FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE LAS BUENAS PRÁCTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27001 PARA LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL.

AUTOR

GUSTAVO XAVIER LEMAPAZMIÑO

AÑO

2017

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE LAS BUENAS PRÁCTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27001 PARA LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL.

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía
Mgs. William Eduardo Villegas Chiliquinga

Autor
Gustavo Xavier Lema Pazmiño

Año
2017

DECLARACIÓN PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación de la UDLA”

_____

William Eduardo Villegas Chiliquinga

Magister en Redes de Comunicaciones

C.I.: 1715338263

DECLARACIÓN PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Milton Nepalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

C.I.: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Gustavo Xavier Lema Pazmiño

C.I.: 1717622292

AGRADECIMIENTO

Este trabajo de titulación agradezco a mi madre Olga Pazmiño por todo el apoyo incondicional, a mi hija por darme las fuerzas para seguir adelante, a mis amigos casi hermanos Danny Morales, Roberto Espinosa, Wilmer López agracias por las palabras de aliento y poder seguir adelante. Por ultimo a mis compañeros de Trabajo de la DGAC por permitir formarle como profesional.

DEDICATORIA

La elaboración de este proyecto de titulación va dedicada con mucho amor y con todo mi esfuerzo, especialmente a Mi Madre Olga Pazmiño quien es la guía en mi camino, Mi Padre Ángel Lema, Mi Hija Sarahi Lema, Mi Novia Saira Chicaiza, mis Hermanos Irina, Stephanie, Ricardo, a Mis segundas Madres Sra. Gloria Ordoñez, Sra. María Ordoñez los cuales fueron los pilares fundamentales para llegar a subir un escalón más profesionalmente.

RESUMEN

La presente tesis describe una investigación referente a un mejoramiento de los procesos de seguridad, políticas y mejoras del área técnica de la Dirección de Aviación Civil del Ecuador (DGAC), por ello se ha generado una evaluación y análisis de la información obtenida, para verificar la vulnerabilidad existente en la red de datos, así como también evidencia la falla en los procesos que se generan en dicha institución.

Por lo dicho anteriormente en la presente tesis se describe el organigrama de la DGAC, actividades por departamentos, servicios que brinda la institución y procesos que se generan en la actualidad, para de ahí generar un análisis exhaustivo de las vulnerabilidades que tiene la infraestructura de red, así como también sus equipos y los procesos administrativo

Cabe recalcar que se tomó en cuenta los procesos de seguridad de la información y normas ISO sobre gestión de seguridad de la información, así como también el Sistema de Gestión de Seguridad de la Información (SGSI), la ISO (International Standards Organization), Estándares ISO y la situación actual de la Dirección de Aviación Civil del Ecuador.

ABSTRACT

This thesis describes an investigation related to an improvement of the security processes, policies and improvements of the Civil Aviation Directorate (DGAC) technical area, for which an evaluation and analysis of the obtained information has been generated, to verify the Vulnerability in the data network, as well as evidence of the failure in the processes that are generated in that institution.

As stated earlier in this thesis describes the organization chart of the DGAC, activities by departments, services provided by the institution and processes that are currently generated, to generate a comprehensive analysis of the vulnerabilities of the network infrastructure, As well as their equipment and administrative processes

It should be noted that information security processes and ISO standards on information security management, as well as the Information Security Management System (ISMS), ISO (International Standards Organization), Standards ISO and the current situation of the Civil Aviation Directorate of Ecuador.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. CAPÍTULO I MARCO TEÓRICO DE LA SEGURIDAD DE LA INFORMACIÓN Y NORMAS ISO SOBRE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.1 Seguridad de la información

La seguridad informática permite salvaguardar la información de una empresa, así mismo enumerar algunos aspectos de la seguridad los que van a permitir controlar accesos, servicios dentro de un sistema informático.

Existen diferentes tipos de amenazas, las cuales son causadas por software maliciosos, virus, troyanos, así como también amenazas por fenómenos físicos y naturales; estas pueden ser visibles para los denominados hackers al momento de no tener niveles de seguridad.

Dentro de un sistema informático se tiene algunos elementos como son la información, el personal y los recursos. Aquí se puede encontrar diferentes normas y principios las que van a permitir seguir lineamientos, reglas y al mismo tiempo poder realizar políticas de seguridad y que la información no sea violada.

1.2 Seguridad informática (SI)

Se puede definir a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Álvaro, 2007).

Es la que se encarga de proteger la información y la infraestructura de los equipos informáticos, por lo que solo pueden acceder personas autorizadas, permitiendo el ingreso a la información con sus respectivos permisos, por lo

cual es importante la disciplina para la seguridad informática que se encarga de crear métodos, normas, y procesos para que un sistema informático sea seguro y confiable es la seguridad informática (Aguilera, 2010).

La SI se define como un conjunto de procedimientos y herramientas que se encargan de la integridad y privacidad de la información y evitar las amenazas, mientras que López. (2010) define como “la disciplina que se encarga de diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema de información seguro y confiable” (Cervigón, 2011).

Según (Areitio, 2008 pág. 2) “La seguridad informática es, una disciplina que continua en constante evolución y su meta final es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativo de las TIC de la organización, a sus socios comerciales, clientes, administración pública, suministradores, etc.”

Por lo expuesto se especifica que la Seguridad Informática son procesos y normas que permiten la seguridad de los sistemas de procesamiento de datos y el almacenamiento de la información, para garantizar la integridad, confidencialidad y disponibilidad de la información.

1.3 Aspectos de la seguridad

1.3.1 Confidencialidad

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Quiroz, M. (2013).

1.3.2 Autenticación

Garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. Quiroz, M. (2013).

1.3.3 Integridad

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. Quiroz, M. (2013).

1.3.4 No desechar

El objeto de este servicio de seguridad consiste en implementar un mecanismo probatorio, que permita demostrar la autoría y envió de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envió. Quiroz, M. (2013).

1.3.5 Disponibilidad

En un sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento. Quiroz, M. (2013).

1.3.6 Autorización

Mediante el servicio de autorización se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático,

una vez superado el proceso de autenticación de cada usuario. Quiroz, M. (2013).

1.3.7 Contabilidad

El servicio de contabilidad o trazabilidad permite registrar monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados. Quiroz, M. (2013).

1.3.8 Reclamación de origen

Mediante la reclamación de origen el sistema de seguridad de información, permite probar quien fue el creador de un mensaje, para verificar la fuente del documento. Quiroz, M. (2013).

1.3.9 Reclamación de propiedad

Este servicio permite probar que un determinado documento o un contenido digital protegido por derechos de autos pertenecen a un determinado usuario y organización que ostenta la titularidad de los derechos de autor. Quiroz, M. (2013).

1.3.10 Anonimato en el uso de los servicios

En la utilización de determinados servicios dentro de las redes y sistemas informáticos también podría resultar conveniente garantizar el anonimato de los usuarios que acceden a los recursos y consumen determinados tipos de servicios preservando de este modo su privacidad. Quiroz, M. (2013).

1.3.11 Protección a la réplica

Mediante este servicio de seguridad se trata de impedir la realización de ataques de repetición por parte de usuarios maliciosos consistentes en la

interceptación y posterior reenvió de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas. Quiroz, M. (2013).

1.4 Elementos de la seguridad

Se tiene 3 elementos principales a proteger en cualquier sistema informático.

1.4.1 Hardware

Se considera por un grupo que forma todos los elementos físicos de un sistema informático como la CPU, medios de almacenamiento primerio y segundario, cableado, tarjetas las cuales conforman elementos mecánicos-electrónicos. Las partes fundamentales como ratón, teclados, microprocesadores, monitores, impresoras, unidades de disco, escáner estos periféricos se consideran como hardware.

1.4.2 Software

Es la agrupación de programas digitales que son el motor del sistema operativo, las aplicaciones, por esta razón se podría detallar que los programas digitales son una serie de órdenes digitales (1) o (0) que los usuarios dan una orden para que el computador ejecute algún evento informático.

1.4.3 Gestión de Seguridad

En el proceso de gestión de la seguridad de información hay una serie de elementos involucrados que son:

- Identificación de todos los activos
- Identificación de las amenazas de los activos
- Identificación de vulnerabilidades
- Identificación de impactos
- Identificación de riesgos
- Aplicación de salvaguardas
- Limitaciones

1.4.3.1 Identificación de todos los activos

Los activos son aquellos elementos relacionados con el entorno como son el personal, los edificios, las instalaciones, los equipos o suministros relacionados con el sistema de las TIC's, como equipos de hardware o software, los relacionados con las funcionalidades de la organización como la capacidad de proporcionar un servicio, crear un producto. (Acosta, 2010)

1.4.3.2 Identificación de las amenazas de los activos

Una amenaza puede causar un incidente fatal, que provocaría daños y pérdidas a las empresas u organizaciones.
Las perdidas pueden ser de ataques directos o indirectos a la base principal de la información. Los ataques se presentan en forma de destrucción, modificación y revelación. (Bahamontes, 2013).

1.4.3.3 Identificación de vulnerabilidades

Una vulnerabilidad puede entenderse como la potencialidad o posibilidad de ocurrencia de materialización de una amenaza sobre un equipo. Las vulnerabilidades asociadas a los activos, influyen las debilidades en el nivel físico de la organización, los procedimientos, el personal, la administración, equipos de hardware, software y toda la información. (Acosta, 2010)

1.4.3.4 Identificación de impactos

El impacto es la consecuencia de la materialización de una amenaza sobre un activo, como la destrucción de ciertos activos, el peligro de la integridad del sistema de información, la perdida de autenticidad, confidencialidad o de disponibilidad.

Las posibles consecuencias indirectas de los impactos, incluyen pérdidas económicas, pérdida de cuota; la cual afectaría por completo a la empresa.

La estimación del impacto permite establecer una proporcionalidad entre las consecuencias de la agresión y el coste de las salvaguardas necesarias. Se debe tener en cuenta también la posible frecuencia de materialización de las amenazas. (Ramos & Hurtado, 2011)

1.4.3.5 Identificación de riesgos

El riego es la posibilidad de que se presente un cierto impacto en toda la organización. Este impacto se puede producir debido a una amenaza explote vulnerabilidades para causar pérdidas o daños.

1.4.3.6 Aplicación de salvaguardas

Las salvaguardas también denominadas como medidas, son procedimientos físicos o lógicos que protegen una amenaza, reducir la vulnerabilidad, limitar el impacto de incidentes no deseados.

Las salvaguardas pueden realizar varias funciones: detección, prevención, limitación, corrección, recuperación, seguimiento. Normalmente resulta beneficioso utilizar salvaguardas que puedan satisfacer múltiples funciones. (Aguilera López, 2010).

1.4.3.7 Limitaciones

Las limitaciones son establecidas y reconocidas por la dirección de la organización y dependen del entorno en el que funcionan. Pueden ser organizativas, financieras, ambientales de personal, de tiempo, legales y técnicas.

Todos estos factores deben considerarse cuando se seleccionan e implantan las salvaguardas. Periódicamente se deben revisar las nuevas limitaciones y las ya existentes e identificar posibles cambios. (Meyer, 2014).

1.5 Datos

Es un conjunto de información que manejan el software y hardware del computador, mismos que permiten formar paquetes que circulan a través de un cable de red, así como también por entradas de una base de datos. (Suárez, R. C. 2007).

1.5.1 Principios de la protección de datos

El marco normativo de la LOPD (Legislación nacional, comunitaria y autonómica), establece una serie de principios relativos al tratamiento y protección de los datos de carácter personal.

1.5.2 Calidad de los datos

Los datos personales que vaya a ser tratado por una determinada empresa o institución deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.
Los datos de carácter personal serán conservados durante los plazos previstos en las disposiciones aplicables o en su caso en las relaciones contractuales entra la empresa y el interesado.

1.5.3 Seguridad de los datos

La LOPD establece en su artículo 9 que el responsable del fichero y en su caso el encargado del tratamiento deberá adoptar las medidas necesarias de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y que puedan evitar su alteración, perdida, tratamiento o acceso no autorizado.

1.5.4 Confidencialidad

Las personas y empresas que intervengan en cualquier fase del tratamiento de datos de carácter personal deben comprometerse a guardar el debido secreto

profesional respecto de los mismo incluso después de haber finalizado la reacción que les unía con la entidad poseedora de los datos personales.

1.5.5 Información en la recolección de datos

El responsable del fichero debe informar a los interesados antes de proceder al tratamiento de sus datos de carácter personal indicando el fichero en que se van a incorporar sus datos. La finalidad del tratamiento y los posibles destinatarios de estos datos.

1.5.6 Comunicación o cesión de datos a terceros

La comunicación o cesión de datos de carácter personal solo es posible si existe un consentimiento previo del afectado. Tras haber sido informado sobre la finalidad de la comunicación o las actividades del cesionario siempre y cuando además la cesión sea necesaria para el cumplimiento de fines directamente relacionados con funciones legitimas del cedente y cesionario.

1.5.7 Datos especialmente protegidos

Se considera datos especialmente protegidos aquellos datos de carácter personal referentes a la ideología, salud, vida sexual, origen racial religión o creencias. Para estos datos la LOPD contemple un nivel mayor de protección.

1.5.8 Aspectos de la seguridad

Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.

Control en el acceso de utilización de ficheros protegidos por la ley contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etc.

Identificación de los autores de la información o de los mensajes Registro del uso de los servicios de un sistema informático etc.

1.6 Amenazas

1.6.1 Amenazas software

Los equipos informáticos infectados con diferentes tipos de virus, por lo que las computadoras quedan desprotegidas lo cual permite vulnerar las seguridades.
En este tipo de amenazas se tiene: software malintencionado, virus, espías, troyanos, gusanos, phishing, spamming, ataques DOS.

1.6.2 Amenazas físicas

Son aquellas que se producen en el sistema informático presentando daños ya sean por causas físicas o fenómenos naturales entre los más comunes son: robos, incendios, desastres naturales.

1.6.3 Amenazas humanas

Se observa a nivel mundial que la información está susceptible para los piratas o más conocidos como hackers ya sea de manera remota o física.

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información son:

- Usuarios
- Programas maliciosos
- Errores de programación
- Intrusos
- Un siniestro
- Personal técnico interno
- Catástrofes naturales

Las amenazas que pesan sobre una empresa son de naturaleza y en constante evolución.
El dominio cubierto por la seguridad informática es muy amplio. Podríamos definirlo como la protección contra todos los daños sufridos o causados por las herramientas informáticas y organizadas por el acto voluntario y de mala fe de un individuo.

Proteger el sistema informativo de una empresa consiste en poner frenos contra cada una de las amenazas potenciales. Dado que ninguna protección es fiable, es necesario multiplicar barreas sucesivas. Así que si cualquier persona desea ingresar pasaría por la primera seguridad, pero actuarían las otras protecciones impidiendo su paso. Por otro lado, es necesario proteger todos los medios de acceso que tenga la empresa. (Aguilera, P., 2010).

1.6.4 Niveles de seguridad

Según, Borghello, Cristian. (2009), el estándar de niveles de seguridad más utilizado internacionalmente es el Trusted Computer Security Evaluation Criteria (TCSEC) Orange Book (2), desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos ITSEC/ITSEM (Information Technology Security) y luego internacionales ISO/IEC (International Electrotechnical Commission).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.” (Borghello, 2009).

Según Borghello. (2009), los niveles de seguridad han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

- **Nivel D**

Involucra los sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Son sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información.

- **Nivel C1: Protección Discrecional**

En este nivel se requiere identificación de usuarios, que permite el acceso a distinta información, cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

- **Nivel C2: Protección de Acceso Controlado**

Este nivel posee la capacidad de restringir que los usuarios ejecuten comandos o tengan acceso a ciertos archivos de importancia, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema, esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

- **Nivel B1: Seguridad Etiquetada**

Establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema

(usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

- **Nivel B2: Protección Estructurada**

En este nivel la Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

- **Nivel B3: Dominios de Seguridad**

Este nivel refuerza los dominios con la instalación de hardware: por ejemplo, el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

- **Nivel A: Protección Verificada**

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.7 Normas de la seguridad informática

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red organizacional.

- Ley Orgánica 15/99 de Protección de Datos de Carácter Personal.
- Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI**).**
- Ley 32/2003, general de telecomunicaciones.
- Ley 59/2003 de firma electrónica.
- R.D.L, 1/1996 Ley de Propiedad Intelectual.
- Ley 17/2001 de Propiedad Industrial.

1.7.1 Normas ISO sobre gestión de seguridad de la información

Las normas ISO/IEC 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)”, proporciona un maco de estandarización para la seguridad de la información comprende un conjunto de normas sobre las siguientes materias:

- Sistema de gestión de la seguridad de la información.
- Valoración de riegos.
- Controles

Esta norma contiene un conjunto de normas relacionadas con la seguridad de la información y su objetivo es que una empresa que las aplique pueda certificarse y son las siguientes:

- **ISO 27000:** Contiene una visión general de las normas de la serie y un conjunto de definiciones y términos que serán usados en la serie.

- **ISO 27001**: Esta norma sustituye a la lSO 17799-1, abarca un conjunto de normas relacionadas con la seguridad informática. Se basa en la norma SS 7799-2 de British Standard, otro organismo de normalización. Según esta norma, que es la principal de la serie, la seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento.

- **ISO 27002:** Corresponde con la ISO 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.

- **ISO 27003:** Esta norma contiene una guía para la implementación de la norma

- **ISO 27004:** Esta norma contiene los estándares en materia de seguridad para poder evaluar el sistema de gestión de la seguridad de la información.

- **ISO 27005:** Recoge el estándar para la gestión del riesgo de la seguridad.

- **ISO 27006:** Involucra requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO 27001

- **ISO 27015:** Contiene una guía para organizaciones del sector financiero y de seguros.

- **ISO 27032:** Abarca una guía sobre ciberseguridad.

- **ISO 27033** Es una norma dedicada a la seguridad en redes dividida en varias partes, entre ellas el diseño e implementación de seguridad en redes, asegurar las comunicaciones entre redes mediante gateways, asegurar las comunicaciones mediante VPN redes inalámbricas.

- **ISO 27034**: Normas sobre seguridad en aplicaciones informáticas.

- **ISO 27799:** Norma de aplicación en el sector hospitalario relativa a la seguridad da la información de los datos de los pacientes.

1.8 Políticas de seguridad.

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos. (Fernández, 2012).

Las políticas son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación. (De Pablos, 2012).

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos. (Fernández, 2012).

Podemos definir una política de Seguridad como una “Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para diversas actualizaciones técnicas y organizativas que se requieran” (RFCs 1244 y 2196).

Un Procedimiento de Seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización. (Veites, 2011).

En la siguiente figura No. 1, se representa la jerarquía de conceptos manejados al hablar de las Políticas, Planes y Procedimientos de Seguridad:

Figura 1. Políticas, Planes y Procedimientos de Seguridad.

Los Procedimientos de Seguridad permiten implementar las Políticas de Seguridad definidas, describiendo cuales son las actividades que se tienen que realizar en el sistema, en qué momento, o lugar quienes serían los responsables de su ejecución y cuáles serían los controles aplicables para supervisar su correcta ejecución.

En este sentido, las políticas definen que se debe proteger en el sistema, mientras que los procedimientos de seguridad describen como se debe conseguir dicha protección. En definitiva, si comparamos las Políticas de seguridad con las Leyes en un Estado de Derecho, los procedimientos serian el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes.

Otro grupo de procedimientos de seguridad estaría relacionado con la instalación, configuración y mantenimiento de distintos elementos de seguridad:

cortafuegos (firewalls) servidores proxy antivirus, Sistemas de Detención de Instrucciones (IDS). (Veites, 2011)

En la siguiente tabla No. 1, se presenta otro ejemplo de la relación entre una determinada directriz o Política de Seguridad, los Procedimientos que de ella se derivan y las tareas concretas que deberían realizar el personal de la organización.

Tabla 1.
Ejemplo de la relación entre una determinada directriz

Política	Procedimiento	Tareas a realizar
Protección del servidor Web de la organización contra acceso no autorizados.	Actualización del software del servidor Web. Revisión de los registros de actividad en el servidor	✓ Revisión diaria de los parches publicados por el fabricante. ✓ Seguimientos de las noticias sobre posibles fallos de seguridad. ✓ Revisión semanal de los “logs” del servidor para detectar situaciones anómalas ✓ Configuración de alertas de seguridad que permiten reaccionar de forma urgente entre determinados tipos de ataques o intentos de intrusión

Tomado de: (Veites, 2011)

Las políticas de seguridad en general son normas o reglas que deben cumplirse y enfocarse en abarcar al personal de una organización, para lo cual busca que se cumpla con las metas, objetivos y los procedimientos aceptables para un área determinada.

1.9 Normas de seguridad vigentes

Existen diferentes formas para proteger los derechos del autor el cual es el propietario de un software como para proteger los datos personales con respecto a su uso fraudulento en los ficheros y bases de datos informáticos, a continuación, la legislación específica.

1.9.1 Protección de los derechos de autor

Para la protección de los derechos de autor, se ha desarrollado la Ley de Propiedad Intelectual, aprobada por el Real Decreto Legislativo 1/1996. Esta ley protege los derechos de autor en general, tanto de los programas informáticos como los de cualquier otra obra de propiedad intelectual.
Los derechos de autor están protegidos en la citada ley, cuyo Libro Primero, Título VII lleva por título <<Programas de ordenador>>

1.9.2 Legislación sobre protección de datos

Para la protección de los datos que encontramos en nuestro ordenamiento jurídico hay diversas leyes, además de ciertas normas publicadas por distintas Comunidades Autónomas como son:

1.9.2.1 Ley orgánica de protección de Datos de Carácter Personal (LOPD)

Sirve para proteger los datos de carácter personal, se promulgo la ley orgánica el 15/12/1999, como Protección de Datos De Carácter Personal, tiene por objeto, como recoge su art.1 <<” garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar>>”

1.9.2.2 Reglamento de Medidas de Seguridad (RMS)

El real decreto 17/20/2007, de 21 de diciembre, aprueba dicho reglamento de desarrollo de la ley orgánica 15/12/1999, de protección de datos de carácter personal.

Este reglamento también desarrolla las disposiciones relativas al ejercicio de la potestad sancionadora a la ley española de Protección de Datos, en el Capítulo III del Título IX del reglamento.

1.9.2.3 Ley General de Telecomunicaciones

La ley 3/2/2003 en el capítulo III aborda el secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas, en especial referencia a los datos de carácter personal como indica en si art.34.

1.9.2.4 Legislación sobre los servicios de la Sociedad de la información y correo electrónico

Este conjunto de leyes ha sido necesario ir publicándolo a medida que se hacía cada vez más necesaria la protección de los usuarios y de la privacidad de los mismos, sobre todo por el auge del comercio electrónico, firma electrónica, los certificados digitales y el DNI electrónico.

1.9.2.5 Ley sobre el DNI electrónico.

El DNI (Documento Nacional de Identidad) se creó en España en marzo de 1944, a través de un decreto.

El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior.

El DNI ha sido el documento identificativo de cada ciudadano y obligatorio a partir de cierta edad.

Con el desarrollo de la sociedad de la información se hace necesaria una mayor medida de confianza en las comunicaciones telemáticas, como respuesta a esto se aprobaron la Ley sobre firma electrónica y el Real Decreto 15/3/2005, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

El objetivo de las anteriores normas es la creación de una serie de instrumentos apropiados que sean capaces de acreditar la identidad de la persona en una comunlcaci6n electrónica.

1.9.2.6 Otras normas a destacar serían:

- ISO 27015: que contiene una guía para organizaciones del sector financiero y de seguros.
- ISO 27032: es una guía sobre cyber seguridad.
- ISO 27033: es una norma dedicada a la seguridad en redes, dividida en varias partes, entre ellas diseño e implementación de seguridades en redes, asegurar las comunicaciones entre redes mediante Gateway, asegurar las comunicaciones mediante VPN, redes inalámbricas.
- ISO 27034: norma sobre seguridad en aplicaciones informáticas.
- ISO 27799: norma de aplicación en el sector sanitario relativo al a seguridad de la información de los datos de los pacientes.

1.10 Sistema de Gestión de Seguridad de la Información (SGSI)

1.10.1 ISO (International Standards Organization)

ISO es una organización independiente y tiene sus orígenes en el año de 1946 al reunirse delegados de 25 países en el instituto de ingenieros civiles en Londres, decididos a crear una organización internacional para facilitar la

coordinación y unificación de estándares industriales. Así en febrero de 1947 la organización ISO inicia sus operaciones de manera oficial. La oficina principal de ISO está ubicada en Ginebra, Suiza y hasta el momento ha publicado más de 2100 estándares internacionales relacionados con los campos de tecnología y manufactura.

Para ISO (International Organization for Standarization) un sistema de gestión queda definido por un proceso de 4 etapas, creado por Walter Andrew Shewhart (1891 – 1967) y popularizado por William Edwards Deming (1900 – 1993), Planificar (Plan), Implementar (Do), Medir (Check) y Mejorar (Act). (Rodrigo Baldecchi, 2014).

1.10.2 Estándares ISO

Los estándares establecidos por ISO están dirigidos a determinar elementos de compatibilidad entre productos, servicios y sistemas creados por diferentes entidades. Estos estándares cubren una amplia lista de industrias, como la agricultura, tecnología, salud, alimentos, etc.

Los estándares se definen por medio de la coordinación de diferentes grupos de expertos en área determinadas, los mismos que representan a las diferentes industrias interesadas en participar.

El estándar ISO-IEC 27001:2013 es la columna vertebral de un Sistema de Gestión de Seguridad (SGSI) de la Información, estableciendo procesos para proteger la confidencialidad, integridad y disponibilidad de la información de una organización y mejora continua del sistema de gestión. Esta información puede ser de carácter financiera, propiedad intelectual, información sensible de los empleados, o información compartida por terceros. Los procesos de SGSI fundamentadas en el estándar ISO-IEC 27001:2013 pueden ser adaptables a las necesidades de una organización independientemente de su tamaño. La información puede ser digital, impresa, videoconferencia, email, etc, la misma que es vulnerable a la amenazas externas e internas de una organización.

1.10.3 Sistema de Gestión de Seguridad de la Información SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) es una plataforma basada en los pilares establecidos en el estándar ISO/IEC 27001.

La seguridad de la información debe ser gestionada a través de un proceso sistemático, incluyendo gestión de riesgos, validación y documentación a nivel organizacional, direccionado a proteger información sensible. Garantizar el control total sobre la seguridad de la información es utópico inclusive en el escenario donde existen recursos ilimitados para implementar un SGSI; por ello el objetivo del SGSI es identificar y atenuar riesgos en el manejo de la información, así como generar procesos y procedimientos estructurados direccionados a mejorar la eficiencia y adaptabilidad de los mecanismos de control de la información incluyendo una fase de revisiones, retroalimentación y mejoras al SGSI.

Cuando se hace referencia a información, se considera todos los datos generados por una organización y que poseen un valor o elemento diferenciador para la misma, independientemente del medio por el cual se almacenan o transmiten. La seguridad de la información se logra mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos, organización, controles, hardware y software y, lo más importante, mediante comportamientos éticos de las personas. (Rodrigo Baldecchi, 2014)

De acuerdo al portal de ISO, las categorías de estándares de gestión de un sistema son los siguientes:

- Calidad
- Seguridad y protección
- Administración General
- Salud y medicina

- Medio Ambiente y Energía
- Industria
- Servicios
- Tecnología Información

A continuación, ilustramos por medio de la tabla No. 2, una lista de estándares por áreas de aplicación:

Tabla 2.
Estándares por áreas

Estándar	Título	Categoría
ISO 9001:2015	Sistemas de gestión de calidad – Requerimientos	Calidad
ISO/AWI 19443	Sistemas de gestión de calidad. Requerimientos específicos para la aplicación de ISO 9001 y IAEA GS-R por entidades dedicadas a la cadena de abastecimiento en el sector de energía nuclear.	Calidad
ISO/NP 21001	Sistemas de gestión por organizaciones educativas	Calidad
ISO 18788:2015	Sistema de gestión para operaciones de seguridad privada	Seguridad
ISO/CD 22000	Sistema de gestión de la calidad de alimentos; requerimientos para cualquier organización en la cadena de alimentos.	Seguridad
ISO 22301:2012	Seguridad societaria. Requerimientos para el sistema de gestión de continuidad de negocios.	Seguridad
ISO 22313:2012	Seguridad societaria. Guía para sistema de gestión de continuidad de	Seguridad

	negocios.	
ISO 24518:2015	Gestión de actividades relacionadas al agua potable y aguas servidas.	Seguridad
ISO/DIS 34001.3	Sistema de gestión de seguridad, Medidas de control antifraude.	Seguridad
ISO/WD 35001	Sistema de gestión de laboratorios con riesgos biológicos.	Seguridad
ISO 39001:2012	Sistema de gestión de seguridad del tráfico en carreteras.	Seguridad
ISO/DIS 45001	Sistema de gestión de salud ocupacional	Seguridad
ISO/DIS 11000	Gestión de relación laboral colaborativa	Gestión General
ISO 19600:2014	Guía para sistema de gestión de concordancia	Gestión General
ISO 30301:2011	Sistema de gestión de información y documentación	Gestión General
ISO/DIS 37001	Sistema de gestión anticorrupción.	Gestión General
ISO/DIS 37101	Sistema de gestión de comunidades con desarrollo sostenible.	Gestión General
ISO/AWI 41001	Sistema de gestión de manejo de instalaciones.	Gestión General
ISO/AWI 50501	Sistema de gestión de políticas de innovación.	Gestión General
ISO 55001:2014	Sistema de gestión de activos	Gestión General
ISO 55002:2014	Gestión de activos basado en la aplicación de ISO 55001	Gestión General
ISO 14001:2015	Sistema de gestión del medioambiente, guía de uso.	Energía y Medio

		Ambiente
ISO 14004:2016	Sistema de gestión del medioambiente, guía de implementación.	Energía y Medio Ambiente
ISO/AWI 19443	Sistema de gestión de calidad, requerimientos específicos para la aplicación de ISO 9001 y IAEA GS-R por organizaciones dedicadas a la energía nuclear.	Energía y Medio Ambiente
ISO 14298:2013	Gestión de tecnología gráfica, y procesos de imprenta.	Industria
ISO/AWI 41001	Gestión de instalaciones, guía de uso.	Industria
ISO 20121:2012	Sistema de gestión de sostenibilidad de eventos.	Servicios
ISO 21101:2014	Turismo de aventura, Sistema de gestión de seguridad.	Servicios
ISO 24518:2015	Actividades relacionadas al agua potable y proceso de manejo de aguas servidas.	Servicios
ISO/WD 24526	Sistema de gestión de eficiencia del agua.	Servicios
ISO/IEC 27001:2013	Tecnologías de la Información. Técnicas de seguridad, Sistema de Gestión de Seguridad de la Información.	Tecnologías de la Información
ISO/IEC 27010:2015	Tecnología de la Información, Sistema de Seguridad de la Información de comunicaciones para sector interno e inter-organizacional	Tecnologías de la Información

Tomado de: (ISO ORG, 2016)

La tabla No. 3, ilustra los estándares definidos por ISO, que aplican al campo de seguridad de la información.

Tabla 3.
Estándares definidos por ISO

Estándar	Título
ISO/IEC 27001:2013	Tecnologías de la Información. Técnicas de seguridad, Sistema de Gestión de Seguridad de la Información.
ISO/IEC DIS 27003	Tecnología de la Información, técnicas de seguridad, Sistema de Seguridad de la Información.
ISO/IEC 27010:2015	Tecnología de la Información, Sistema de Seguridad de la Información de comunicaciones para sector interno e inter-organizacional
ISO/IEC 27013	Tecnología de la Información, técnicas de seguridad, guía sobre la implementación integrada de ISO/IEC 27001 y ISO/IEC 20000-1
ISO/IEC 90003:2014	Ingeniería de software, guía para la aplicación de ISO 9001:2008
ISO/IEC CD 19770-1	Tecnología de la Información, gestión de activos de software, procesos y evaluación de conformancia
ISO/IEC 20000-1:2011	Tecnología de la Información, gestión de servicio

Tomado de: (ISO ORG, 2016)

Las características de la información y su impacto en los niveles de competitividad, imagen corporativa, rentabilidad y normativas legales se fundamentan en las siguientes definiciones:

a. Confidencialidad: esta información es sensible y no debe ser revelados sin autorización
b. Integridad: Validar la información y llevar adelante un proceso de control de cambios a la misma.

c. Disponibilidad: información accesible solo cuando exista la necesidad por el personal asignado con el know how respectivo.

1.10.4 Amenazas

Las seguridades de la información de distintas organizaciones están constantemente expuestas a diversas amenazas como el espionaje, sabotaje, fraude electrónico, o vandalismo; las amenazas pueden ser de origen externo como interno. Algunas de las fallas en la protección de la información pueden ser de carácter intencional y otras involuntariamente como la negligencia del personal en el manejo de la información o falta de procedimientos y procesos claros. Un ejemplo son los ataques cibernéticos a través de virus informáticos, son mecanismos premeditados destinados a provocar y una denegación de servicio. Como resultado al implementar un SGSI, se debe contemplar la necesidad de una adaptabilidad dinámica a las variaciones del entorno de operación de la empresa u organización en general.

Las amenazas se clasifican de la siguiente manera:

- **Criminalidad**: Ataques provocados por la influencia humana, irrespetando normas legales establecidas en la constitución. Ejemplo: robo de información, espionaje, virus, etc.

- **Actividades de origen físico**: Causados por eventos naturales, deficiencias técnicas, y participación humana. Ejemplo: Incendio, desastre natural, sobrecarga eléctrica, etc.

- **Negligencia Organizacional**: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

2. CAPÍTULO II SITUACIÓN ACTUAL DE LA INSTITUCIÓN

2.1. Dirección de Aviación Civil del Ecuador

El 9 de agosto de 1946, el Presidente José María Velasco Ibarra crea la Dirección General de Aviación Civil, mediante Decreto Supremo Nro. 1693-b, publicado en el registro oficial 671, del 28 de mismo mes y año.

La Dirección General de Aviación Civil, nació adscrita a la Comandancia General de la Aeronáutica; el 4 de diciembre de 1951 se crea la Junta de Aviación Civil Ecuatoriana, adscrita al Ministerio de Obras Públicas y Comunicaciones, a la cual se le otorga como organismo ejecutivo, la Dirección General de Aviación Civil con la misión de desarrollar la aviación como un nuevo medio de transporte en el país y velar por el progreso y la seguridad de las operaciones aéreas.

El 12 de julio de 1963, mediante Decreto Supremo No. 006, la Dirección General de Aviación Civil es agregada al Ministerio de Defensa Nacional, a través de la Fuerza Aérea Ecuatoriana. (Dirección General de Aviación Civil, 2015)

La dirección de aviación civil del ecuador (DGAC) tiene su sede principal en la ciudad de Quito, cuyo rol principal es la gestión de seguridad y prevención aeronáutica.

Dentro de sus responsabilidades principales está la investigación de accidentes, así como los incidentes de aviación.

En la tabla No. 4, se describen los objetivos establecidos por la DGAC que son los siguientes:

Tabla 4.
Objetivos Estratégicos de la DGAC

Objetivo	Descripción
1	Incrementar la seguridad ocupacional del transporte aéreo en el

	Ecuador
2	Incrementar la eficiencia y la calidad de los servicios aeronáuticos y aeroportuarios
3	Incrementar la facilitación y la seguridad de la aviación civil en el Ecuador
4	Incrementar el desarrollo del talento humano de la DGAC
5	Incrementar el uso eficiente del presupuesto de la DGAC
6	Incrementar la eficiencia operacional de la DGAC

Tomado de: (Dirección de Aviación Civil, 2013)

2.1.1. Organigrama

La Dirección General de Aviación Civil está organizada en áreas funcionales establecidas por procesos. Su estructura puede observarse en la figura No. 2; por su amplio campo de acción también debe relacionarse a nivel nacional e internacional, cumpliendo con los estándares exigidos en ambos lugares.

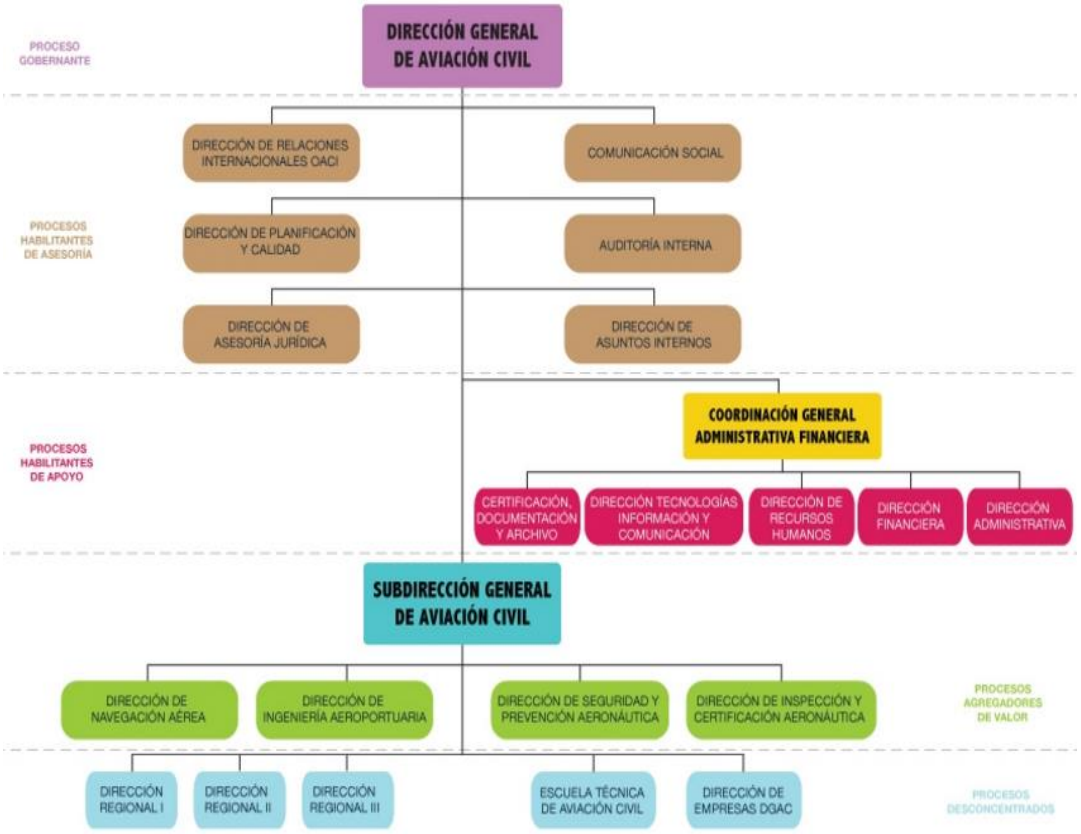


Figura 2.
Estructura Organizacional de la DGAC
Tomado de: (Dirección de Aviación Civil, 2013)

Durante la participación del Ecuador, en la Asamblea 39 de la Organización de Aviación Civil International (OACI), el Mgs. Dillon, representante de la DGAC del Ecuador menciono que el “Gobierno del Ecuador establece a la aviación, a su infraestructura aeroportuaria y al sistema de navegación aérea, como un objetivo estratégico del Estado. Bajo este contexto se reestructuro la institución de aviación civil, sus normas y regulaciones con procesos sólidos para la vigilancia de seguridad ocupacional”. (DGAC, 2016)

2.2. Situación Actual de la Gestión de Seguridad de la Información en la DGAC

La seguridad de la información en una entidad como la DGAC es crítica para el éxito de sus operaciones y planes de escalabilidad a mediano y largo plazo, por ello dentro de este capítulo se analizará las vulnerabilidades que existen actualmente en la organización, en lo que se refiere a la gestión de seguridad de la información.

Uno de los objetivos principales de la DGAC es contar con un Sistema Integrado de Gestión, para proporcionar productos enmarcados en estándares nacionales e internacionales de calidad, con cuidado del medio ambiente y garantizando un nivel óptimo de seguridad y salud ocupacional de todo el recurso humano que labora en la actividad aeronáutica; propiciando una mejora continua. (Dirección de Aviación Civil, 2015)

Para el análisis respectivo se toma como referencia el estándar ISO27001, con énfasis en la protección de información en diferentes formatos como son los documentos digitales, documentos físicos, terminales, y redes de acceso a la información. Esto con el fin de identificar cuan expuesta se encuentra la información crítica de una organización, la misma que es un elemento diferenciador con respecto a sus competidores ya sea a nivel local o internacional.

Como resultado se puede clasificar la información, identificando si la confidencialidad de la información está asegurada, la integridad de la misma está protegida y la disponibilidad de la información está al alcance únicamente de las personas autorizadas.

2.2.1 Situación Actual de la Infraestructura de red en la DGAC

La DGAC cuenta con una infraestructura de red basada en tres regiones que se pueden ver en la figura No. 3, las cuales están como:

La Región 1 está en la Matriz y se encuentra en el segmento de la WAN: 10.10.20.0/30; y la LAN está en la 172.20.200.0/16
La Región 2 está en Guayaquil y se encuentra en los segmentos de: WAN: 10.10.20.0/30 y LAN: 172.25.200.0/16

La Región 3 está ubicada en la Amazonía con los segmentos de red que son: WAN: 10.10.10.0/30 y LAN: 172.33.160.0/24

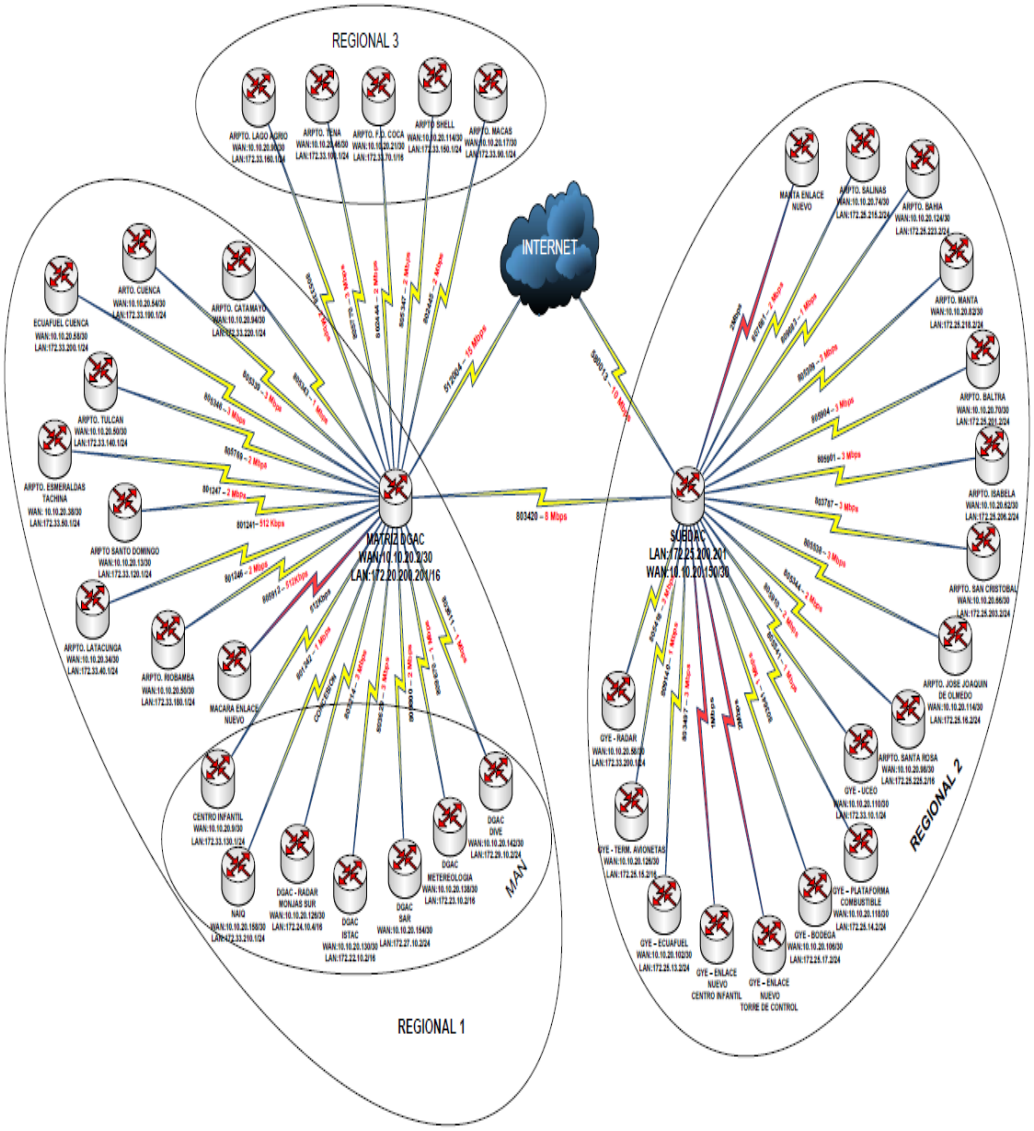


Figura 3: Infraestructura de red en la DGAC

2.2.2 Diagrama Data Center

A continuación, en la figura No. 4, se visualiza la infraestructura del Data Center de la DGAC, mismo que cuenta con 5 servidores y un nodo de almacenamiento de datos.

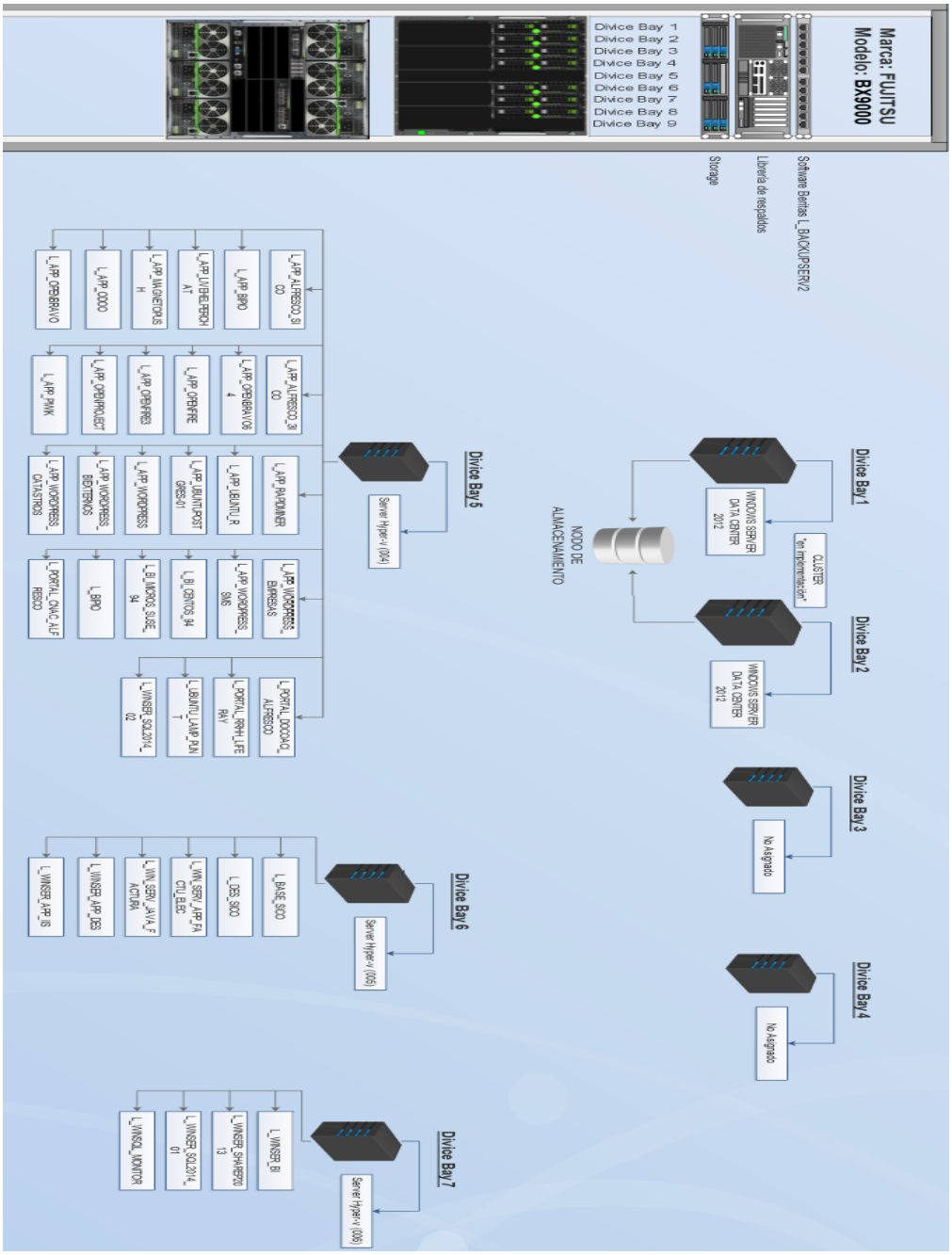


Figura 4. Diagrama Data Center

2.2.3 Esquema de red Activa DGAC

A continuación, en la figura No. 5, se describe el esquema de la red de datos activa de la DGAC.

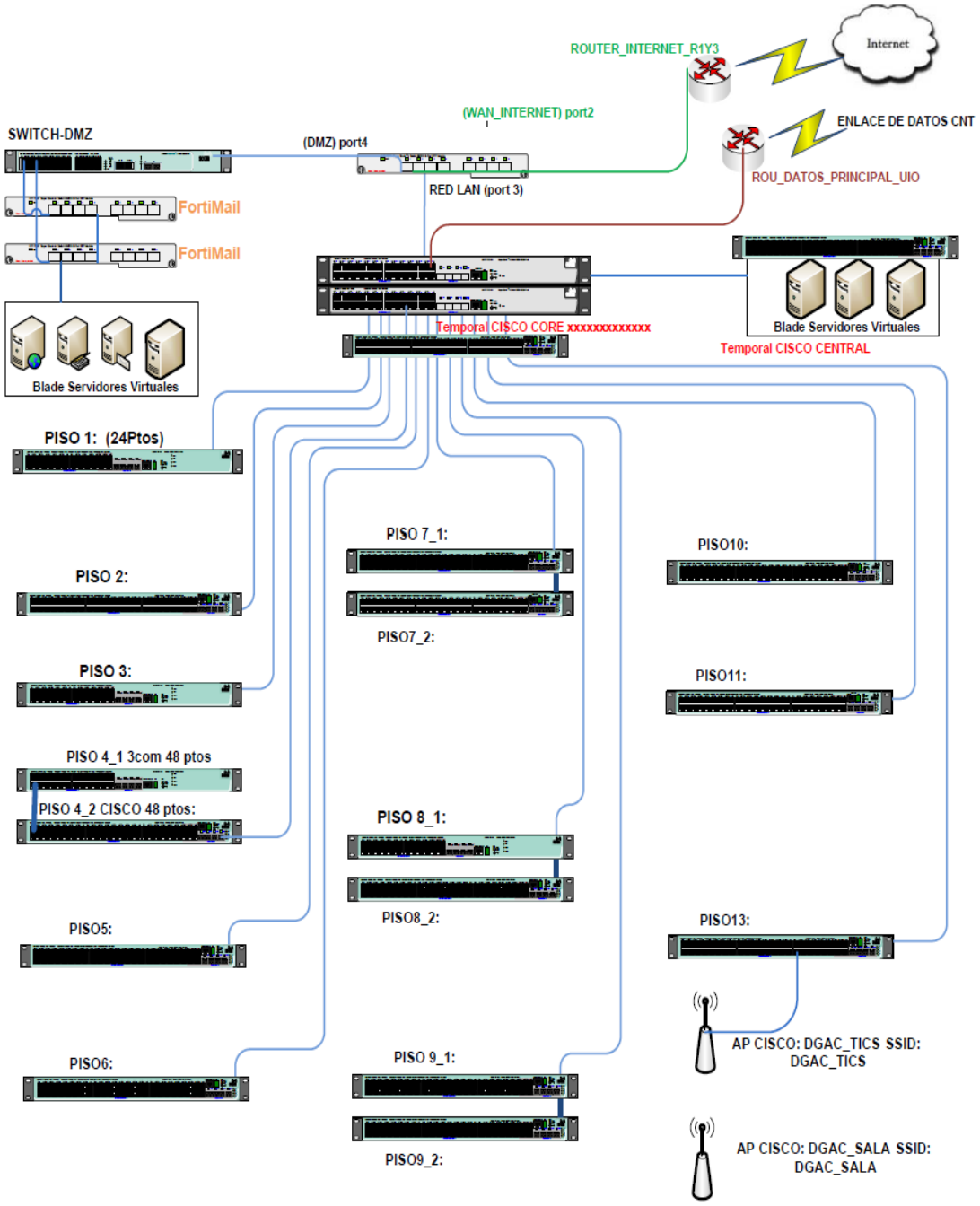


Figura 5. Esquema de red Activa DGAC

2.2.4 Control de Acceso

Esta es una de las actividades más críticas en el acceso a un sistema informático y requiere de controles específicos. Luego de un análisis exhaustivo aun no existen políticas claras sobre el control de acceso, ni documentación o procesos de revisión constante, con base en los niveles de riesgo de los activos de la DGAC, en la actualidad el administrador de sistemas controla el acceso de usuarios mediante un registro de personas autorizadas, así como personas a las cuales deben ser revocadas sus privilegios de acceso a información y asignación de contraseñas.

En el control de acceso a la red de la DGAC únicamente se tiene identificado los equipos y puertos para dicha función, así como accesos locales y remotos.
En cuanto a la recepción y envío de correos electrónicos, estos no tienen ningún tipo de cifrado, lo cual implica que puede transmitirse información sensible sin ningún tipo de control del mismo.

El control de acceso a sistemas operativos puede estar sujeto a ataques de intrusión como “Fingerprintig y footprinting”. No se ha realizado un estudio exhaustivo a nivel de la DGAC para determinar las debilidades de los sistemas operativos, ni tampoco un control de las versiones instaladas en todos los terminales, esto representa un peligro para la organización ya que un intruso puede identificar el sistema operativo más vulnerable e infiltrarse y llegar hasta la raíz (root), con todos los privilegios que esto implica para realizar cambios de forma general en una plataforma informática.

2.3. Clasificación de la Información

Como descripción de la Información puede definirse como el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que se debe proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando diferentes tecnologías lógicas, físicas o procedimentales. (Ferrer Rodrigo, 2012)

Por lo dicho anteriormente se especifica que la información en una organización es clasificada de acuerdo a la sensibilidad de la misma. De acuerdo a la clasificación de la información se aplican ciertos tipos de controles para proteger dicha información. La información que maneja la DGAC tiene diferentes formas como documentos físicos, emails, redes de comunicación (Messenger), conversaciones telefónicas, videoconferencias y dispositivos de almacenamiento internos y externos como son: discos duros, CDs, flash memory, entre otros.

La DGAC maneja distintos tipos de información incluyendo información pública, información confidencial, e información secreta. La información pública es de libre disponibilidad para el público en general y no representa riesgo alguno para la organización si se difunde la misma. La información confidencial en la DGAC requiere de un acceso autorizado, y puede representar un riesgo significativo si se comparte con personas fuera de la organización, inclusive a nivel interno con personas no autorizadas.

Actualmente no existe evidencia en la DGAC de procesos de control del manejo de información confidencial; por ello la información debe ser encriptados todos los archivos de datos sensibles, tanto de producción como de cualquier otro ambiente y en cualquiera de las siguientes situaciones: procesamiento diario, conservación en los sistemas, transmisión electrónica en redes, generación de copias de respaldo, y conservación en logos de eventos. (Chacón, Patricio. 2008)

La información secreta de la DGAC requiere de niveles estrictos de seguridad de la información, ya que su difusión a personal no autorizada puede ocasionar graves daños a la organización que origina la información, como se describe en la tabla No. 5.

Tabla 5.
Clasificación de la Información

Categorías de Información	Medidas de Seguridad	Tipo de Acceso
Pública	Bajo	Público
Confidencial	Medio	Personal Autorizado con Know How
Secreta	Alto	Exclusivo, Encriptadas

Tampoco se observa que la DGAC etiquete la información de acuerdo a su clasificación, ni marcado de dispositivos de almacenamiento como CDs y que estos estén guardados en lugares protegidos.

No existen métodos de encriptación en videoconferencias o llamada telefónicas, así como tampoco existen procesos para destruir información sensible como es el caso de las trituradoras, ni mecanismos de transportación calificados.

2.3.1 Riesgos en el Manejo de la Información

Identificar los activos de la organización y la detección de los riesgos a los cuales están expuestas es el primer paso en el análisis de riesgos. Las fallas de seguridad se pueden convertir en una amenaza letal a la supervivencia de una organización en un segmento de mercado específico. En el caso de la DGAC, esta organización maneja información relevante al sistema de gestión de operaciones aeronáuticas, la cual está direccionada a proteger la integridad física de los pasajeros que transitan por el espacio aéreo ecuatoriano las 24 horas del día. En el hipotético caso de un ciberataque, todo el sistema de control aéreo puede verse afectado, representando un peligro a la seguridad nacional y seguridad de los pasajeros.

“Un análisis de riesgos demanda: identificar los bienes y amenazas, cuantificar el impacto en el negocio de las posibles amenazas, calcular el riesgo,

establecer un balance entre el impacto que tendrá un riesgo y el costo de una contramedida. (Chacón, Patricio 2008)

A continuación, en la figura No. 6 se describe la evaluación de riesgos, sus consecuencias y probabilidad.

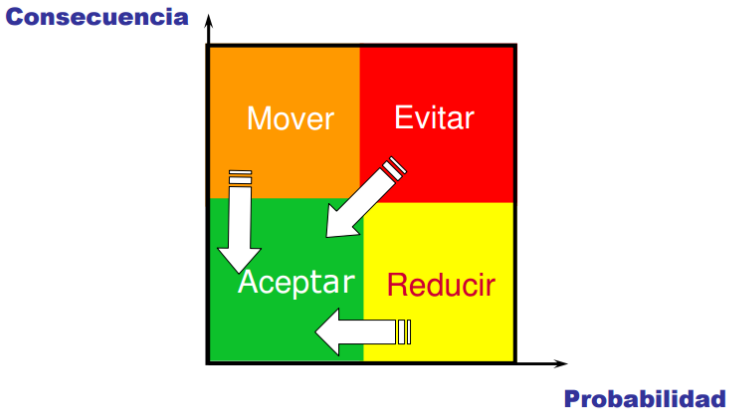


Figura 6. Evaluación de Riesgos
Tomado de: (Ferrer, 2016)

Es crucial identificar y generar un inventario de todos los bienes que posee toda organización, incluyendo infraestructura y la información como propiedad intelectual, con el fin de conocer el valor y costos de mantener y proteger los mismos. Esto además debe ser difundido entre todos los miembros de una organización, incluyendo directores, personal administrativo y los usuarios en general.

Para el análisis de riesgos en una organización como la DGAC, se utilizan herramientas estadísticas con datos cuantitativos y cualitativos, a través de un sistema de encuestas, y un proceso de entrevistas a los miembros que tienen acceso directo a la infraestructura e información de dicha organización.

También se puede considerar como un método de evaluación de riesgos con sus respectivas probabilidades de ocurrencia e impacto junto con una lista de las vulnerabilidades a la que se exponen.

2.4. Puntos neurálgicos de la institución

Para generar la presente investigación, se ha verificado que la DGAC posee algunos puntos neurálgicos, por ello se solicita una adecuada implementación de normas acorde a la seguridad de los datos ya que se debe evitar posibles ataques premeditados o accidentales que puedan ir en contra de la seguridad informática de la Institución y sus objetivos organizacionales.

Por lo dicho se puede aseverar que la situación actual de la Institución evidencia ataques en el área de seguridad de la información ya que se han dado amenaza contra los tres pilares fundamentales de la seguridad que son: confidencialidad, integridad y disponibilidad.

En el área informática de la DGAC, se pudo detectarte cuatro puntos neurálgicos que deberían ser atendidos de una manera inmediata, orientados en la seguridad lógica en las áreas administrativas de la Institución las cuales estas son:

- Manejo de Contraseñas.
- Manejo de Perfiles de Usuario.
- Estandarización de procesos para la administración de hardware y software.
- Manejo de Backups.

2.5. Encuestas

Como parte de una metodología de análisis de conocimiento sobre el alcance de la tecnología junto con sus vulnerabilidades y los procesos de gestión de la información dentro de una organización, se eligió como herramienta a la encuesta como punto de partida. Con base en las recomendaciones del estándar ISO27001 se procedió a generar una encuesta para un grupo de usuarios de la DGAC elegidos de manera aleatoria en las oficinas de la ciudad de Quito, la misma que contiene las siguientes temáticas:

- Nivel de conocimiento de los usuarios sobre la estructura general (Organigrama) de la organización, junto con sus objetivos, misión, visión, jerarquía, responsabilidades y competencias por áreas funcionales.
- Nivel de conocimiento de los usuarios sobre las herramientas tecnológicas que utilizan y posibles amenazas a la seguridad de la información.
- Técnicas o niveles de seguridad utilizadas por los usuarios para acceder y manejar información interna y externa.
- Técnicas o niveles de seguridad utilizadas por los usuarios para el acceso a infraestructura.
- Uso adecuado de contraseña, normas protección de la información en sus escritorios, dispositivos de almacenamiento y monitores.

En la figura No. 7, se describe la encuesta que se generó a la DGAC, misma que fue desarrollada utilizando SurveyMonkey, un software especializado en obtener datos estadísticos a partir de encuestas. El objetivo de realizar las encuestas es identificar las amenazas y debilidades de la plataforma tecnológica y los procesos de gestión de seguridad de la información dentro de la DGAC sede Quito. Los resultados obtenidos en las encuestas son considerados en la propuesta de implementación de un SGSI en el capítulo tres de este documento, el cual incluye mejores controles para la protección de la información, fundamentadas en los pilares de disponibilidad, confidencialidad e integridad del manejo de información. El usuario dentro de la organización independientemente de su jerarquía debe tener claros cuáles son sus obligaciones y responsabilidades en la seguridad de la información de la DGAC.

Análisis de Riesgos en SGSI DGAC

1. Tiene software implementado en su computadora para detectar, prevenir y recuperarse de un ataque de softare malicioso, ejemplo un ataque de un virus informático?

- Si
- No
- Parcialmente

Comentarios

2. Como usuario, conoce usted sobre los peligros de un ataque de software malicioso o virus informático?

- Si
- No

Comentarios

3. Ha recibido usted algun tipo de capacitación sobre el software utilizado para detectar, prevenir y recuperarse de un ataque informático en su organización?

- Si
- No
- Parcialmente
- Comentarios

4. Actualiza usted periodicamente el software antivirus?

- Si
- No
- Comentarios

5. Al enviar correos electrónicos de carácter profesional con información sensible de su organización, utiliza algun tipo de encriptación?

- Si
- No

Comentarios

6. Conoce sobre las categorías en las cuales se clasifica la información de su organización y el manejo que se debe dar a la misma? Ejemplo: Información Pública, Confidencial, Secreta.

- Si
- No

Comentarios

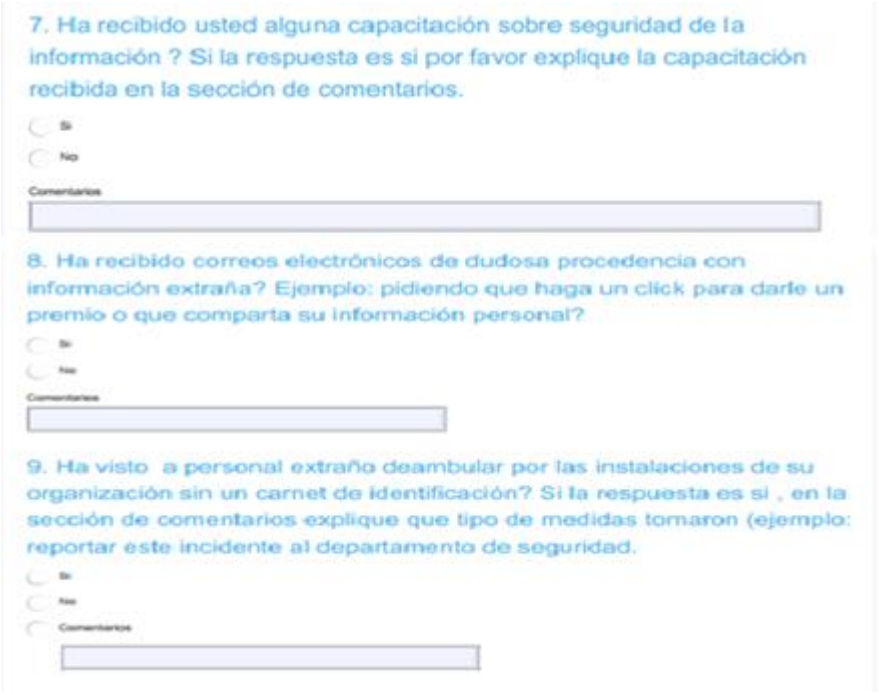


Figura 7. Desarrollo de Encuesta para SGSI en la DGAC

2.6. Herramientas para la identificación de vulnerabilidades

En el proceso de identificación de vulnerabilidades de la plataforma informática de la DGAC, se utilizaron checklists de validación y programas con software especializado en identificar vulnerabilidades. A continuación, se incluye la tabla No. 6 detallando los campos a ser evaluados en este proceso de detección de vulnerabilidades a nivel organizacional.

Tabla 6.
Análisis de infraestructura por aplicación critica

Seguridad Física	Desastres Naturales
	Controles de Acceso y Monitoreo
	Control de Incendios
	Inundaciones
Seguridad de acceso a Infraestructura de Comunicaciones e Internet	Monitorización
	Control de Acceso • Políticas de Firewall • VPN • Detección de Intrusos • Infraestructura de Comunicaciones • Routers • Switches • Firewall • Hubs • Email
Seguridad de Sistema Operativo	Unix
	Windows
	Linux

Tomado de: (Chacón, 2008)

2.7. Seguridad física y acceso a infraestructura de comunicaciones e internet

Identificación de riesgos con características físicas, se considera a la zona donde está ubicada la organización y determina si están expuestas a riesgos como desastres naturales por terremotos, erupciones volcánicas del Cotopaxi y Pichincha, inundaciones, descargas eléctricas naturales, incendios, entre otros.

2.7.1 Amenazas por erupción volcánica

En el caso de la DGAC cuya oficina está ubicada en la calle Buenos Aires OE1-53 y Avenida 10 de agosto, en la ciudad de Quito, este si está expuesta a una posible erupción volcánica, ya que posee un peligro moderado por el flujo de lodo y escombros en el escenario de una erupción volcánica del Volcán Guagua Pichincha, como se puede observar en la figura No. 8, proporcionada por el Instituto Geofísico de la Escuela Politécnica Nacional (IEPN).

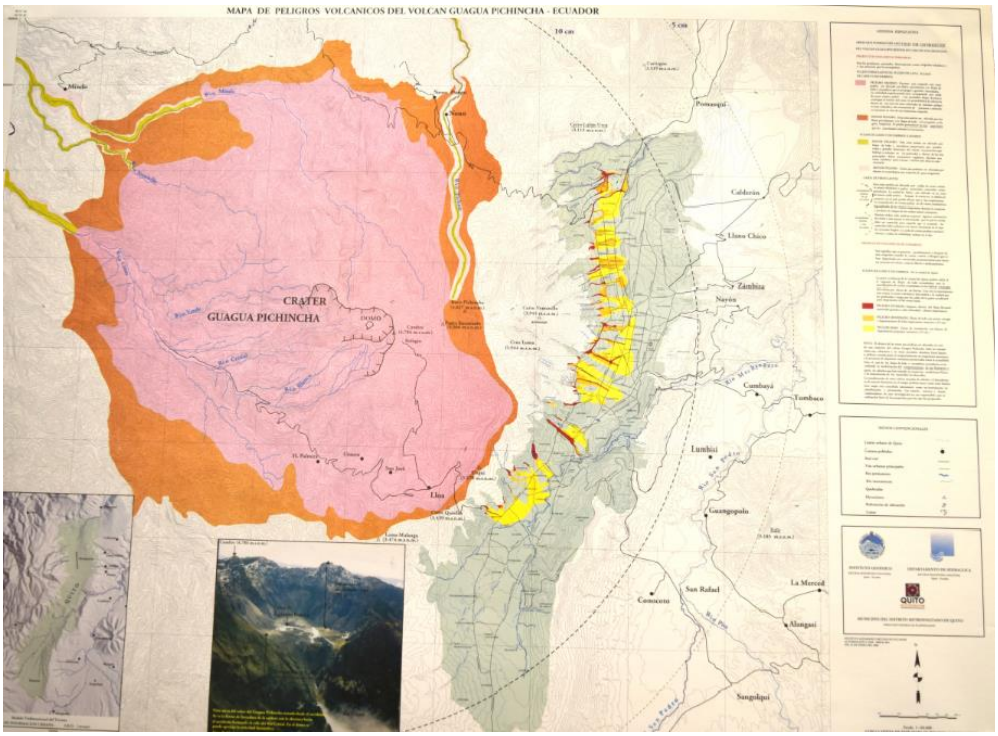


Figura 8. Mapa de Peligros Volcánicos del Volcán Guagua Pichincha
Adaptado de: (Instituto Geofísico de la Escuela Politécnica Nacional, 2016)

De acuerdo al portal del IGEPN las características del Volcán Guagua pichincha son las siguientes (Ver tabla No. 7):

Tabla 7.
Características del Volcán Guagua Pichincha

Nombre	Guagua Pichincha
Coordenadas	0,171º S, 78, 609º W
Altura	4776 m snm
Diámetro	13 km (Guagua Pichincha)

	26 km (Ruco Pichincha)
Tipo de volcán	Estrato volcán compuesto
Última erupción	1999 - 2001
Estado	Activo
Actividad reciente	Actividad hidrotermal y fumarólica
Monitoreo	Sismicidad, deformación, aguas termales

En el caso del Volcán Cotopaxi, no existe riesgo alguno con respecto a la ubicación geográfica de la oficina del DGAC en la ciudad de Quito.

2.7.2 Controles de Acceso y Monitoreo

Con respecto al control de acceso, circulación y permanencia de los usuarios en las instalaciones de la DGAC en la ciudad de quito, está plenamente controlado por un sistema de permisos de identificación automatizado, la cual requiere que el personal autorizado de la organización disponga de una credencial de identificación expedida por la autoridad competente.

También tiene un sistema de control y monitoreo de televisión CCTV instalado, y que vigila 24 horas al día los 7 días de la semana. La tecnología CCTV instalada en la DGAC dispone de algoritmos de detección y reconocimiento facial el cual permite detectar la entrada de intrusos en zonas restringidas a personal autorizado.

2.7.3 Control de Incendios

En el caso de control de incendios la DGAC si cuenta con equipos de protección y alarmas contra incendios/humo, incluyendo lámparas de emergencia y el uso de señalética para guiar a las personas a las respectivas salidas de emergencia.

2.7.4 Seguridad de Acceso a Infraestructura de Comunicaciones e Internet

Para monitorear la seguridad de acceso a internet se utilizó el software GFI Languard de la empresa estadounidense GFI Languard, el cual es un scanner para determinar la seguridad de una red identificando las vulnerabilidades del mismo; GFI Languard es una herramienta útil para realizar auditorías de software y redes, esto a nivel de computadoras y dispositivos móviles en Windows y Linux. El software GFI Languard se ejecuta a través de los siguientes pasos esenciales, como se puede visualizar en la figura No. 9:

- En primer lugar, determina los equipos que están al alcance e intenta recopilar conjuntos de información de los equipos de destino como parte de sus operaciones de detección d redes, a través de un subconjunto de protocolos SMB, NETBIOS e ICMP.
- En segundo lugar, una vez identificado los objetivos, GFI LanGuard realiza un examen en profundidad para enumerar toda la información relacionada con el equipo de destino y utiliza varias técnicas para acceder a esta información, misma que incluye verificaciones de propiedades de archivos y carpetas, verificaciones de registros, verificación de rastreo de puertos (TCP/UDP) y más.

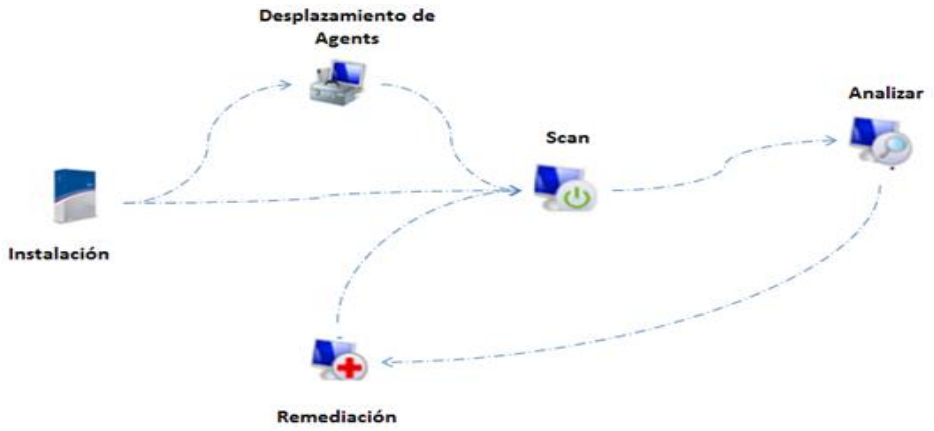


Figura 9. Funcionamiento de GFI Languard
Tomado de: (Manual GFI Languard, 2014)

2.7.5 Administración de las comunicaciones

Existen ciertos procesos en los cuales se documentan brevemente las tareas requeridas para determinada función, y se denomina procedimientos Operativos de Seguridad (POS), lo que permite identificar a las personas responsables y su nivel de competencias dentro de la organización. En el caso de la DGAC, esta tiene un alto grado de interacción con otras entidades tanto públicas como privadas, incluyendo proveedores de productos y servicios, de ahí la importancia de documentar las formas en que se comparte información entre entidades.

En el momento actual, en la Dirección de Aviación Civil se maneja el intercambio de información de manera aislada y sin una plataforma de control informático que registre y monitoree estos hechos. Tampoco existen indicios de que exista protección contra el código móvil y maligno. El objetivo de este apartado es la protección de la integridad del software y la información almacenada en los sistemas. El código móvil es aquel que se transfiere de un equipo a otro para ser ejecutado en el destino final, este empleo es muy común en las arquitecturas cliente-servidor, y se está haciendo más común en las arquitecturas “víctima-gusano”, por supuesto con un empleo no tan deseado. (Corletti, Alejandro. 2006)

2.7.6 Monitorización

En el caso de monitorización, actualmente la DGAC no cuenta con un proceso definido para monitorear el acceso y actividades no autorizadas en la red. Tampoco se monitorea la actividad de los administradores de los sistemas de información, lo que representa una amenaza seria a la integridad de la información, en caso que una persona no autorizada obtenga acceso a una cuenta de administración y tenga el control de toda la infraestructura informática.

En la mayoría de los casos de intrusión, el intruso evita dejar huellas para evitar ser descubierto, por ello se puede definir que la intrusión se define como cualquier acceso a la información confidencial de la institución, por parte de una persona externa de forma no autorizada (Chacón Patricio, 2008)

Por esto es de gran importancia realizar auditorías a los logs que registran las actividades realizadas por los usuarios en red; esto es parte de la propuesta de implementación de un SGSI a detallarse en el capítulo 3 de este trabajo de titulación.

2.8. Evaluación de Riesgos

Al realizar un análisis inicial de la situación actual de la gestión de la seguridad de la información en la DGAC, misma que permite presentar una matriz de riesgo con prioridades y probabilidades de ocurrencia. Esta información es útil al proponer una estructura para la implementación de un SGSI en la DGAC.
En la tabla No. 8 se describen los rangos de riesgo, mismos que se clasifican de la siguiente manera.

Tabla 8.
Evaluación de Riesgos

Riesgo	Rango
Bajo	1-3
Medio	4-6
Alto	7-10
Seguridad Física	**Riesgo**
Desastres Naturales	4 (Medio)
Controles de Acceso y Monitoreo	1 (Bajo)
Control de Incendios	1(Bajo)
Inundaciones	1(Bajo)

Seguridad de Acceso a Infraestructura de Comunicaciones e Internet	Riesgo
Monitorización	8 (Alto)
Control de Acceso ○ Políticas de Firewall ○ VPN ○ Detección de Intrusos ○ Infraestructura de Comunicaciones ○ Routers ○ Switches ○ Firewall ○ Hubs ○ Email	8(Alto)
Seguridad de Sistema Operativo	**Riesgo**
Unix	3 (Bajo)
Windows	3 (Bajo)
Linux	3 (Bajo)

Cabe destacar que la DGAC no tiene un sistema de gestión de seguridad de la información; este es el motivo por el cual se realizará un análisis de las vulnerabilidades actuales y se procederá a proponer un diseño para la implementación del SGSI en la DGAC en el capítulo 3.

3. CAPÍTULO III ANÁLISIS DE LA MEJOR SOLUCIÓN DEL RIESGO

3.1. Análisis del modelo organizacional

El modelo organizacional de la Dirección General de Aviación Civil está organizado en áreas funcionales establecidas por procesos, mismas que se describen a continuación.

La DGAC está constituida por: procesos habilitantes de asesoría, procesos habilitantes de apoyo, procesos agregados de valor y los procesos desconcentrados.

3.1.1. Procesos habilitantes de asesoría

Los procesos habilitantes de asesorías están divididos en 6 direcciones importantes que son:

- Dirección de relaciones internacionales OACI.
- Dirección de planificación y calidad.
- Dirección de asesoría jurídica.
- Comunicación social.
- Auditoría interna.
- Dirección de asuntos internos.

3.1.2. Procesos habilitantes de apoyo

Como parte importante de la DGAC y como Coordinación Administrativa está la Coordinación General Administrativa Financiera, misma que tiene las siguientes áreas que son:

- Certificación, documentación y archivo.
- Dirección tecnologías información y comunicación
- Dirección de recursos humanos.

- Dirección financiera.
- Dirección administrativa.

3.1.3. Procesos agregados de valor

La DGAC cuenta dentro de su organigrama una parte principal en sus procesos administrativos, por lo cual se ha generado la Subdirección General de Aviación Civil, la cual cuenta con diferentes direcciones de áreas que se describen a continuación:

- Dirección de navegación aérea.
- Dirección de ingeniería aeroportuaria.
- Dirección de seguridad y prevención aeronáutica.
- Dirección de inspección y certificación aeronáutica.

3.1.4. Procesos desconcentrados

En cuanto a los procesos desconcentrados la Subdirección General de Aviación Civil, se describen las siguientes direcciones:

- Dirección regional I.
- Dirección regional II.
- Dirección regional III.
- Escuela técnica de aviación civil.
- Dirección de empresas DGAC.

3.2. Análisis actual de la situación de las políticas informáticas de la Dirección General de Aviación Civil

La Dirección General de Aviación Civil, en la Resolución No. 000329/2012, en el cual el Directorio General de Aviación Civil considera las siguientes políticas para el uso de equipos informáticos:

El artículo 3 describe que las Políticas para el uso de equipos informáticos, están basados en 21 puntos importantes que son:

a) El equipo informático será utilizado exclusivamente para actividades institucionales.
b) La Dirección de Tecnologías de la Información y Comunicación (DTICs), entregarán los equipos a los encargados de la DGAC, mismos que serán comprobados su funcionamiento.
c) Cada equipo entregado tendrá el software que necesite cada área.
d) Ninguna persona tiene autorización para instalar un software que no esté autorizado por la DGAC.
e) Cada usuario tendrá una contraseña alfanumérica para el acceso de los equipos informáticos.
f) Cada usuario deberá cambiar si contraseña de forma periódica.
g) Todos los usuarios respetarán la configuración inicial que fue establecida por la Dirección de Tecnologías.
h) Si algún servidor público desea instalar alguna aplicación informática, deberá hacer una solicitud escrita a la Dirección de Tecnologías de la Información y Comunicación, para dicho proceso se deberá presentar los habilitantes necesarios.
i) Solo el personal autorizado de la Dirección de TICs podrá hacer los mantenimientos preventivos y exhaustivos a los equipos informáticos.
j) En caso de existir un daño en los equipos, el usuario deberá comunicar a los entes correspondientes, el mantenimiento del mismo, dicha comunicación deberá ser de forma escrita a través del correo electrónico institucional o de ser el caso en forma telefónica.
k) Las Unidades que pertenecen a la Dirección de TICs, no podrán ingresar de forma arbitraria o sin autorización de la Dirección de TICs, a equipos informáticos entregado por la DGAC.
l) Las unidades de las TICs y/o servidores de la DGAC, no podrán manipular la información, mucho menos hacer uso inadecuado de la

información institucional, sin previa autorización del responsable de dicho equipo.

m) La DTICs autorizará el soporte técnico necesario para el buen uso de los equipos informáticos.

n) En caso de que algún equipo informático necesite ser configurado a sus parámetros iniciales de fábrica, la DTICs, notificara dicho proceso al encargado en custodia de dichos equipos.

o) Ningún servidor público tiene autorización para mover los equipos, sin previa autorización escrita por el Director de cada área.

p) No se autoriza la utilización de los equipos informáticos para actividades personales o no institucionales.

q) Los usuarios no tienen autorización para la utilización de equipos personales.

r) Si algún servidor público desea incorporar un equipo, deberá pedir la autorización correspondiente a las Unidades de Tecnologías de la Información y Comunicación.

s) No se podrá ingerir bebidas, ni mucho menos se podrá comer cerca de los equipos informáticos, y en caso de ocurrir algún percance, la DTICs realizará el proceso administrativo para la respectiva sanción.

t) Los usuarios deberán mantener sus equipos asignados por la DGAC en óptimo funcionamiento, evitando así el mal uso de dichos dispositivos.

u) Los usos de los recursos informáticos son de carácter estrictamente institucional, y el mal uso del mismo será sancionado de acuerdo a la legislación existente.

En la tabla No. 9 se describe la asociación de las Normas ISO.

Tabla 9.
Asociación Normas ISO

Descripción	Cumple con la ISO 27001	Observación
Los equipos informáticos serán utilizados exclusivamente para actividades institucionales.	SI	Si se cumple parcialmente Generar registros

La Dirección de Tecnologías de la Información y Comunicación (DTICs), entregarán los equipos a los encargados de la DGAC, mismos que serán comprobados su funcionamiento.	SI	Si se cumple parcialmente Generar registros
Cada equipo entregado tendrá el software que necesite cada área	NO	No se cumple Generar un control de las aplicaciones que necesitan
Cada usuario deberá cambiar si contraseña de forma periódica	NO	No se cumple Generar como política
Si algún servidor público desea instalar alguna aplicación informática, deberá hacer una solicitud escrita a la Dirección de Tecnologías de la Información y Comunicación, para dicho proceso se deberá presentar los habilitantes necesarios	SI	Generar normas de la presentación de documentos
Solo el personal autorizado de la Dirección de TICs podrá hacer los mantenimientos preventivos y exhaustivos a los equipos informáticos	SI	Si se cumple parcialmente Generar registros
En caso de existir un daño en los equipos, el usuario deberá comunicar a los entes correspondientes, el mantenimiento del mismo, dicha comunicación deberá ser de forma escrita a través del correo electrónico institucional o de ser el caso en forma telefónica	SI	Se cumple
Las Unidades que pertenecen a la Dirección de TICs, no podrán ingresar de forma arbitraria o sin autorización de la Dirección de TICs, a equipos	SI	Se cumple

informáticos entregado por la DGAC		
Las unidades de las TICs y/o servidores de la DGAC, no podrán manipular la información, mucho menos hacer uso inadecuado de la información institucional, sin previa autorización del responsable de dicho equipo	SI	Se cumple parcialmente Generar políticas de penalidad por el mal uso de la información
La DTICs autorizará el soporte técnico necesario para el buen uso de los equipos informáticos	SI	Se cumple
En caso de que algún equipo informático necesite ser configurado a sus parámetros iniciales de fábrica, la DTICs, notificara dicho proceso al encargado en custodia de dichos equipos	SI	Se cumple
Ningún servidor público tiene autorización para mover los equipos, sin previa autorización escrita por el Director de cada área	SI	Se cumple
No se autoriza la utilización de los equipos informáticos para actividades personales o no institucionales	NO	No se cumple Generar políticas
Los usuarios no tienen autorización para la utilización de equipos personales	NO	No se cumple Generar políticas Y APLICAR
Si algún servidor público desea incorporar un equipo, deberá pedir la autorización correspondiente a las Unidades de Tecnologías de la Información y Comunicación	NO	No se cumple Generar políticas
No se podrá ingerir bebidas, ni mucho menos se podrá comer cerca de los equipos informáticos, y en caso de	NO	No se cumple Generar registro de dichas políticas

ocurrir algún percance, la DTICs realizará el proceso administrativo para la respectiva sanción		
Los usuarios deberán mantener sus equipos asignados por la DGAC en óptimo funcionamiento, evitando así el mal uso de dichos dispositivos	SI	Se cumple parcialmente Generar políticas
Los usos de los recursos informáticos son de carácter estrictamente institucional, y el mal uso del mismo será sancionado de acuerdo a la legislación existente	SI	Se cumple parcialmente Generar políticas

3.3. Análisis y evaluación de riesgos

3.3.1. Análisis de Riesgos en SGSI – DGAC

Para el análisis de riesgos se tomó como instrumento la encuesta, misma que se generó a la DGAC y fue desarrollada utilizando SurveyMonkey, un software especializado en obtener datos estadísticos a partir de encuestas. El objetivo de realizar dicho instrumento es identificar las amenazas y debilidades de la plataforma tecnológica y los procesos de gestión de seguridad de la información dentro de la DGAC sede Quito.

Los resultados que se presenta a continuación en la tabla No. 10 y la figura No. 10, fueron realizados a 20 usuarios dentro de la DGAC, y se describen a continuación:

Tabla 10.
Análisis de Riesgos en SGSI – DGAC

		Resultados			Comentarios
	Preguntas:	Si	No	No sabe	
1	¿Tiene software implementado en su	6	8	6	No tienen conocimiento

	computadora para detectar, prevenir, y recuperarse de un ataque de software malicioso, ejemplo un ataque de virus informático?				
2	¿Cómo usuario, conoce usted sobre los peligros de un ataque de software malicioso o virus informático?	12	8		No tienen conocimiento
3	¿Ha recibido usted algún tipo de capacitación sobre el software utilizado para detectar, prevenir, y recuperarse de un ataque informático en su organización?		19	1	No tienen conocimiento
4	¿Actualiza usted periódicamente el software antivirus?		18	2	No tienen conocimiento
5	¿Al enviar correos electrónicos de carácter profesional con información sensible de su organización, utiliza algún tipo de	1	16	3	No tienen conocimiento

	encriptación?				
6	¿Conoce sobre las categorías en las cuales se clasifica la información de su organización y el manejo que se debe dar a la misma? Ejemplo: Información Pública, Confidencial, Secreta.	6	9	5	No tienen conocimiento
7	¿Ha recibido usted algún tipo de capacitación sobre seguridad de la información? Si la respuesta es sí, por favor explique la capacitación recibida en la sección de comentarios.	2	15	3	Recibieron capacitación al ser parte del departamento de sistemas.
8	¿Ha recibido correos electrónicos de dudosa procedencia con información extraña? Ejemplo: ¿pidiendo que hagan un click para darle un premio o que comparta información personal?	17	3		No tienen conocimiento

9	¿Ha visto a personal extraño deambular por las instalaciones de su organización sin un carnet de identificación? Si la respuesta es sí, en la sección de comentarios explique qué tipo de medidas tomaron (ejemplo: reportar este incidente al departamento de seguridad.	9	11		No tomaron ninguna acción

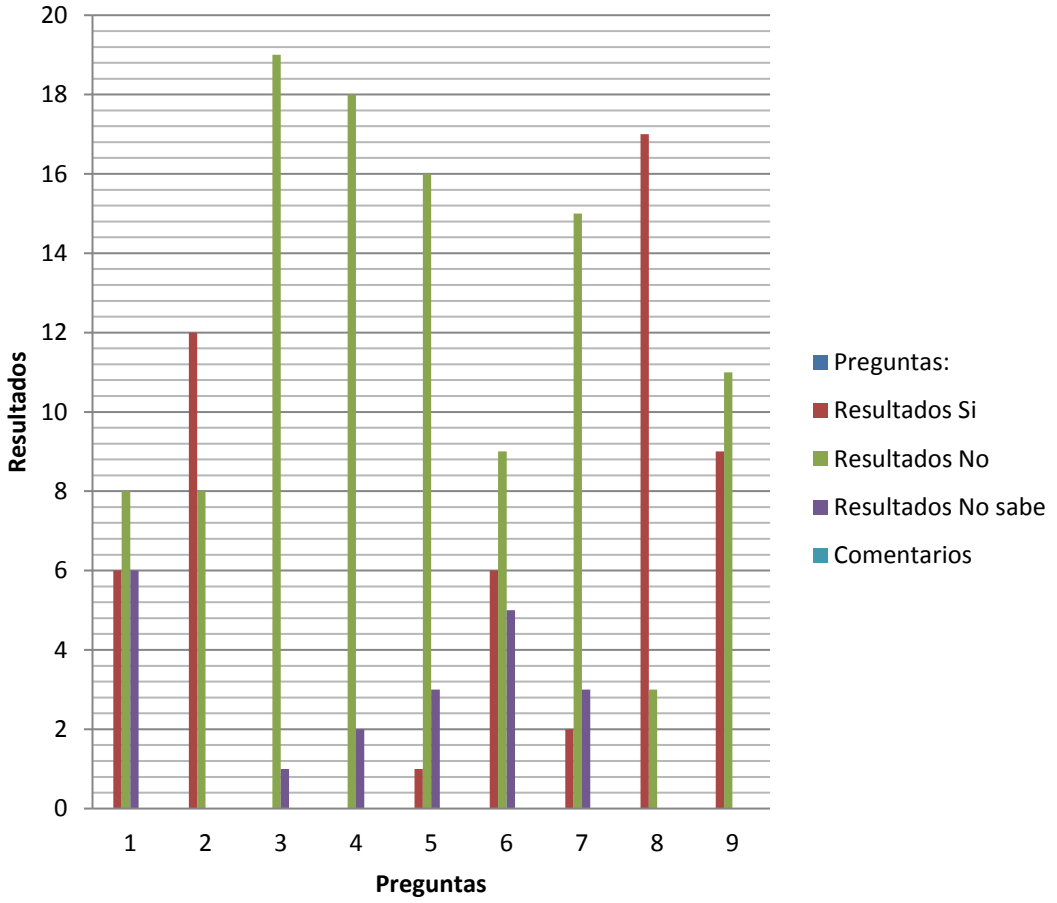


Figura 10. Resultados del análisis de riesgos**.**

3.4. Análisis general de la seguridad de la red

En el Anexo 1, se presenta un resumen ejecutivo que muestra el nivel de vulnerabilidad de la red, las computadoras más vulnerables, el estado del agente y el estado de auditoría, las tendencias de vulnerabilidades a lo largo del tiempo, la información sobre sistemas operativos, servidores y estaciones de trabajo, por lo cual en las figuras No. 11, 12, 13, se describen un extracto de dicho informe.

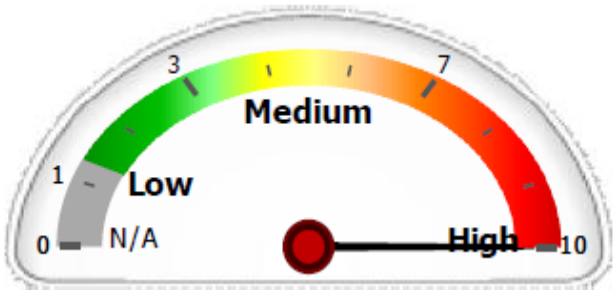


Figura 11. Nivel de vulnerabilidad.

Figura 12. Distribución de la vulnerabilidad informática.

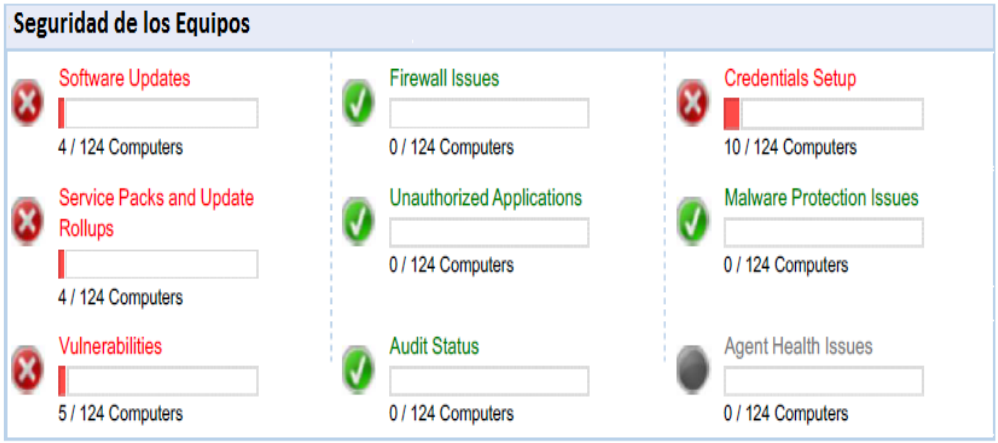
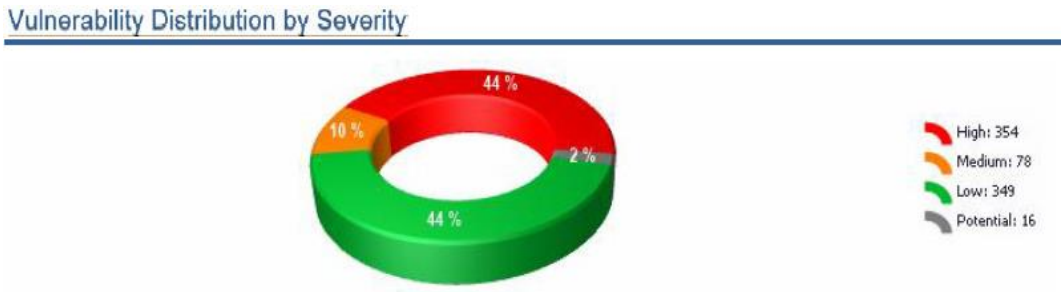


Figura 13. Seguridad en los equipos.

3.5. Estado de la vulnerabilidad

En el Anexo 2, se muestra información estadística relacionada con las vulnerabilidades detectadas en los equipos de destino.

Las vulnerabilidades pueden agruparse por nombre de equipo, severidad de vulnerabilidad, marca de tiempo y categoría, como se muestra en la figura No. 14.



Vulnerability Distribution by Computer

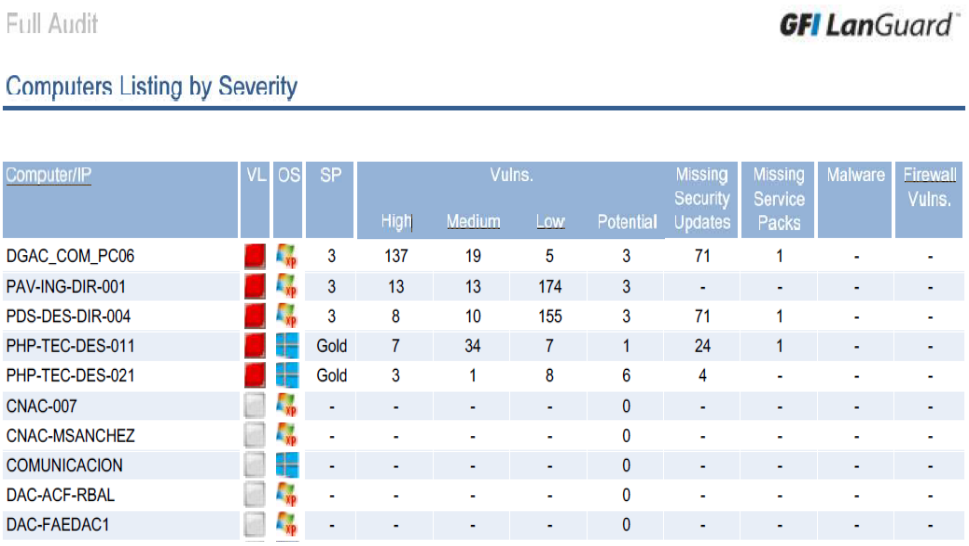
Computer/IP	High	Medium	Low	Potential
DGAC_COM_PC06	214	20	5	3
PAV-ING-DIR-001	13	13	174	3
PDS-DES-DIR-004	86	10	155	3
PHP-TEC-DES-011	34	34	7	1
PHP-TEC-DES-021	7	1	8	6

Vulnerability Listing by Computer

Figura 14. Vulnerabilidades detectadas en los equipos de destino.

3.6. Auditoría completa

En el anexo 3, se describe un informe técnico que contiene toda la información recuperada durante una auditoría. El informe contiene información sobre vulnerabilidades, puertos abiertos, hardware y software (Ver figura No. 15).


Full Audit

GFI LanGuard

Computers Listing by Severity

Computer/IP	VL	OS	SP	Vulns.				Missing Security Updates	Missing Service Packs	Malware	Firewall Vulns.
				High	Medium	Low	Potential				
DGAC_COM_PC06			3	137	19	5	3	71	1	-	-
PAV-ING-DIR-001			3	13	13	174	3	-	-	-	-
PDS-DES-DIR-004			3	8	10	155	3	71	1	-	-
PHP-TEC-DES-011			Gold	7	34	7	1	24	1	-	-
PHP-TEC-DES-021			Gold	3	1	8	6	4	-	-	-
CNAC-007			-	-	-	-	0	-	-	-	-
CNAC-MSANCHEZ			-	-	-	-	0	-	-	-	-
COMUNICACION			-	-	-	-	0	-	-	-	-
DAC-ACF-RBAL			-	-	-	-	0	-	-	-	-
DAC-FAEDAC1			-	-	-	-	0	-	-	-	-

Figura 15. Auditoría General.

3.7. Auditoria de software

El Anexo 4, muestra todas las aplicaciones no autorizadas instaladas en los equipos de destino que se encuentran durante una auditoría, el informe incluye información sobre antivirus, antispyware e incluye un inventario de aplicaciones (Ver figura No. 16)

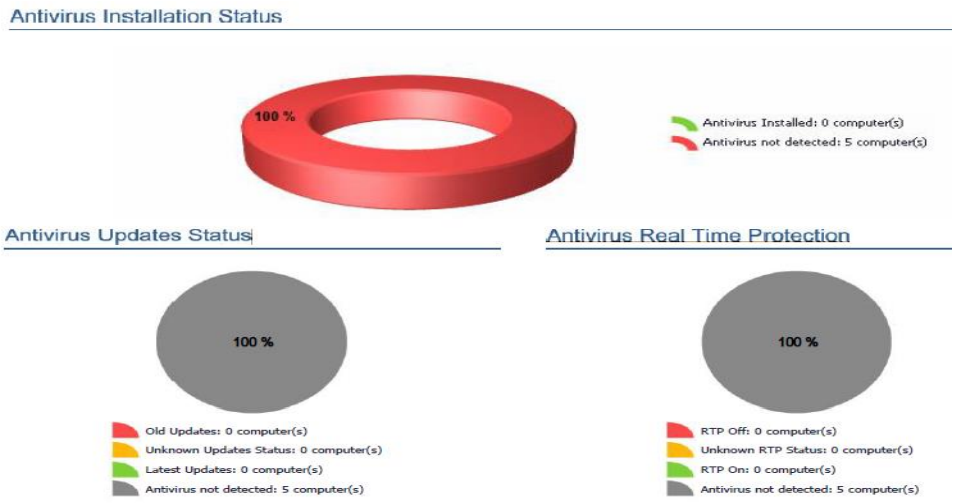


Figura 16. Auditoría de Software.

3.8. Historial de escaneo

En la figura No. 17, se describe una visión general de las auditorías de seguridad de la red realizadas a lo largo del tiempo y se puede visualizar por completo en el anexo 5, dicho informe incluye información sobre las computadoras más escaneadas, las computadoras menos escaneadas, el estado de auditoría y la lista de historiales.

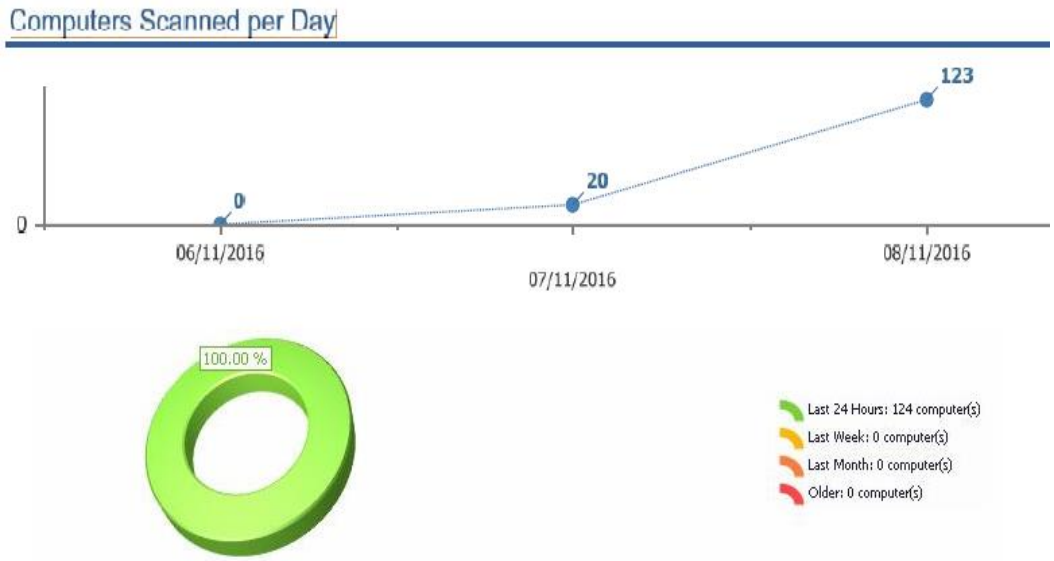
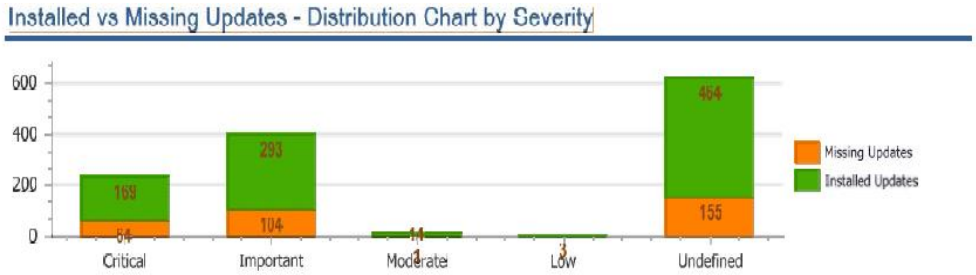
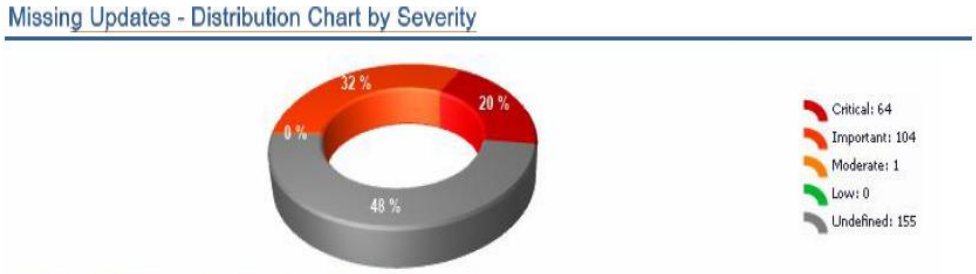


Figura 17. Auditorías de seguridad de la red.

3.9. Estado de revisión

El anexo 6, muestra información estadística relacionada con las actualizaciones faltantes e instaladas, detectadas en los equipos de destino. Las actualizaciones se pueden agrupar por nombre de equipo, gravedad, fecha y hora, proveedor y categoría, como se ve en la figura No. 18.





Missing Updates - Distribution Table by Computer

Computer/IP	Critical	Important	Moderate	Low	Undefined
DGAC_COM_PC06	30	41	1	0	43
PDS-DES-DIR-004	24	48	0	0	37
PHP-TEC-DES-011	8	14	0	0	50
PHP-TEC-DES-021	2	1	0	0	25

Figura 18. Actualizaciones.

3.10. Descripción actual de las Políticas de seguridad

La Dirección General de Aviación Civil, describe sus políticas de seguridad, basadas la Resolución No. 000329/2012, en el cual el Directorio General de Aviación Civil considera:

Que, el artículo 91 de la Constitución de la República del Ecuador, establece: “La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa y fidedigna”.

Que, el artículo 5 de la Ley de Comercio Electrónico, Firmas y mensajes de Datos instruye que: “Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención”.

Que, el artículo 9 de la Ley Comercio Electrónico, Firmas y mensajes de Datos instruye que: “Para la elaboración, trasferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o trasmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros”.

Que, el inciso segundo del artículo 6 de la Ley Orgánica de Trasparencia y Acceso a la Información Pública al referirse a la información confidencial, señala “El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes”.

Que, el artículo 10 de la Ley Orgánica de Trasparencia y Acceso a la Información Pública dispone: “Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho de la información se pueda ejercer a plenitud, por lo que en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción”.

Que, el artículo 3 del Reglamento General Sustitutivo de Bienes del Sector Público: “Instituye la obligación de la máxima autoridad de cada entidad u organismo, el orientar y dirigir la correcta conservación y cuidado de los bienes públicos que han sido adquiridos o asignados para uso y que se hallen en poder de la entidad y que la conservación, buen uso y mantenimiento de los bienes, será la responsabilidad directa del servidor que los ha recibido para el desempeño de sus funciones y labores oficiales”.

Que, el inciso cuarto del artículo 3 de la reglamento ibídem, señala que: “El daño, pérdida o destrucción del bien, por negligencia comprobada o mal uso, no imputable al deterioro normal de las cosas, será de responsabilidad del servidor que lo tiene a su cargo, y de los servidores que de cualquier manera

tienen acceso al bien, cuando realicen acciones de mantenimiento o reparación por mantenimiento propio o del usuario; salvo que se conozca o compruebe la identidad de la persona causante de la afectación del bien".

Que, el artículo 95 del Reglamento General Sustitutivo de Bienes del Sector Público, se refiere a que: "Todas las entidades públicas, deberán tener un plan anual de Mantenimiento de Equipos Informáticos, el mismo que deben contar con cronogramas, financiamiento y estar aprobado por las máximas autoridades".

Que, artículo 96 del reglamento ibídem, establece que: "El mantenimiento de equipos informáticos estarán a cargo de la Unidad responsable de esta actividad en cada institución".

Que, de conformidad con el Reglamento Orgánico de Gestión Organizacional por Procesos de la Dirección General de Aviación Civil, publicado en el Registro Oficial Edición Especial No. 32 de 1 de marzo del 2010, le corresponde a la Dirección de Tecnologías de la Información y Comunicación, "Planificar y gestionar los procesos que involucren las Tecnologías de la Información y Comunicaciones (TICs), a fin de facilitar el logro de los objetivos institucionales".

Que, al a Dirección de Tecnologías de la Información y Comunicación, le corresponde: "dar cumplimiento con lo establecido en el numeral 3.5.2 del Reglamento Orgánico de Gestión Organizacional por Procesos de la Dirección General de Aviación Civil".

Que, "se debe regular el uso de los bienes, servicios y sistemas informáticos, con el objeto de sistematizar y optimizar la utilización de los mismos, para bridar una mejor calidad en el desarrollo y cumplimiento de las funciones de cada uno de los servidores de la Dirección General de Aviación Civil".

Que, “de conformidad con el Reglamento Orgánico de Gestión Organizacional por Procesos de la Dirección General de Aviación Civil, le corresponde a la Dirección Administrativa gestionar la dotación, mantenimiento y control de suministros, bienes y servicios requeridos por las áreas de la institución, aplicando la normativa vigente, a fin de lograr los objetivos institucionales”.

Que, “mediante memorando No. DGAC-HK-2011-0104-M de 8 de julio de 2011, el Coordinador Administrativo Financiero, dispone a la Dirección de Tecnologías de la Información y Comunicación se elabore un Reglamento para el uso y control de los Recursos Informáticos y de comunicaciones de la Dirección General de Aviación Civil”.

4. CAPÍTULO IV DESARROLLO DE LA SOLUCIÓN

4.1. Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

El escenario donde se realiza el intercambio de información sensible de una organización cada vez se torna más complejo, por ello las distintas organizaciones se ven obligadas a proteger su activo más importante como es la información; “Esta necesidad se ve agravada, debido a que los datos de una empresa y su complejidad de análisis crecen exponencialmente.

Por lo dicho anteriormente el presente capitulo describe las directrices que debe seguir la DGAC para la implementación de un SGSI, certificado en base a las normas ISO 27001, las cuales están basadas en:

- La implantación de ISO/IEC 27001 en una organización, la cual describe que un proyecto debe tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance.
- De ser necesario se recomienda la ayuda de consultores externos para lograr el alcance esperando en la organización basado en los Sistema de Gestión de la Seguridad de la Información elegida.
- Las organizaciones que hayan proporcionado sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos mediante la aplicación de las buenas prácticas de ISO/IEC, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.
- El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática.

Luego del proceso de diagnóstico inicial de vulnerabilidades del sistema de manejo de información en la DGAC, se identificó en los capítulos anteriores

que esta no tiene un proceso definido ni mecanismos de control para proteger la información de una manera adecuada.

Los controles definidos en este plan de implementación de SGSI en la DGAC tienen características técnicas y organizativas, por ello deben ser documentados adecuadamente a través de los procedimientos descritos en este capítulo. Esta documentación será revisada durante la fase de certificación del sistema de gestión de la información basado en la norma ISO 27001 para la DGAC. En el proceso de implementación del SGSI deben participar el personal de áreas operativas y administrativas, departamento de TI enfocados en mantener la integridad de la información, y tomando en cuenta los riesgos operativos, procesos de seguridad y procedimientos de implementación tecnológica.

Es crítico definir una metodología de trabajo, misma que describe los ejes principales a considerarse en el proceso de implementación del SGSI en la DGAC.

Por lo dicho anteriormente se pretende certificar un SGSI en la DGAC, el cual constara con procesos mediante el cual una entidad de certificación externa, independiente y acreditada audite el sistema de la DGAC, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

4.2. Política de Protección de la Información

Basado en las normas de la ISO/IEC 27001, la cual describe que la Política de Protección de la Información, está basada en la seguridad de los datos y que en las instituciones no deben trabajar personas que no tengan registros de identificación, así como también cada administrador de la red, debe poseer claves de acceso para la protección de la infraestructura de datos y de la comunicación.

Las políticas de protección tienen como objetivo principal garantizar la seguridad de la información de la DGAC, y se debe iniciar con la planificación y ejecución de un plan piloto a nivel organizacional. Uno de las acciones más importantes es socializar el alcance del proyecto con las autoridades y personal, con el fin de obtener su apoyo en las diversas fases de implementación del SGSI; especialmente los beneficios que implica contar con un sistema eficaz de gestión de seguridad de la información. Uno de los primeros pasos es el levantamiento de información con el fin de resaltar las vulnerabilidades existentes y luego generar las políticas que proporcionen instrucciones claras sobre el manejo apropiado de información en computadoras y sistema de comunicación de la organización.

4.3. Elementos de Control Organizativo de la Seguridad de la Información

A nivel organizacional la información puede ser compartida a nivel interno, entre diversas áreas funcionales como también a nivel externo con ciertos subcontratistas si es el caso. Por ello es importante que la DGAC defina políticas claras en cuanto al manejo de información interna y externa, detallando el alcance del acceso a la información en un contrato de confidencialidad entre las partes involucradas. Como primer paso se debe establecer un departamento de seguridad de la información, mismo que creara una estructura a nivel organizacional para la distribución de funciones y responsabilidades en el manejo y protección de la información; su principal objetivo debe ser el garantizar la implementación de medidas de seguridad en el acceso a la información por el personal interno y externo.

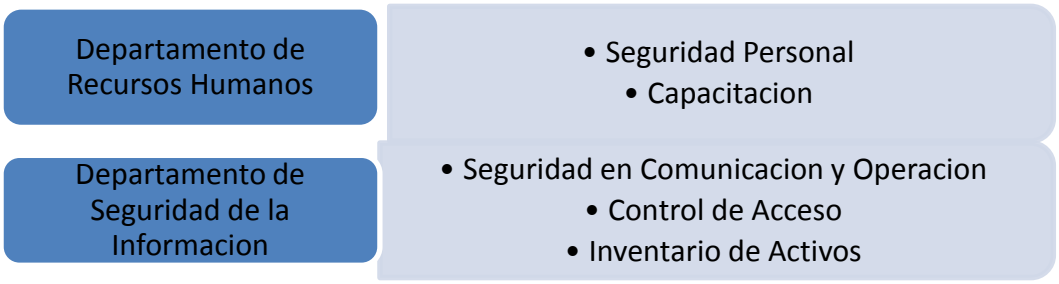


Figura 19. Roles en la Seguridad de la Información

Las funciones del departamento de seguridad de la información deben seguir los siguientes lineamientos:

- Funciones Generales y por áreas.
- Planificación y proceso de aprobación de funciones generales de SGSI.
- Observación de cambios en el reporte de vulnerabilidades y riesgos a la seguridad de la información.
- Generación de una base de datos que registren los incidentes reportados en relación a la seguridad de la información.
- Analizar e implementar procesos técnicos orientados a incrementar el nivel de seguridad de la información a través de las distintas áreas funcionales que conforman la DGAC.
- Establecer procesos de auditoria de la seguridad de la información.
- Evaluar el desempeño de los controles de seguridad de la información.
- Difundir la importancia del SGSI y obtener retroalimentación de los participantes.
- Organizar campañas de capacitación a nivel organizacional.

El departamento de seguridad debe garantizar que todos los procesos orientados a la seguridad de la información se mantengan actualizados y bajo una supervisión constante. En cuanto al control de la seguridad de la información y la relación a nivel externo. En el caso de subcontratistas, el departamento de seguridad de la información debe considerar las siguientes directrices:

- Establecer procesos para la recuperación y destrucción de información compartida con colaboradores externos al finalizar un contrato.
- Establecer restricciones en el número de copias y nivel de difusión de la información.

- Analizar el nivel de acceso a la información requerido por el personal y el nivel de acceso idóneo para los mismos.
- Definir las obligaciones y responsabilidades legales de las personas que acceden a la información.
- Control de acceso basado en un análisis estricto que involucra contraseñas, identificadores de usuario único, lista actualizada de usuarios y privilegios de acceso a la información, entre otras.
- Capacitación de usuarios en el tema de seguridad de la información
- Control de instalación de hardware y software.
- Actualización de software para combatir software malicioso.
- Presentación de reportes sobre el nivel de protección, vulnerabilidades e incidentes en el manejo de la información.

4.4. Política de Autenticación de Usuarios

Las contraseñas asignadas a los usuarios deben estar enlazadas a su identificación con el fin de validar su acceso al sistema de información. El administrador de la red tiene la responsabilidad de coordinar con el departamento de recursos humanos, la activación y desactivación de cuentas de usuarios, especialmente en el caso de desvinculación de personal. Esta revisión de cuentas debe hacerlo mensualmente, con el fin de revocar el acceso a usuarios que ya no estén presentes en la organización o que no requieran acceso a la información. A los nuevos usuarios es imprescindible que firmen acuerdo de confidencialidad y protección de la información.

Para la verificación de usuarios y permiso de acceso a la información se deben considerar los siguientes parámetros en las cuentas:

- Identificación.
- Clave de acceso.
- Fecha de autorización y expiración.
- Contador de 5 minutos de inactividad para desligar al usuario.
- Registro de intentos fallidos.

- Área funcional o grupo de trabajo.

4.5. Identificación de Activos de Información

La DGAC debe identificar los activos de red y sus niveles de relevancia, dependiendo de la criticidad de su información con el fin de que sea categorizada. Por ello es esencial realizar un inventario de activos con el fin de que sean identificados y asignados a una persona responsable dentro de un departamento funcional específico. Esto permitirá a la DGAC garantizar que los activos reciban un nivel adecuado de protección.

Una vez que se asignen propietarios a los activos identificados anteriormente, estos tienen la responsabilidad de clasificarla de acuerdo a su nivel de sensibilidad y reportar al departamento de seguridad para su respectiva documentación. El propietario debe informar al departamento de seguridad de la información cualquier cambio que ocurra en la clasificación de la información; el proceso de revisión de modificaciones debe realizarse cada dos meses como máximo. El representante del departamento de sistemas informáticos es responsable de limitar el acceso a la información de acuerdo a su clasificación. Para clasificar la información se deben considerar las siguientes categorías:

- Criticidad Baja: ninguno de los valores asignados supera el 2
- Criticidad Media: alguno de los valores asignados es 2
- Criticidad Alta: algunos de los valores asignados son 3

4.6. Seguridad de los Recursos Humanos

El objetivo principal de esta política es garantizar que el personal, subcontratistas y usuarios externos entiendan su responsabilidad en el manejo de información y el nivel de acceso a la información requerido para que puedan cumplir con sus funciones. Este proceso está orientado a reducir el mal uso de la información, como también el acceso inadecuado a la infraestructura existente, en especial el error humano.

En el análisis del control de activos y de seguridad de los recursos humanos se recomienda trabajar con la metodología MAGERIT 12 y 13, así como también concientizar respecto a la existencia de riesgos, ofrecer un método sistemático para analizar los riesgos a los que se ve expuesta la información, ayudar, descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y preparar a la organización para procesos de evaluación.

Para lograr los objetivos expuestos anteriormente, es necesario capacitar a los propietarios de la información de manera continua, en temas como normas de seguridad, competencias, responsabilidades y sanciones en caso de no cumplir con las normas. Al contratar personal nuevo, con el personal existente e incluyendo usuarios externos, se debe proporcionar las herramientas adecuadas para su desarrollo, así como también capacitación en la firma de compromisos de confidencialidad de la información.

El plan de capacitación debe ser coordinado entre el departamento de seguridad de la información y el departamento de recursos humanos. En cuanto a la protección de información, derechos y obligaciones del empleado en la seguridad de la información, se deberá educar para que describan los procesos que se generan en relación con las leyes de propiedad intelectual, así como también en la legislación de protección de datos, cabe destacar que todas estas informaciones se encontraran aclarados e incluidos en los términos y condiciones de contrato.

4.7. Seguridad Física y Ambiental

El perímetro de seguridad debe ser definido en relación al área a ser protegida donde se encuentra la información. También es importante identificar áreas donde se permite el acceso restringido a personal autorizado; esto reduce el riesgo de acceso físico no autorizado. Debido a que gran parte de la información está en forma física en papel, es necesario establece políticas para su almacenamiento o destrucción si es el caso.

El control del entorno ambiental también es fundamental para evitar daños en la infraestructura informática, por lo cual se describe las falencias a mejorar.

Tabla 11.
Tabla de procesos a mejorar

Descripción	Implementación en la DGCA	Observación
Los equipos informáticos serán utilizados exclusivamente para actividades institucionales.	En proceso de aplicación	Creación de registros
La Dirección de Tecnologías de la Información y Comunicación (DTICs), entregarán los equipos a los encargados de la DGAC, mismos que serán comprobados su funcionamiento.	En proceso de aplicación	Creación de registros
Cada equipo entregado tendrá el software que necesite cada área	En proceso de aplicación	Generación de informes de control de las aplicaciones que necesitan
Cada usuario deberá cambiar si contraseña de forma periódica	En proceso de aplicación	Informe de solicitud para la creación de una política de empresa
Si algún servidor público desea instalar alguna aplicación informática,	En proceso de aplicación	Generación de informes para la presentación de documentos

deberá hacer una solicitud escrita a la Dirección de Tecnologías de la Información y Comunicación, para dicho proceso se deberá presentar los habilitantes necesarios		
Solo el personal autorizado de la Dirección de TICs podrá hacer los mantenimientos preventivos y exhaustivos a los equipos informáticos	En proceso de aplicación	Creación de registros
Las unidades de las TICs y/o servidores de la DGAC, no podrán manipular la información, mucho menos hacer uso inadecuado de la información institucional, sin previa autorización del responsable de dicho equipo	En proceso de aplicación	Generación de políticas de penalidad por el mal uso de la información
No se autoriza la utilización de los equipos informáticos para actividades personales o no institucionales	En proceso de aplicación	Políticas para la penalidad por el mal uso

Los usuarios no tienen autorización para la utilización de equipos personales	En proceso de aplicación	Políticas para la penalidad por el mal uso
Si algún servidor público desea incorporar un equipo, deberá pedir la autorización correspondiente a las Unidades de Tecnologías de la Información y Comunicación	En proceso de aplicación	Políticas para la penalidad por el mal uso
No se podrá ingerir bebidas, ni mucho menos se podrá comer cerca de los equipos informáticos, y en caso de ocurrir algún percance, la DTICs realizará el proceso administrativo para la respectiva sanción	En proceso de aplicación	Creación de registros
Los usuarios deberán mantener sus equipos asignados por la DGAC en óptimo funcionamiento, evitando así el mal uso de	En proceso de aplicación	Generación de informes de mantenimiento

dichos dispositivos		
Los usos de los recursos informáticos son de carácter estrictamente institucional, y el mal uso del mismo será sancionado de acuerdo a la legislación existente	En proceso de aplicación	Generación de informes de mantenimiento

4.8. Seguridad de Comunicaciones

Los canales de comunicación establecidos para el intercambio de información deben garantizar la confidencialidad, integridad y disponibilidad del mismo. Es necesario definir a los actores responsables de la operación y procedimientos para la gestión de intercambio de información. El responsable de la red informática debe tener conocimiento de acuerdos de intercambio de información con usuarios externos para aplicar políticas de protección de la información; una de estas políticas es la implementación de controles de acceso a la información, esto describe al personal con los privilegios y permisos autorizados y la penalización a personas que intenten acceder sin la debida autorización.

Una política de uso de contraseñas es importante para proteger el acceso e intercambio de información dentro de la DGAC; esta política auténtica y autoriza al usuario a ingresar al sistema informático donde puede acceder a información de la organización. Las contraseñas deben contener una mezcla de caracteres especiales, que no sean comunes y no tengan relación al nombre o características del usuario. Se debe capacitar al usuario sobre el manejo de contraseñas y la importancia de nunca compartir o difundir detalles del mismo.

La identificación del usuario debe basarse en la asignación de un número de identificación único, con el objetivo de rastrear las actividades de los usuarios

como por ejemplo el número de impresiones, ingreso a las instalaciones, consumo de alimentos, entre otros.

Por lo dicho anteriormente, a continuación, se describe los procesos que se deben tomar en cuenta para las políticas de control de acceso:

- Control de acceso a bases de datos y red de información.
- Autenticación y autorización de acceso a usuarios.
- Administración de red de comunicación y gestión de la información con usuarios o proveedores externos.
- Mantener un log de actividades.
- Limitar el acceso únicamente a usuarios autorizados.
- Bloquear el acceso a usuarios anónimos.
- Bloquear el acceso luego de varios intentos fallidos por ingresar al sistema de gestión de la información.
- Bloquear cuentas inactivas.
- Cambiar contraseñas.
- Auditoría de SGSI con GFI software cada dos meses.

El acceso al sistema de comunicación remota también debe ser controlado, con herramientas tecnológicas que monitoreen el tráfico como el caso de wireshark, y la vulnerabilidad de los puertos de comunicación abiertos.

Por ello se presenta un detalle para las políticas de restricción a la información.

- Manejo de privilegios de acceso a la información de acuerdo al perfil del usuario.
- Limitar el acceso a usuarios sin el know how requerido.
- Establecer restricciones a la lectura, escritura o supresión de información.
- Monitorear actividades de usuarios.

- Contraseñas con un mínimo de 8 caracteres, combinados entre números, caracteres alfabéticos y signos de puntuación.
- Modificación de contraseñas predefinidas en equipos de computación y redes inalámbricas.

La documentación de la topología de red, así como el diseño e implementación de sistemas de comunicación redundantes es relevante ya que evitaría el colapso del sistema informático en caso de un ataque cibernético.

4.9. Modificaciones en Software

En el escenario donde exista un cambio en el sistema operativo, el departamento de informática debe realizar un análisis detallado del impacto de este cambio en el nivel de seguridad de la información.

Antes de cualquier cambio, se debe requerir que exista un procedimiento establecido para una actualización de sistemas operativos, mismos que deben ser analizados en cuanto a sus vulnerabilidades y nivel de protección ante ataques informáticos. Todos estos detalles deben ser documentados por la persona responsable, y comunicados a las partes involucradas en el proceso.

El administrador de la red debe revisar constantemente el proceso de control de aplicaciones o programas instalados en las computadoras, con el fin de garantizar la integridad del sistema informático. Dentro de los procedimientos debe informarse con anterioridad a todo el personal sobre cualquier cambio operativo que se lleve a cabo dentro de la organización, en caso de que se requiera que los usuarios suspendan sus actividades durante el proceso de cambios.

La actualización de la documentación no debe ser crítica, incluyendo los casos donde se modifiquen los números telefónicos o direcciones IP. La definición de modelos de buenas prácticas en el manejo de aplicaciones y procesos criptográficos debe reducir el nivel de riesgo.

En el caso de modificar patches de software de un proveedor, el responsable del área de sistemas debe primero analizar los términos de la licencia para evitar una multa. También se debe analizar el impacto del cambio en términos de seguridad de la información, documentando las modificaciones realizadas y observaciones sobre las vulnerabilidades que esta pueda ocasionar.

El software GFI Languard debe ser instalado en cada computador para detectar canales ocultos donde pueden recibir ataques de código troyano y así evitar ser expuestos a una filtración de información, por lo que antes de seleccionar un software se debe analizar lo siguiente:

- Adquirir programas a proveedores acreditados o productos ya evaluados.
- Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- Controlar el acceso y las modificaciones al código instalado.
- Utilizar herramientas para la protección contra la infección del software con código malicioso, en este caso la CMS utilizo el antivirus Symantec.

El software GFI languard que se recomienda implementar como parte de este sistema de SGSI en la DGAC, calcula el ancho de banda utilizado por todo el sistema informático, y determina estadísticas del tráfico de red, con el objetivo de realizar un dimensionamiento de red efectivo y evitar cuellos de botella a largo plazo. El software GFI también monitorea el estado de las aplicaciones instaladas en los computadores, así como las vulnerabilidades y los intentos de intrusión al sistema, esto con el fin de evitar un ataque de denegación de servicio (DoS).

EL software antivirus debe ser instalado en todo computador sin excepción y la conexión a una red externa debe realizarse a través de un servidor proxy. Al

manejar información confidencial también es crítico encriptar la información que se va a transmitir. En la actualidad existen muchos programas que ofrecen este tipo de servicio como CripText, Kapersky, Cryptzone, entre otros. Los responsables de esta área deben seleccionar el producto y proveedor más adecuado el servicio de incitación de la información.

4.10. Detección y Gestión de Incidentes

Es necesario que la DGAC mantenga una bitácora de los incidentes detectados con una descripción detallada, fecha y hora del mismo. Esto con el fin de darle seguimiento a los incidentes y determinar cuáles han sido resueltos y cuales requiere una resolución. La estadística obtenida del reporte de incidentes debe ser socializado con las autoridades y personal pertinente. Los datos obtenidos deben usarse para establecer un plan de mejoras a mediano y largo plazo.

4.11. Normativas Legales

Las siguientes normativas legales deben considerarse al establecer mecanismos de control en el SGSL de la DGAC:

Propiedad Intelectual: El departamento legal de la DGAC debe considerar las normativas establecidas por el Instituto Ecuatoriano de Propiedad Intelectual en el caso de que requieran patentar cierta información.

La Propiedad Intelectual se refiere a las creaciones de la mente, tales como obras literarias, artísticas, investigaciones científicas e industriales, así como los símbolos, nombres e imágenes utilizadas en el comercio. La Propiedad Intelectual otorga al autor, creador e inventor el derecho de ser reconocido como titular de su creación o invento y, por consiguiente, ser beneficiario del mismo.

Los Estados son los responsables de garantizar una legislación clara para precautelar este bien común. En Ecuador, el Instituto Ecuatoriano de la

Propiedad Intelectual (IEPI), es el organismo encargado de proteger, fomentar, divulgar y conducir el buen uso de la Propiedad Intelectual desde el enfoque de tres áreas distintas: Propiedad Industrial, Derecho de Autor y las Obtenciones Vegetales. (IEPI, 2016)

En la Ley de Comercio Electrónico (2012), debe considerarse algunos artículos de esta ley como son los siguientes:

“Art. 1. Objeto de la Ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas”

4.11.1 De las infracciones informáticas

Art. 57. Infracciones informáticas. Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley. Reformas al Código Penal

Art. 58. A continuación del Art. 202, inclúyanse los siguientes artículos enumerados:

El que, empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de

reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Obtención y utilización no autorizada de información. - La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica." (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos 2002-67)

4.12. Capacitación

La capacitación es un elemento de gran relevancia en el proceso de implementación de un SGSI y debe incluir a todo el personal de la DGAC incluyendo autoridades, personal técnico y administrativo.

El plan de capacitación debe ser coordinado entre el departamento de recursos humanos y el departamento de seguridad informática. Los temas a cubrir en el curso de capacitación deben incluir, pero no limitarse a los siguientes:

Tabla 12.
Plan de capacitación

	Área Técnica	Administrativa	Autoridades
Riesgos de ataques informáticos	X	X	X
Características del software	X		

de detección de vulnerabilidades GFI Languard			
Manejo de técnicas criptográficas para proteger la información	X	X	X
Clasificación de Información	X	X	X
Seguridad Física	X	X	X
Procesos para el control y seguridad de la información	X	X	X
Definición de roles, y estructura organizativa	X	X	X
Técnicas avanzadas de encriptación	X		

4.13. Inventarios

Las siguientes formas son recomendadas para realizar inventario de activos y auditorias técnicas internas.

Tabla 13.
Inventario de Activos

Departamento Asignado	Activo	Características	Representante / Responsable
• **Área Informática** • **Área Financiera** • **Departamento Legal** • **Operaciones** • **Área Administrativ**	Ejemplo: 30 Computadoras Aplicaciones: GFI Languard Antivirus: Kapersky	Monitor, Mouse, Quemador de Disco, Impresora Software detección de vulnerabilidades informáticas Software para detección de virus informático	Administrador de Red

a • **Recursos Humanos**			

4.14. Riesgos

En la tabla No. 14 se describen las listas de activos, riesgos, vulnerabilidades y acciones que se deben tomar una vez implementado la norma.

Tabla 14.
Análisis de Riesgos

Lista de Activos	Riesgo	Vulnerabilidad	Acción
• Equipos de Oficina • Servidores • Personal • Instalaciones • Suministro Eléctrico • Patches de Software • Sistema de comunicación • Correo Electrónico • Documentación	Ejemplo: Daño por inundación Acceso no autorizado Saturación de suministro de electricidad Hurto	Falta de protección adecuada Falta de control en el acceso Mal funcionamiento del UPS Falta de control físico	Mitigar

4.15. Análisis Costo Beneficio

Se intenta señalar e indicar la mejor solución los costos generados para una futura implementación, son justificables en función de las pérdidas económicas que se pueden generar por las fallas de seguridad corregidas en la presente tesis.

Una vez que los sistemas informáticos en la DGAC dejan de funcionar puede tolerar como máximo 12 horas sin que la información perdida se vuelva imposible de recuperar y la institución empiece a asumir pérdidas por la falta de

información. Aun cuando la información pueda ser recuperada esto también implica costos en cuanto a tiempo de trabajo de los empleados que deben cumplir horas extras para poder actualizar el sistema.

Al costo de pérdida de información también se debe agregar las horas laborales que el personal que depende íntegramente de la aplicación para realizar su trabajo, permanece inactivo pero que finalmente se pagan. Esto sucede especialmente en la parte administrativa donde la mayoría de procesos se desencadenan de acuerdo al flujo se información de dependencia a dependencia.

Una vez diseñado y aprobado el proyecto, se realizará la capacitación al personal técnico y administrativo de la DGAC, el mismo que consta de doce personas, entre las cuales están:

4 Técnicos de infraestructura.
4 Técnicos en proyectos.
4 Técnicos en el área de Networking.
1 Director del área.
1 Secretaria.

El costo estimado de la capacitación en los procesos para la implementación de la norma está alrededor de 16400 dólares anuales, por lo cual generaría una inversión en la administración e implementación de la infraestructura.
Cabe destacar que todo este proceso permitirá un rendimiento más óptimo en la red de datos, así como también evitará la pérdida de datos y un control permanente de la información ya que por ser una entidad que posee información con carácter secreto debe tener discreción y seguridad en la información.

Respecto al impacto de la normativa en la organización de las empresas, estas perciben mejoras en su propia organización, en la estandarización de los

procedimientos de trabajo y mejoras en la implicación y comunicación con los empleados.

Por lo dicho anteriormente, a continuación, se presenta un análisis costo-beneficio, el cual evidencia que el proyecto será rentable cuando la relación costo-beneficio es mayor que la unidad.

B/C > 1 → el proyecto es rentable

Por ello se puede especificar que la relación costo-beneficio (B/C), también conocida como índice neto de rentabilidad, es un cociente que se obtiene al dividir el Valor Actual de los Ingresos totales netos o beneficios netos (VAI) entre el Valor Actual de los Costos de inversión o costos totales (VAC) de un proyecto.

B/C = VAI / VAC (Ecuación 1)

A continuación, se presenta el B/C para los próximos dos años, la cual tiene una proyección de ingresos al final de los 2 años de $ 50000, esperando una tasa de rentabilidad del 12 % anual y con una inversión de $ 32800 (Presupuesto capacitación por año - $ 16400), para ello se considera el 20 % de interés anual, lo cual se toma como referencia la tasa de interés de los bancos y se obtiene los siguientes resultados:

B/C = VAI / VAC (Ecuación 1)

B/C = (50000 / (1 + 0.12) * 2) / (32800 / (1 + 0.20) * 2)

B/C = 89285,71 / 54666,66

B/C = 1.63

Como la relación costo-beneficio es mayor que 1, se puede afirmar el proyecto es rentable en los próximos 2 años.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

La globalización económica incremento la necesidad de acceder a información y compartir la misma en un tiempo record.; como resultado, el desarrollo de tecnologías de comunicación más eficientes ha tomado gran impulso, eliminando muchas barreras como la distancia y facilitando la interacción entre diversos individuos, tal acepción toleran una serie de pasos que elimina y deja sin efecto la calidad de las distancias y divisiones territoriales, surgiendo así una renovación del tiempo, distancia y espacio de las relaciones globales.

En el proceso de estructuración del análisis de las vulnerabilidades del sistema informático actual de la DGAC se debe generar de forma periódica el software GFI Languard, mismo que permite observar las áreas más susceptibles a un ataque informático.

El monitoreo del tráfico de red con GFI Languard es crucial para evitar los conocidos cuellos de botella, tomando una iniciativa de carácter proactivo en términos de escalabilidad del SGSI.

Mantener al personal capacitado en las áreas respectivas para que cada uno de ellos conozca su rol y así evitar contratiempos en la parte administrativa y técnica.

La Dirección de Aviación Civil tiene como fin garantizar la seguridad de la información y contar con procesos bien estructurados, razón por la cual deberá implementar un SGSI con fundamento en la norma ISO 27001 expuesta en este proyecto de titulación.

El plan de implementación de un SGSI en la DGAC se realizó mediante un proceso integral, y socialización con toda la organización, ya que el SGSI

provee los procesos idóneos para mitigar y eliminar los riesgos en la seguridad de la información considerados como activos en la DGAC.

Mediante la utilización del software GFI Languard se completó una auditoria informática el cual develo varias vulnerabilidades del sistema actual de gestión de la información en la DGAC.

Se identificó los activos de la organización, áreas de competencia, personal responsable y políticas de manejo de la información.

La norma ISO27001 ofrece una metodología eficiente reconocida a nivel internacional para la implementación exitosa de un SGSI en la DGAC, para evitar vulnerabilidades y generar la implementación de procesos en el manejo de información, así como también la administración de manera óptima de la seguridad de la información.

Se estableció una matriz de responsabilidades administrativas y técnicas con el fin de cumplir con las normativas establecidas por la ISO, permitiendo mejorar las temáticas de capacitación especificadas en este proyecto de titulación, lo cual son esenciales para generar una cultura de manejo y protección de la información sensible en la DGAC.

Con un plan de implementación de SGSI, la DGAC apunta a ser parte de un grupo selecto de entidades que garantizan la protección de activos relevantes como infraestructura e información, ofreciendo un servicio de calidad tanto a clientes internos como externos.

5.2. Recomendaciones

Es importante definir el rol de las personas responsables dentro de la organización y su alcance dentro del SGSI para proteger la información.

La estandarización y validación de procesos para el control de la información es fundamental para garantizar el éxito de la implementación del SGSI en la DGAC.

Se debe limitar la entrega de privilegios a usuarios sin antes completar un análisis detallado de la necesidad que tienen los mismos en acceder a la información, por ello la planificación juega a un rol importante y debe tener el aval de las autoridades y alta gerencia de la organización.

El proceso de implementación del SGSI debe ser planificado y apoyado por las autoridades de la DGAC, por lo que es importante recibir el aporte de todas las áreas que forman parte de la DGAC para tener resultados óptimos.

Los procesos de capacitación en los nuevos procesos basados en las ISO, debe ser constante con el fin de mantener una posición proactiva y una cultura de protección de la información.
El software de análisis de vulnerabilidades debe ser licenciado para evitar obstáculos legales relacionados a propiedad intelectual.

Los procesos de SGSI a ser implementados en el DGAC, deberán cumplir los requerimientos y expectativas establecidas por la dicha institución, orientadas a fortalecer la gestión de la información.

Mejorar la gestión de la información debe ser una prioridad para toda organización para ofrecer calidad de servicio y establecer relaciones de confianza óptimas con cliente y la sociedad.

La aplicación de la norma 27001 representa la columna vertebral de un modelo de gestión de la información exitoso.

Las auditorías en seguridad de la información internas y externa deben ser frecuentes para recopilar datos actualizados y poder realizar un análisis objetivo de la información.

REFERENCIAS.

Aguilera, P. (2010), Seguridad informática: Madrid, España: Editex, S.A.

Alfonso García Cervigón & María del Pilar Alegre Ramos. (2011), Seguridad Informática: Bogotá, Colombia: Ediciones Parainfo.

Alvarado, V. L. (2013). Plan de seguridad de la información. (Tesis de grado). Escuela Politécnica Nacional, Ecuador.

Álvarez, Flor. (2007). Implementación de un Sistema de Seguridad de la Información basado en la Norma ISO 27001, Para la Intranet de la Corporación Metropolitana de Salud. (Tesis de grado). Escuela Politécnica Nacional, Ecuador.

Areitio, JB, (2008), Seguridad de la información. Redes, informática y sistemas de información: Madrid, España: Editorial Paraninfo.

Ascencio, G. (2006), Seguridad en Internet: Madrid, España: Nowtilus.

Baldeechi, R. (2014) SONDA. Implementación efectiva de un SGSI ISO 27001, 6th Edición.

Bertolín, J. A. (2008), Seguridad de la información. Redes, informática y sistemas de información: Barcelona, España: Editorial Paraninfo.

Capa, D. S. (2015). http://dspace.ucuenca.edu.ec/. Recuperado el 30 Septiembre de 2016 de http://dspace.ucuenca.edu.ec/bitstream/123456789/22371/1/tesis.pdf

Chacón, Patricio (2008). Propuesta de un modelo de gestión de seguridad de la información para institutos superiores tecnológicos de educación aeronáutica (Tesis de grado). Escuela Politécnica Nacional, Ecuador.

Congreso Nacional. (2002). Ley de Comercio Electrónico. Recuperado el 29 de Septiembre de 2016 de http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador_ley_2002-67_17042002_comelectronico.pdf

Farley, M. T. (1997), Guía Lan times de seguridad e integridad de datos: Madrid, España: McGraw-Hill.

Fernández, M, (2012), Modelo para el gobierno de las TIC basado en las normas ISO: Madrid, España: Aenor Ediciones.

Guerra, María. (2012). Optimización del proceso de seguridad operacional en el aeropuerto internacional mariscal sucre de Quito (Tesis de grado). Escuela Politécnica Nacional, Ecuador.

Instituto Ecuatoriano de Propiedad Intelectual. (2016). Ley de Propiedad Intelectual. Recuperado el 15 de Octubre de 2016 de http://www.propiedadintelectual.gob.ec/propiedad-intelectual/

Instituto Geofísico Nacional. (2012). Mapa de Peligros del Volcán Guagua Pichincha. Recuperado el 16 de Octubre de 2016 de http://www.igepn.edu.ec/guagua-pichincha/mapa-de-peligros-guagua-pichincha. Escuela Politécnica Nacional. Quito. Ecuador

ISO España (s.f). Sistema de Gestión de Seguridad de la Información. Recuperado el 30 de Septiembre de 2016 de http://www.iso27000.es/iso27000.html.

ISO (s.f). ISO/IEC 27001 - Information security management. Recuperado el 30 de Septiembre de 2016 de http://www.iso.org/iso/standards/management-standards/iso27001.htm

Jesús, c. S. (2011), Seguridad informática: Bogotá, Colombia: ra-ma editorial.

López, A, (2010), Seguridad informática: Madrid, España: Editorial Editex.

María del pilar alegre y Alfonso García. (2011). Seguridad informática: Madrid, España: Editorial paraninfo.

Marino, L. (2010). Seguridad Informática. Mayo 13,2016, de SlideShare, Sitio web. Recuperado el 30 de Septiembre de 2016 de http://es.slideshare.net/jemarinoi/seguridad-informtica-1125964

Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado el 30 de Septiembre de 2016 de http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf.

Mifsud, E. (2012). Observatorio Tecnológico. Recuperado el 30 de Septiembre de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

Murazzo, M. A., Rodríguez, N. R., Vergara, R., Carrizo, F., González, F., & Grosso, E. (2013, June). Administración de QoS en ambientes de redes de servicios convergentes. In XV Workshop de Investigadores en Ciencias de la Computación. Montevideo Uruguay.

Quiroz, M. (2013). Aspectos generales de Seguridad Informática. Recuperado el 30 de Septiembre de 2016 de http://es.slideshare.net/mariorafaelquirozmartinez/aspectos-generales-de-seguridad-informtica

Royer, JM, (2004), Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones: Barcelona, España- Editorial Eni.

Santos, j. C. (2011), Seguridad informática: Bogotá, Colombia: ra-ma españa.

Borghello, Cristian. (2009). Seguridad de la Información. Recuperado el 30 de Septiembre de http://www.segu-info.com.ar/politicas/

Suárez, R. C. (2007). Tecnologías de la información y la comunicación: Introducción a los sistemas de información y de telecomunicación: Madrid, España. Ideas propias Editorial SL.

Veites, Á. G. (2011), Seguridad Informática Básico: Bogotá, Colombia: StarBook editorial y publicaciones.

Vieites, á. G. (2013), Seguridad en equipos informáticos: Bogotá, Colombia: starbook editorial España.

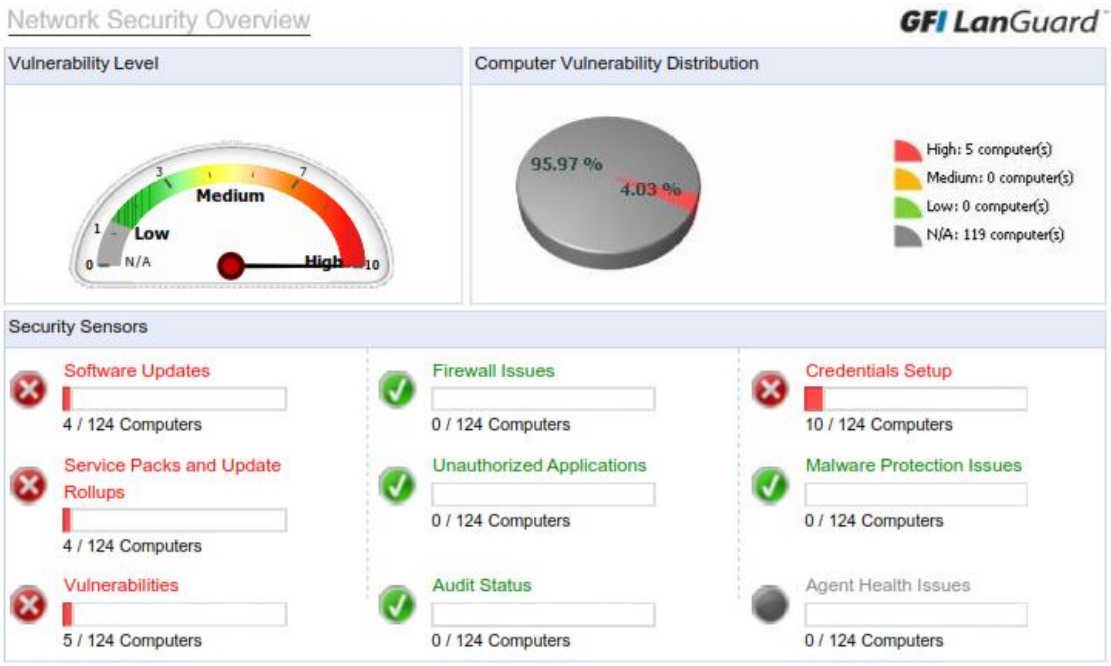
ANEXOS

1. ANEXO

GFI LanGuard

Network Security Overview

Description	An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and workstations.
Generated on	08/11/2016 11:20:08
Generated by	gustavo.lema
Advanced Settings	
Report items	All
Target	Entire Network;



Most Vulnerable Computers

- PHP-TEC-DES-011(192.168.213.1)
- PDS-DES-DIR-004(172.16.0.221)
- PAV-ING-DIR-001(172.16.0.191)
- PHP-TEC-DES-021(172.16.0.13)
- DGAC_COM_PC06(172.16.0.190)

Agent Status

- Installed: 0 computer(s)
- Install in Progress: 0 computer(s)
- Uninstall in Progress: 0 computer(s)
- Not Installed: 124 computer(s)
- Deployment Errors: 0 computer(s)

Audit Status

- Last 24 Hours: 124 computer(s)
- Last Week: 0 computer(s)
- Last Month: 0 computer(s)
- Older: 0 computer(s)

Vulnerability Trends Over Time

Computers by Network Role

- Server: 0 computer(s)
- Workstation: 20 computer(s)
- Mobile Device: 0 computer(s)
- N/A: 104 computer(s)

Computers by Operating System

- N/A: 99 computer(s)
- Windows XP: 17 computer(s)
- Windows 8.1 x64: 3 computer(s)
- Windows 7 x64: 2 computer(s)
- Windows 8: 1 computer(s)
- Windows 8 x64: 1 computer(s)
- Windows 7: 1 computer(s)

2. ANEXO

Vulnerability Status

Description	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Generated on	08/11/2016 11:22:56
Generated by	gustavo.lema
Advanced Settings	
Report items	All
Target	Entire Network;
Grouped by	'Computer' - Ascending AND 'Vulnerability Severity' - Descending
Sorted by	'Vulnerability Timestamp' - Ascending

Vulnerability Distribution by Severity

Vulnerability Distribution by Computer

Computer/IP	High	Medium	Low	Potential
DGAC_COM_PC06	214	20	5	3
PAV-ING-DIR-001	13	13	174	3
PDS-DES-DIR-004	86	10	155	3
PHP-TEC-DES-011	34	34	7	1
PHP-TEC-DES-021	7	1	8	6

Vulnerability Listing by Computer

DGAC_COM_PC06

High

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
AutoRun is enabled	N/A	High	-	2007-05-10
Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted.It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.				
Security Update for Office 2007 (KB934062)	Office	High	-	2007-05-15
Security Update for the 2007 Microsoft Office System (KB936514)	Office	High	-	2007-07-10
Security Update for Microsoft Office Excel 2007 (KB936509)	Office	High	-	2007-07-10
Security Update for Microsoft Office Publisher 2007 (KB936646)	Office	High	-	2007-07-10
Security Update for the 2007 Microsoft Office System (KB936960)	Office	High	-	2007-08-14
Security Update for Microsoft Office Outlook 2007 (KB946983)	Office	High	-	2008-03-11
Security Update for Microsoft Office Publisher 2007 (KB950114)	Office	High	-	2008-05-13
remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse schannel.dll that is located in the same folder as an ISP file.				

3. ANEXO

Full Audit

Description	A technical report containing all the information retrieved during an audit. Amongst others, the report contains information on, vulnerabilities, open ports, hardware and software.
Generated on	08/11/2016 11:27:00
Generated by	gustavo.lema

Advanced Settings

Report items	All
Target	Entire Network;

Computers Listing by Severity

Computer/IP	VL	OS	SP	Vulns.				Missing Security Updates	Missing Service Packs	Malware	Firewall Vulns.
				High	Medium	Low	Potential				
DGAC_COM_PC06			3	137	19	5	3	71	1	-	-
PAV-ING-DIR-001			3	13	13	174	3	-	-	-	-
PDS-DES-DIR-004			3	8	10	155	3	71	1	-	-
PHP-TEC-DES-011			Gold	7	34	7	1	24	1	-	-
PHP-TEC-DES-021			Gold	3	1	8	6	4	-	-	-
CNAC-007			-	-	-	-	0	-	-	-	-
CNAC-MSANCHEZ			-	-	-	-	0	-	-	-	-
COMUNICACION			-	-	-	-	0	-	-	-	-
DAC-ACF-RBAL			-	-	-	-	0	-	-	-	-
DAC-FAEDAC1			-	-	-	-	0	-	-	-	-
DAC-PC			-	-	-	-	0	-	-	-	-
DGAC_AUD_PC10			-	-	-	-	0	-	-	-	-
DGAC-9AF2C18C00			-	-	-	-	0	-	-	-	-
JURIDICA			-	-	-	-	0	-	-	-	-
PAV-ING-CON-002			-	-	-	-	0	-	-	-	-
PAV-ING-CON-003			-	-	-	-	0	-	-	-	-
PAV-ING-CON-004			-	-	-	-	0	-	-	-	-
PAV-ING-FIS-003			-	-	-	-	0	-	-	-	-
PAV-ING-PRO-001			-	-	-	-	0	-	-	-	-
PAV-ING-PRO-003			-	-	-	-	0	-	-	-	-
PAV-ING-PRO-004			-	-	-	-	0	-	-	-	-
PAV-ING-PRO-006			-	-	-	-	0	-	-	-	-

PHP-TEC-DES-011

Scan Errors

Context	Description	Timestamp
Enumerating installed applications.	Full security applications audit failed.	08/11/2016 10:04:54

Vulnerability Assessment

Missing Service Packs and Update Rollups

Vulnerability Name	Product	CVSS Score	Timestamp
Update for Windows 8.1 for x64-based Systems (KB3182203)	Windows	-	2016-09-20
Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2 x64 Edition - October 2016 (KB890830)	Windows	-	2016-10-11
Microsoft SQL Server 2012 Service Pack 3 (KB3072779)	SQL Server	-	2016-07-01
Update for Windows 8.1 for x64-based Systems (KB3192321)	Windows	-	2016-10-18

Missing Security Updates

High

Vulnerability Name	Product	CVSS Score	Timestamp
APSB15-24: Adobe Acrobat 10.1.16 Pro and Standard	Adobe Acrobat	-	2015-10-13
MS16-107: Security Update for Microsoft Outlook 2013 (KB3118280) 32-Bit Edition	Office	-	2016-09-13
MS16-107: Security Update for Microsoft Office 2013 (KB3118268) 32-Bit Edition	Office	-	2016-09-13
MS16-121: Security Update for Microsoft Word 2013 (KB3118345) 32-Bit Edition	Office	-	2016-10-13
MS16-107: Security Update for Microsoft PowerPoint 2013 (KB3115487) 32-Bit Edition	Office	-	2016-09-13
MS16-128: Security Update for Adobe Flash Player for Windows 8.1 for x64-based Systems (KB3201860)	Windows	-	2016-10-27
Security Update for Windows 8.1 for x64-based Systems (KB3174644)	Windows	-	2016-09-13
MS16-120: October, 2016 Security Only Quality Update for Windows 8.1 for x64-based Systems (KB3192392)	Windows	-	2016-10-11
MS16-127: Security Update for Adobe Flash Player for Windows 8.1 for x64-based Systems (KB3194343)	Windows	-	2016-10-11
MS16-035: Security Update for Microsoft .NET Framework 4.5.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3135994)	Windows	-	2016-10-11
MS16-114: Security Update for Windows 8.1 for x64-based Systems (KB3177186)	Windows	-	2016-09-13
MS16-120: October, 2016 Security and Quality Rollup for .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB3188743)	Windows	-	2016-10-11

4. ANEXO

Software Audit

Description	Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on antivirus, antispyware and includes an applications inventory.
Generated on	08/11/2016 14:00:27
Generated by	gustavo.lema

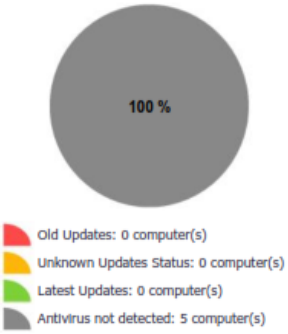
Advanced Settings

Report items	All
Target	Entire Network;
Grouped by	'Application Category' - Ascending AND 'Application Name' - Ascending
Sorted by	'Application Vendor' - Ascending

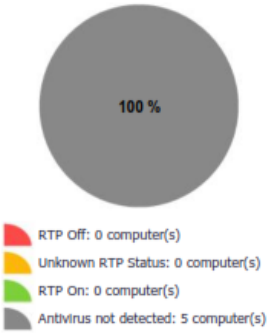
Antivirus Status

Antivirus Installation Status

Antivirus Updates Status

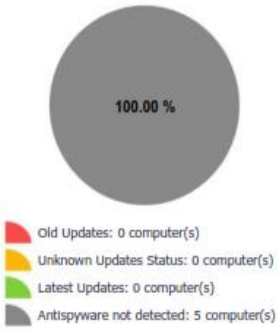


Antivirus Real Time Protection

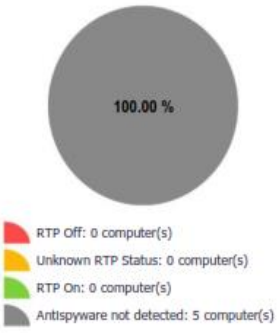


Antispyware Installation Status

Antispyware Updates Status



Antispyware Real Time Protection

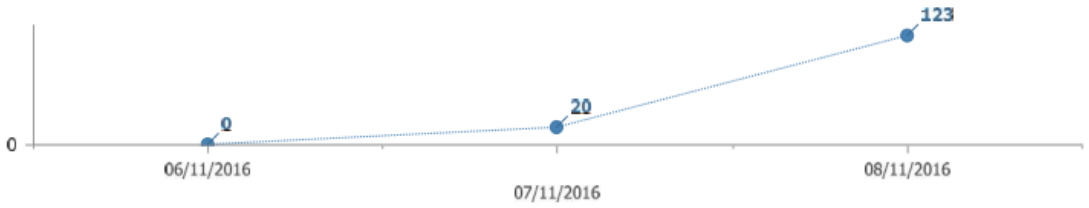


Computers without Antivirus Installed

Host Name	IP address	Operating System	SP
PHP-TEC-DES-011	192.168.213.1	Windows 8.1 x64	Gold
PDS-DES-DIR-004	172.16.0.221	Windows XP	3
PAV-ING-DIR-001	172.16.0.191	Windows XP	3
PHP-TEC-DES-021	172.16.0.13	Windows 8.1 x64	Gold
DGAC_COM_PC06	172.16.0.190	Windows XP	3

Applications Inventory

Computers Scanned per Day



Top 10 Most Scanned Computers

IP address	Host Name	Count
192.168.213.1	PHP-TEC-DES-011	3
172.16.0.3	PHP-TEC-DES-012	2
172.16.0.191	PAV-ING-DIR-001	2
172.16.1.37	PAV-SEG-DIR-008	2
172.16.1.48	PHP-REC-CAP-001	2
172.16.0.140	PAV-NAV-DIR-003	2
172.16.0.132	PDS-RE1-INF-004	2
172.16.0.213	PHP-SEC-SEC-003	2
172.16.0.221	PDS-DES-DIR-004	2
172.16.0.131	PAV-INS-OPE-001	2

5. ANEXO

Scan History

Description	An overview of the network security audits performed over time. Amongst others, the report includes information on the most scanned computers, the least scanned computers, auditing status and history listing.
Generated on	08/11/2016 14:29:23
Generated by	gustavo.lema
Advanced Settings	
Report items	All
Target	Entire Network;
Filters	Show History For Last Month

Top 10 Least Scanned Computers

IP address	Host Name	Count
172.16.0.155	PHA-REL-REL-006	1
172.16.0.106	CNAC-MSANCHEZ	1
172.16.1.0	PDS-RE1-NAV-007	1
172.16.0.216	PHP-FIN-TES-001	1
172.16.0.58	PAV-NAV-TRA-008	1
172.16.0.125	PAV-ING-PRO-006	1
172.16.0.1	PAV-NAV-CNS-005	1
172.16.0.12	DAC-PC	1
172.16.0.27	PDS-RE1-ING-007	1
172.16.0.168	PAV-INS-TRA-017	1

Nodes not audited last 30 days

6. ANEXO

Remediation History

Description	Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on remediation actions per day, remediation distribution by category and a remediation list grouped by computers.
Generated on	08/11/2016 14:30:04
Generated by	gustavo.lema

Advanced Settings

Report items	All
Target	Entire Network;
Filters	Show History For Last Month
Grouped by	'Computer' - Ascending AND 'Remediation Date' - Ascending
Sorted by	'Remediation Type' - Ascending

GFI LanGuard

Computers Remediated per Day

No records matching the current criteria were found!

Remediation Actions Distribution by Run Type

No records matching the current criteria were found!

Remediation Actions Distribution by Category

No records matching the current criteria were found!

Remediation Actions Distribution by Update Type

No records matching the current criteria were found!