipos infectados con virus o troyanos. De acuerdo a lo indicado por la Dirección de TIC, se revisó en los registros manuales de incidentes y se pudo observar la cantidad de infecciones en PCs atendidas por los técnicos, comparando con los reportes de incidentes de los funcionarios en la actualidad. Otro punto clave es la prohibición a los funcionarios de la instalación de software sin licencias, permitiendo con esto evitar que instalen software infectados y dando cumplimiento a normas de Contraloría.

Virus infecciones de equipos	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
89 Incidentes reportados de virus desde el 2012 hasta el inicio del EGSI.	4 incidentes reportados después de la implementación del EGSI.

Tabla 49: Comparación de cantidad de máquinas infectadas por virus antes y después del EGSI.

Software sin licencias instalados en PCs	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
175 programas instalados sin licencia en PCs antes del EGSI.	0 programas instalados sin licencia.

Tabla 50: Comparación de programas sin licencia instalados antes y después del EGSI.

- **Política de puesto de trabajo despejado y pantalla limpia:** Anteriormente la institución no tenía una política, donde exigía a los funcionarios a tener los escritorios de las PCs sin muchos iconos, a ser más ordenados, el no dejar los documentos impresos en la bandeja de la impresora, no dejar los *memory flash* en los equipos, siendo estos puntos críticos para la fuga de la información.
- **Separación y enrutamiento de las redes:** La Autoridad Portuaria de Manta actualmente tiene configurado segmentos de red VLAN para separar los PCs de los servidores e impresoras, scanner, otros. Anteriormente se los tenía en un solo segmento de red, pero por los problemas de IP, crearon otro segmento de red, creciendo de manera desordenada.

VLANs en la red de la Autoridad Portuaria de Manta	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
2 VLANs tenían todos los equipos tecnológicos.	6 VLANs: 1 para servidores 1 para equipos de red 1 para PCs 1 para impresoras, scanner 1 para Telefonía IP 1 para equipos del CCTV

Tabla 51: Comparación de VLANs implementadas en la red antes y después del EGSI.

- **Sistema de Gestión de Contraseñas:** La Autoridad Portuaria de Manta desde la implementación de *Active Directory*, cuenta con políticas de control para el manejo de las contraseñas, pero existían usuarios los cuales no cambiaban sus contraseñas, tal como lo pide el EGSI y como estaba implementado.

Usuarios que no realizaban cambio de contraseña	
Antes de la implementación del EGSI	Después de la Implementación del EGSI
32 usuarios	0 usuarios

Tabla 52: Comparación de cuentas de usuario sin política de cambio de contraseña antes y después del EGSI.

- **Cuentas de usuario para acceso a los sistemas:** Anteriormente no se les creaba a todos los funcionarios las cuentas de usuario, ingresaban con cuentas genéricas. En la actualidad personal que trabaja en un computador inmediatamente al momento de ingresar se le crea una cuenta de usuario.
- **Reporte sobre los incidentes:** Anteriormente en la institución los funcionarios reportaban vía telefónica, vía escrita por memo o de manera personal sus incidentes tecnológicos. En la actualidad con la implementación del EGSI se adquirió una herramienta para el reporte de incidentes tecnológicos y los de seguridad de la información.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- El EGSI, propuesto por el Gobierno para implementar controles en la seguridad de la información ha sido de mucha ayuda para la Autoridad Portuaria de Manta, ya que no era un tema en la agenda de los responsables de la seguridad ni de tecnología, ahora con este esquema existen controles que dan cobertura a todas las áreas de la institución.
- La implementación de dicho Esquema Gubernamental, demanda de mucho esfuerzo en especial en instituciones públicas como la Autoridad Portuaria de Manta, por toda la carga y responsabilidad de trabajo que es llevada por una sola persona, como lo es el Oficial de Seguridad de la Información.
- La implementación y ejecución del Esquema Gubernamental, no depende de una sola persona sino del apoyo de todos los funcionarios, en especial de los altos directivos de la institución, ya que de nada servirá la contratación de las últimas herramientas tecnológicas, ni la creación de políticas y procedimientos, sino van a ser cumplidos y utilizados por los funcionarios de la institución.
- El Esquema Gubernamental de Seguridad de la Información, por estar basado en la Norma ISO 27002, de donde se obtuvieron los controles, podemos indicar que es aplicable a todas las empresas públicas que deben de implementar, ya que en su gran mayoría se basa en funciones primordiales, básicas para la seguridad de la información.
- Hay que tener muy en cuenta que la implementación del EGSI en la Autoridad Portuaria de Manta no significa que dicha institución, esté preparada para certificar en la Norma ISO 27002, de la cual está basado el Esquema Gubernamental, pero sí tiene avances significativos para aspirar a una certificación a corto plazo de sus procesos.

- Y se puede dejar en claro que el problema de seguridad de la información, no se resuelve de un día para otro, sino que se requiere de un trabajo continuo, enfocados en los controles que se detallan en el EGSI y de otras Normas de Seguridad de la Información.

RECOMENDACIONES:

- Por parte de los altos directivos de la Autoridad de Manta, se necesita de su apoyo para que se dé cumplimiento con los controles que se han implementado en la institución.
- Los funcionarios y terceros deberán de cumplir con los controles implementados, políticas y procedimientos, relacionados con la seguridad de la información.
- La SNAP y la Subsecretaría de Gobierno Electrónico, debería buscar un mecanismo para integrarse y analizar los problemas que se presentan a los Oficiales de Seguridad de la Información al momento de la implementación del Esquema Gubernamental, generar mayor apoyo, colaborar con técnicas y/o herramientas que sean de ayuda para el responsable, ya que si los altos directivos de la institución, notan que el Oficial de Seguridad de la Información, tiene el apoyo de parte de la SNAP, por ende generará un compromiso de apoyo.
- La seguridad informática, tiene un precio muy alto, la protección de los datos de la empresa, minimizar los riesgos, por lo que la Autoridad Portuaria de Manta, debe direccionar más recursos económicos para la seguridad de la información, lo que en la actualidad no ocurre.

GLOSARIO DE TÉRMINOS

Activo: En esta investigación se hace referencia a la información y demás componentes que sean de valor para la institución.

Amenaza: En lo relacionado a tecnología es un evento interno o externo que puede generar inconvenientes a los sistemas informáticos.

Ataque: Considerado como un evento que atenta al performance de un sistema informático.

Auditoría: Es el proceso de examinar sistemas o actividades para validar la integridad de la información.

Hacker: Persona con un alto conocimiento que intenta vulnerar las seguridades informáticas para lograr un objetivo específico, como puede ser el de robar información, paralizar algún servicio, infectar equipos, etc.

IEC: Comisión Electrotécnica Internacional o en inglés International Electrotechnical Commission.

ISO: Organización Internacional de Estandarización o en inglés International Organization for Standardization.

Políticas: Son un conjunto de reglas o controles que va dirigido a los usuarios de una institución para su respectivo cumplimiento.

Riesgo: Considerado como la probabilidad de una amenaza.

Seguridad de la Información: Son un grupo de directrices enfocado en la protección de la información.

SPAM: Correos maliciosos enviados de forma masiva mediante el internet.

Usuario: Sujeto de la institución o externo que acceden a datos o recursos informáticos en esta investigación.

Virus: Es el más conocido del grupo de los ataques informáticos, el cual incluye un código malicioso y se copia dentro de los programas para reducir el performance del equipo informático.

BIBLIOGRAFÍA

Academia Marítima de Seguridad Integral ASI LTDA. (agosto de 2014). Plan de Protección de la Instalación Portuaria. Recuperado de http:/www.cursospbip.com/Cursos/images/PDFs/Articulos/LISTA_CHEQUEO_CODIGO_PPIP_5.pdf

Asociación Latinoamericana de Integración. (2014). PBIP. Recuperado de http://www.aladi.org/nsfaladi/estudios.nsf/decd25d818b0d76c032567da0062fec1/c2742fc7a6a0313203256ea200600a79/$FILE/167.pdf

Autoridad Portuaria de Esmeraldas. (19 de enero de 2015). Quiénes Somos. Recuperado de http://www.puertoesmeraldas.gob.ec/index.php/inicio/quienes-somos

Autoridad Portuaria de Guayaquil. (19 de enero de 2015). Institucional. Recuperado de El Puerto: http://www.apg.gob.ec/institucional/acerca

Autoridad Portuaria de Manta. (19 de enero de 2015). Antecedentes. Recuperado de http://www.puertodemanta.gob.ec/quienes-somos/antecedentes

Autoridad Portuaria de Puerto Bolívar. (19 de enero de 2015). Información Corporativa. Recuperado de http://www.puertobolivar.gob.ec/index.php/resena/informacion-corporativa

Autoridad Portuaria de Puerto Bolívar. (19 de Enero de 2015). Reseña Histórica. Recuperado de http://www.puertobolivar.gob.ec/index.php/resena/resena-historica

Autoridad Portuaria Nacional de Perú. (2014). Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP/ISPS). Recuperado de http://www.apn.gob.pe/c/document_library/get_file?p_l_id=24204&folderId=24750&name=DLFE-1501.pdf

BASC. (agosto de 2014). Norma y Estándares BASC. Recuperado de http://wbasco.org/espanol/documentos/viejos/resumen-norma-estandares.pdf

BASC Guayaquil. (2014). Empresas Certificadas. Recuperado de http://basc-guayaquil.org/empresas-certificadas/?search=name

BASC Pichincha. (2014). Empresas certificadas. Recuperado de http://www.basc-pichincha.org/index.php?option=com_content&view=article&id=59&Itemid=128

Business Alliance for Secure Commerce. (2014). Quienes somos. Recuperado de http://www.wbasco.org/espanol/quienessomos.htm

CENTRO DE ARTIGOS. (2014). Seguridad de la información, Historia, Principios básicos, La gestión del riesgo, Proceso, Continuidad del negocio, Leyes y reglamentos, Fuentes de las normas, Conclusión. Recuperado de http://centrodeartigo.com/articulos-enciclopedicos/article_80922.html

Deloitte. (2014). Acuerdo No. 166. Recuperado de www.deloitte.com/assets/Dcom.../Acuerdo_166%2023-sep-2013.pdf

Derecho Ecuador. (29 de Agosto de 2014). Registro Oficial No 88 - miércoles 25 de septiembre de 2013 Segundo Suplemento. Recuperado de

http://www.derechoecuador.com/productos/producto/catalogo/registros-oficiales/2013/septiembre/code/RegistroOficialNo88-Miercoles25deSeptiembrede2013S/registro-oficial-no-88---miercoles-25-de-septiembre-de--2013-segundo-suplemento

Empresa Nacional de Puertos S.A. (agosto de 2014). Código Internacional para la Protección Marítima de los Buques y de Instalaciones Portuarias (P.B.I.P.). Recuperado de http://enapu.com.pe/spn/pdf/pbip.pdf

Instituto Nacional de Estadísticas Informáticas. (marzo de 2000). Concepto sobre seguridad de la información. Recuperado de http://www.softeam.com.ar/utn/Documentos%20Seguridad/conceptos_seguridad_de_informacion.pdf

Instituto Uruguayo de Normas Técnicas. (2014). UNIT-ISO / IEC 27000. Recuperado de http://www.unit.org.uy/iso27000/iso27000.php

INTECO - Instituto Nacional de Tecnologías de la Comunicación. (2014). Conceptos de Seguridad. Recuperado de http://www.inteco.es/Formacion/Conceptos_de_seguridad/

INTECO - Instituto Nacional de Tecnologías de la Comunicación. (2014). Normativas. Recuperado de http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI/

ISO 27000. (16 de Enero de 2011). ISO/IEC 27002:2005 Dominios (11), Objetivos de control (39) y Controles (133). Recuperado de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

ISO 27000.ES. (agosto de 2014). ISO 27000. Recuperado de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27000. Es el portal de ISO 27001 en español. (2012). DESTACADOS ISO 27000. Recuperado de http://www.iso27000.es/iso27000.html

ISO 9001 Calidad para todos. (5 de Agosto de 2012). Origen y Fundación de la ISO. Recuperado de http://iso9001calidadparatodos.com/origen-y-fundacion-de-la-iso.html

Logisman. (23 de Agosto de 2011). Familia ISO 27000: Seguridad de la información. Recuperado de http://custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

Noticias Jurídicas. (2014). Base de datos de legislación. Recuperado de Código internacional para la protección de los buques en instalaciones portuarias (Código PBIP): http://noticias.juridicas.com/base_datos/Admin/cod121202-aec.html

Organización ISO. (2014). THE ISO STORY. Recuperado de http://www.iso.org/iso/home/about/the_iso_story.htm

Prefectura Naval Argentina. (17 de Diciembre de 2002). Examen y adopción del Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP). Recuperado de Organización Marítima Internacional: http://www.prefecturanaval.gov.ar/web/es/doc/cod_pbip.pdf

Secretaria Nacional de Administración Pública. (2014). Normativa y Base Legal. Recuperado de Documentación: http://www1.gobiernoelectronico.gob.ec/index.php/normativa-legal

Secretaría Nacional de Planificación y Desarrollo. (25 de Septiembre de 2013). Esquema Gubernamental de Seguridad de la Información EGSI. Recuperado de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf

Universidad Nacional Autónoma de México. (2014). Fundamentos de Seguridad Informática. Recuperado de Estándares ISO 17799: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ISO17.php

Universidad Nacional del Noreste. (2004). Seguridad marítima y portuaria: nuevas reglas en el mundo. Recuperado de http://www.unne.edu.ar/unnevieja/Web/cyt/com2004/1-Sociales/S-040.pdf

Universidad Tecnológica Región Norte de Guerrero. (10 de noviembre de 2010). NORMA ISO 27000. Recuperado de Seguridad de la Información: http://www.slideshare.net/nestorjgp/norma-27000

World BASC Organization. (18 de enero de 2015). Quienes Somos. Recuperado de http://www.wbasco.org/espanol/quienessomos.htm

Datos de autores

Carlos Ernesto Manosalvas García (Guayaquil, Ecuador, 1981). Magíster en Administración de empresas con mención en Telecomunicaciones. Especialista en tecnología Microsoft con más de 15 años de experiencia, en la implementación de sistemas informáticos relacionado a servidores de colaboración, mensajería, comunicaciones unificadas, entre otros. Certificado como Auditor interno ISO 27001-2015, enfocado en la seguridad de la información. Jefe de Infraestructura Sistemas del GADMC-Guayaquil, Oficial de Seguridad de la Información en Autoridad Portuaria de Manta, Docente de la Facultad de Ciencias Informáticas de la ULEAM y actualmente Director de Tecnología de la Información y Comunicación del GADMC-Manta. cmanosalvas@outlook.com

Jéssica Fernanda Ostaiza Macías (Manta, Ecuador, 1987). Magíster en Administración de empresas con mención en Negocios Internacionales. Auditora BASC internacional, en temas de puertos marítimos, exportaciones y seguridad por la alianza empresarial internacional para un comercio seguro. Directora de Seguridad Integral en la Autoridad Portuaria de Manta, Jefa de Comercio Exterior en empresas exportadoras de pescado y actualmente docente de la Facultad de Ciencias de la Comunicaciones de la ULEAM. Jessicaostaiza172@hotmail.com

Danny Galindo Aguaiza Tenelema. (Portoviejo, Ecuador, 1980). Máster en Redes de Comunicaciones. Ingeniero en Sistemas. Especialista en: Infraestructura tecnológica, servidores y sistemas informáticos. Experto en Uso de Tecnologías de información y comunicación. Consultor y experto en Excel Financiero y Contable. Docente de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) facultades de Contabilidad y Auditoría y Enfermería. dannyaguaiza@hotmail.com

Ulises Alexander Carofilis Moreira. (Manta-Ecuador) Máster en Redes de Comunicaciones, Ingeniero en Sistemas, 10 años de experiencia en el manejo, instalación y desarrollo de sistemas de Votación electrónica en parlamentos legislativos, conocedor e investigador de nuevas técnicas de migración y estudios de protocolos de red basadas al uso de sistemas informáticos e Internet de las cosas, consultor&asesor en el área de sistemas y aplicaciones de Software libre, tanto en herramientas de licenciamiento gratuito en servidores y terminales. Parte del equipo de Desarrolladores de aplicaciones informáticas de la Asamblea Constituyente y Asamblea Nacional del Ecuador que implemento el primer sistema de votación electrónica para estas instituciones. ucarofilis@gmail.com

ISBN: 978-9942-775-01-6
9789942775016