ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA., UTILIZANDO LA NORMA ISO 27001:2013"

TRABAJO DE TITULACIÓN

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por

JOSEPH ALEXANDER GUAMAN SEIS

Guayaquil – Ecuador

2017

AGRADECIMIENTO

A Dios por bendecirme cada día de mi vida y permitirme cumplir este objetivo. A la Escuela Superior Politécnica del Litoral, a sus autoridades, profesores y facilitadores, un agradecimiento muy especial al Ing. Jorge Olaya Tapia y a la Mgs. Laura Ureta Arreaga por sus lineamientos, predisposición, paciencia y guía para la elaboración de este proyecto. A la Armada del Ecuador y al Comando Conjunto de las FF.AA. por el apoyo brindado en la consecución de este trabajo.

A mi familia por la paciencia e impulso en la culminación de este sueño.

DEDICATORIA

El presente trabajo lo dedico a mi Madre quien descansa en la paz del Señor desde el año 1976 junto a mis abuelitas Margarita y Petrona. A mi padre Rosendo, mis tíos, mis hermanas, mis sobrinos, mis primos y todos mis seres queridos que los llevo en mi corazón. A mi familia, a mi adorada hija Dafna Jordana quien me prestó el tiempo que le pertenecía y me motivó siempre con sus notitas “no te rindas”, “tu puedes” ¡Gracias mi muñeca de oro!, a Aníbal Sebastián y Franz Alexander que son mi inspiración, a todas aquellas personas que de una u otra forma colaboraron en la realización de este gran sueño hecho realidad…

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire Cobo
PRESIDENTE

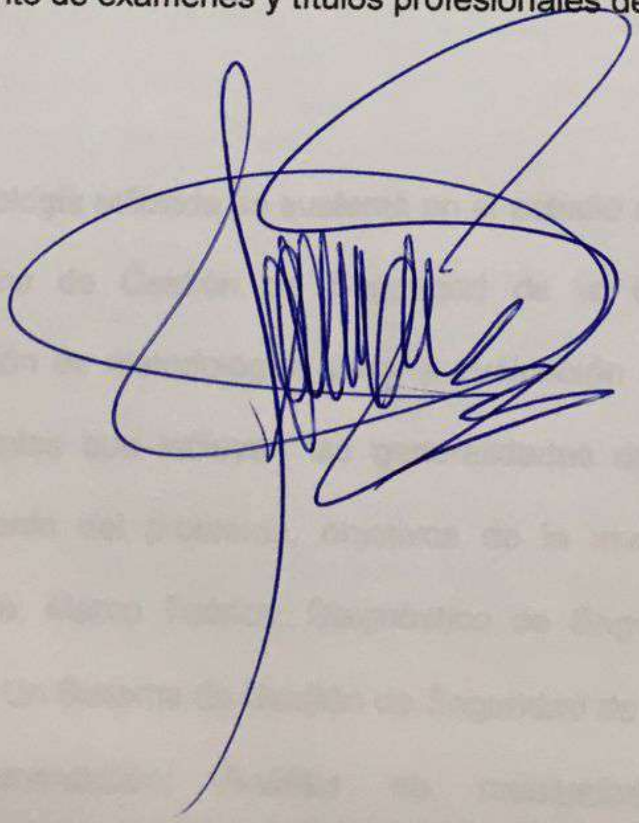
Ing. Jorge Olaya Tapia, PhD.
DIRECTOR DEL PROYECTO DE GRADUACIÓN

Mgs. Laura Ureta Arreaga
MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de exámenes y títulos profesionales de la ESPOL)



RESUMEN

El presente Proyecto de Titulación tiene como objetivo principal Diseñar un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con el fin de contribuir a la modernización de las Fuerzas Armadas.

La metodología utilizada se sustentó en el estudio diagnóstico y el Diseño de un Sistema de Gestión de Seguridad de la Información, usando una combinación de metodologías para la evaluación de los riesgos, consta de seis capítulos que incluyen las generalidades del proyecto como son el planteamiento del problema, objetivos de la investigación, justificación e importancia; Marco Teórico; Diagnóstico de Seguridad de la Información; Diseño de Un Sistema de Gestión de Seguridad de la Información; Propuesta de Implementación; Análisis de resultados; y, Conclusiones y Recomendaciones.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

COMACO	**:**	Comando Conjunto de las Fuerzas Armadas
DIRTIC	**:**	Dirección de Informática de la Armada
DTIC'S	**:**	Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto
FF.AA.	**:**	Fuerzas Armadas del Ecuador
SENAIN	:	Secretaría de Inteligencia del Ecuador
SGSI	**:**	Sistema de Gestión de Seguridad de la Información
TI	**:**	Tecnología de la Información
WEB	**:**	World Wide Web

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Proyecto de Titulación tiene como Objetivo Diseñar un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con el fin de contribuir a la modernización de las Fuerzas Armadas.

Se desarrolló bajo la modalidad de estudios de proyecto apoyado tanto en una investigación de campo como en la investigación monográfica documental que permitió la elaboración y desarrollo de una propuesta de un modelo operativo viable para solventar los problemas de seguridad de la información.

La metodología utilizada se sustentó en el estudio diagnóstico y el diseño de un Sistema de Gestión de Seguridad de la Información y usando una combinación de metodologías para la evaluación de los riesgos que ayude a la toma de decisión sobre las opciones de tratamiento de riesgo adecuado.

El Proyecto de Titulación consta de seis capítulos en los cuales se desarrolla cada tema que permite obtener, aplicar y conocer los resultados de la propuesta del diseño: el Capítulo 1, conformado por el planteamiento del problema, objetivos de la investigación, justificación e importancia, alcance y limitaciones del objeto de estudio. Capítulo 2, denominado Marco Teórico, que contiene los antecedentes de investigación, bases teóricas, bases legales. Capítulo 3, Diagnóstico de Seguridad de la Información, la recolección de datos, técnicas de análisis de datos, los resultados y observación directa. Capítulo 4, Diseño de Un Sistema de Gestión de Seguridad de la Información, el cual muestra la identificación del riesgo, análisis del el riesgo, valoración y evaluación. Capítulo 5, se exponen la propuesta de implementación y operación del Sistema. Capítulo 6, Análisis de

Resultados y finalmente las conclusiones y recomendaciones de del Proyecto.

CAPÍTULO 1

1. GENERALIDADES

1.1 Antecedente

La falta de control de seguridad de los recursos tecnológicos en las instituciones del Ecuador, es la causa principal para que se detecten errores, fraudes y serios problemas de seguridad, esto facilita el aumento desmesurado de los índices de delitos informáticos. [1], como se ilustra en la Figura 1.1.

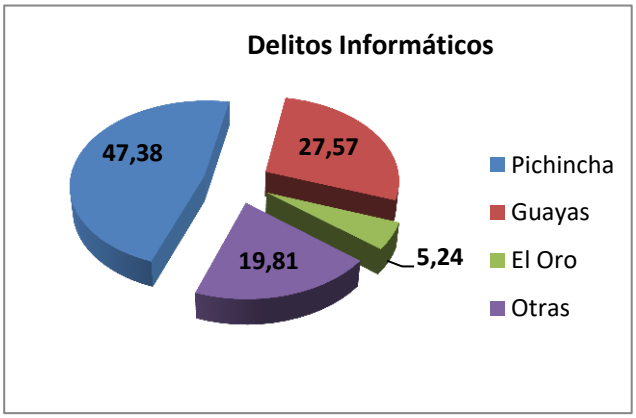


Figura 1.1 Provincias con mayor porcentaje de incidencias en delitos informáticos.

Fuente: http://www.fiscalia.gob.ec

La Fiscalía General del Estado, registra de enero a agosto del 2015 un total de 1026 denuncias por delitos informáticos en el Ecuador, según cifras del Ministerio Público, la mayoría es de apropiación fraudulenta por medios electrónicos (646), luego el fraude por medios electrónicos con inutilización de alarmas, descifrado de claves o encriptados (147). También está el acceso no consentido a un sistema informático, telemático o telecomunicación (91) y también existen otros tipos de denuncias. El delito informático o ciberdelito se relaciona con actividades delincuenciales típicas como: robos, estafas, falsificaciones, sabotaje, [2].

Hoy en día, uno de los temas de mayor importancia y trascendencia de toda la sociedad, es la seguridad y resguardo de la información de las instituciones, más aun el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las Fuerzas Armadas que maneja información militar secreta y clasificada[1].

En la actualidad, la filtración de llamadas telefónicas, documentos e información confidencial de Instituciones del Ecuador ha provocado problemas muy serios, a pesar de que la Secretaría de Inteligencia del Ecuador (SENAIN) ha ratificado que desde esa entidad no se realiza espionaje, sino que se trabaja de forma coordinada con la Fiscalía General del Estado para combatir el crimen organizado en el país, [3].

Debido a que las amenazas provienen de diversos orígenes, algunos sin poder ser anticipados se tiene la necesidad urgente del Diseño de un Sistema de Seguridad de la Información para precautelar los datos tan sensibles del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las Fuerzas Armadas.

[1] (COMACO) Manual de Elaboración de Documentación de las Fuerzas Armadas.

1.2 Descripción del Problema

Las Fuerzas Armadas posee el Sistema de Comunicaciones Militares (SC)[2], que es una infraestructura informática que interconecta a los repartos navales y militares de las Fuerzas Armadas, que es utilizada para trasmitir información (voz, datos y video), servicios automatizados y sistemas corporativos, [4].

La utilización de los servicios y sistemas corporativos a través del Sistema de Comunicaciones Militares y el acceso indebido a la información en determinadas redes locales, requieren la implementación de seguridades para el uso de estos servicios por los usuarios de los repartos navales y militares.

Se ha detectado accesos indebidos a las redes administrativas debido a los diferentes puntos de internet que existen, la falta de implementación de políticas de seguridad, evaluación de los riesgo e implementación de controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información; así, como el limitado personal especializado existente para implementar tales políticas.

Es necesario realizar el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección

[2] D.G.P. COGMAR-INF-002-2010-O; 12-JUL-2010. Directiva de Seguridad de la Información. Es una infraestructura de intranet que utiliza las Fuerzas Armadas a nivel nacional.

de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, que minimicen los riesgos físicos y lógicos de la información que se transmite, procesa, almacena y distribuye a través del Sistema de Comunicaciones, para la utilización de los servicios y sistemas por los usuarios de los repartos militares y navales.

1.3 Solución Propuesta

La presente propuesta, permitirá efectuar el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., basado en la norma ISO/IEC 27001:2013 para los sistemas de información.

Se realizará la evaluación de los riesgos de seguridad de la información del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del COMACO, para determinar la necesidad de realizar el Diseño de un Sistema de Gestión de Seguridad de la Información, mediante el análisis general de la situación actual de la seguridad de la información para los sistemas de información.

Finalmente se realizará el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la

Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. utilizando la norma ISO 27001:2013.

Al realizar el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. utilizando la norma ISO 27001:2013, permitirá que los riesgos de la seguridad de la información sean asumidos, gestionados y minimizados por la Institución de una forma evaluada, documentada y estructurada.

Para el diseño se utilizará las normas ISO/IEC 27001:2013, que permita aplicar controles, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información, [5].

El Diseño del Sistema de Gestión Seguridad del Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, establecerá nuevas políticas de seguridad, reglas, planes y acciones para asegurar la información y mejorar la gestión de la seguridad, socializando con los miembros de la Institución la importancia y sensibilidad de la información y la seguridad.

Debido a la estructura organizacional de las Fuerzas Armadas, el ámbito de aplicación del presente trabajo, alcanza a repartos militares

donde existe una relación jerárquica militar o de subordinación, la metodología que en él se propone se centra en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones, subordinada al Comando Conjunto de las FF.AA., en la que aportará aspectos metodológicos, lineamientos y políticas de seguridad de la información para la institución.

En cuanto a las limitaciones es importante tomar en cuenta que los aspectos que conforman la confidencialidad de la información en las Fuerzas Armadas son un factor importante en el desarrollo de la investigación y es por eso que la información mostrada del Comando Conjunto de las FF.AA. y de la Dirección de Tecnologías de la Información y Comunicaciones es referencial y solo para efectos académicos respectivos, en vista que la información militar[3] es secreta y confidencial.

Para la implementación, operación, revisión, mantenimiento y mejora del Sistema Gestión de Seguridad del Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, sólo se especificará los lineamientos generales.

[3] (COMACO) Manual de Elaboración de Documentación de las Fuerzas Armadas.

1.4 Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013, que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con el fin de contribuir a la modernización de las Fuerzas Armadas.

1.5 Objetivo Específicos

Los objetivos específicos para este trabajo son:

1. Evaluar los riesgos de seguridad de la información del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

2. Analizar los requerimientos de seguridad de la información.

3. Diseñar un Sistema de Gestión de Seguridad de Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

4. Realizar una propuesta de implementación y operación del Sistema de Gestión de Seguridad de Información para el Departamento

de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

1.6 Metodología

La investigación parte desde un enfoque predominantemente cuantitativo bajo modalidades de investigación de campo y bibliográfica-documental, con un tipo de investigación exploratoria-descriptiva que será aplicada en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones, lo que nos permitirá diseñar un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

El paso del plano abstracto al plano operativo de la investigación se lo realizará a través de la construcción de matrices de operativización de las variables de la hipótesis de trabajo formulada, mismas que contendrán las variables objeto de la investigación, su definición conceptual, dimensiones, indicadores, ítems básicos y técnicas e instrumentos. Lo que nos permitirá la elaboración de los cuestionarios correspondientes para su aplicación.

Para obtener la información del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. se aplicarán los cuestionarios

respectivos, previa a la gestión administrativa que se realice con el Departamento correspondiente de la Dirección de Tecnologías de la Información y Comunicaciones del COMACO. Una vez conseguida la información se procederá a su revisión y preparación para su procesamiento utilizando la estadística descriptiva.

Las conclusiones y recomendaciones del trabajo realizado utilizarán deducción e inducción apoyadas también en el método empírico.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1 Bases Teóricas

El presente trabajo tiene como objeto establecer el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., utilizando la norma ISO 27001:2013.

Se trabajará en base a los conceptos establecidos que son: Seguridad Informática, Seguridad en los Sistemas Informáticos, Propiedades de la

Seguridad Informática, Objetivos de la Seguridad, Términos de Riesgos, Factores de Riesgos, Análisis del Riesgo y su Evaluación, Medidas de Seguridad, Estandarización y Seguridad de las Tecnología de Información, Sistema de Gestión de Seguridad de la Información y Herramientas para el Análisis de Riesgo.

2.1.1 Seguridad Informática

Define a la seguridad como los medios informáticos en los que se genera, gestiona, almacena o destruye esta información, susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o institucional, por lo cual la información es el elemento principal a proteger, resguardar y recuperar en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones, [6].

Para profundizar en la seguridad informática, es necesario tomar en cuenta las siguientes definiciones:

Activo: Cualquier cosa que tenga valor para la organización, que funcione correctamente y alcance los objetivos propuestos, [5].

Amenaza: Es la causa potencial de un daño a un activo de información que puede desencadenar un incidente en la

organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto: Nivel de afectación en el activo de información que se genera al existir el riesgo, Consecuencias de que la amenaza ocurra.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Desastre: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la normal operación de un proceso.

Riesgo y vulnerabilidad se podrían incluir en un mismo concepto, la vulnerabilidad está ligada a una amenaza y el riesgo a un impacto.

En el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando

Conjunto de las FF.AA. se protegerá la información que se trasmite a través del Sistema de Comunicaciones Militares para la utilización de los Sistemas y servicios Informáticos por parte de los usuarios de los Repartos Navales y Militares

2.1.2 Seguridad en los Sistemas Informáticos

Define que la seguridad en los sistemas informáticos consiste en asegurar que los recursos del sistema de información como material informático o programas de una organización sean utilizados de la manera que se planificó y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, [7].

La seguridad en los sistemas informáticos tiene por objetivo utilizar herramientas para verificar los sistemas informáticos que deben ser protegidos desde el punto de vista lógico y físico con un conjunto de soluciones técnicas, métodos y planes de seguridad para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático, [7].

Es importante indicar que en las instituciones verificar la seguridad informática genera un costo y se debe estar consciente de que la seguridad absoluta es imposible, por lo

cual la seguridad en los sistemas informáticos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del COMACO, indicará claramente el nivel de seguridad que se quiere alcanzar.

2.1.3 Propiedad de la Seguridad Informática

Establece que para lograr los objetivos de la seguridad informática se debe tomar en cuenta las definiciones sobre los atributos o propiedades principales que debe cumplir todo sistema informático, [6].

Confidencialidad: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados.

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

2.1.4 Objetivos de la Seguridad Informática

El Objetivo de la en seguridad informática es garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información, mediante normas, procedimientos y herramientas. Al respecto señala los objetivos que se deben llevar a cabo, [4].

Autenticación de usuarios: Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema informático, la red o accede a una base de datos, es posible autenticarse de tres maneras: Por lo que uno sabe (una contraseña), Por lo que uno tiene (una tarjeta magnética) y Por lo que uno es (las huellas digitales o biométricas).

Autorización: Que controla el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.

Auditoría: Verifica el correcto funcionamiento de las políticas o medidas de seguridad tomadas.

Encriptación: Ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.

Copias de seguridad e imágenes de respaldo: Contingencia para que en caso de fallos nos permita la recuperación de la información perdida o dañada.

Antivirus: Programas que permite estar protegido contra las amenazas de los virus.

Cortafuegos o firewall: Programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.

Servidores proxys: Ordenadores con software especial, que hacen de intermediario entre la red interna de una institución y una red externa, como pueda ser Internet. Estos servidores,

entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios.

Utilización firma electrónica o certificado digital: Mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos.

Conjunto de leyes: Encaminadas a la protección de datos personales que obligan a las empresas a asegurar la confidencialidad.

2.1.5 Término de Riesgo

Los riesgos informáticos son procesos que deben ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, y también como una función esencial de administración por parte de toda la organización, por lo cual es necesario aclarar los siguientes términos, [6].

a) Valorización del riesgo: Consiste en analizar las amenazas de los sistemas informáticos, las vulnerabilidades del mismo y el impacto potencial si se concretan dichas amenazas, [5].

b) Evaluación del riesgo: Comprende la identificación de activos informáticos sus vulnerabilidades y amenazas a los que se encuentran expuestos de esta manera poder así evaluar su probabilidad de ocurrencia y el impacto que generaría, con el fin de determinar, los controles adecuados para calcular, aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, [5].

c) Análisis de riesgo: Es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management), es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado, [5].

d) Gestión de riesgo: La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo como eliminar el riesgo, compartir el riesgo o aceptar el riesgo, [5].

2.1.6 Factores de Riesgo

Define que es el riesgo constituye un evento o condición con cierta incertidumbre y si este ocurre tiene un efecto positivo o negativo en los objetivos de una Institución, [6].

Hoy en día la mayoría de las empresas soportan sus procesos operativos con TI. Se ha generado un alto grado de dependencia de la tecnología informática. Las organizaciones tienen una elevada inversión en tecnología, por su adquisición, mantenimiento y seguridad.

Es importante recalcar que los factores de riesgos se clasifican en:

Ambientales/Físicos o de Operatividad: Lluvias, Inundaciones, terremotos, Tormentas, rayos, calor, entre otros.

Tecnológicos o de Integridad: Falla de hardware y/o Software, falla en el servicio eléctrico ataque por virus informáticos, etc.

Humanos o de Confiabilidad: Hurto adulteración, fraude, revelación, sabotaje, Crackers, Hackers, Robo de Contraseñas, entre otros.

Los riegos relacionados con la informática son:

1. Riesgos de Integridad
2. Riesgos de Relación
3. Riesgos de Acceso

4. Riesgos de Utilidad

5. Riesgos de Infraestructura

6. Otros Riesgos

2.1.7 Análisis de Riesgo y su Evaluación

Es necesario para una institución realizar una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, [5]. Una vez que se tenga clara esta identificación de riesgos, se podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información, [6].

Actualmente existen muchas metodologías para la gestión de riesgos en las instituciones, partiendo de la identificación de activos de información, centrándose en todos aquellos recursos involucrados en la gestión de la información como datos, hardware, documentos escritos y recurso humano, sobre cual se realizará la identificación de las amenazas o riesgos y las vulnerabilidades.

Para que la institución decida cómo actuar ante los diferentes riesgos es necesario realizar una valoración de riesgos para

determinar cuáles son los más críticos para la institución, en términos de la posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo.

La valoración del impacto puede medirse en función de varios factores en la institución: la pérdida económica si es posible cuantificar la cantidad de dinero que se pierde; la reputación de la empresa dependiendo si el riesgo pueda afectar la imagen de la institución; y, de acuerdo al nivel de afectación por la pérdida o daño de la información.

Se puede afrontar un riesgo de cuatro formas:

Aceptarlo: Ser consciente de que el riesgo existe y hacer un monitoreo sobre él.

Transferirlo: Tomar algún tipo de seguro que reduzca el monto de una eventual pérdida.

Mitigarlo: Implementación de medidas preventivas o correctivas para reducir la posibilidad de ocurrencia o el impacto del riesgo.

Evitarlo: Eliminar los activos de información o la actividad asociada, si el nivel de riesgo es demasiado alto para que la institución lo asuma.

2.2 Sistema de Gestión de Seguridad de la Información

Define al Sistema de Gestión de Seguridad de la Información, como el sistema de gestión global que permite preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo, [5].

El Sistema de Gestión de Seguridad de la Información por ser un proceso continuo se debe revisar y mantener periódicamente, por lo cual la gestión de la seguridad de la información constituye un conjunto de mecanismos compuestos por distintos factores y elementos como el planeamiento, la asignación, la evaluación y la auditoría, [6].

En el Sistema de Gestión de Seguridad de la Información se debe diseñar, implementar y mantener una serie de procesos que permitan gestionar de manera eficiente la información para asegurar su integridad, confidencialidad y disponibilidad**,** con estándares confiables y funcionales, creando un modelo propio de gestión para que el sistema sea eficiente, [6].

2.2.1 Iso/Iec 27001:2013

Es un conjunto de lineamientos que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), [5].

El origen es británico y en el año 2005, la Organización Internacional para la Normalización (ISO) la oficializó como norma. La Figura 2.1, muestra la historia de la ISO 27001 a lo largo del tiempo.

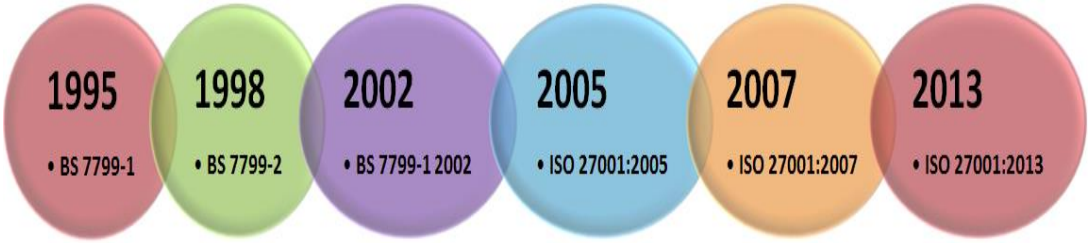


Figura 2.1 Historia de ISO 27001.

Fuente: http://www.iso27000.es

La revisión de la familia de normas ISO 27000 e ISO/IEC 27001, tuvo que acoplarse con otras normas como ISO/IEC 27003 que es una guía de implementación del SGSI; ISO/IEC 27004 con información de acerca del monitoreo y las mediciones sobre el SGSI y la ISO/IEC 27005 con todos los lineamientos para gestión de riesgos de seguridad de la información, como se muestra en la Figura 2.2.

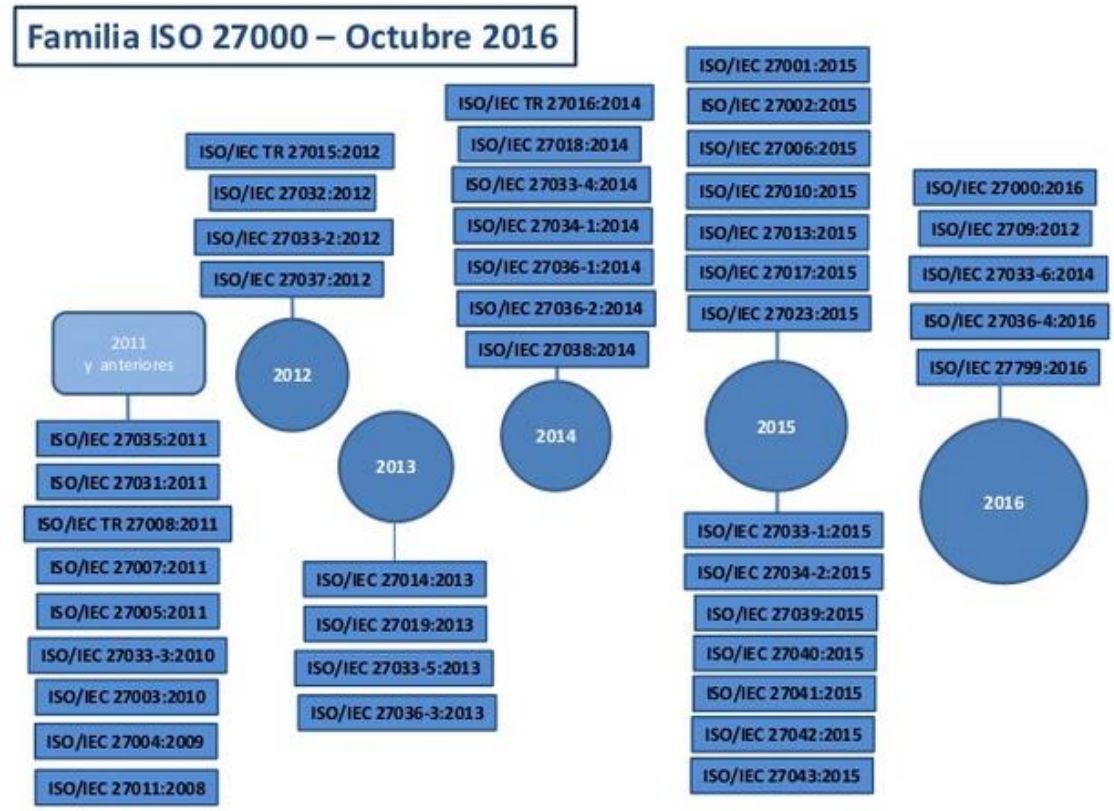


Figura 2.2 Familia de estándares de la ISO 27000.

Fuente: http://www.iso27000.es

Esta norma adopta el modelo “Planificar – Hacer – Verificar – Actuar” (PHVA), el cual es aplicado para estructurar todos los procesos del SGSI, la Figura 2.3, ilustra cómo un SGSI toma como entrada los requisitos y expectativas de seguridad de la información.

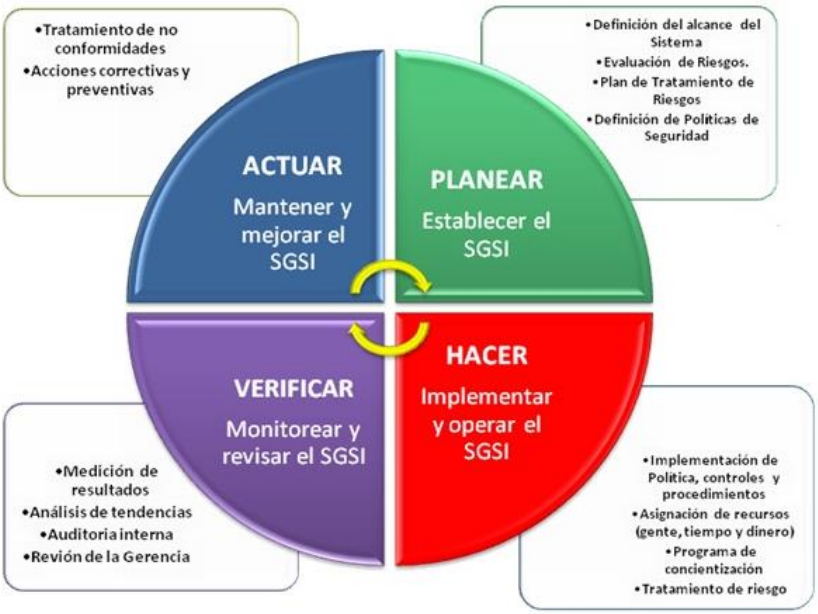


Figura 2.3 Modelo de PHVA del SGSI. ISO/IEC 27001:2013.

Fuente: http://www.iso27000.es

En la Figura 2.4, se ilustra la presentación de los distintos componentes del modelo ISO 27001:2013, el modelo está concebido para que opere con base en insumos provenientes de clientes, proveedores, usuarios, accionistas, socios y otras partes interesadas.

El modelo ISO 27001:2013, en su óptica de procesos, también permite que cada organización influencie el desempeño del

modelo a través de consideraciones estratégicas, tales como objetivos y políticas.

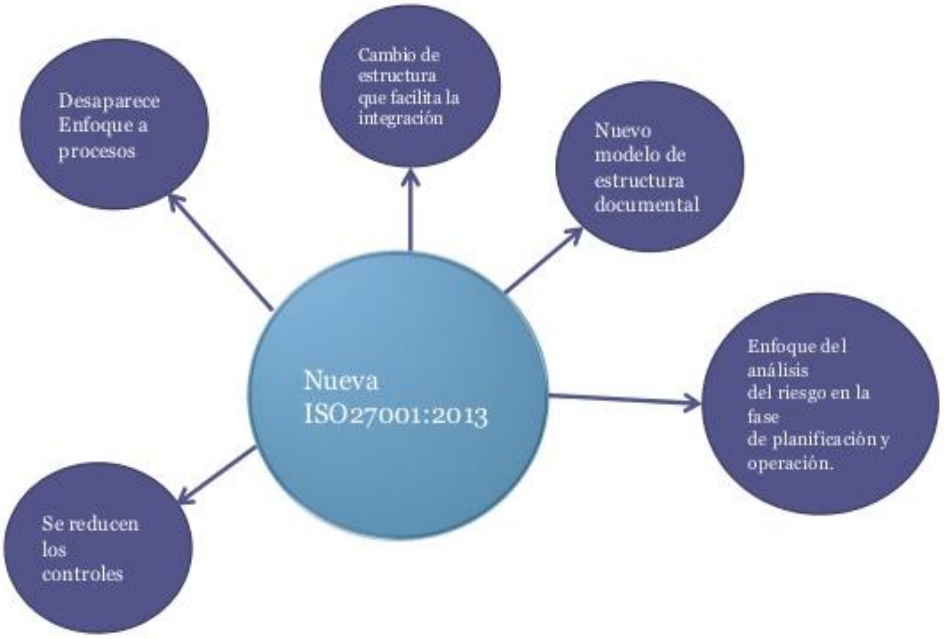


Figura 2.4 Enfoque del ISO 27001:2013

Fuente: http://www.iso27000.es

2.2.2 Herramientas para el Análisis de Riesgo

Existen varias herramientas propietarias y de libre acceso para realizar el análisis de riesgos como CRAMM, COBRA, RA2 Art of Risk, MAGERIT, OCTAVE, Threat and Risk Assesment

Working Guide (Canadá), Guideline del NSW de Australia y El IT Baseline Protección Model del BSI Alemán.

Herramientas propietarias.

CRAMM: Es la metodología de análisis de riesgos desarrollado por la **Agencia Central de Comunicación y Telecomunicación** del gobierno británico. El significado del acrónimo proviene de **CCTA Risk Analysis and Management Method**. Su versión inicial data de 1987, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento, [8]. Tiene tres partes:

1. Valorización de activos, en escala de 1 a 10.

2. Evaluación de amenazas y vulnerabilidades. Niveles de 1 a 5 para las amenazas, y de 1 a 3 para las vulnerabilidades.

3. Cálculo del riesgo, de 1 a 7 según una matriz. Más de 3000 contramedidas estructuradas en la base de datos y que pueden priorizarse.

COBRA: (Análisis de Riesgo Objetivo y Bifuncional), desarrollada por C & A Systems en cooperación con

instituciones financieras. Especialmente prevista para verificar el cumplimiento de la norma ISO 27001, provee un completo análisis de riesgo, compatible con la mayoría de las metodologías conocidas cualitativas y cuantitativas.

Lo forman varios programas: Risk Consultant, el principal, incluyen las bases de conocimiento que se personalizan y modifican con el Module Manager.

RA2 Art of Risk: Producto de Aexis y Xisec trabaja con análisis cualitativo de riesgo basado en modelado estadístico. Desarrollado conforme la ISO 17799 y la ISO 27001, usa también los principios contenidos en la MICTS2.

Permite seleccionar los controles ISO 17799 y producir evidencia a los auditores que se han llevado a cabo los pasos de la ISO 27001 para certificación. Produce directamente el SoA adecuado para la certificación ISO 27001.

MAGERIT: Del Ministerio de las Administraciones Públicas (MAP) de España. La aplicación se puede ver en cuatro etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas. En la versión 2.0, la documentación consta de tres partes:

1. Método. Análisis y gestión de riesgos, proyectos.

2. Catálogo de Elementos. Amenazas y salvaguardas.

3. Guía de Técnicas. Tipo de análisis, diagramas, planificación de proyectos.

Herramientas de libre acceso.

OCTAVE: Evaluación de factores operacionalmente críticos: amenazas, activos de sistemas y personal, y vulnerabilidades. Hay dos versiones: Octave y Octave-S (Small, pequeñas empresas); éste último para equipos pequeños de personal de seguridad. El Octave-S define una técnica de valuación basada en riesgos, desarrollada en 10 volúmenes. El proceso incluye tres fases:

1. Construcción de perfiles de amenazas en base a los activos
2. Identificación de la infraestructura de las vulnerabilidades.
3. Desarrollo de la estrategia y planes de seguridad.

Threat and Risk Assesment Working Guide (Canadá): Considera vulnerabilidades de sistemas, personal, objetos y externas, con cinco niveles como resultado de tres niveles de severidad y tres de exposición. Trabaja con cinco niveles de

amenazas, caracterizando los agentes de amenazas en tres niveles de capacidad y otros tres de motivación- incorpora los escenarios de amenazas, donde estipula analizar el impacto en función de la sensibilidad de los activos y tasa de vulnerabilidad, así como de la frecuencia de ocurrencia. No define bien los riesgos finales.

Guideline del NSW de Australia: Tiene tres partes principales.

1. Revisión del proceso de gestión de riesgo, ejemplo de amenazas y vulnerabilidades y una guía para la selección de los controles de seguridad.
2. Incluye una tabla que relaciona cada control de la norma ISO 17799:2000 con diferentes tipos de control: protección, prevención, detección, respuesta y recuperación.
3. Tabla que relaciona cada control con los parámetros CIA: Confidencialidad, Integridad y Disponibilidad, así como también con la Autenticación, Responsabilidad y Confiabilidad.

El IT Baseline Protección Model del BSI Alemán: Permite establecer los riesgos en base a los activos, amenazas y contramedidas. No trabaja directamente con vulnerabilidades. Esta herramientas clasifica los activos en 35 tipos en 7

categorías; las amenazas en un total de 200 con cinco tipos: Fuerza mayor, Deficiencias organizacionales, Fallas humanas, Fallas técnicas y Actos deliberados; y, Contramedidas: Unos 600 de diferentes tipos. Además incluye una tabla de contramedidas vs. Amenazas.

En relación a lo antes expuesto y para efecto de esta investigación en la cual se realizará el análisis de riesgo en las Instituciones Militares, utilizaremos las herramientas CRAMM y BSI Alemán.

2.3 Bases Legales

Los planteamientos legales se basaron en los lineamientos, normas, procedimientos y estándares que establecen los artículos que tienen correspondencia con esta investigación.

2.3.1 Estándares Internacionales

ISO/IEC 27001:2013 – Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos, [5].

ISO/IEC 27001:2005 – Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información, [9].

ISO/IEC 17799:2005 – Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información Organización Internacional de Estándares (ISO), [10].

2.3.2 Leyes Nacionales

NTE INEN - ISO/IEC 27002:2009 – Tecnologías de la Información– Técnicas de Seguridad – Código de Práctica para la Gestión de la Seguridad de la Información, [11].

2.3.3 Normativa Interna

D.G.P. COGMAR-INF-002-2010-O – 12 de Julio del 2010 – Directiva General Permanente Seguridad de la Información, [12].

COMACO. 2012 – Comando Conjunto de las Fuerzas Armadas – Estatuto Orgánico por Procesos, [13].

CAPÍTULO 3

DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA.

3.1 Diagnóstico.

En esta fase se realizará el análisis general de la situación actual de la seguridad de la información en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

Se desarrollaron las primeras etapas de la metodología de análisis de información, a través de la aplicación de una investigación de campo al

personal que labora en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

El Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se encuentra conformada por las siguientes Divisiones: Dirección, Subdirección, Departamento de Software, Departamento de Servicios, Departamento de Plataformas Tecnológicas, Departamento de Seguridad e Investigación, [14].

3.2 Población y Muestra.

Define a un universo como "el conjunto de sujetos o elementos que tienen una característica común, observable y susceptible de ser medida", población "Es el total de mediciones o conteo de una característica común asociada a un conjunto bien definido de individuos u objetos", y a la muestra como "un subgrupo de la población de interés sobre el cual se recolectarán datos, y que tiene que definirse o delimitarse de antemano con precisión, éste deberá ser representativo de dicha población". Para seleccionar la población, es necesario considerar cuál será la unidad de análisis, lo que permitirá definir con qué elementos (personas) se va a trabajar, [9].

En la presente investigación la población que determinó la necesidad de realizar diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se encuentra constituido por cincuenta y uno (51) empleados que laboran en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., de acuerdo a lo que se ilustra en el Tabla 1.

Además se señala que "…si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra…". De acuerdo a esto podemos determinar que la muestra para nuestro proyecto es aquella representada por la totalidad de los individuos que permiten obtener información sobre el tema a investigar, [9].

Tabla 1 Descripción de la Población de la DTIC´S.

Fuente: Autor

Departamento u Oficina	Cantidad Personas
DTIC´S DEL CC.FF.AA.	
DIRECCIÓN	2
Departamento de Software	3
Sección Software Administrativo	2

Sección Software Operativo	5
Departamento de Servicios	3
Sección Servicios Especiales	5
Sección Servicios de Internet	4
Sección Configuración de Servicios	4
Sección Servicios de Aplicaciones	4
Sección Servicios de Mantenimiento de Hardware	5
Departamento de Plataformas Tecnológicas	3
Sección Administración de Servidores	6
Departamento de Seguridad e Investigación	5
Total	**51**

En la Tabla 1, se describe que los sujetos de estudio de la presente investigación se encuentran conformado por cincuenta y uno (51) personas que laboran en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

3.3 Técnicas e Instrumentos de Recolección de Datos.

Para este proyecto se realizó la recolección de información en forma directa a fin de diagnosticar como se encuentra la seguridad de la información en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., [9] determina que una técnica es un

procedimiento estandarizado que se ha utilizado con éxito en el ámbito de la ciencia.

Además se determina que el instrumento de recolección de datos es un dispositivo de sustrato material que sirve para registrar los datos obtenidos a través de las diferentes fuentes. Así como un cuestionario consiste en *"Un conjunto de preguntas respecto a una o más variables a medir relacionadas con los indicadores que se obtienen de la operacionalización de los objetivos específicos.",* [9].

Para obtener la información se elaboró el instrumento en función de los objetivos definidos en la presente investigación, con el propósito de interrogar a los sujetos de estudio, a través de un cuestionario estructurado con preguntas cerradas.

El cuestionario consta de cuarenta y cuatro (44) ítems de acuerdo a como se indica en el **Anexo "C"**, con opciones de respuestas en un formato de escala tipo Likert; Siempre (S), Casi Siempre (CS) Algunas veces (AV), Casi Nunca (CN) y Nunca (N), con el fin de diagnosticar cómo se encuentra la Seguridad de la Información en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

Las preguntas desarrolladas y verificadas cubren todos los aspectos de riesgos y amenazas a la confiabilidad, integridad y la disponibilidad de

la información y están basadas en los requerimientos de la institución, pero para realizar un ordenamiento se tomó en cuenta los objetivos de control de la ISO 27001:20013, [5].

1. Políticas de seguridad de la Información
2. Organización de la Seguridad de la Información
3. Seguridad de los Recursos Humanos
4. Gestión de los Activos.
5. Control de Acceso
6. Criptografía
7. Seguridad Física y Medioambiental
8. Seguridad de las Operaciones
9. Seguridad de las Comunicaciones
10. Adquisición, desarrollo y mantenimiento del sistema
11. Relación con los proveedores
12. Gestión de los incidentes de Seguridad de la Información
13. Gestión de los aspectos de Seguridad de la Información para la continuidad del negocio

14. Cumplimiento

En este Proyecto por la naturaleza del estudio y en función de los datos que se requieren en la investigación, se utilizó la técnica de observación directa, no participante y sistemática en la realidad, [9], indica que “la observación requiere de una mayor precisión en cuanto al análisis y clasificación de su contenido y consiste en el registro sistemático, válido y confiable de comportamiento”.

Se determina que en la observación no participativa “el investigador asumirá un papel de espectador de los hechos, del conjunto de actividades y relaciones laborales que se producen cotidianamente”; y, que el termino sistemático se refiere a que “se observa todo lo relativo a los antecedentes, forma, duración y frecuencia en que se originan los mismos”, [9].

3.4 Validez del Instrumento

Define que “los instrumentos de mediciones científicas deben dar lecturas no sesgadas con un muy pequeño error de medición”, La validez de contenido se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se mide, [10].

La validez de constructo indica al grado en que una medición se relaciona consistentemente con otras, de acuerdo con varias hipótesis

derivadas teóricamente sobre esa variable, por lo cual se considera un constructo como una variable medida dentro de un esquema teórico, [10].

Para determinar la validez del instrumento se utilizó la técnica de juicio de expertos, donde se eligieron cuatro especialistas, Ingenieros en Sistemas con títulos de Magíster, versados en el tema, quienes a través de un formato de validación como se ilustra en el **Anexo D**.

La técnica de juicio de expertos se utilizó con la finalidad de modificar la redacción de los ítems y determinar la existencia o no de ambigüedad en la redacción de los mismos, buscando la mayor claridad, congruencia y pertinencia posible, [17].

Luego de las correcciones y recomendaciones del caso se procedió a la elaboración del instrumento definitivo a ser aplicado a los sujetos de la muestra.

3.5 Confiabilidad del Instrumento

La referencia [9] considera que la confiabilidad de un instrumento de medición, es “el grado en que su aplicación repetida al mismo sujeto u objeto, produce iguales resultados”.

En este proyecto, la confiabilidad del instrumento se determinó previa aplicación a un grupo de cincuenta y uno (51) personas, perteneciente al Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. y a las diferentes Divisiones.

Al obtener los resultados se procesaron estadísticamente mediante el método Alpha de Cronbach, debido a que es el método que más se adapta en los casos de la medición de constructos a través de escalas, allí no existen respuestas correctas ni incorrectas, el sujeto que realiza la encuesta marca el valor de la escala que considera representa mejor su punto de vista.

El coeficiente Alpha de Cronbach indica la capacidad que tiene el instrumento para arrojar resultados similares en repetidas ocasiones.

Para determinar el resultado del coeficiente Alpha de Cronbach se emplea la siguiente fórmula:

FÓRMULA

$$\boldsymbol{\alpha} = \left(\frac{\boldsymbol{k}}{\boldsymbol{k-1}}\right) * \left(\mathbf{1} - \frac{\sum \boldsymbol{Si^2}}{\boldsymbol{St^2}}\right)$$

Dónde:

$\sum \mathbf{Si^2}$ Es la sumatoria de la varianza por ítems.

$\mathbf{St^2}$ Es la varianza total.

$\boldsymbol{k}$ Es el número de preguntas o ítems.

Para este proyecto el índice de confiabilidad debe ser menor o igual a uno (1) para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la exactitud y objetividad en los resultados. En [9] sugiere las recomendaciones siguientes para especificar los criterios establecidos para el análisis del coeficiente de Alpha de Cronbach:

Tabla 2 Criterios de Confiabilidad.

Fuente: Autor

Valores de Alpha	Criterios
De –1 a 0	No es confiable
De 0.01 a 0.49	Baja confiabilidad
De 0.50 a 0. 75	Moderada confiabilidad
De 0.76 a 0.89	Fuerte confiabilidad
De 0.90 a 1.00	Alta confiabilidad

Luego de aplicar el método Alpha de Cronbach como se indica en el **Anexo E**, se obtuvo una confiabilidad de 0,96 lo cual indica que es altamente confiable.

3.6 Técnicas de Análisis de los Datos

La técnica de análisis de datos que se utilizó es el método de Análisis Exploratorio o Estadística Descriptiva, el mismo que ayuda a comprender la estructura de los datos, detectar tanto un patrón de comportamiento general así como comportamiento individual del mismo. Una forma de realizar esto es mediante gráficos. Otra forma de describir los datos es resumiendo los datos en uno, dos o más números que caractericen al conjunto de datos con fidelidad. En [9] indica que esta técnica permite explorar los datos, detectar datos erróneos o inesperados y nos ayudan a decidir qué métodos estadísticos pueden ser empleados en etapas posteriores del análisis de manera de obtener conclusiones válidas.

Al obtener los resultados de los datos, producto de la aplicación del instrumento se procedió a su ordenación para analizarlos mediante el análisis exploratorio o estadística descriptiva. En [9] señala como “el uso de bases estadísticas de frecuencias y porcentajes; complementados con cuadros y gráficos estadísticos con sus respectivos análisis”

3.7 Resultados

Para este proyecto se presenta los resultados de la aplicación del cuestionario dirigido al personal técnico de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., fue tabulada manualmente, según las categorías de respuestas: S = Siempre, CS = Casi Siempre, AV = Algunas Veces, CN = Casi Nunca y N = Nunca, según lo establecido por escalamiento líkert el valor uno (1) es asignado a N (Nunca) y el máximo valor de cinco (5) a S (Siempre).

Para presentar los resultados se usaron los recursos de la estadística descriptiva que permitió el diseñó de los cuadros, donde se organizaron los datos recabados en distribuciones por frecuencias absolutas y luego a porcentajes, se representó gráficamente mediante diagramas de barras cada una de las preguntas del instrumento de recolección de datos.

Con el objeto de visualizar en forma rápida los resultados se agruparon con relación a las dimensiones señaladas en la definición operacional de los aspectos a investigar y representados gráficamente de acuerdo a las alternativas seleccionadas.

Posteriormente, se completó este proceso con un análisis e interpretación de los datos en función de la norma ISO/IEC 27001:2013 y las bases teóricas que sustentaron la investigación, [5].

D**imensión:** Política de Seguridad.

Esta dimensión contiene dos (2) ítems que permiten verificar si proporciona orientación y apoyo de la Dirección para la seguridad del a Información, en concordancia con los requisitos del negocio, las leyes y las regulaciones pertinentes.

Tabla 3 Resultados de las respuestas dadas a las preguntas sobre la dimensión Políticas de Seguridad

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
1	1,96	11,76	13,73	1,96	70,59
2	0,00	5,88	7,84	13,73	72,55

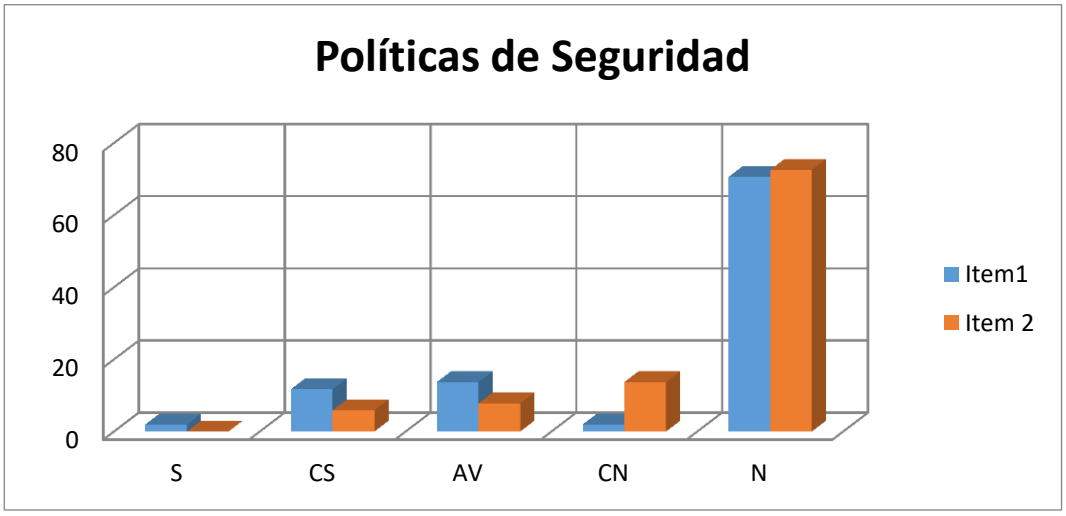


Figura 3.1 Porcentajes de las respuestas dadas a las preguntas sobre Políticas de Seguridad.

Fuente: Autor

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en el Tabla 3 y Figura 3.1 referido a la dimensión: Políticas de Seguridad.

Ítem 1: ¿Existe una preocupación dentro de la DTIC´S por la elaboración de un documento de políticas de seguridad de información con los procedimientos a seguir para cada uno de los riesgos más graves que tiene la información? la mayor tendencia porcentual se presentó en la alternativa nunca con un 70,59%, lo cual indica que no existe una preocupación por elaborar un documento de política de seguridad de la información.

Ítem 2, ¿Se revisan periódicamente las medidas y procedimientos de seguridad para determinar si son efectivos?, un 72,55% piensa que Nunca lo hacen, esto refleja que no se tiene una consciencia de la importancia de tomar medidas para proteger la información.

En conclusión, para poder dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos del Comando Conjunto de las FF.AA., se deben realizar dos documentos para considerar la seguridad de la información: el primero será un manual de política de seguridad de la información que representará el nivel político o estratégico del Comando Conjunto de las FF.AA., deberá ser elaborado por el Departamento de Informática de la Dirección de

Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. y aprobado por el mando militar, lo cual definirá las grandes líneas a seguir y el nivel de compromiso del Comando Conjunto de las FF.AA.

El segundo documento será el plan de seguridad, como nivel de planeamiento táctico, el cual definirá el “Cómo”. Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones que se deberán cumplir el Comando Conjunto de las FF.AA.

Dimensión: Organización de la Seguridad de la Información

Esta dimensión contiene un (1) ítem que permiten establecer un marco de trabajo de la Dirección para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización.

Tabla 4 Resultados de las respuestas dadas a la pregunta sobre la dimensión de la Organización de la Seguridad de la Información

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
4	0,00	5,88	7,00	17,65	66,67

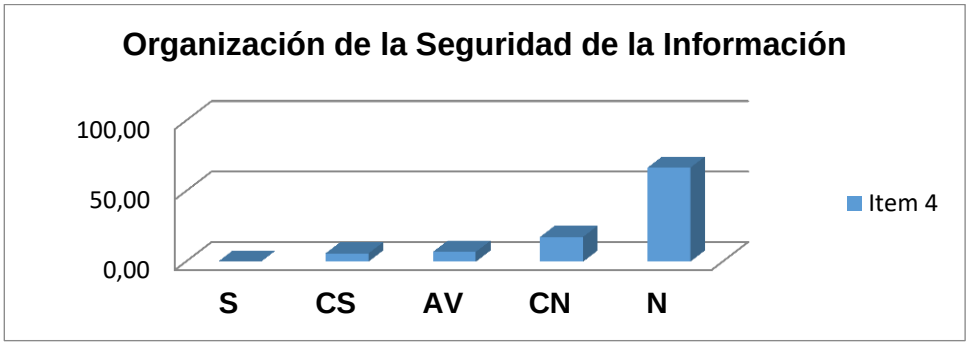


Figura 3.2 Porcentajes de la respuesta dada a la pregunta sobre Organización de la Seguridad de la Información.

Fuente: Autor

En el Tabla 4 y Figura 3.2, se observan el resultado obtenido en cuanto a la dimensión organización de la seguridad de la información

Ítem 3, ¿Se definen claramente todas las responsabilidades en torno a la seguridad de la información?, la mayor tendencia con un 66,67% se presentó para las alternativas Nunca, es evidente que no existe una política clara en referencia a la seguridad de la información.

En conclusión, existe una alta tendencia en el ítem hacia la alternativa Nunca, los sujetos de estudios señalan que la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. no llevan las políticas de seguridad de la información y están definidas claramente todas las responsabilidades individuales para alcanzarla.

Dimensión: Seguridad de Recursos Humanos.

Esta dimensión contiene dos (2) ítems que permiten obtener información asegurando si los empleados y contratistas entienden sus responsabilidades y estén adecuados a los roles para los cuales están siendo considerados, cumplan sus responsabilidades de seguridad de la información y proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.

Tabla 5 Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad de Recursos Humanos.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
4	84,31	9,80	3,92	1,96	0
5	74,51	13,73	5,88	3,92	1,96

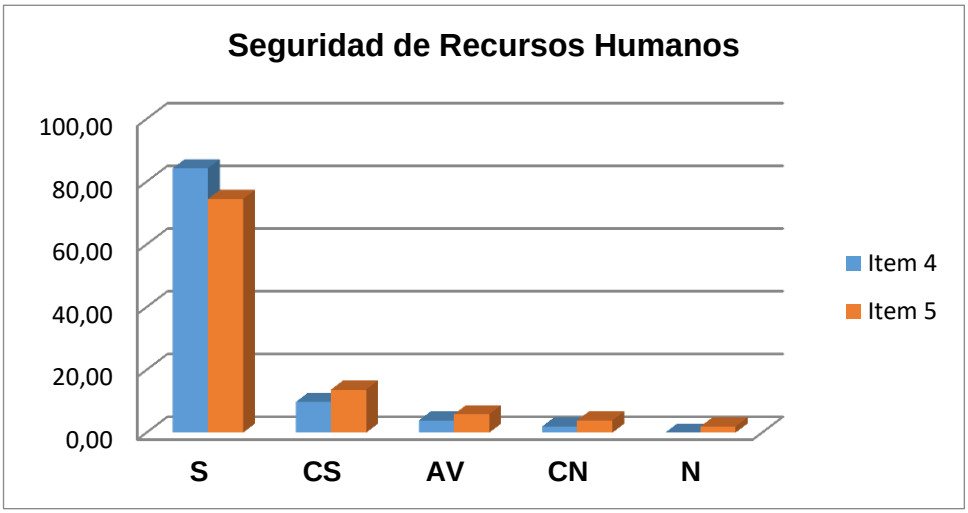


Figura 3.3 Porcentajes de las respuestas dadas a las preguntas sobre Seguridad de Recursos Humanos.

Fuente: Autor

En la Tabla 7 y Figura 3.3, se visualizan los resultados de la dimensión seguridad de recursos humanos.

Ítem 4 ¿Se realiza una verificación de los antecedentes de los candidatos para ocupar cargos administrativos, contratistas y usuarios externos de acuerdo con las leyes, reglamentaciones y ética pertinentes a los requisitos de la DTIC´S, clasificación de información a ser ingresado y los riesgos percibidos?, la mayor incidencia de respuesta la presentó la alternativa Siempre con un 84,31%, lo que permite determinar que se realiza una verificación de los documentos suministrados por el aspirante y sus antecedentes para poder optar al cargo de acuerdo con las responsabilidades que desempeñará.

Ítem 5 ¿La DTIC´S aplica procesos disciplinarios a los usuarios que cometan un incumplimiento de seguridad?, con un 74,51% en la alternativa Siempre, se evidencia que existe un proceso disciplinario formal para los funcionarios que incurran en faltas que atente a la seguridad de la información, igualmente se realizan supervisiones al personal para evitar posibles fraudes.

En conclusión, existe una alta tendencia en el ítem hacia la alternativa Siempre, en la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. se lleva un buen

control de antecedentes del personal externo y se aplican procesos disciplinarios estrictamente.

Dimensión: Gestión de Activos.

Este indicador contiene cuatro (4) ítems que permiten identificar los activos de la organización y definir las responsabilidades de protección pertinentes, asegurar que la información reciba un nivel de protección adecuado, según su importancia para la organización y prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.

Tabla 6 Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Activos.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
6	64,71	21,57	5,88	5,88	1,96
7	70,59	11,76	9,80	3,92	3,92
8	68,63	13,73	7,84	5,88	3,92
9	80,39	13,73	1,96	1,96	1,96

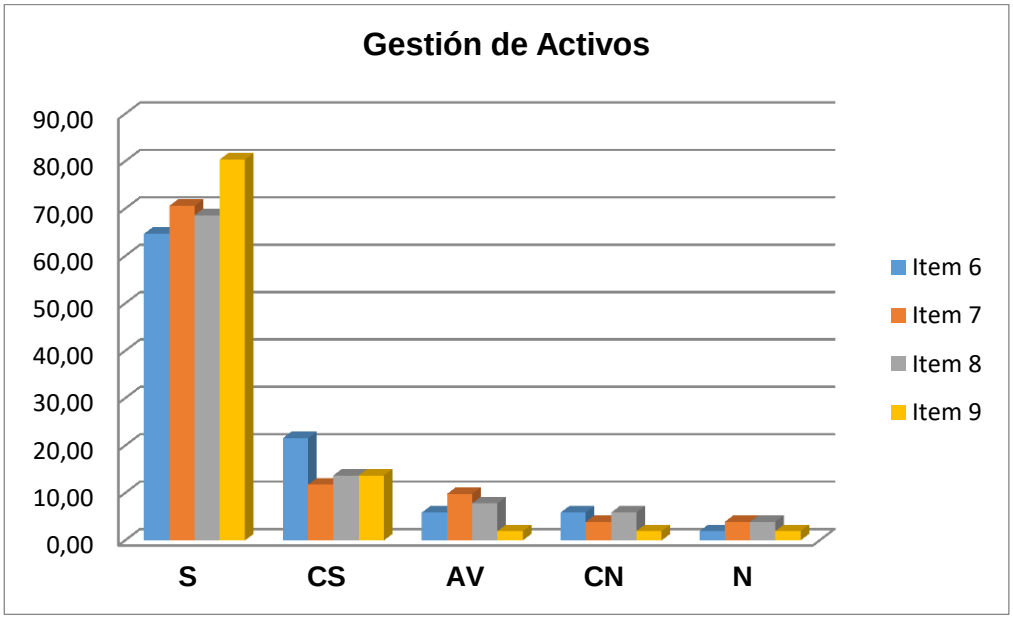


Figura 3.4 Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Activos.

Fuente: Autor

Los resultados obtenidos en la dimensión gestión de activos expresados en el Tabla 6 y el Figura 3.4.

En el ítem 6 ¿Se realizan inventarios en cada oficina o unidad administrativa de los equipos informáticos y de comunicaciones, con el serial del equipo, software instalados, usuario asignado, ubicación, entre otros?, el 64.71% opinó que Siempre se realizan los inventarios.

Ítem 7 ¿La DTIC´S se asegura de que los empleados, contratista y usuarios devuelvan todos los activos de la DTIC´S que posean una vez

terminado su empleo, contrato o acuerdo? coincidieron que la alternativa que más se ajustó fue Casi Siempre presentando un 11,76% y Siempre con 70,59% respectivamente, lo que demuestra que se encuentra establecido un procedimiento para la devolución de todos los activos la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. y toman las debidas previsiones para retirar todos los derechos de accesos a la información.

Ítem 8 ¿Se dan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la DTIC´S?, el 68,63% opinó que Siempre se dan directrices, lo que refleja que la información está inventariada y clasificada y existe un procedimiento con un esquema de clasificación establecido para etiquetar los activos de información.

Ítem 9 ¿Se registran, analizan y se toman acciones apropiadas cuando se detectan fallas en las actividades y procesamiento de la información no autorizada?, presentaron una alta incidencia en la alternativa Siempre con un 80,39% y Casi Siempre 13,76% respectivamente, estos resultados confirman que se llevan registros de auditorías de los eventos de seguridad que ocurren en los sistemas de información.

En conclusión: La Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. cuenta con un departamento de activos fijos el cual es el encargado de realizar el inventario de todos los activos importantes, y que posee activos que están inventariados. Existe una metodología para realizar esta actividad donde cada activo de información está asociado con el lugar donde se procesa la información y que a su vez es el responsable por el mismo.

Dimensión: Control de Accesos.

Esta dimensión contiene seis (06) ítems que permite restringir el acceso a la información y a los recursos de procesamiento de información, asegurar el acceso de usuarios autorizados a fin de prevenir el acceso no autorizado a los sistemas y servicios, responsabilizar a los usuarios para que salvaguarden su información de autenticación y prevenir el acceso no autorizado a los sistemas y aplicaciones.

Tabla 7 Resultados de las respuestas dadas a las preguntas sobre la dimensión Control de Accesos.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
10	58,82	25,49	9,80	3,92	1,96
11	23,53	60,78	9,80	3,92	1,96
12	21,57	56,86	17,65	1,96	1,96
13	68,63	17,65	3,92	7,84	1,96
14	66,67	13,73	5,88	13,73	0,00
15	9,80	15,69	66,67	3,92	3,92

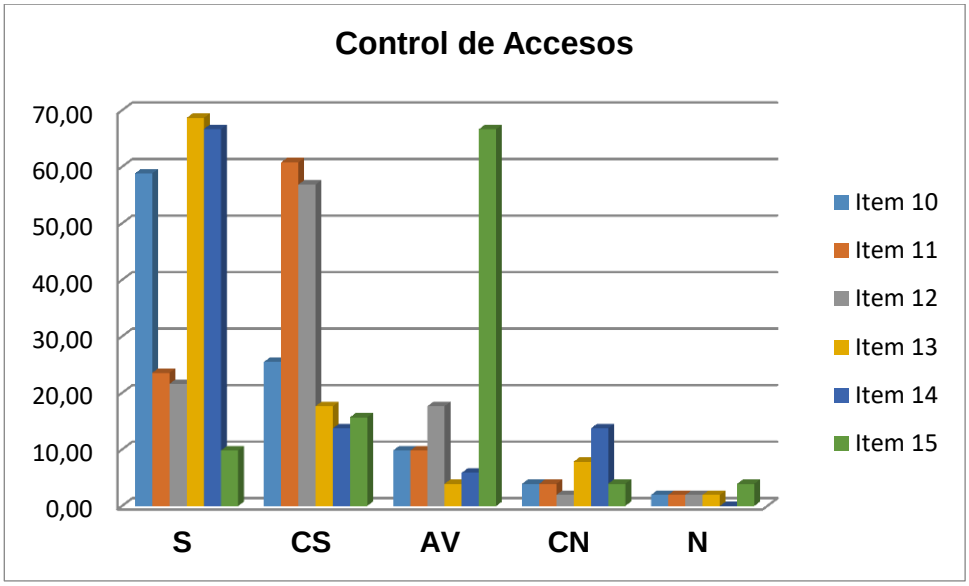


Figura 3.5 Porcentajes de las respuestas dadas a las preguntas sobre Control de Accesos.

Fuente: Autor

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en el Tabla 7 y Figura 3.5 referido a la dimensión control de accesos.

Ítem 10 ¿Se establecen, documentan y revisan las políticas de control de accesos a la información?, el 58,82% respondió que Siempre, lo cual nos permite inferir que existe una política de control de accesos.

Ítem 11 ¿Se realizan procedimientos formales de registros de usuarios para conceder y revocar el acceso a los sistemas y servicios de

información?, muestra una alta incidencia por la alternativa Casi Siempre con un 60,78%, lo que nos indica que existe un procedimiento formal de registro y revocación de usuarios y administración de privilegios y contraseñas de cada uno de los usuarios

El ítem 12 ¿Se retiran los derechos de acceso a todos los empleados, contratistas y usuarios a la información y al recurso para el procesamiento de la información una vez terminado su empleo, contrato o acuerdo, o una vez realizado el cambio a otra dependencia?, la alternativa que más se ajustó fue Casi Siempre presentando un 56,86%, lo que demuestra que se toman las debidas previsiones para retirar todos los derechos de accesos a la información.

Ítem 13 ¿Se les motiva a los usuarios seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas?, el 68,63% opino que Siempre, esto refleja que los usuarios tienen claro el uso de contraseñas, así como también evidencia que existen procedimientos formales para la selección y uso de contraseñas.

Ítem 14. ¿Se controla a través de un proceso de gestión formal la asignación de contraseñas de usuarios para prevenir el acceso no autorizado a los sistemas de información?, muestra una alta incidencia por la alternativa Siempre con un 66,67%, lo que nos indica que existe un procedimiento formal de registro y revocación de usuarios y una

adecuada administración de los privilegios y de las contraseñas de cada uno de los usuarios.

Ítem 15 ¿Se restringe de acuerdo con las políticas de control el acceso a la información y a las funciones del sistema de aplicación? referido al indicador restricción de acceso a la información, el 66,67% respondió que Algunas Veces se hace, esto evidencia que no existe una política de control de acceso definida.

En conclusión, los resultados obtenidos muestran una inclinación hacia la alternativa Siempre, Casi siempre y Algunas Veces. Es de destacar, que el control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema y para lograrlo debe existir una política de control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.

Dimensión: Criptografía.

Este indicador contiene cuatro (1) ítems que permite asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

Tabla 8 Resultados de la respuesta dadas a la pregunta sobre la dimensión Criptografía.

Fuente: Autor

Ítems	S	CS	AV	CN	N
16	29,41	56,86	9,80	1,96	1,96

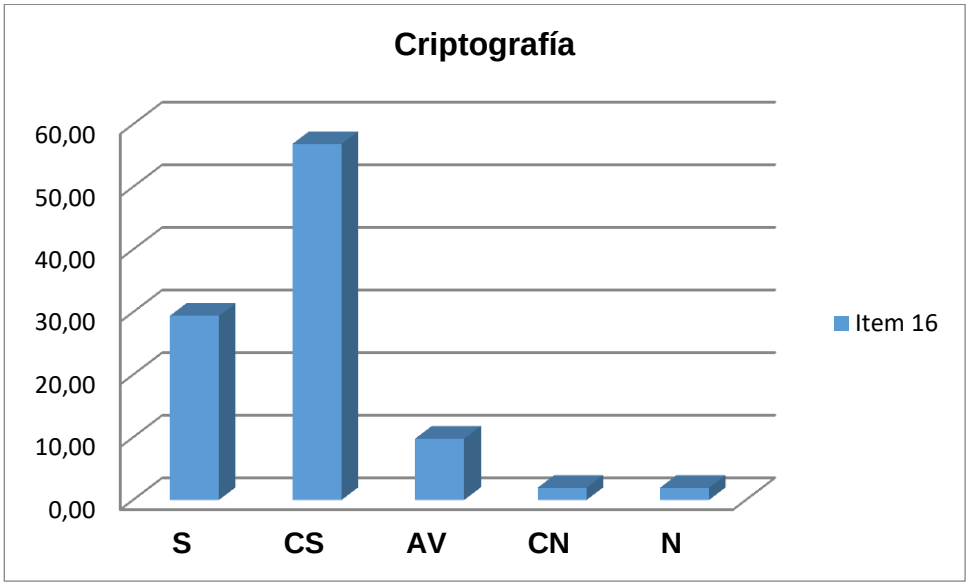


Figura 3.6 Porcentajes de la respuesta dada a las pregunta sobre Criptografía.

Fuente: Autor

El resultado obtenido en la dimensión Criptografía se expresas en el Tabla 8 y el Figura 3.6.

Ítem 16 ¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de la confidencialidad, autenticidad o integridad de la información?, el 56,86% opinó que Casi Siempre se protegen la confidencialidad, autenticidad o integridad de la información.

En conclusión, el resultado anterior demuestra fortalecimiento para la protección de la confidencialidad, autenticidad o integridad de la información.

Dimensión: Seguridad Física y Ambiental.

Esta dimensión contiene nueve (9) ítems que permiten evitar el acceso físico no autorizado, daño e interferencia a la información y recursos de procesamiento de la información de la organización y prevenir la pérdida, daño, robo o el compromiso de los activos, así como la interrupción de las operaciones de la organización.

Tabla 9 Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad Física y Ambiental.

Fuente: Autor

Ítems	S	CS	AV	CN	N
17	58,82	23,53	13,73	1,96	1,96
18	60,78	25,49	11,76	1,96	0,00
19	64,71	21,57	9,80	3,92	0,00
20	64,71	23,53	11,76	0,00	0,00
21	60,78	21,57	11,76	1,96	3,92
22	62,75	25,49	7,84	3,92	0,00
23	62,75	19,61	15,69	1,96	0,00
24	17,65	58,82	13,73	5,88	3,92
25	11,76	64,71	13,73	9,80	0,00

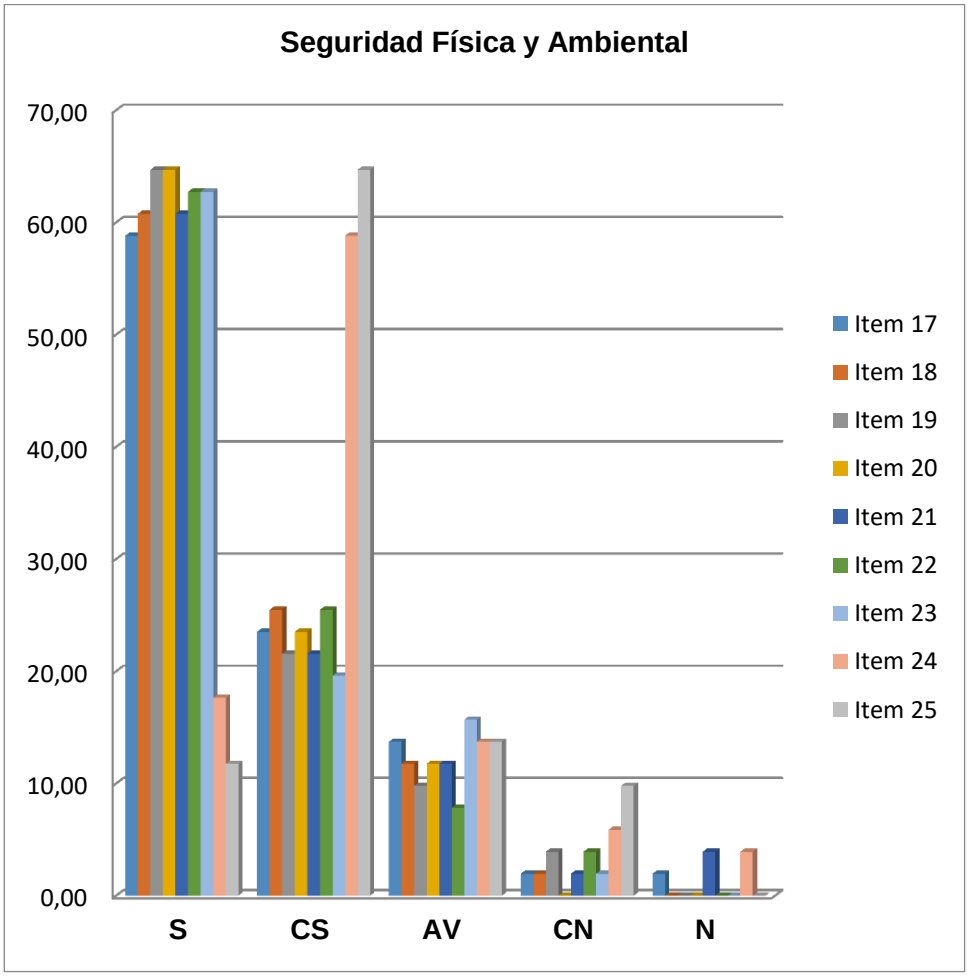


Figura 3.7 Porcentajes de las respuestas dadas a las preguntas sobre Seguridad Física y Ambiental.

Fuente: Autor

En la Tabla 9 y Figura 3.7, muestra los resultados aportados por los sujetos de estudios en relación a la seguridad física y ambiental.

Ítems 17 ¿En la DTIC´S se establecen adecuadamente los perímetros de seguridad (barreras tales cómo paredes, puertas de entradas

controladas por tarjetas o puesto de recepción manual) a las áreas que contienen la información y las instalaciones de procesamiento de la información?, la alternativa Siempre presentó un 58,82%, lo que permite determinar que se encuentran establecidos los perímetros de seguridad a las áreas vulnerables.

Ítem 18 ¿Se diseñan y aplican controles de entradas apropiados a las áreas de seguridad a fin de asegurar el permiso de acceso sólo al personal autorizado?, el 60,78 % afirma que se aplican controles de entradas para personal autorizado.

Ítem 19 ¿Existe un procedimiento o control de admisión al edificio administrativo para aquellas personas que no posean carnet institucional, tal como los visitantes?, el 64,71% establece que si existen procedimientos de control de acceso al edificio para usuarios de visita.

Ítem 20 ¿Se diseñan y aplican protección física a las oficinas contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre?, presentan una alta tendencia a la alternativa Siempre con un 72.73%, determinando que se encuentran establecidos los perímetros de seguridad para las áreas que contienen información crítica de la Dirección de Tecnologías de la Información y Comunicaciones el Comando Conjunto de las FF.AA.

Ítem 21 ¿Se toman previsiones de ubicar o proteger los equipos para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado?, los resultados indican una tendencia positiva hacia las alternativas Siempre con un 64,71%, esto demuestra que existe preocupación por prevenir pérdidas, daños o robo de los activos de información.

El ítem 22 ¿Se protegen los equipos contra fallas de energía y otras interrupciones eléctricas causadas por problemas en los servicios de apoyo?, la alternativa Siempre presentó un 62,75%, lo que permite determinar que conocen sobre las medidas que se deben considerar para proteger los equipos contra las fallas de energía u otras interrupciones eléctricas.

El ítem 23 ¿Se protegen debidamente el cableado de energía eléctrica y de comunicaciones que transporta datos contra la interceptación o daños?, el 62,75% respondió que Siempre, lo cual se evidencia la seguridad del cableado.

El ítem 24 ¿La DTIC´S da instrucciones claras y firmes a los usuarios para que prohíban el traslado o retiro de equipo, información o software sin autorización?, el 58,82% opinó que Casi Siempre evidenciando que existe una política de seguridad que controle el retiro de los activos de información.

El ítem 25 ¿Se toman las previsiones para que todos los dispositivos de almacenamiento de datos (Pendrive, CD, Disco duros, entre otros), sean eliminados o formateado completamente antes de su utilización?, el 64,71% se inclinó por la alternativa Casi Siempre evidenciando mejoras en la seguridad de la información cuando se reutilizan o eliminan equipos sin tomar las previsiones de remover toda la información existentes en el mismo.

En conclusión, los resultados mostrados anteriormente demuestran que existen mejoras en la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. garantizando la seguridad física tanto a las instalaciones como a los equipos.

Dimensión: Seguridad de las Operaciones.

Esta dimensión contiene seis (6) ítems que permite asegurar la operación correcta y segura de los recursos de procesamiento de información, estén protegidos contra malware, proteger la pérdida de información, registrar eventos y generar evidencia, asegurar la integridad de los sistemas en producción, prevenir la explotación de vulnerabilidades técnicas y minimizar el impacto de las actividades de auditoría en los sistemas de producción.

Tabla 10 Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad de las Operaciones.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
26	5,88	23,53	54,90	13,73	1,96
27	11,76	56,86	21,57	9,80	0,00
28	0,00	3,92	21,57	60,78	13,73
29	9,80	21,57	68,63	0,00	0,00
30	54,90	29,41	7,84	5,88	1,96
31	0,00	0,00	17,65	72,55	9,80

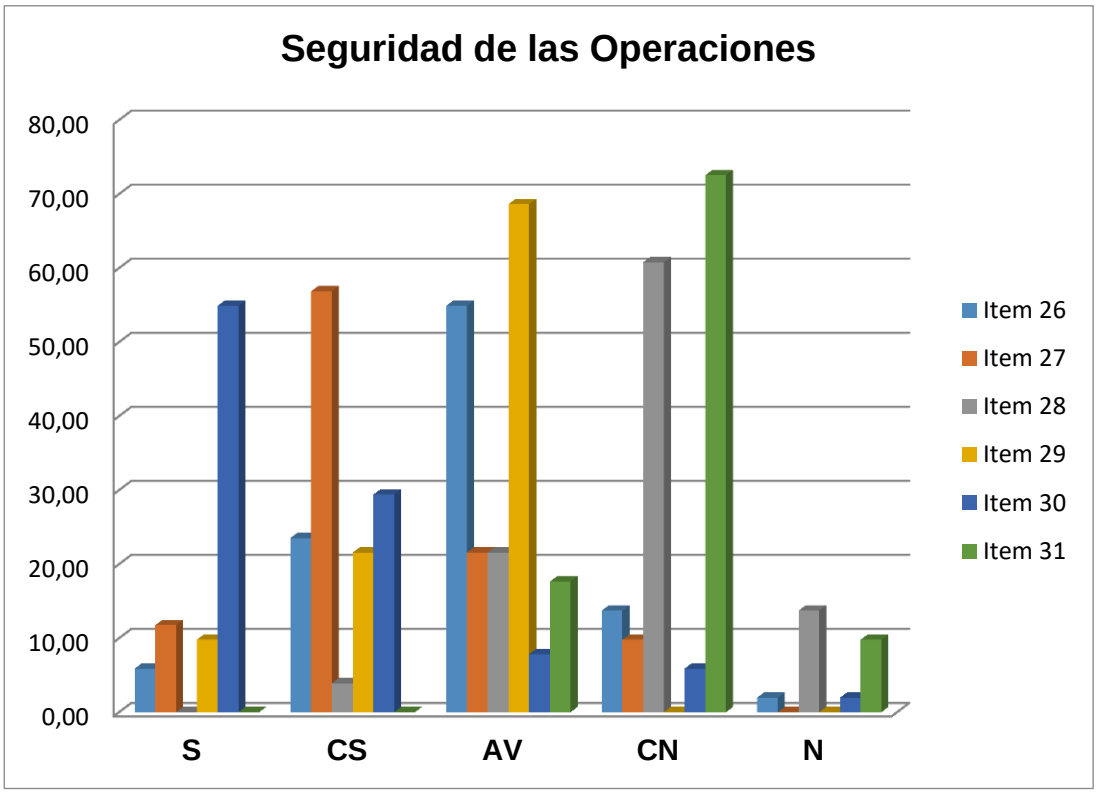


Figura 3.8 Porcentajes de las respuestas dadas a las preguntas sobre Seguridad de las Operaciones.

Fuente: Autor

En la Tabla 10 y Figura 3.8, se observan los resultados obtenidos para la dimensión Seguridad de las operaciones.

Ítems 26 ¿Los procedimientos operativos son documentados, mantenidos y están disponibles a todos los usuarios que lo necesitan?, con el 54,90% en la alternativa Algunas Veces y el Ítem 27 ¿Se controlan los cambios de los recursos y sistemas de procesamiento de la información?, con un 56,86% en la alternativa Casi Siempre, indica que no se realizan mayores esfuerzo por documentar los procedimientos, lo cual es negativo, ya que la documentación de los procedimientos permite el manteniendo de los mismos.

Ítem 28 ¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus?, con un 60,78% en la alternativa Casi Nunca, permitieron concluir que los usuarios tiene poco conocimiento para detectar los códigos maliciosos y no existen procedimientos formales para adiestrarlos para que puedan evitarlos y así proteger la información.

Ítem 29 ¿Se realizan copias de seguridad de la información y software de acuerdo con la política de copia de seguridad emitida?, el 68,63% opinó que Algunas Veces, lo que permite determinar que no se realizan backups de la información y de los sistemas de información.

El ítem 30 ¿Se sincronizan los relojes de todos los sistemas de procesamiento de la información pertinentes dentro de la DTIC´S con una fuente de tiempo exacta acordada?, el 54,90% opinó que Siempre se tiene una sincronización de toda la infraestructura de servidores.

Ítem 31 ¿Se planifican actividades de auditorías que involucren comprobaciones en los sistemas operativos y sistemas de información a fin de minimizar el riesgo de interrupción de los procesos de la DTIC´S?, el 72,55% señaló que Casi Nunca. Estos resultados evidencian, la poca importancia que se le presta a la protección de la información clasificada.

En conclusión, los resultados mostrados anteriormente demuestran que se debe mejorar en la Seguridad de las Operaciones en la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. para garantizar la operación segura y correcta de los recursos de procesamiento de la información.

Dimensión: Seguridad de las Comunicaciones.

Esta dimensión contiene tres (3) ítems que permiten asegurar la protección de la información en las redes y la protección de los recursos de procesamiento de la información que la soportan, mantener la seguridad de la información que se transfiere dentro de la organización y con cualquier entidad externa.

Tabla 11 Resultados de las respuestas dadas a las preguntas sobre la dimensión Seguridad de las Comunicaciones.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
32	64,71	23,53	5,88	3,92	1,96
33	1,96	5,88	21,57	56,86	13,73
34	0,00	9,80	68,63	19,61	1,96

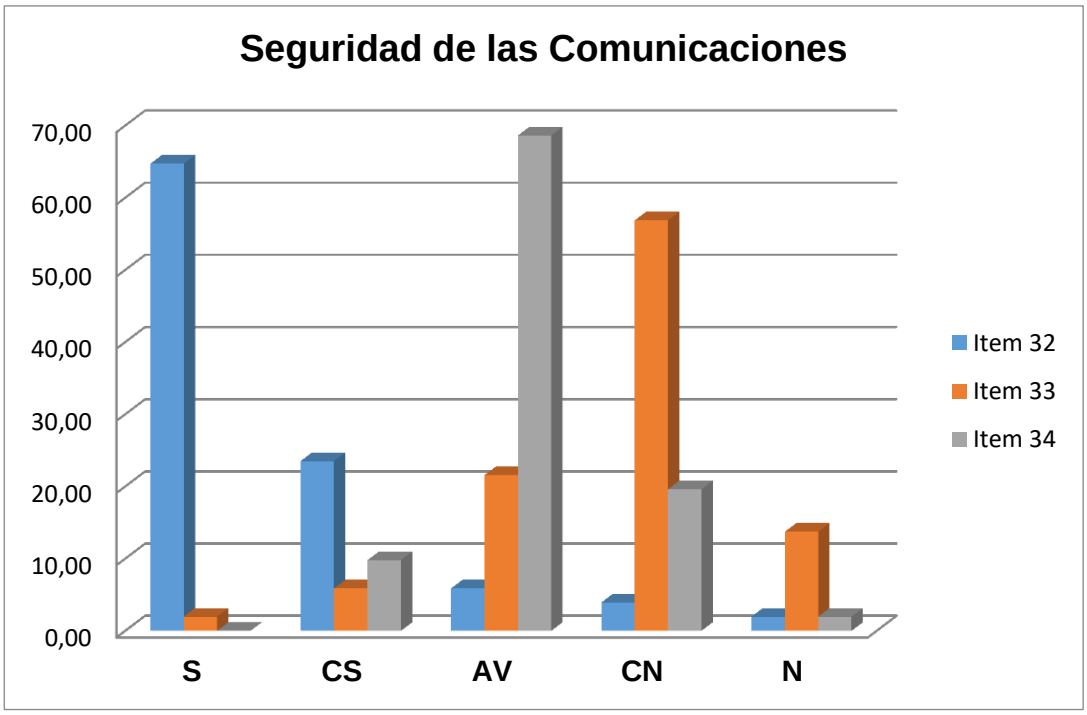


Figura 3.9 Porcentajes de las respuestas dadas a las preguntas sobre Seguridad de las Comunicaciones.

Fuente: Autor

En la Tabla 11 y Figura 3.9, se observan los resultados obtenidos para la dimensión Seguridad de las Comunicaciones.

Ítem 32 ¿Se gestionan y controlan adecuadamente la red de datos a fin de protegerla de las amenazas y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito?, el 64,71% opinó que Siempre, lo que se deduce que se lleva una buena administración y control de la red y se implementan todas las medidas posibles para evitar amenazas y mantener la seguridad de los sistemas.

Ítem 33 ¿Se establecen procedimientos para controlar el intercambio de información a través de la utilización de toda clase de recursos de comunicación, por ejemplo el uso de teléfonos celulares y laptops por parte de personas ajenas a la DTIC´S?, el 56,86% opinó que Casi Nunca, lo que indican que no existe políticas y procedimientos de intercambio de información.

El ítem 34 ¿Se definen los requisitos para los acuerdos de confidencialidad o no divulgación de la información?, presentó la alternativa Algunas Veces con un 68,63%, es evidente que se deben identificar los requisitos para los acuerdos de no divulgación de la información para proteger la información de carácter institucional.

En conclusión los sujetos de estudios señalan que en la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. se asegura la protección de la información en

las redes, no existen procedimientos para la trasferencia de información y se debe mejorar los acuerdos de confidencialidad o no divulgación de la información.

Dimensión: Adquisición, Desarrollo y Mantenimiento del Sistema.

Esta dimensión contiene un (01) ítem que permiten verificar si la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida de desarrollo y la protección de los datos utilizados para prueba.

Tabla 12 Resultados de las respuestas dadas a las pregunta sobre la dimensión Adquisición, Desarrollo y Mantenimiento del Sistema.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
35	23,53	56,86	9,80	5,88	3,92

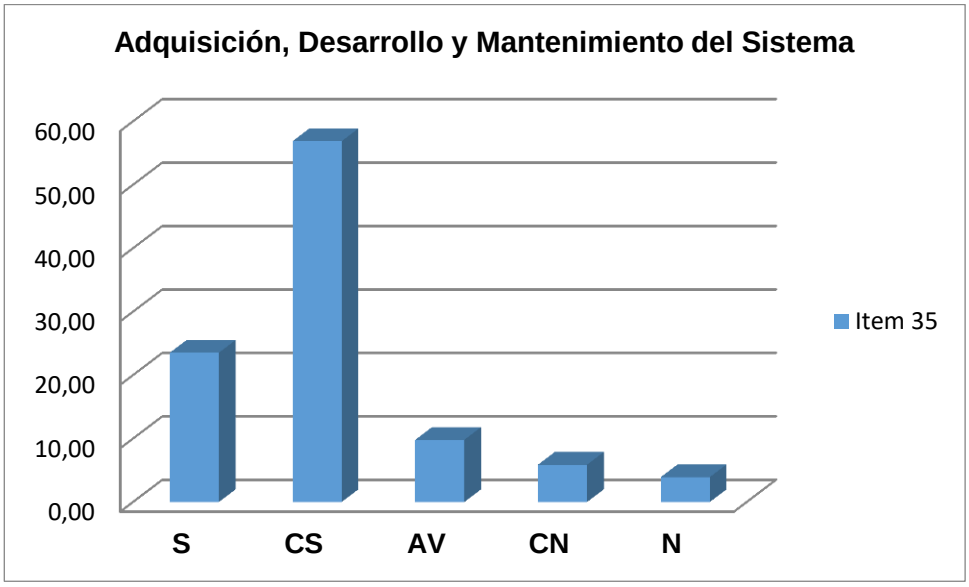


Figura 3.10 Porcentajes de las respuestas dadas a la pregunta sobre Adquisición, Desarrollo y Mantenimiento del Sistema.

Fuente: Autor

En la Tabla 12 y Figura 3.10, muestra los resultados aportados por los sujetos de estudios en relación a la adquisición, desarrollo y mantenimiento del sistema.

Ítem 35 ¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes?, el 56,86% opinó que Casi Siempre se especifican los requisitos de control de seguridad para los nuevos sistemas de información.

En conclusión, el resultado anterior demuestra fortalecimiento de seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información.

Dimensión: Relación con los Proveedores.

Esta dimensión contiene un (01) ítem que permiten asegurar la protección de los activos de la organización las cuales acceden los proveedores y mantener un determinado nivel de seguridad de la información y entrega de servicio, en línea con los acuerdos del proveedor.

Tabla 13 Resultados de las respuestas dadas a las pregunta sobre la dimensión Relación con los Proveedores.

Fuente: Autor

Ítems	S	CS	AV	CN	N
36	29,41	47,06	13,73	5,88	3,92

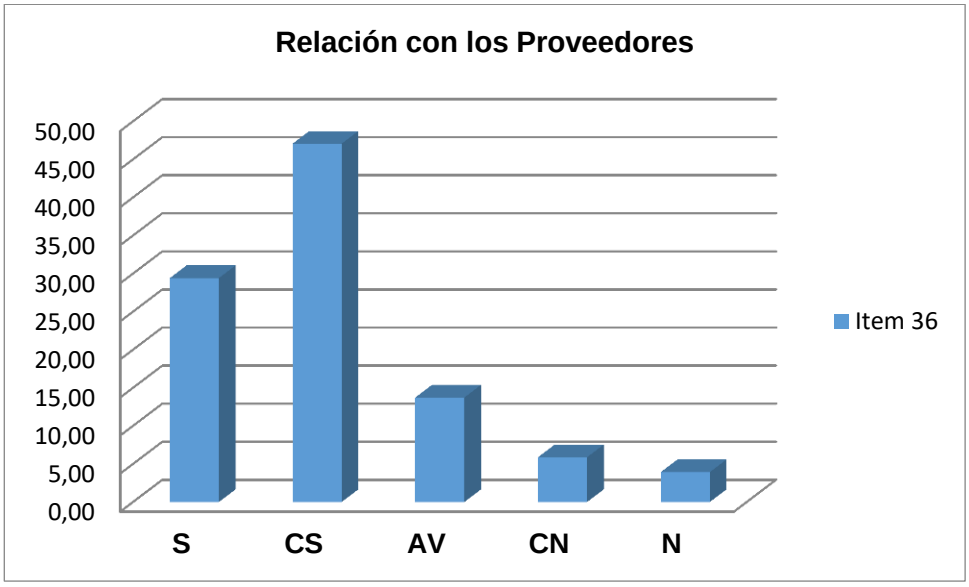


Figura 3.11 Porcentajes de las respuestas dadas a la pregunta sobre Relación con los Proveedores.

Fuente: Autor

En la Tabla 13 y Figura 3.11, muestra los resultados aportados por los sujetos de estudios en relación a la Relación con los Proveedores.

Ítem 36 ¿Se tienen previstos mecanismos de seguridad para preservar la información de intervenciones externas?, el 47,06% manifestó que Casi Siempre, lo cual se determina que están identificados los riesgos de la información de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. y en consecuencia están implementados los controles apropiados antes de otorgar el acceso a partes externas.

En conclusión, el resultado anterior demuestra se llevan las políticas de seguridad de la información y están definidas claramente todas las responsabilidades individuales para alcanzarla, de igual manera están definidos los requisitos para los acuerdos de confidencialidad de la información y se consideran todos los requisitos de seguridad antes de dar acceso al cliente o usuario de la información externa a DTIC´S.

Dimensión: Gestión de Incidentes de Seguridad de la Información

Esta dimensión contiene cuatro (04) ítems que permitieron asegurar un enfoque consistente y eficaz de la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos de seguridad y debilidades.

Tabla 14 Resultados de las respuestas dadas a las preguntas sobre la dimensión Gestión de Incidentes de Seguridad de la Información.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
37	9,80	17,65	60,78	7,84	3,92
38	56,86	23,53	13,73	3,92	1,96
39	13,73	68,63	9,80	5,88	1,96
40	1,96	19,61	66,67	7,84	3,92

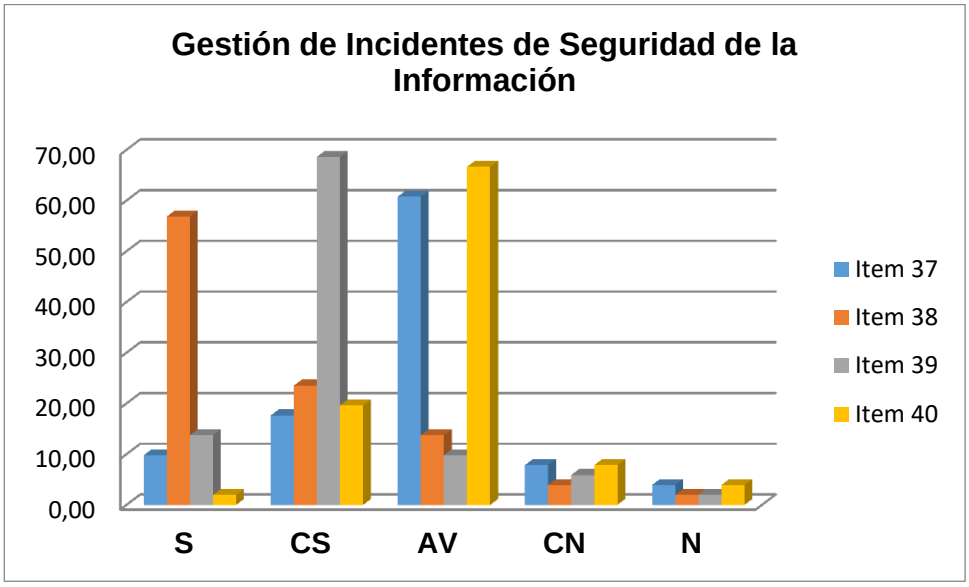


Figura 3.12 Porcentajes de las respuestas dadas a las preguntas sobre Gestión de Incidentes de Seguridad de la Información.

Fuente: Autor

Los resultados obtenidos en la dimensión gestión de incidentes de seguridad de la información se muestran en la Tabla 14 y Figura 3.12.

En relación a la gestión de los incidentes y mejoras de seguridad de la información, los ítem 37 ¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información?, los resultados señalan un 60,78% opinó que Algunas Veces se establecen responsabilidades.

Para obtener información acerca de los reportes de eventos y debilidades de seguridad de la información se emplearon dos

preguntas, el ítem 38 ¿Se reportan los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente como sea posible? y el ítem 39 ¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada?, los mayores porcentajes de respuestas son 56,86% fueron para las alternativas Siempre y 68,63% Casi Siempre, esto refleja que existen procedimientos para los incidentes de seguridad.

Ítem 40 ¿Se establecen mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de seguridad de información?, un 66,67% respondió que Algunas Veces se establecen mecanismos para cuantificar los incidentes de seguridad.

En conclusión, existe una alta tendencia positiva en los resultados, los que demuestra que se están realizando una administración de los incidentes de seguridad de la información.

Dimensión: Aspectos de Seguridad de Información en la Gestión de Continuidad del Negocio.

Esta dimensión contiene un (01) ítem que tiene como objetivo incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad de negocio de la organización y

asegurar la disponibilidad de los recursos de procesamiento de información.

Tabla 15 Resultados de las respuestas dadas a la pregunta sobre la dimensión Aspectos de Seguridad de Información en la Gestión de Continuidad del Negocio.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
41	1,96	5,88	33,33	45,10	13,73

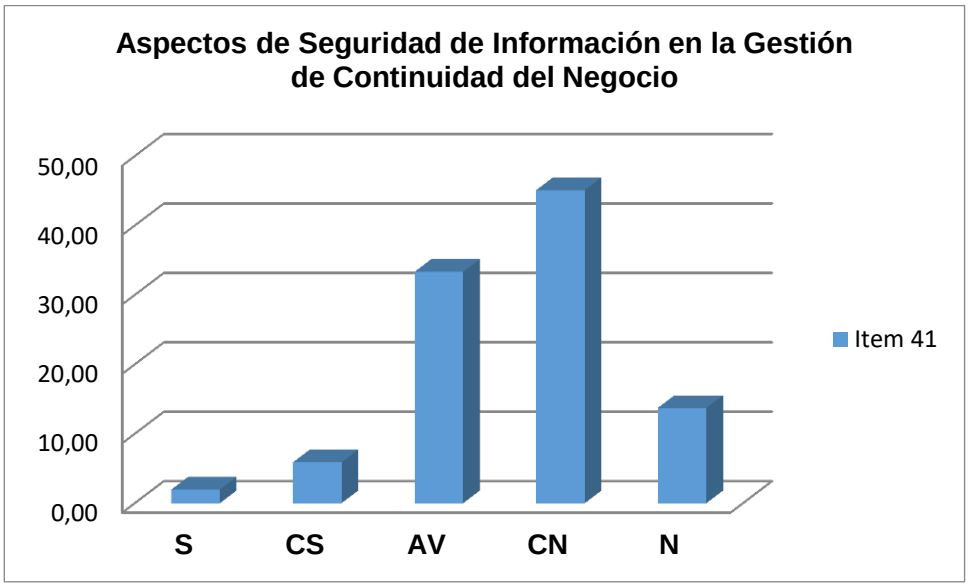


Figura 3.13 Porcentajes de las respuestas dadas a las preguntas sobre Aspectos de Seguridad de Información en la Gestión de Continuidad del Negocio.

Fuente: Autor

Las respuestas visualizadas en la Tabla 15, Figura 3.13, permiten evaluar en relación a la dimensión Aspectos de Seguridad de Información en la Gestión de Continuidad del Negocio. En este sentido,

el ítem 41 ¿Se identifican los eventos que pueden causar las interrupciones a los procesos de la DTIC´S, al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información?, se observa una tendencia negativa siendo la alternativa Casi Nunca la que presenta mayor puntuación con un 45,10%, esto refleja que no están identificados aquellos eventos que pueden causar interrupción del servicio.

En conclusión, se evidencia que se tienen poco conocimiento para proteger los procesos de seguridad de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. de los efectos de fallas significativas de los sistemas de información y asegurar su reanudación oportuna.

Dimensión: Cumplimiento

Esta dimensión contiene tres (03) ítems que permiten evitar incumplimientos de las obligaciones legales, reglamentarias, regulatorios o contractuales relacionadas con la seguridad de la información y de todos los requisitos de seguridad, así como asegurar que la seguridad de la información se implemente y opere de acuerdo a las políticas y procedimientos de la organización.

Tabla 16 Resultados de las respuestas dadas a las preguntas sobre la dimensión Cumplimiento.

Fuente: Autor

Ítems	%S	%CS	%AV	%CN	%N
42	0,00	5,88	21,57	68,63	3,92
43	0,00	3,92	25,49	60,78	9,80
44	1,96	3,92	29,41	52,94	11,76

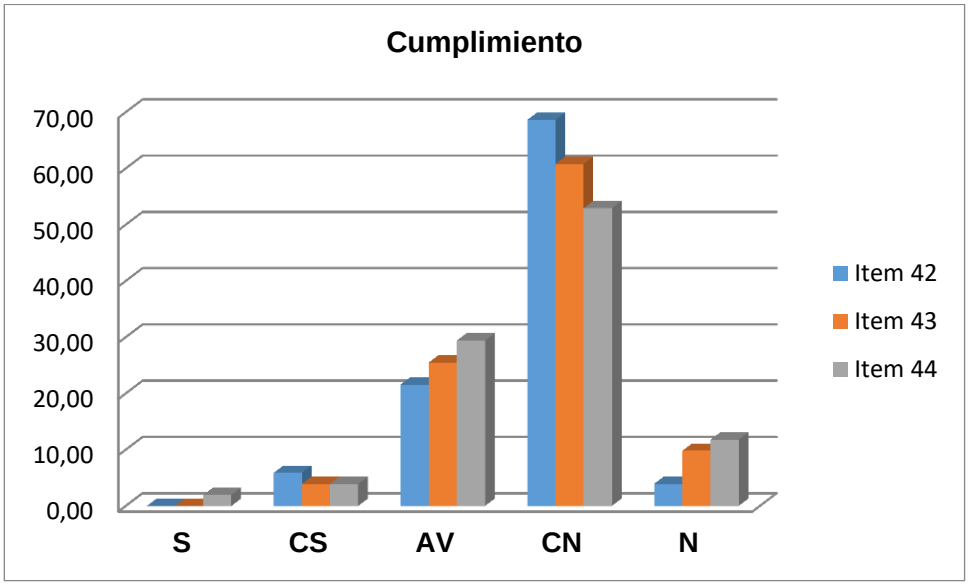


Figura 3.14 Porcentajes de las respuestas dadas a las preguntas sobre Cumplimiento.

Fuente: Autor

En la Tabla 16 y el Figura 3.14, reflejan las respuestas emitas por los sujetos de estudio sobre la dimensión Cumplimiento.

Ítem 42 ¿Se definen, documentan y se actualizan todos los requisitos legales, reglamentarios y contractuales para cada sistema de información de la DTIC´S? Las respuestas dadas son negativas, con un 68,63% para la alternativa Casi Nunca.

Ítem el 43 ¿Se implementa procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados?, las respuestas dadas son negativas, con 60,78% para la alternativa Casi Nunca.

En el ítem 44 ¿Se protegen los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales de la DTIC´S?, el 52,94% opinó que Casi Nunca, estos resultados evidencian la poca importancia que se le presta a la protección de la información clasificada.

En conclusión, los resultados permite inferir que no se consideran o no se identifica la legislación aplicable a los sistemas de información que tiene la Dirección de Tecnologías de la Información y Comunicaciones así como de las instituciones militares, lo que hace suponer que no está definido explícitamente y documentando todo lo que guarde relación

con los requisitos legales, derecho de la propiedad intelectual, el uso de productos de software reservados.

3.8 Observación Directa

Para verificar la observación directa, no participante y sistemática de la realidad del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. y tomando como guía la norma (ISO/IEC 27001:2013, 2013), en el **Anexo F**, se encuentra los objetivos de control y controles listados en la Tabla A.1. [5].

A continuación en la Tabla 17 se detallan las observaciones realizadas en relación a cada uno de los objetivos de control.

Tabla 17 Observación directa.
Fuente: Autor

Cláusulas	Objetivo de control	Controles	Observación directa
A.5 Políticas de seguridad de la información	A.5.1 Gestión de la Gerencia para la seguridad de la información	A.5.1.1 Políticas de la seguridad de la información	No existe un documento de política de seguridad de información
		A.5.1.2 Revisión de las políticas de seguridad de la información	No son revisadas las políticas de seguridad de la información.
A.6. Organización de la Seguridad de la información	A.6.1. Organización Interna	A.6.1.1 Funciones y responsabilidades de la seguridad de la información	No están definidas claramente todas las responsabilidades de seguridad de la información
A.7 Seguridad de los recursos humanos	A.7.1. Antes de reclutarlo	A.7.1.1 Filtración	Se lleva a cabo la verificación de los antecedentes de todos los candidatos al empleo por el departamento correspondiente

	A.7.2 Durante el trabajo	A.7.2.3 Procesos disciplinarios	No existe proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
A.8 Gestión de los Activos	A.8.1 Responsabilidades sobre los activos	A.8.1.1 Inventario de activos	Se tiene una mediana documentación de lo que debería ser un inventario de servicios de información y de hardware
		A.8.1.4 Retorno de los activos	No se cumple en su totalidad la devolución de todos los activos de la DTIC'S una vez terminado la relación laboral.
	A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la información	No está clasificada la información de acuerdo con su valor, sensibilidad y criticidad.
		A.8.2.3 Manejo de los activos	No existen procedimiento para el manejo y almacenamiento de la información.
A.9 Control de acceso	A.9.1 Requisitos del negocio sobre control del acceso	A.9.1.1 Política de control de acceso	Existe una política de control de acceso.
	A.9.2 Gestión del acceso al usuario	A.9.2.1 Registro y des-registro del usuario	Existe un procedimiento formal.
		A.9.2.6 Retiro o ajuste de los derechos de acceso	Se mantienen lazos de amistad y se observa que empleados que han sido cambiados de oficinas mantienen acceso a la información y recursos para el procesamiento de la información
	A.9.3 Responsabilidades del usuario	A.9.3.1 Uso de información secreta de autenticación	Se solicita a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.3 Sistema de gestión de la clave	Los sistemas de gestión de la clave deben son interactivos lo cual aseguran la calidad de las claves.
		A.9.4.4 Uso de programas utilitarios de privilegio	No se restringe el uso de programas utilitarios
A.10 Criptografía	A.10.1 Controles de la criptografía	A.10.1.1 Política del uso de controles criptográficos	Existen políticas de uso de controles criptográficos para proteger la información.
A.11 Seguridad física y medioambiental	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física	El cuarto de cableado principal y de servidores si presenta seguridad, la puerta principal es de aluminio y vidrio, las paredes son de cemento y el techo no está desprotegido

		A.11.1.2 Controles físicos de los ingresos	Se protege las áreas seguras mediante controles adecuados de ingreso de sólo personal autorizado.
		A.11.1.3 Seguridad de las oficinas, salas e instalaciones	Existen mecanismos de seguridad física para el ingreso a las salas, oficinas e instalaciones.
		A.11.1.4 Protección contra las amenazas externas y medioambientales	Existen planes de contingencia contra los desastres naturales y accidentes.
	A.11.2 Equipos	A.11.2.1 Ubicación y protección de los equipos	Los equipos se encuentran ubicados y protegidos en un Data Center, lo cual minimiza los riesgos y peligros del medio ambiente y acceso no autorizado.
		A.11.2.2 Servicios públicos de soporte	Se observa que el cableado de energía eléctrica y de comunicaciones que transporta datos se encuentra protegido, no se violentan todas las normas del cableado estructurado, no está certificado.
		A.11.2.3 Seguridad en el cableado	No se encuentran protegidos el cableado de interferencia, intercepción o daño al cableado de energía o telecomunicaciones
		A.11.2.5 Retiro de los activos	No existen procedimientos para el retiro de equipos y software
		A.11.2.7 Disposición o re-uso seguro de los equipos	No existen procedimientos para verificación de los equipos que contienen medios de comunicación de la información y garantizar que se haya extraído la información sensible.
A.12 Seguridad de las operaciones	A.12.1 Procedimientos y responsabilidades operaciones	A.12.1.1 Documentación de los procedimientos operacionales	Se está realizando la documentación de los servidores y servicios que tienen en la DTIC'S, el personal desconoce de esta documentación, debe realizar adiestramiento.
		A.12.1.2 Cambios en la gerencia	Se actualiza los cambios en la organización y los sistemas que afectan la seguridad de la información
	A.12.2 Protección contra el malware (programa malicioso)	A.12.2.1 Controles contra el malware	Existen antivirus en las estaciones de trabajo, pero los usuarios no tienen conciencia y bajan información no autorizada lo cual ponen en riesgo a los

			sistemas de información.
	A.12.3 Backup	A.12.3.1 Backup de la información	Tienen respaldo y copias de seguridad de la información y software pero falta procedimientos.
	A.12.4 Logeo y monitoreo	A.12.4.4 Sincronización de los relojes	Se sincronizan toda la plataforma de servidores
	A.12.7 Consideraciones de las auditorías sobre los sistemas de información	A.12.7.1 Controles de la auditoría sobre los sistemas de información	No se planifican actividades de auditoria que involucren comprobaciones en los sistemas operativos.
A.13 Seguridad de las comunicaciones	A.13.1 Gestión de la seguridad de las redes	A.13.1.1 Controles en las redes	La DTIC´S, cuenta con un Administrador de red y una división de redes y comunicaciones lo cual permite mejorar la administración y la seguridad de las redes.
	A.13.2. Transferencia de la información	A.13.2.1 Políticas y procedimientos de la transferencia de la información	No existen políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación
		A.13.2.4 Confidencialidad o acuerdos no divulgados	No existen documentos ni requisitos para la confidencialidad o acuerdos no divulgados de la organización sobre la protección de la información.
A.14.1Adqusición, desarrollo y mantenimiento del sistema	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificaciones de los requisitos de la seguridad de la información	Se especifican los requisitos de control de seguridad en los sistemas de información
A.15 Relación con los proveedores	A.15.1 Seguridad de la información en las relaciones con los proveedores	A.15.1.2 Consideración de la seguridad en los acuerdos con los proveedores	Se establecen los acuerdos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.
A.16 Gestión de los incidentes de seguridad de la información	A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora	A.16.1.1 Responsabilidades y procedimientos	No existen procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información
		A.16.1.2 Reporte de los eventos de seguridad de la información	Existen registros de los incidentes de seguridad.
		A.16.1.3 Reporte de las debilidades de la seguridad de la información	Existe reporte de debilidades sospechadas a los sistemas.

		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información	No existe almacenado el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información para futuros incidentes.
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio	A.17.1 Continuidad de la seguridad de la información	A.17.1.1 Continuidad de los planes de seguridad de la información	No están identificados los eventos de seguridad que causan interrupciones al servicio en la DTIC'S.
A.18 Cumplimiento	A.18.1 Cumplimiento de los requisitos legales y contractuales	A.18.1.1 Identificación de la ley aplicable y de los requisitos contractuales	Falta documentación de los sistemas de información
		A.18.1.2 Derechos de propiedad intelectuales	La DITIC'S si presenta documentación técnica y tiene licencias de Software
		A.18.1.3 Protección de los registros	Los archivos de información de cada una de las oficinas presentan buena protección.

3.9 Conclusiones del Diagnóstico

Tomando en consideración los objetivos de la investigación y el análisis e interpretación de las respuestas dadas por los sujetos de estudio en el instrumento aplicado y las observaciones hechas directamente en relación a los requerimientos de la institución, las conclusiones del estudio son las siguientes:

1. En la Cláusula Políticas de seguridad de la información, en la DTIC´S no existe un documento de política de seguridad de información, por la cual estas políticas no son conocidas ni revisadas.

2. En la Cláusula Organización de la Seguridad de la información, no están definidas claramente todas las responsabilidades de seguridad de la información.

3. En la Cláusula Seguridad de los recursos humanos, se lleva a cabo la verificación de los antecedentes de todos los candidatos al empleo por el departamento correspondiente, pero No existe proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad.

4. En la Cláusula Gestión de los Activos, no se cumple en su totalidad la devolución de todos los activos de la DTIC'S una vez terminado la relación laboral y no existen procedimiento para el manejo y almacenamiento de la información.

5. En la Cláusula Control de acceso, existe una política de control de acceso, pero existe un procedimiento formal y finalmente no se restringe el uso de programas utilitarios.

6. En la Cláusula Adquisición, desarrollo y mantenimiento del sistema, se especifican los requisitos de control de seguridad en los sistemas de información.

7. En la Cláusula Relación con los proveedores, se establecen los acuerdos relacionados a la seguridad de la información con cada

proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.

8. En la Cláusula Gestión de los incidentes de seguridad de la información, no existen procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información, existen registros de los incidentes de seguridad, existe reporte de debilidades sospechadas a los sistemas y no existe almacenado el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información para futuros incidentes.

9. En la Cláusula Gestión de los aspectos de la seguridad de la información para la continuidad del negocio, no están identificados los eventos de seguridad que causan interrupciones al servicio en la DTIC’S.

10. En la Cláusula Cumplimiento, falta documentación de los sistemas de información, la DITIC’S si presenta documentación técnica y tiene licencias de Software y los archivos de información de cada una de las oficinas presentan buena protección.

3.10 Recomandaciones del Diagnóstico

1. Realizar un documento de política de seguridad de información, las mismas que deberán ser revisadas y conocidas por la DTIC'S.

2. Definir las responsabilidades de seguridad de la información, las mismas que permitiran mantener la seguridad de la información.

3. Levar un registro de la verificación de los antecedentes de todos los candidatos que van ha ingresar a laborar en la institución, a fin de realizar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad.

4. Controlar que se cumpla en su totalidad la devolución de todos los activos de la DTIC'S una vez terminado la relación laboral y no existen procedimiento para el manejo y almacenamiento de la información.

5. Revisar periodicamente la política de control de acceso, a traves de un procedimiento formal para restringir el uso de programas utilitarios.

6. Sueprvisa el desarrollo y mantenimiento del sistema verificando los requisitos de control de seguridad en los sistemas de información.

7. Verificar los acuerdos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización a fin de precautelar la seguridad de la información.

8. Supervisar los procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información, mediante los registros de los incidentes de seguridad y los reporte de debilidades sospechadas a los sistemas a fin de precautelar la seguridad.

9. Supervisar la Gestión de los aspectos de la seguridad de la información para la continuidad del negocio, verificando e identificado los eventos de seguridad que causan interrupciones al servicio en la DTIC’S.

10. Verificar la documentación técnica de los sistemas de información y licencias de Software de la DITIC’S a fin de asegurar los sistemas de información.

CAPÍTULO 4

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA.

Una vez identificada la necesidad en la fase de diagnóstico y estudiada necesidad de establecer el Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se procedió al establecimiento del Diseño del SGSI.

4.1 Descripción de la Propuesta.

Para realizar el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se utilizará la norma ISO/IEC 27001:2013, el cual adopta el enfoque de procesos basado en el ciclo Deming "Planificar – Hacer – Verificar – Actuar" (PHVA), al flujo de la información militar a través del Sistema de Comunicaciones[4], al utilizar los servicios y sistemas informáticos por los usuarios de los repartos navales y militares, [5].

El Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. tiene como función básica Planificar, gestionar, controlar, integrar, e implementar proyectos, sistemas y servicios informáticos; manteniendo su disponibilidad y operatividad, para facilitar el cumplimiento de las tareas operativas y administrativas en las Instituciones Militares[5].

La Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las Fuerzas Armadas, poseen una estructura orgánica funcional de acuerdo a como se ilustra en el **Anexo A** y

[4] D.G.P. COGMAR-INF-002-2010-O. Directiva General Permanente. Seguridad de la Información.
[5] DTIC'S. Estatuto Orgánico por Procesos. Función Básica.

Anexo B, lo que permite la toma de decisiones de forma oportuna, brindando disponibilidad en la vinculación del talento humano del que dispone esta institución.

El SGSI propuesto dentro de este proyecto de titulación exige una serie de requisitos para que se establezca a través de la fase denominada “Planificar” una vez establecido el modelo se implementa en la institución la fase “Hacer”, [5].

Cuando el modelo propuesto se haya implantado y esté funcionando, se deberá “monitorear y revisar” durante la fase “verificar” finalmente, se procede a “Actuar” y tomar correctivos necesarios.

Este modelo propuesto permite realizar una identificación de activos de información, distinguir entre el análisis y evaluación del riesgo y visualizar la relación causa - efecto entre los elementos del riesgo.

4.2 Alcance del Diseño del SGSI

El alcance del Diseño de un Sistema Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se encuentra de acuerdo a los requerimientos de la COMACO y basados en la norma ISO/IEC 27001:2013, [5] ubicado en la ciudad de Quito, en el Edificio del Comando Conjunto de

las Fuerzas Armadas, segundo piso y Subsuelo de acuerdo a como se ilustra en el **Anexo G** y **Anexo H.**

El proyecto abarcará el alcance del diseño del SGSI, política del SGSI, enfoque de evaluación de riesgo, identificación del riesgo, análisis de riesgo y su evaluación, plan de tratamiento del riesgo y el proceso de toma de decisión gerencia y la revisión de los riesgos y la reevaluación.

Al realizar el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., permitirá que los riesgos de la seguridad de la información sean asumidos, gestionados y minimizados por el COMACO de una forma evaluada, documentada y estructurada.

Es importante aclarar que los aspectos que conforman la confidencialidad de la información en el Comando Conjunto de las Fuerzas Armadas, es un factor importante en el desarrollo de la investigación y es por eso que la información mostrada es referencial y solo para efectos académicos respectivos, en vista que la información militar[6] es secreta y confidencial.

Para la implementación, operación, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información para el

[6] (COMACO) Manual de Elaboración de Documentación de las Fuerzas Armadas.

Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., sólo se especificará los lineamientos generales.

Para identificar con precisión las interfaces y dependencias del SGSI con otras entidades de la DTIC'S y entidades civiles y militares externas, se optó por utilizar la metodología propuesta por [6], el método de las elipses, el cual definido como "…*método que permite, dado un determinado alcance de un SGSI, identificar sus interfaces, interdependencias con áreas y procesos, así como averiguar el tipo de memorando de entendimiento que existe o debiera de elaborarse, así como los contratos existentes y los grados de acuerdo necesarios*".

Se realizaron los siguientes pasos:

a) Se determina en la elipse concéntrica los distintos procesos y subprocesos que se realizan la DTIC'S.

b) Se determinó en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tiene con otros procesos de la DTIC'S y las entidades Militares

c) Se determinó aquellas organizaciones extrínsecas a la DTIC'S que tienen interacción con los procesos y subprocesos identificados en la elipse concéntrica

d) Se vinculó con flechas los tipos de interacción y la direccionalidad que tiene el flujo de información, la Figura 4.1 muestra este método aplicado a la DTIC'S.

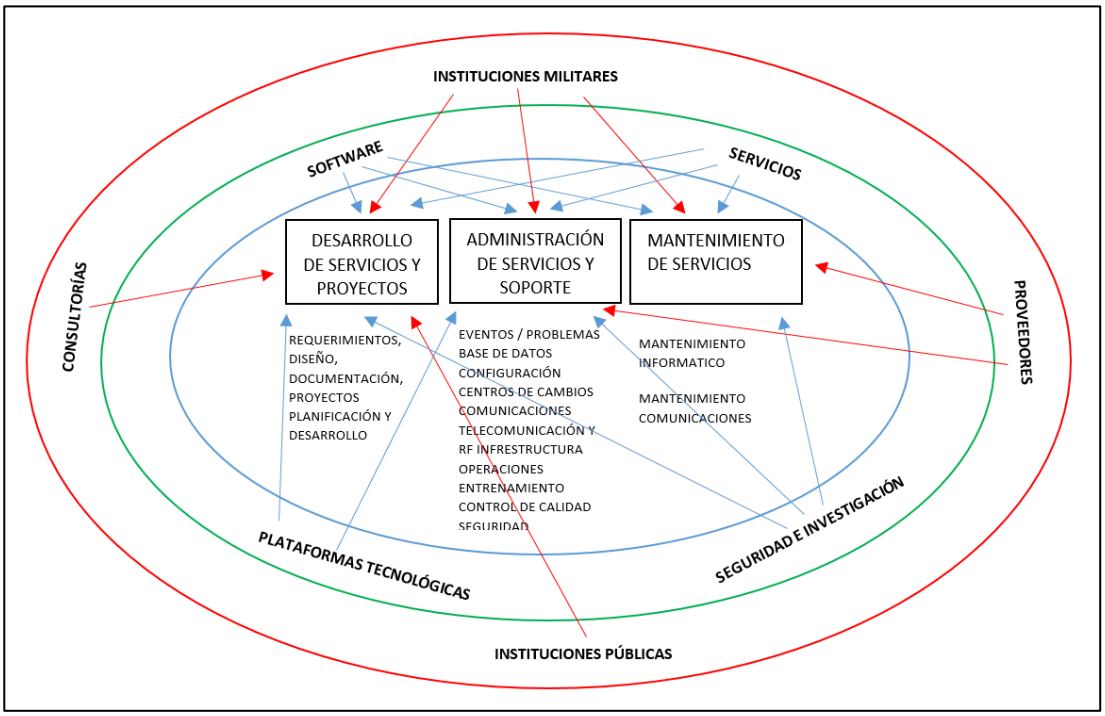


Figura 4.1 Metodología de las elipses de la DTIC'S.
Fuente: Autor.

La interconexión física de los elementos activos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se detalla en la Figura 6 los cuales son los activos que se utilizarán para el Diseño del Sistema de Gestión de Seguridad de la Información.

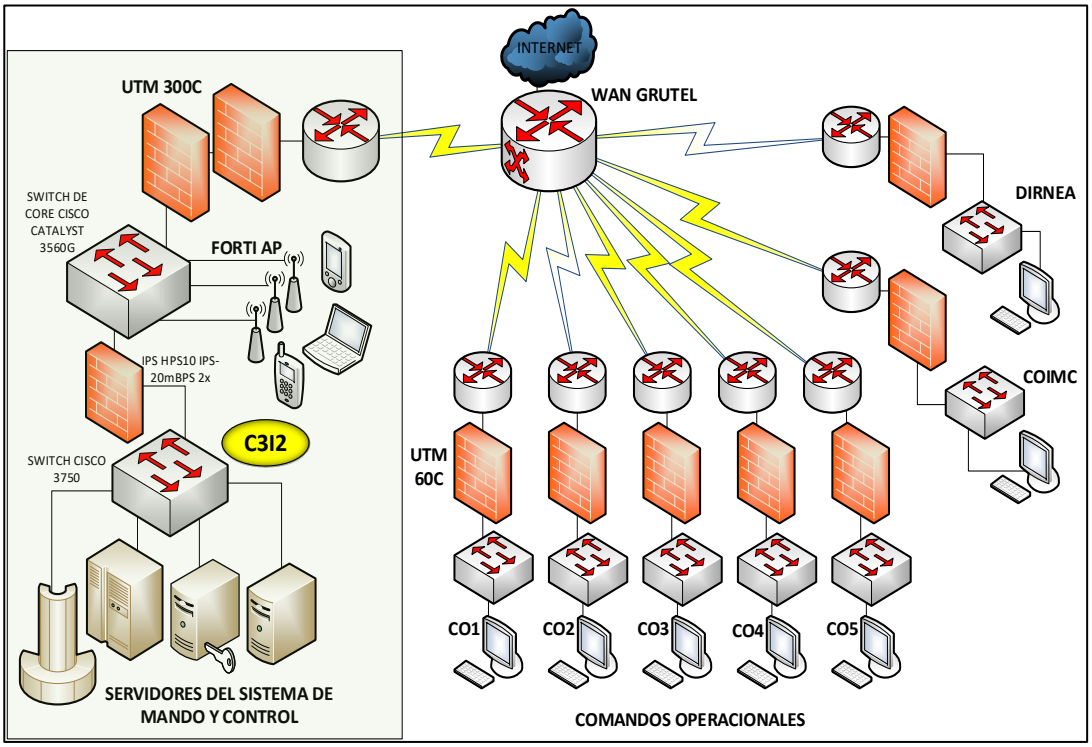


Figura 4.2 Diagrama Físico de red de la DTIC'S.
Fuente: Autor.

4.3 Política de un SGSI

La DTIC'S establecerá una política de seguridad para apoyar al Diseño del Sistema de Seguridad de Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

En el **Anexo H**, se observan las políticas de seguridad de la información para el Departamento de Informática de la Dirección de Tecnologías de

la Información y Comunicaciones del Comando Conjunto de las FF.AA., las mismas que contienen:

1. Alcance de la política
2. Definiciones
3. Descripción de las políticas
    a. Acceso a la información
    b. Administración de cambios
    c. Seguridad de la información
    d. Seguridad para los servicios informáticos
    e. Seguridad en los recursos informáticos
    f. Seguridad en comunicaciones
    g. Seguridad para los usuarios externos
    h. Software utilizado
    i. Actualización de hardware
    j. Almacenamiento y respaldo
    k. Contingencia
    l. Auditoría
    m. Seguridad física
    n. Estaciones de trabajo

o. Administración de la seguridad

4.4 Enfoque de Evaluación de Riesgo

El enfoque para el riesgo en una organización están determinados de manera muy precisa por el ISO/IEC 27001:2013. En el Capítulo 2, se determina que la metodología de evaluación de riesgo empleada es herramienta CRAMM, y el IT Baseline Protection Model del BSI Alemán.

La herramienta CRAMM (**CCTA Risk Analysis and Management Method)** (**Agencia Central de Comunicación y Telecomunicación)** creado por el Gobierno británico en 1987, puede usarse con ISO 27001 así como para el manejo de riesgo de negocios. Esta herramienta utiliza una escala de 1 a 10 para la valorización de los activos, de 1 a 5 niveles para las amenazas y de 1 a 3 para las vulnerabilidades y el cálculo del riesgo de 1 a 7 según una matriz, [8].

El IT Baseline Protection Model del BSI Alemán, permite establecer los riesgos en base a los activos, amenazas y contramedidas. Presenta una tabla de 200 amenazas clasificadas en cinco tipos: fuerza mayor, deficiencias organizacionales, fallas humanas, fallas técnicas y actos deliberados, tiene la desventaja de no trabajar directamente con vulnerabilidades.

Por lo anterior descrito, para la evaluación de riesgo de este proyecto no es recomendable trabajar con una sola metodología, es importante conocer las bondades de cada una y aprovecharlas para adaptarla en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

4.5 Identificación del Riesgo

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo contemplará:

1. Identificar los activos dentro del alcance del SGSI y los dueños de esos activos
2. Identificar las amenazas a esos activos
3. Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas
4. Identificar los impactos que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener sobre los activos.

4.5.1 Identificación de los Activos

Se realizó el levantamiento de información y la situación actual de los activos de información del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., clasificando en 7 clases de activos considerando de acuerdo a los activos que posee el Comando Conjunto de las FF.AA., mirando los criterios de confidencialidad, integridad y disponibilidad, [18].

Se identificaron los activos considerados vitales por el nivel de impacto que representa a la misma en el caso de si fallara o faltara, por tal motivo se generó un listado de los mismos, en el cual se asignó y clasificó a cada uno de los activos por su nivel de importancia (escala 1 – 10), siendo el valor de 10 como el activo de mayor importancia, como se detalla en la Tabla 18.

Tabla 18 Activos clasificados.
Fuente: Autor.

ACTIVOS CLASIFICADOS	
Clase 1 – Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones
Clase 2 – Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Clase 3 – Equipos informáticos	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Clase 4 – Software	Programas, aplicativos, desarrollos, software base, sistema de información

Clase 5 – Servicios	Contempla servicios prestados por el sistema
Clase 6 – Datos / Información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad.

CLASE 1 - INSTALACIONES			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
1.1	Centro Principal de Procesamiento	8	Centro Principal de procesamiento donde reside la infraestructura para soporta la operación del negocio
1.2	Centro Alterno de Procesamiento	5	Centro Alterno de procesamiento que contiene la infraestructura para la continuidad del negocio
1.3	Cuartos de comunicaciones	9	Instalación física donde residen los rack de comunicaciones
1.4	Área administración de plataforma	9	Instalación física donde están ubicados los administradores de plataforma

CLASE 2 – REDES DE COMUNICACIONES			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
2.1	Red LAN	9	Red LAN corporativa de la entidad
2.2	Red WAN	7	Red WAN de la entidad
2.3	Red WIFI corporativa	2	Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red corporativa de la entidad
2.4	Red WIFI invitados	5	Red Wifi para invitados

CLASE 3 – EQUIPOS INFORMÁTICOS			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
3.1	Servidores de Adm. Prod. y BDD	2	Servidores que soportan los servicios y bases de administración
3.2	SAN	9	Unidades de almacenamiento donde reside la información de la entidad
3.3	Dispositivos de red	6	Equipos y dispositivos de red activos (switch, router)
3.4	Computadores Administradores	2	Computadores que utilizan los administradores de plataforma
3.5	Equipos de seguridad perimetral	3	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad

CLASE 4 – SOFTWARE			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
4.1	Sistema de Control de Acceso	4	Sistema para controlar el acceso a las áreas de la entidad
4.2	Herramienta de Virtualización	3	Herramienta utilizada para la virtualización de servidores
4.3	Sistema Gestor Base de Datos	8	Sistema de gestión y administración de las bases de datos de la entidad
4.4	Sistema administración de la SAN	8	Sistema para administrar la SAN
4.5	Intranet	8	Intranet de la Entidad

CLASE 5 - SERVICIOS			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
5.1	Directorio activo	9	Servicio establecido donde están los objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red
5.2	Bases de datos	6	Bases de datos que almacenan la información de la entidad
5.3	FileServer	4	Almacenamiento de los documentos electrónicos que manejan las áreas de la entidad
5.4	Gestión de privilegios	5	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos.

CLASE 6 – DATOS / INFORMACIÓN			
Nro.	**Nombre Activo Primario**	**Nivel**	**Descripción general**
6.1	Identidad del Usuario	10	Información que identifica a un funcionario (nombre, cedula, datos biométricos como la huella, código del usuario, etc)
6.2	Datos de autenticación Usuarios genéricos	2	Usuario y Contraseña que utiliza los usuarios para ingresar a los recursos tecnológicos y aplicaciones. Usuario genéricos que utilizan las aplicaciones para conectarse a las bases de datos
6.3	Log de evento de seguridad	7	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones
6.4	Manuales técnicos de administración	10	Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la plataforma

Una vez determinado los activos de acuerdo con el alcance del Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se procede a identificar las amenazas y vulnerabilidades del mismo.

4.5.2 Identificación de Amenazas

Los activos de información están sujetos a distintas formas de amenazas, una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus

activos, se puede hacer algo indeseable o una ocurrencia natural.

Las amenazas pueden ser de distintos tipos con base en su origen, en la Tabla 17 se muestra una clasificación de 5 tipos de amenazas y 5 niveles de amenazas que afectan a los activos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 19 Amenazas definidas.
Fuente: Autor.

AMENAZAS DEFINIDAS

Tipo
1.- Fuerza Mayor
2.- Deficiencias organizacionales
3.- Fallas humanas
4.- Fallas técnicas
5.- Actos deliberados

Niveles de Amenazas	
Muy Baja	1
Baja	2
Media	3
Alta	4
Muy alta	5

TIPO 1 - FUERZA MAYOR			
Nro.	**Nivel**	**Descripción**	**Detalle**
1.1	3	Pérdida de personal	Por enfermedad, accidentes, muerte, huelgas que conduzcan a que tareas de TI cruciales no se puedan efectuar.
1.2	4	Fallas de los sistemas de TI	De un único componente que puede afectar toda la operación de TI. Fallas del ISP.
1.3	2	Rayos	Que causen alto voltaje o el disparo de extinguidores automáticos de incendio paralizando las operaciones.
1.4	4	Incendio	Además del daño directo el causado por el agua con que se ataca el incendio. Descuido en el manejo de material combustible, uso impropio de dispositivos eléctricos, fallas en el equipamiento eléctrico.

1.5	3	Inundación	Por lluvia, inundaciones, agua usada en un incendio, bloqueo de drenajes.
1.6	2	Cables quemados	Corte de conexiones, formación de gases agresivos, material aislante no resistente al fuego, fuego humeante sin llama en cables empaquetados.
1.7	2	Polvo y suciedad	Por trabajos realizados en paredes, pisos, actualizaciones de hardware, materiales de empaquetado.
1.8	2	Efectos de catástrofes en el ambiente	En los alrededores de la DTIC'S, desde accidentes técnicos y daños por colisiones.
1.9	2	Problemas causados por grandes eventos públicos	Interrupción de operaciones, violencias, cortes de líneas de transmisión.
1.10	2	Tormentas	Desprendimiento de instalaciones en azoteas (por ejemplo aire acondicionado), paredes débiles que caen y cortan cables.

TIPO 2 - DEFICIENCIAS ORGANIZACIONALES			
2.1	4	Falta o insuficiencia de reglas de seguridad en general	Organización: asignación responsabilidades, gestión de recursos.
2.2	5	Conocimiento insuficiente de documentos sobre reglas y procedimientos	Falta información procedimientos manejo de dispositivos de almacenamiento y e-mails.
2.3	2	Recursos incompatibles o inadecuados	Memoria principal o espacio en disco insuficiente.
2.4	3	Monitoreo insuficiente de las medidas de seguridad de IT	No se imprimen las entradas de consola para su análisis. Los servidores que se usan para comunicaciones externas deben chequearse semanalmente en cuanto a integridad.
2.5	2	Mantenimiento faltante o inadecuado	Baterías de UPS. Presión extinguidores.
2.6	1	Uso no autorizado de derechos	Derechos de admisión a hardware o software asignados a personas equivocadas, o un derecho abusado.
2.7	1	Uso no controlado de recursos	Los medios privados que pueden entrar virus en las PCs. Productos de limpieza no adecuados.
2.8	2	Ajuste deficiente a los cambios en el uso de IT	Cambios de derechos en personal por vacaciones. No se imprimen los cambios de procedimientos.
2.9	3	Medio de datos no disponible cuando se lo requiere	Falta de rotulación adecuada o almacenamiento en lugares no previstos.
2.10	3	Dimensionamiento insuficiente de redes y centro de cómputo	Sala de servidores, centros de cómputo. Capacidad red y computadores, extendida en línea por volumen de datos o nuevos servicios. Cableado. Nuevas normas.
2.11	2	Documentación insuficiente del cableado	Consecuencias por desconocimiento cableado interno y externo. Trabajos de terceros.
2.12	1	Protección inadecuada de dispositivos de distribución de energía	Si son accesibles en corredores y cajas de escaleras, cualquier persona podría manipularlos y causar una caída de energía.
2.13	2	Cambios no regulados de usuarios en laptops	Ante cambios de usuarios en móviles puede quedar información sensible o virus. Y si no se controlan esos cambios no se sabe quién los usó y cuándo.
2.14	1	Etiquetado inadecuado de medios de datos	El que recibe podría no poder identificar el origen, la información almacenada, o el propósito. Podría afectar una secuencia, los errores y correcciones que no quedan claros.

2.15	1	Entrega inapropiada de medios de datos	Puede caer en manos inapropiada. Direccionamiento, empaquetado, fallas de responsabilidad en recepción.
2.16	1	Provisión inadecuada de papel para impresoras	Papel, fuente de energía
2.17	4	Pérdida de confidencialidad de datos sensibles de la red a proteger	Si no hay protección con un firewall queda mucha información expuesta a Internet y hasta el resto puede deducirse u obtenerse con mayor facilidad.
2.18	2	Reducción de la velocidad de transmisión	Restricción de ancho de banda, retardos.
2.19	3	Procedimientos faltantes o inadecuados para test y liberación de software	Si no se hacen pruebas antes de instalar algo nuevo, pueden volverse amenazas. Sobre todo si se lo hace sin mayores conocimientos.
2.20	3	Documentación faltante o inadecuada	Varios: descripción de productos, uso por administrador y usuario y de sistema. Impactan la selección y toma de decisiones. Archivos temporales con información sensible, configuraciones que cambian y pueden afectar aplicaciones que estaban corriendo, cableado.
2.21	2	Violación de derechos de autor	Software pirata.
2.22	4	Prueba de software con datos de producción	Pensando que así se obtiene una evaluación definitiva de las funciones y performance. Puede ser que sean copias y en un ambiente aislado pero como son datos reales están expuestos a terceros no autorizados a leer esa información.
2.23	2	Planificación inadecuada de los dominios	En redes Windows pueden ocurrir relaciones de confianza inadecuadas. Esto puede darse especialmente cuando los derechos de acceso se hacen muy amplios asumiendo que nadie de otro dominio accederá los recursos locales.
2.24	3	Protección inadecuada del sistema Windows	Por defecto hay amplios derechos de acceso al sistema de archivos y registro.
2.25	1	Restricción inapropiada del ambiente de usuarios	Algunas permitidos, prohibidos todas los demás. O la inversa: algunas prohibidas, permitidas todas las demás.
2.26	2	Mecanismos de seguridad de bases de datos faltantes o implementados inadecuadamente	El software de BD trae generalmente mecanismos de seguridad que protegen los datos de accesos no autorizados, pero estos mecanismos generalmente no son automáticos sino que se activan manualmente por parte del administrador. Sino no se podría garantizar confidencialidad e integridad, así como tampoco identificar violaciones de seguridad de registro. Podría haber pérdidas de datos y la destrucción de la BD.
2.27	2	Complejidad del DBMS	Si los mecanismos de seguridad propios no son suficientes, o si las medidas que recomienda el fabricante no se tienen en cuenta. En cuanto al concepto de DB: que los datos específicos de la aplicación no se almacenen en medios separados, o el no uso de db triggers y procedimientos almacenados, o si su uso no es consistente resulta fácil a manipulaciones que pueden afectar la integridad.

2.28	3	Complejidad del acceso a las bases de datos	Que los derechos sean muy restrictivos y no se puedan realizar algunas tareas. O que sean muy laxos permitiendo manipulaciones. Si los usuarios pueden acceder directamente a la DB. Salvaguardas insuficientes para el acceso remoto a la DB. Restricciones a las consultas.
2.29	1	Organización deficiente del cambio de usuario en bases de datos	Varios usuarios compartiendo una DB en la misma estación de trabajo y que no se desconectan.
2.30	3	Deficiencias conceptuales de las redes	Usuarios trabajando en grupos teniendo presente confidencialidad e integridad. Nuevas aplicaciones con mayores exigencias de ancho de banda. Pérdida de disponibilidad con redes propietarias. Componentes que no soportan ciertos protocolos.
2.31	1	Descripción inadecuada de archivos	Varios mensajes del mismo origen sin identificación adecuada, cuando a una serie de mensajes se hacen correcciones en uno de ellos.
2.32	2	Almacenamiento inadecuado de un medio en casos de emergencias	Por falta de capacidad de almacenamiento que se haga back up solamente de los archivos log y de configuración.
2.33	1	Operación de componentes no registrados	Componentes agregados desconocidos para el administrador.
2.34	4	Manejo inapropiado de los incidentes de seguridad	Si no hay procedimientos apropiados para manejar incidentes se puede llegar a tomar decisiones incorrectas que afecten la seguridad (componentes que se mantienen pese a conocerse serias debilidades, o viceversa, se saca algo cuyo riesgo es menor.
2.35	3	Administración inapropiada de derechos de acceso	Porque intervienen muchas personas. No hay registro sistemático de todos los usuarios; quedan cuentas abiertas o se acumulan derechos por cambios de actividades. Cuidado especial con los grupos.

TIPO 3 - FALLAS HUMANAS			
3.1	2	Pérdida de confidencialidad /integridad de datos por errores de los usuarios	Impresiones en papel que caen en manos inapropiadas. Dispositivos de almacenamiento despachados sin borrar los datos anteriores. Derechos de acceso incorrectos que pueden hacer que se modifiquen datos críticos.
3.2	2	Destrucción negligente de equipamiento o datos	Apagado computador al aparecer mensaje de error que puede producir errores de integridad. Humedad de café, etc.
3.3	4	No cumplimiento con las medidas de seguridad de TI	Por negligencia o pruebas insuficientes. Podrían producirse daños que podrían haberse previsto o al menos minimizados.
3.4	1	Conexión inadmisible de cables	Por documentación o etiquetado deficiente. Puede ocasionar el paso de datos adicionales o a direcciones equivocadas.
3.5	2	Daño inadvertido de cables	Por falta protección, cables colgando, en el suelo, perforaciones, agua.
3.6	2	Riesgos planteados por el personal de limpieza o externo	Manejo inapropiado de equipos, uso indebido o robo de componentes.

3.7	2	Uso impropio del sistema de TI	Negligencia o ignorancia de medidas de seguridad. Falta de información de la operación y funcionamiento correcto del sistema de TI.
3.8	3	Administración inapropiada de los sistemas de TI	Negligencia de medidas de seguridad. Si algunos puntos de acceso se crean o no se deshabilitan por no ser necesarios para la operación regular.
3.9	1	Transferencia de registros de datos incorrecta o indeseada	Datos anteriores que no debieran aparecer. Si se envían electrónicamente las listas podrían no estar actualizadas respecto de personal que no trabaja más.
3.10	3	Exportación incorrecta de sistemas de archivos bajo Linux	Los discos exportados en Linux pueden montarse por cualquier computador con el nombre definido en /etc/exports. El usuario de ese computador puede asumir cualquier UID/GID, es decir que sólo se pueden proteger los archivos pertenecientes al root. Los archivos de todos los demás usuarios están completamente desprotegidos, especialmente los que pertenecen a usuarios privilegiados como bin o daemon.
3.11	4	Configuración impropia del sendmail	Errores de configuración que permitan obtener las IDs de usuario y grupo que estén configurados con las opciones u y g (normalmente daemon).
3.12	1	Administración incorrecta del sitio y derechos de acceso a los datos	Derechos de acceso incorrectos pueden permitir acceder a datos de auditoria así como ocultar las manipulaciones.
3.13	1	Cambio incorrecto de usuarios de PC	Eliminación de un usuario antes de ingresar otro por negligencia o conveniencia. Fallaría la auditoria de logs.
3.14	2	Administración impropia de una DBMS	Administración impropia de la DB, así como derechos de acceso demasiado generoso, irregularidad o falta de monitoreo, backups inadecuados, UDs inválidas pero no desactivadas, pueden producir pérdida de datos, manipulación intencional o inadvertida de datos, acceso no autorizado a datos confidenciales, pérdida de integridad de la DB, caída y destrucción.
3.15	3	Configuración inadecuada de los componentes activos de las redes	Configuración incorrecta de VLAN, tablas de enrutado en subredes sea el enrutado estático o de actualización automática por medio del RIP u OSPF, componentes que filtran protocolos y direcciones de red pero que también pueden permitir las conexiones de sistemas de TI externos dentro de la red protegida.
3.16	1	Interrupción de un servidor en operación	Servidor de gestión interrumpido se pierde lo que estaba en memoria, aparecerán inconsistencias en los datos administrados.
3.17	3	Errores en la configuración y operación	Información que ofrece el servidor Web o un servidor DNS, contenidos ejecutables de un e-mail, archivos bajados, programas que se abren sin ser necesarios y que pueden usarse para ataques.
3.18	4	Manejo inapropiado de contraseñas	Que no las conozcan otras personas. Tarjetas de ingreso perdidas. Nombres comunes, etc.
3.19	3	Falta de cuidado en el manejo de la información	Contraseñas escritas a la vista, información divulgada en celulares, viajando. Reparación de una máquina y quedan los datos para otro usuario.

TIPO 4 - FALLAS TECNICAS			
4.1	2	Interrupciones en la fuente de energía	Cortes breves (UPS), UPS en condiciones para switch back.
4.2	2	Fallas de las redes internas de alimentación	Electricidad, teléfono, aire acondicionado. También por temperatura, agua, etc.
4.3	2	Medios de datos defectuosos	Discos con caída de la cabeza, CD por ralladuras superficiales.
4.4	5	Reconocimiento de vulnerabilidades en el software	Errores no intencionales del programa no conocidos por usuario. Se siguen encontrando debilidades. Contramedida
4.5	4	Diversidad de posibilidades de acceso a sistemas de TI en red	Además del ingreso "directo" con contraseña, por sendmail que puede introducir textos, ftp anónimo sin contraseña, telnet registro completo. Windows más seguro.
4.6	1	Errores de transmisión de datos	Los errores en la ruta de transmisión o en los dispositivos de conexión pueden producir pérdidas o que la información se vuelva ilegible.
4.7	1	Defectos técnicos en dispositivos de impresión	Disponibilidad e integridad pueden verse afectadas.
4.8	1	Pérdida de datos debido al agotamiento del medio de almacenamiento	No se puede almacenar más datos, email entrante se rechaza, no se pueden mantener auditorias.
4.9	4	Fallas de una base de datos	Por errores o acto de sabotaje puede tener amplias consecuencias dependiendo de las funciones y significado de la DB. Consecuencias pérdidas financieras, interrupción parcial o total de las operaciones.
4.10	2	Pérdida de datos en una base de datos	Por manipulación inadvertida, caídas de la DB e intrusiones deliberadas. Podría impedirse la ejecución, perderse la correlación de datos. Puede ocurrir cuando se cambia el modelo de la DB.
4.11	3	Pérdida de integridad/consistencia de una base de datos	Corrupción parcial o datos no inteligibles por manipulación de datos no intencionales, chequeos inadecuados de la sincronización de transacciones e intrusiones deliberadas.
4.12	5	Falla o mal funcionamiento de un componente de red	Puede afectar a toda la red o secciones de la misma. Podría ser un switch que afecta toda su área o componentes activos en el camino de las comunicaciones (y no hay caminos redundantes) o para redundancia o balanceo de carga (con las consiguientes restricciones de ancho de banda).
4.13	4	Autenticación faltante o de pobre calidad	Pueden hacer que personas no autorizadas logren acceder al sistema, que no se puedan identificar las causas de problemas o no se pueda determinar el origen de los datos. Esto ocurre por contraseñas débiles, o no se los cambia con regularidad o hay fallas de seguridad frente a los que no se reacciona.
4.14	2	Falla de componentes de un sistema de gestión de red o de sistemas	Pueden fallar los componentes administrados o los de monitoreo mismo, la estación central de gestión o algún elementos de conmutación durante la transmisión correspondiente.
4.15	4	Vulnerabilidades o errores de software	Tanto standard como los demás. Quizás encripción de standard no es suficiente. Funciones sin documentar. Errores de seguridad en la programación, desborde de buffers.
4.16	1	Reconocimiento automático del DVD-ROM	Si el reconocimiento de DVD-ROM está activado en Windows puede ejecutarse algún programa peligroso en el momento del arranque.

TIPO 5 -ACTOS DELIBERADOS			
5.1	2	Manipulación/destrucción de equipamiento o accesorios de TI	Equipos, accesorios y documentación. Inspección indebida de datos sensibles. Destrucción de medios de datos.
5.2	3	Manipulación de datos o software	Adquisición errónea de datos, cambios derechos de acceso, modificación de datos contables o de mail. Depende de los derechos de acceso de la persona.
5.3	3	Ingreso no autorizado a un edificio	Robo o alteración al poder entrar especialmente en la noche.
5.4	3	Robo	Equipamiento TI, accesorios, software, datos, con información confidencial.
5.5	5	Vandalismo	Es como un ataque interno y externo pero no determinado por empleados frustrados, clima de trabajo propicio.
5.6	4	Ataques	Sobre los operadores de TI.
5.7	3	Intercepción de líneas	Existencia de programas debug de archivos que se pueden usar para otras causas.
5.8	3	Uso no autorizado de sistemas de TI	Sin identificación y autenticación no se puede controlar el uso no autorizado. Elección de contraseñas. Uso de diccionarios para romperlas.
5.9	1	Intercepción de llamadas telefónicas y transmisiones de datos	Por conferencia oculta o intercepción de línea.
5.10	1	Escuchas furtivas de salas	Terminales con micrófonos o uso del handsfree.
5.11	2	Mal uso de los derechos del administrador	Cuando se usan los privilegios del root de Unix para dañar el sistema o los usuarios. Puede ser con archivos con root como propietario y el bit seteado o por medio del comando su.
5.12	3	Caballos de Troya	Funciones escondida sin documentar. Cualquier programa más archivos batch, secuencias de control que sean interpretados por sistemas operativos o aplicaciones.
5.13	4	Virus de computador	Puede destruir datos de buteo, de archivos y macro virus.
5.14	1	Copia no autorizada de medios de datos	Puede ocurrir cuando se lo reemplaza o transporta que se han copias.
5.15	1	Uso no autorizado de dispositivos de impresión	Que usen papel con membrete de la empresa para cualquier uso particular o dañino para la empresa.
5.16	1	Visualización no autorizada de datos transmitivos	Si están en lugar abierto, cualquiera podría leer un mensaje que entra.
5.17	3	Ingeniería social	Generalmente mediante llamadas telefónicas haciéndose pasar por otros empleados, secretarias de jefes o administradores para solucionar posibles errores. Hasta se puede usar para saber si una persona no estará por unos días y así intentar usar su cuenta.
5.18	3	Macro virus	Vienen con archivos de Word o Excel. Se ejecutan al cargar el archivo.
5.19	4	Falsificación de dirección IP	Usado para ataques indirectos por medio de intermediarios con la dirección de origen falsificada como si proviniera de otro usuario de modo que las respuestas múltiples irán a la dirección de la víctima.
5.20	3	Abuso del protocolo ICMP	Por ser el ICMP un protocolo para información de errores y diagnóstico puede ser manipulado indebidamente por un hacker.

5.21	4	Mal uso de los derechos de administrador en sistemas Windows	Puede asumir propiedad de cualquier archivo. Podrían que quede registrado hace back up. Alteración de hora o seguimiento detallado de la actividad de usuario.
5.22	3	Manipulación de datos o software en sistemas de bases de datos	Provoca que los datos sean alterados o no puedan usarse por acción directa sobre los mismos o eliminación o modificación de archivos.
5.23	3	Conexión no autorizada de dispositivos de computación a una red.	Puede ocurrir conectándose al cableado de la red o directamente a las interfaces de dispositivos de interconexión.
5.24	2	Ejecución no autorizada de funciones de gestión de red.	Por medio del acceso a puertos administrativos de dispositivos de interconexión en forma local o remota.
5.25	1	Acceso no autorizado a componentes activos de red	Estos dispositivos tienen puerto USB lo que permite su administración. Así podría leerse su configuración y lo que puede deducirse de la misma.
5.26	3	Pérdida de confiabilidad en la información clasificada	Referida tanto a datos confidenciales tanto de la empresa como personales, así como también a la referida a contraseñas y certificados digitales.
5.27	4	Falsificación de DNS	Ataque que consiste en alterar las tablas de equivalencia de nombres de sitios o máquinas con sus respectivas direcciones IP.
5.28	3	Pérdida de integridad de información que debiera estar protegida.	Imposibilidad de lectura, o alteración de datos accidental o maliciosamente.
5.29	3	Adquisición no autorizada de derechos de administrador con Windows	Esta cuenta no puede eliminarse ni deshabilitarse por lo que no reacciona frente a sucesivos intentos de registro. Una administración remota pasará la contraseña lo que facilita su escaneado. También están en el registro y en archivos conocidos así como en dispositivos de almacenamiento y cintas de backups. También se podría lograr agregar una cuenta al grupo administrador.
5.30	1	Sabotaje	Manipulación o daño de objetos. Robo de UPS.

Utilizando las amenazas clasificadas, se procederá a realizar un cruce de las amenazas y los activos como se describe en la Tabla 20. Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en la intención de hacer daño.

Tabla 20 Cruce de las amenazas Vs. Activos.

Fuente: Autor.

Amenazas	Activos																								
	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	3.5	4.1	4.2	4.3	4.4	4.5	5.1	5.2	5.3	5.4	6.1	6.2	6.3	6.4
1.1		X			X									X	X	X			X	X						X
1.2	X				X					X				X	X	X			X	X		X				X
1.3							X	X		X		X		X	X				X			X		X		
1.4							X	X	X	X	X	X	X	X	X	X			X			X		X		
1.5							X	X	X	X	X	X		X	X	X			X			X		X		
1.6								X		X		X		X	X	X			X			X		X		
1.7								X		X	X	X		X	X	X			X			X		X		
1.8	X	X						X	X	X	X	X		X	X	X			X			X		X		
1.9	X		X				X	X	X	X	X	X		X	X	X			X			X		X		
1.10							X	X	X	X	X	X	X	X	X	X			X			X		X		
2.1			X	X	X	X		X		X	X	X		X	X	X			X	X	X				X	
2.2			X	X		X				X																X
2.3																									X	X
2.4			X	X	X	X				X	X					X										
2.5			X			X								X	X									X		X
2.6						X		X			X			X	X				X		X					X
2.7														X	X	X										X
2.8			X			X																				
2.9																					X					X
2.10						X				X	X	X								X						
2.11								X		X		X								X						
2.12			X								X	X		X	X	X			X					X		X
2.13				X										X												
2.14											X										X					
2.15			X																		X					
2.16					X																X			X		
2.17																	X						X			X
2.18																		X							X	X
2.19			X			X														X					X	X

2.20																				X					X	X
2.21			X																	X	X				X	X
2.22						X														X						X
2.23														X	X	X		X								
2.24														X	X	X		X								X
2.25																										X
2.26																										X
2.27																										X
2.28																										X
2.29																X			X	X						X
2.30			X								X															X
2.31			X																		X					X
2.32				X																X	X					
2.33						X					X					X			X	X	X					X
2.34																				X	X					X
2.35													X													
3.1					X															X	X					X
3.2					X										X	X			X							X
3.3					X						X	X		X	X	X			X						X	X
3.4																					X					
3.5														X	X	X			X							X
3.6					X						X			X	X					X						
3.7			X	X		X					X			X	X					X						X
3.8																				X						X
3.9																					X					X
3.10																	X						X			
3.11																	X									
3.12											X									X						X
3.13																				X	X					X
3.14																										X
3.15																			X	X						X
3.16																				X						X
3.17														X	X	X									X	X

3.18			X	X							X			X	X	X			X							X
3.19														X	X	X										X
4.1			X		X					X				X	X	X	X		X			X	X	X		
4.2										X				X	X	X			X			X		X		
4.3																										X
4.4																									X	X
4.5											X							X			X					
4.6																					X					
4.7					X																X					
4.8			X																							X
4.9																										X
4.10			X																							X
4.11			X																							X
4.12														X	X	X			X							X
4.13																	X						X			X
4.14																									X	
4.15																										
4.16																		X								
5.1			X		X									X	X	X			X			X		X		X
5.2					X																			X		X
5.3											X			X	X	X			X			X		X		X
5.4	X								X	X	X	X		X	X	X			X							
5.5	X				X		X	X	X	X	X	X	X	X	X	X			X							
5.6	X	X			X									X	X	X			X							X
5.7											X			X	X	X										X
5.8														X	X	X										X
5.9			X		X						X															
5.10					X																					
5.11	X		X		X									X	X	X			X							X
5.12			X	X										X	X	X									X	X
5.13			X	X	X									X	X	X		X							X	
5.14			X		X						X															X
5.15	X																									

5.16					X																					
5.17					X						X															X
5.18			X	X	X									X	X	X		X							X	X
5.19														X	X	X										X
5.20																X			X							X
5.21																		X								
5.22																										X
5.23					X																					X
5.24																X			X							X
5.25																X			X							
5.26					X																					X
5.27																										X
5.28					X						X															X
5.29	X	X	X	X					X	X	X	X		X	X	X		X	X	X				X		X
5.30																										X

4.5.3 Identificación de Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Al respecto (Alexander, 2007), define la vulnerabilidad como una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema. Las vulnerabilidades no causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

En la Tabla 21, se presenta las vulnerabilidades clasificadas en tipo 1: física, organizacionales y operacionales, tipo 2: técnica para plataforma Linux, tipo 3: técnica para plataforma Windows y tipo 4: técnica de otros dispositivos.

Tabla 21 Vulnerabilidades clasificadas.
Fuente: Autor.

VULNERABILIDADES CLASIFICADAS		
TIPO 1 - FÍSICAS, ORGANIZACIONALES Y OPERACIONALES		
Nro.	**Nivel**	**Descripción**
1,1		**SEGURIDAD LÓGICA**
1.1.1		**Identificación**
1.1.1.1	1	Datos del perfil de usuarios dados de alta
1.1.1.2	2	Gestión de bajas de usuarios
1.1.1.3	2	Mantenimiento de cuentas
1.1.1.4	2	Manejo de los permisos para los accesos
1.1.1.6	1	Identificación única o grupal
1.1.1.7	1	Gestión de grupos

1.1.1.8	2	Súper usuario
1.1.1.9	1	Visualización del logeo en pantalla
1.1.2		**Autenticación**
1.1.2.1	2	Manejo de los datos de autenticación
1.1.2.2	1	Manejo de intentos de logeo
1.1.3		**Contraseñas**
1.1.3.1	2	Generación de contraseñas
1.1.3.2	1	Gestión de cambio de contraseñas
1.1.4		**Control de acceso lógico**
1.1.4.1	1	Modelo y aplicación
1.1.4.2	2	Criterios de acceso
1.1.4.3	3	Mecanismos de control de acceso interno
1.1.4.4	3	Control de acceso externo
1,2		**SEGURIDAD EN LAS COMUNICACIONES**
1.2.1		**Configuración de la red**
1.2.1.1	3	Comunicaciones vía modem
1.2.1.2	2	Recursos compartidos de discos de PC
1.2.1.3	1	Estado de puertos de servicios no necesarios
1.2.2		**Virus y Antivirus**
1.2.2.1	3	No está habilitado para envío y recepción de mail
1.2.2.2	2	Actualizaciones no adecuadamente frecuentes
1.2.2.3	2	No es suficiente la frecuencia de escaneado de las unidades de las computadores
1.2.2.4	1	No se generan discos de restauración en las PCs bajo Windows
1.2.3		**Documentación, normas**
1.2.3.1	1	Grado y detalle de la información documentada de la red
1.2.3.2	2	Gestión y procesos de parches
1.2.3.3	1	Documentación de la configuración de las PCs
1.2.4		**Ataques a la red**
1.2.4.1	1	Antecedentes de ataques ocurridos a la red
1.2.5		**Firewall**
1.2.5.1	3	Tipo, configuración y nivel de control de firewall
1.2.5.2	1	Pruebas de configuración de firewall
1.2.5		**Control impresión y envío de datos**
1.2.5.1	2	Control de envíos de datos
1.2.5.2	1	Distribución de datos recibidos
1,3		**SEGURIDAD EN LAS APLICACIONES**
1.3.1		**Sistema Operativo**
1.3.1.1	1	Requisitos de seguridad considerados al elegir el sistema operativo
1.3.2		**Control de datos de aplicaciones**
1.3.2.1	1	Existencia de control de cambios para archivos de sistema o bases de datos
1.3.2.2	3	Confidencialidad de datos de laptops y notebooks
1.3.2.3	2	Logs de transacciones y sus detalles
1.3.3		**Control de datos en el desarrollo**
1.3.3.1	1	Existencia de control de cambios para el desarrollo
1.3.3.2	1	Control del contenido de archivos de entrada
1.3.3.3	2	Control de validez de datos ingresados manualmente
1.3.3.4	1	Control de consistencia de datos de salida
1.3.4		**Seguridad de bases de datos**
1.3.4.1	2	Control de acceso propio de las bases de datos
1.3.4.2	1	Control de instancias de uso
1.3.4.3	1	Chequeo regulares de seguridad
1.3.4.4	1	Marcado o borrado de archivos eliminados
1.3.5		**Control de aplicaciones**
1.3.5.1	2	Controles con que se realiza la instalación y actualización de parches
1.3.5.2	1	Documentación de la instalación o actualización de software

1.3.5.3	2	Control de aplicaciones en máquinas de usuarios
1.3.5.4	1	Control de información que bajan los usuarios de la Web
1.3.6		**Mantenimiento de aplicaciones**
1.3.6.1	1	Documentación de cambios de emergencia
1.3.6.2	1	Control regular de programas y servicios innecesarios
1.3.6.3	1	Gestión de cambios complejos en archivos de configuración
1.3.6.4	2	Registro de cambios en las configuraciones
1.3.7		**Ciclo de vida**
1.3.7.1	1	Metodología usada para el desarrollo
1.3.7.2	2	Manejo del código fuente y documentación con desarrollos por terceros
1.3.7.3	1	Uso métricas en el desarrollo
1.3.7.4	1	Registros históricos de las modificaciones
1.3.7.5	2	Existencia de requisitos de seguridad
1.3.7.6	1	Medidas de seguridad durante las implementaciones
1.3.7.7	1	Forma y documentación de pruebas
1.3.7.8	1	Metodología usada para el mantenimiento
1.3.7.9	1	Detalles de la documentación generada en el desarrollo
1,4		**SEGURIDAD FISICA**
1.4.1		**Control de acceso al centro de cómputos**
1.4.1.1	2	Restricción de acceso a personas ajenas al área
1.4.1.2	1	Control personal de limpieza en locales con servidores
1.4.2		**Control de acceso a los equipos de los usuarios**
1.4.2.1	2	Habilitación del NetBIOS
1.4.2.2	1	Habilitación y control de dispositivos externos
1.4.2.3	3	Control de virus
1.4.2.4	2	Existencia de grabadoras de CD y DVD
1.4.2.5	1	Agregado no autorizado de dispositivos externos
1.4.2.6	2	Control y revisión de dispositivos instalados en las PCs
1.4.2.7	1	Apagado o no de los servidores
1.4.3		**Utilidades de soporte**
1.4.3.1	2	Gestión de fallas dispositivos externos al funcionamiento del equipamiento de TI
1.4.4		**Estructura del edificio**
1.4.4.1	1	Tipo, condiciones e instalación del cableado de red
1.4.4.2	1	Falta de información de otras instalaciones que corran en paralelo
1.4.4.3	1	Actividades que pueden afectar las operaciones
1.4.4.4	1	Actividades externas que pueden afectar las operaciones
1.4.4.5	2	Protecciones antirrayos
1.4.5		**Clasificación de datos y hardware**
1.4.5.1	1	Forma de rotular computadoras y periféricos
1.4.5.2	1	Inventario de recursos de hardware y software
1.4.6		**Backup**
1.4.6.1	2	Frecuencia de backups
1.4.6.2	2	Datos que se backapean
1.4.6.3	2	Tipos de backup que se realizan
1.4.6.4	2	Medios de almacenamiento de backups
1.4.6.5	1	Rotación de medios
1.4.6.6	1	Herramientas de backup
1.4.6.7	2	Responsables del backup
1.4.6.8	1	Procedimientos de backup
1.4.6.9	2	Pruebas periódicas de recuperación
1.4.6.10	2	Lugar de almacenamiento y controles de acceso
1.4.6.11	1	Rotulación y documentación de backups
1,5		**ADMINISTRACION DEL CENTRO DE COMPUTO**
1.5.1		**Contramedidas**
1.5.1.1	1	Tipo y regularidad de chequeos
1.5.1.2	2	Planificación y documentación de actividades del área

1.5.1.3	1	Documentación detallada del equipamiento
1.5.1.4	2	Documentación y manuales de procedimientos y seguridad
1.5.2		**Responsabilidad del equipo de seguridad**
1.5.2.1	3	Administración de emergencias
1,6		**REGISTROS Y AUDITORÍAS**
1.6.1		**Auditorías generales**
1.6.1.1	2	Realización y objetos auditados
1.6.1.2	1	Monitoreo y herramientas
1.6.1.3	2	Gestión de logs
1.6.1.4	1	Utilidad auditoría para rastreo de acciones
1.6.1.5	1	Históricos generados
1.6.2		**Logs**
1.6.2.1	3	Control de acceso
1.6.2.2	2	Identificación y almacenamiento
1.6.2.3	2	Información contenida en los logs
1.6.2.4	1	Análisis que se realiza
1.6.3		**Auditoría de servidores**
1.6.3.1	1	Trabajos de mayor uso CPU y memoria
1.6.3.2	1	Datos de mayor tráfico, CPU y memoria
1.6.3.3	1	Aplicaciones de mayor tráfico, CPU y memoria
1.6.4		**Auditoría de control de acceso**
1.6.4.1	2	Existencia de logs
1.6.4.2	2	Almacenamiento y acceso
1.6.4.3	1	Duración y tratamiento posterior al vencimiento
1.6.4.4	2	Contenido de los logs
1.6.5		**Auditoría de redes**
1.6.5.1	1	Monitoreo de red
1.6.5.2	1	Periodicidad de chequeos
1.6.5.3	1	Datos revisados y estadísticas
1,7		**PLAN DE CONTINGENCIAS**
1.7.1		**Plan de contingencias**
1.7.1.1	2	Existencia, justificaciones
1.7.1.2	1	Alcance del plan
1.7.1.3	2	Responsabilidades y entrenamiento
1.7.1.4	2	Documentación
1.7.2		**Plan de recuperación de desastres**
1.7.2.1	3	Responsabilidades
1.7.2.2	2	Identificación de funciones críticas
1.7.2.3	2	Grupo y responsable
1.7.2.4	2	Inventario de equipamiento
1.7.3		**Administradores de aplicaciones y sistemas**
1.7.3.1	1	Personal de desarrollo
1.7.3.2	2	Técnicos
1.7.3.3	2	Administradores de Redes
1.7.4		**Gerencia en seguridad**
1.7.4.1	3	Visón y compromiso general y medio en la seguridad
1.7.4.2	3	Reglas de seguridad
1.7.4.3	1	Personal en general - procedimientos
1.7.4.4	2	Personal de desarrollo - procedimientos
1.7.4.5	3	Técnicos - procedimientos
1.7.4.6	3	Administradores de redes - procedimientos
TIPO 2 - TECNICAS DE PLATAFORMAS LINUX		
2,1		**SERVICIOS ACTIVOS INNECESARIOS**
2.1.1	2	Hay habilitados servicios innecesarios
2,2		**Bind/DNS**
2.2.1	2	Instalación/ISC, versión y parches

2.2.2	2	Actualización dinámica del DNS
2.2.3	2	Demonio named habilitado en servidores no DNS
2,3		**RPC**
2.3.1	3	RPC Habilitado
2.3.3	2	Servicios RPC que se pueden explotar
2,4		**SNMP**
2.4.1	2	Versión y puertos habilitados
2.4.2	3	Nombres comunidad por default
2.4.3	2	Chequeo registros MIB
2,5		**Shell seguro**
2.5.1	1	Instalación y versión
2,6		**Servicios NIS/NFS**
2.6 .1	3	Versión NIS
2.6 .2	3	Ubicación password del root con NIS
2.6 .3	2	Versión NFS
2.6 .4	3	Configuración archivo export y montaje de sistema de archivos NFS
2,7		**Open SSL**
2.7.1	1	Versión
2,8		**FTP**
2.8.1	3	Habilitación y funcionalidad anónima
2.8.2	3	Sin uso de password en el modo de subida
2.8.3	3	No hay restricciones y mecanismos para direcciones IP o dominios
2.8.4	3	No se usan restricciones propias del servidor ftp
2.8.5	3	Especificación de las cuentas administrativas en archivo ftpusers
2.8.6	3	No hay diferenciación archivos contraseñas con los del OS
2.8.7	2	Permisos y propietarios del raíz y subdirectorios etc y bin del ftp anónimo
2.8.8	2	Permisos y propietarios de archivos de subdirectorios etc y bin
2.8.9	2	Permisos y propietarios directorio home ~ftp/
2.8.10	3	Existencia de archivos .rhosts y .forward
2.8.11	3	Restricciones de escritura para everyone en directorios ftp y sus archivos
2,9		**Otras de contraseñas**
2.9.1	2	Hay cuentas extras con UID 0, o sin contraseñas en el archivo passwd
2.9.2	3	tftp habilitado
2.9.3	3	tftp necesario pero sin precauciones de acceso restringido
2.9.4	2	No se usa un programa para mejorar la elección de contraseñas
2,10		**Otros Servicios de red**
2.10.1	2	Permisos y propietarios no adecuados en archivos de servicios de red
2.10.2	2	Cron acepta usuarios ordinarios
2.10.3	3	Se puede registrar como root en la consola en forma remota
2.10.4	3	Terminales no adecuados en el archivo de terminal seguro
2,11		**Seguridad sistema de archivos**
2.11.1	2	Archivos .exrc no justificados
2.11.2	2	Archivos .forward en directorios home de usuarios
2.11.3	2	Umask inadecuado de algunos programas
2.11.4	2	Restricciones de acceso no adecuadas en algunos archivos bajo /etc
2.11.5	3	Escritura indebida de los archivos log
2.11.6	2	Características extendidas (inmutabilidad y sólo anexado) no habilitadas
2.11.7	2	Inadecuados permisos, propiedad y grupo de /vmunix
2.11.8	3	Archivos que no debieran ser propiedad sino de root, y si /tmp no tiene el sticky-bit
2.11.9	3	Archivos o directorios no esperados que son escribibles por cualquiera
2.11.10	2	Archivos que no debieran tener seteados el bit SUID o SGID
2.11.11	2	Umask inadecuado de algunos usuarios
2.11.12	2	Archivos ordinarios en el directorio /dev
2.11.13	2	Archivos especiales fuera de /dev

2.11.14	2	Archivos ejecutables y sus directorios ascendentes escribibles por grupos o cualquiera
2.11.15	2	Archivos sin propietarios
2,12		**Monitoreo del sistema**
2.12.1	3	No se han definido los archivos log adecuados para seguridad
2.12.2	2	No se usan las extensiones de seguridad de Linux para los archivos log
2.12.3	3	Ausencia de registro de las actividades de los administradores
2.12.4	2	Falta de control de las modificaciones de archivos de sistema
2,13		**Servicios de archivos**
2.13.1	2	Inadecuados permisos y propiedad del archivo /etc/export
2,14		**Linux**
2.14.1	3	Parches y actualizaciones
Tipo 3 - TECNICAS DE PLATAFORMAS WINDOWS		
3,1		**IIS**
3.1.1	3	Versión y parches del IIS
3.1.2	2	Versiones actuales del IIS; ACL y directorios
3.1.3	2	Habilitación del log del IIS
3.1.4	3	WebDav ntdll.dll en IIS
3.1.5	2	Aplicaciones de muestra en directorios iissamples, iishelp y msadc
3,2		**SQL Server**
3.2.1	3	Versión y parches del SQL Server
3.2.2	2	Log autenticación servidor SQL
3.2.3	2	Cuenta SA, contraseña
3,3		**Autenticación**
3.3.1	3	Autenticación, algoritmo usado
3.3.2	3	Archivo hashes LM, habilitación autenticación a través de la red
3,4		**Internet Explorer**
3.4.1	3	Versión y parches del Internet Explorer
3.4.2	2	Nivel seguridad del IE
3,5		**RAS**
3.5.1	3	Uso SMB, conectividad NetBios
3.5.2	2	Sesión nula, registro anónimo
3.5.3	3	Acceso remoto al registry
3.5.4	3	rpc y parches
3,6		**MDAC/RDS**
3.6.1	3	Versión y parches del MDAC
3.6.2	2	Archivo msadcs.dll con Windows
3.6.3	1	Versión y SP del Jet Engine
3,7		**Windows Scripting Host**
3.7.1	3	Habilitación del Windows Scripting Host
3.7.2	1	Forma de ejecución de scripts
3,8		**Outlook**
3.8.1	2	Ventana de vista previa del Outlook
3.8.2	1	Restricción zona de seguridad del Outlook
3,9		**Trasferencia de datos**
3.9.1.	3	Puertos de aplicaciones de transferencia
3.9.2	2	Existencia en disco de transferencia
3,1		**SNMP**
3.10.1	2	Versión y puertos habilitados del SNMP
3.10.2	3	Nombres comunidad por default del SNMP
3.10.3	2	Chequeo registros MIB del SNMP
3,11		**Acceso remoto al registry**
3.11.1	3	Registros bajo SecurePipeServers
3,12		**Otros seteados del registry**
3.12.1	3	Registro Winlogon
3.12.2	2	Registro LanMan Print Services, para no poder agregar drivers impresión

3.12.3	2	Registro Subsystems, OS/2 y Posix
3.12.4	2	Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema
3.12.5	2	Registro Session Manager, atributos recursos compartidos, borrado archivo páginas
3,14		**Otras cuestiones de contraseñas**
3.14.1	2	Uso del passfilt.dll
3.14.2	1	Uso del syskey.exe
3,15		**Sistema de archivos**
3.15.1	3	Se usa FAT
3.15.2	2	Grupos Everyone (Todos) y/o Usuarios controlados
3,16		**Logs de auditoria**
3.16.1	2	Logs en Event Viewer
3.16.2	1	Nombres existentes en registro HKLM\System\CurentControlSer\\Control\Lsa
3,17		**Utilitarios de cuidado**
3.17.1	2	Existencia y/o restricciones de acceso de archivos ejecutables de cuidado
3.17.2	1	Ubicación de los archivos ejecutables de cuidado
3.17.3	2	Existencia del programa rollback.exe
3,18		**Subsistemas de cuidado**
3.18.1	2	Existencia de c:\windows\system32\os2 y subdirectorios
3.18.2	2	Archivos del os2 y posix en c:\windows\system32
3.18.3	1	Registros os2 subsystem for windows
Tipo 4 - TECNICAS DE OTROS DISPOSITIVOS		
4,1	2	**Grupos de PCs**
4,2	3	**Grupos de laptops y notebooks**
4,3	3	**Routers**
4,4	3	**Switches**
4,5	2	**Otros dispositivos**

Con las vulnerabilidades clasificadas en el Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA., se procederá a verificar cada una de ellas con los activos del Sistema de Gestión de Seguridad de la Información SGSI, de acuerdo a como se indica en el **Anexo I**, a continuación en la Tabla 22 se presentan el resumen de las vulnerabilidades.

Tabla 22 Resumen de las vulnerabilidades para la DTIC'S.
Fuente: Autor.

	Vulnerabilidades Físicas, Organizacionales y Operacionales	Plataforma Linux Firewall	Plataforma Windows		
			Servidor1	Servidor2	Servidor3
Total de vulnerabilidades potenciales	129	55	43	43	43
Vulnerabilidades no presente	10	9	3	11	7
Vulnerabilidades de nivel 1	56	2	5	4	5
Vulnerabilidades de nivel 2	51	23	20	17	20
Vulnerabilidades de nivel 3	12	21	15	11	11
Nivel Relativo de Vulnerabilidad Total	162	83	67	57	61
Servidores más vulnerables			***		
Servidores más vulnerable en el Nivel 3		***	***		

4.5.4 Cálculo de Amenazas y Vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo, define el riesgo como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular, [19].

En la Tabla 23 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones

del Comando Conjunto de las FF.AA. como son: Centro Principal de Procesamiento.

Tabla 23 Cruce de las Amenazas y las Vulnerabilidades del Centro Principal de Procesamiento (Activo 1.1).
Fuente: Autor.

No.	Div.	Amenaza Descripción	Vulnerabilidades							
1.2	4	Fallas de los sistemas TI	1.7.1.1	1.7.1.2	1.7.1.3	1.7.1.4	1.7.2.1	1.7.2.2	1.7.2.3	1.7.2.4
1.3	2	Rayos	1.4.4.5							
1.4	4	Incendio	1.4.3.1							
1.5	3	Inundación	1.4.4.2							
1.6	2	Cables quemados	1.4.3.1							
1.7	2	Polvo y suciedad	1.4.4.3							
1.8	2	Efectos de catástrofes en el ambiente	1.4.4.4							
1.9	2	Problemas causados por grandes eventos públicos	1.4.4.4							
1.10	2	Tormentas	1.4.4.4							
2.1	4	Falta o insuficiencia de reglas de seguridad en general	1.2.3.1	1.2.4.1	1.5.1.4					
2.2	5	Conocimiento insuficiente de documentos sobre reglas y procedimientos	1.5.2.1							
2.4	3	Monitoreo insuficiente de las medidas de seguridad IT	1.6.1.1	1.6.1.2	1.6.1.3	1.6.1.4	1.6.1.5			
2.10	3	Dimensionamiento insuficiente de redes y centro de cómputo	1.5.1.1							
2.11	2	Documentación insuficiente del cableado	1.4.4.1							
5.4	3	Robo	1.4.1.1							
5.5	5	Vandalismo	1.4.4.3	1.4.4.4						
5.29	1	Sabotaje	1.4.1.1	1.4.1.2	1.4.4.3	1.4.4.4				

En la Tabla 24 se describe las vulnerabilidades potenciales que pueden afectar al Centro Principal de Procesamiento del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 24 Vulnerabilidades potenciales que pueden afectar al Centro Principal de Procesamiento (Activo 1.1).
Fuente: Autor.

Nro.	Nivel	Vulnerabilidades Potenciales
1.2.3.1	1	Grado y detalle de la información documentada de la red
1.2.4.1	1	Antecedentes de ataques ocurridos a la red
1.4.1.1	2	Restricción de acceso a personas ajenas al área
1.4.1.2	1	Control personal de limpieza en locales con servidores
1.4.3.1	2	Gestión de fallas dispositivos externos al funcionamiento del equipamiento TI
1.4.4.1	1	Tipo, condiciones e instalación del cableado de red
1.4.4.2	1	Falta de información de otras instalaciones que corran en paralelo
1.4.4.3	1	Actividades que pueden afectar las operaciones
1.4.4.4	1	Actividades externas que pueden afectar las operaciones
1.4.4.5	2	Protecciones antirrayos
1.5.1.1	1	Tipo y regularidad de chequeos
1.5.1.4	2	Documentación y manuales de procedimientos y seguridad
1.5.2.1	3	Administración de emergencias
1.6.1.1	2	Realización y objetos auditados
1.6.1.2	1	Monitoreo y herramientas
1.6.1.3	2	Gestión de logs
1.6.1.4	1	Utilidad auditoria para rastreo de acciones
1.6.1.5	1	Históricos generados
1.7.1.1	2	Existencia, justificaciones
1.7.1.2	1	Alcance del plan
1.7.1.3	2	Responsabilidades y entrenamiento
1.7.1.4	2	Documentación
1.7.2.1	3	Responsabilidades
1.7.2.2	2	Identificación de funciones críticas
1.7.2.3	2	Grupo y responsable
1.7.2.4	2	Inventario de equipamiento

En la Tabla 25 se describe las amenazas y vulnerabilidades verificadas de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA. como son: Centro Principal de Procesamiento.

Tabla 25 Amenazas vs. Vulnerabilidades verificadas para el Centro Principal de Procesamiento (Activo 1.1).
Fuente: Autor.

	Amen.	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	2.1	2.2	2.4	2.10	2.11	5.4	5.5	5.29
Vulner.	Nivel	4	2	4	3	2	2	2	2	2	4	5	3	3	2	3	5	1
1.2.3.1	1										X							
1.2.4.1	1										X							
1.4.1.1	2															X		X
1.4.1.2	1																	X
1.4.3.1	2			X		X												
1.4.4.1	1														X			
1.4.4.2	1				X													
1.4.4.3	1						X										X	X
1.4.4.4	1							X	X	X							X	X
1.4.4.5	2		X															
1.5.1.1	1													X				
1.5.1.4	2										X							
1.5.2.1	3											X						
1.6.1.1	2												X					
1.6.1.2	1												X					
1.6.1.3	2												X					
1.6.1.4	1												X					
1.6.1.5	1												X					
1.7.1.1	2	X																
1.7.1.2	1	X																
1.7.1.3	2	X																
1.7.1.4	2	X																
1.7.2.1	3	X																
1.7.2.2	2	X																
1.7.2.3	2	X																
1.7.2.4	2	X																

En la Tabla 26 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la

Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Servidor de Producción.

Tabla 26 Cruce de las Amenazas y las Vulnerabilidades Servidor de Producción. (Activo 3.1)
Fuente: Autor.

AMENAZAS			Vulnerabilidades							
Nro.	Div.	Descripción								
2.1	4	Falta o insuficiencia de reglas de seguridad en general	1.7.4.2							
2.3	2	Recursos incompatibles o inadecuados	1.6.3.1	1.6.3.2	1.6.3.3					
2.18	3	Procedimientos faltantes o inadecuados para test y liberación de software	1.3.5.1	1.3.5.2	1.3.6.1	1.3.6.3	1.3.7.3	1.3.7.6		
2.19	3	Documentación faltante o inadecuada	1.4.5.2							
2.20	2	Violación de derechos de autor	1.2.3.3	1.3.5.4						
2.21	4	Prueba de software con datos de producción	1.3.7.7							
3.3	4	No cumplimiento con las medidas de seguridad TI	1.1.1.2	1.1.1.3	1.3.5.4	1.7.4.2	1.7.4.3	1.7.4.4	1.7.4.5	1.7.4.6
3.15	3	Errores en la configuración y operación	1.2.3.3	1.2.5.1	1.3.6.3	1.7.3.1	1.7.3.2	1.7.3.3		
4.4	5	Reconocimiento de vulnerabilidades en el software	1.3.7.8							
4.14	4	Vulnerabilidades o errores de software	1.3.2.1 1.3.4.4	1.3.2.2 1.3.5.1	1.3.3.1 1.3.5.2	1.3.3.2 1.3.5.3	1.3.3.3	1.3.3.4	1.3.4.1	1.3.4.3
5.12	3	Caballos de Troya	1.2.2.3							
5.13	4	Virus de computador	1.2.2.1	1.2.2.3	1.2.2.4					
5.18	3	Macro virus	1.2.2.1							

En la Tabla 27 se describe las vulnerabilidades potenciales que pueden afectar al Servidor de Producción del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 27 Vulnerabilidades Potenciales que pueden afectar Servidor de Producción. (Activo 3.1)
Fuente: Autor.

Nro.	Nivel	Descripción
1.1.1.2	2	Gestión de bajas de usuarios
1.1.1.3	2	Mantenimiento de cuentas
1.2.2.1	3	No está habilitado para envío y recepción de mail
1.2.2.3	2	No es suficiente la frecuencia de escaneado de las unidades de las computadores
1.2.2.4	1	No se generan discos de recuperación en las PCs bajo Windows
1.2.3.1	1	Grado y detalle de la información documentada de la red
1.2.3.3	1	Documentación de la configuración de las PCs
1.2.5.1	3	Tipo, configuración y nivel de control de firewall
1.3.2.1	1	Existencia de control de cambios para archivos de sistema o bases de datos
1.3.2.2	3	Confidencialidad de datos de laptops y notebooks
1.3.2.3	2	Logs de transacciones y sus detalles
1.3.3.1	1	Existencia de control de cambios para el desarrollo
1.3.3.2	1	Control del contenido de archivos de entrada
1.3.3.3	2	Control de validez de datos ingresados manualmente
1.3.3.4	1	Control de consistencia de datos de salida
1.3.4.1	2	Control de acceso propio de las bases de datos
1.3.4.2	1	Control de instancias de uso
1.3.4.3	1	Chequeo regulares de seguridad
1.3.4.4	1	Marcado o borrado de archivos eliminados
1.3.5.1	2	Controles con que se realiza la instalación y actualización de parches
1.3.5.2	1	Documentación de la instalación o actualización de software
1.3.5.3	2	Control de aplicaciones en máquinas de usuarios
1.3.5.4	1	Control de información que bajan los usuarios de la Web
1.3.6.1	1	Documentación de cambios de emergencia
1.3.6.3	1	Gestión de cambios complejos en archivos de configuración
1.3.6.4	2	Registro de cambios en las configuraciones

1.3.7.3	1	Uso métricas en el desarrollo
1.3.7.6	1	Medidas de seguridad durante las implementaciones
1.3.7.7	1	Forma y documentación de pruebas
1.3.7.8	1	Metodología usada para el mantenimiento
1.4.5.2	1	Inventario de recursos de hardware y software
1.5.1.3	1	Documentación detallada del equipamiento
1.6.3.1	1	Trabajos de mayor uso CPU y memoria
1.6.3.2	1	Datos de mayor tráfico, CPU y memoria
1.6.3.3	1	Aplicaciones de mayor tráfico, CPU y memoria
1.7.3.1	1	Personal de desarrollo
1.7.3.2	2	Técnicos
1.7.3.3	2	Administradores de redes
1.7.4.1	3	Visión y compromiso gerencial superior y medio en la seguridad.
1.7.4.2	3	Reglas de seguridad
1.7.4.3	1	Personal en general - procedimientos
1.7.4.4	2	Personal de desarrollo - procedimientos
1.7.4.5	3	Técnicos - procedimientos
1.7.4.6	3	Administradores de redes - procedimientos

En la Tabla 28 se describe las amenazas y vulnerabilidades verificadas de los activos más importantes de la Dirección de Tecnologías de la Información y Comunicaciones como son: Servidor de Producción.

Tabla 28 Amenazas Vs. Vulnerabilidades verificadas Servidor de Producción. (Activo 3.1)
Fuente: Autor.

	Amen.	2.1	2.3	2.18	2.19	2.20	2.21	3.3	3.15	4.4	4.14	5.12	5.13	5.18
Vulner.	**Nivel**	**4**	**2**	**3**	**3**	**2**	**4**	**4**	**3**	**5**	**4**	**3**	**4**	**3**
1.1.1.2	2							X						
1.1.1.3	2							X						
1.2.2.1	3												X	X
1.2.2.3	2											X	X	
1.2.2.4	1												X	
1.2.3.1	1													
1.2.3.3	1					X			X					
1.2.5.1	3								X					
1.3.2.1	1										X			
1.3.2.2	3										X			
1.3.2.3	2													

1.3.3.1	1										X			
1.3.3.2	1										X			
1.3.3.3	2										X			
1.3.3.4	1										X			
1.3.4.1	2										X			
1.3.4.2	1													
1.3.4.3	1										X			
1.3.4.4	1										X			
1.3.5.1	2			X							X			
1.3.5.2	1			X							X			
1.3.5.3	2										X			
1.3.5.4	1					X		X						
1.3.6.1	1			X										
1.3.6.3	1			X					X					
1.3.6.4	2													
1.3.7.3	1			X										
1.3.7.6	1			X										
1.3.7.7	1						X							
1.3.7.8	1									X				
1.4.5.2	1				X									
1.5.1.3	1													
1.6.3.1	1			X										
1.6.3.2	1			X										
1.6.3.3	1			X										
1.7.3.1	1								X					
1.7.3.2	2								X					
1.7.3.3	2								X					
1.7.4.1	3													
1.7.4.2	3		X					X						
1.7.4.3	1							X						
1.7.4.4	2							X						
1.7.4.5	3							X						
1.7.4.6	3							X						

En la Tabla 29 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Servidor Administración.

Tabla 29 Cruce de las Amenazas y las vulnerabilidades Servidor Administración (Activo 3.1).
Fuente: Autor.

Amenaza			Vulnerabilidades
No.	**Div.**	**Descripción**	
2.18	2	Reducción de la velocidad de transmisión o ejecución debido transmisión de datos	1.3.5.4
2.23	2	Planificación inadecuada de los dominios	1.1.4.3 3.1.1 3.1.2 3.1.3 3.1.4 3.1.5 3.2.1 3.2.2 3.2.3 3.3.1 3.3.2 3.4.1 3.4.2 3.5.1 3.5.2 3.5.3 3.5.4 3.6.1 3.6.2
2.24	3	Protección inadecuada del sistema Windows	3.6.3 3.7.1 3.7.2 3.8.1 3.8.2 3.9.1 3.9.2 3.10.1 3.10.2 3.10.3 3.11.1 3.12.1 3.12.2 3.12.3 3.12.4 3.12.5 3.14.1 3.14.2 3.15.1 3.15.2 3.16.1 3.16.2 3.17.1 3.17.2 3.17.3 3.18.1 3.18.2 3.18.3
4.5	4	Diversidad de posibilidades de acceso a sistemas de TI en red	1.6.2.1
4.16	1	Reconocimiento automático del DVD-ROM	3.12.1
5.13	4	Virus de computador	1.2.2.1 1.2.2.3 1.2.2.4
5.18	3	Macro virus	1.2.2.1 1.2.2.3
5.21	4	Mal uso de los derechos de administrador en sistemas Windows	1.6.1.4 1.6.1.5
5.29	3	Adquisición no autorizada de derechos de administrador con Windows	3.3.1 3.17.1

En la Tabla 30 se describe las vulnerabilidades potenciales que pueden afectar al Servidor de Administración de del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 30 Vulnerabilidades Potenciales del Servidor de Administración (Activo 3.1).
Fuente: Autor.

Nro.	Nivel	Descripción
1.1.4.3	3	Mecanismos de control de acceso interno
1.2.2.1	3	No está habilitado para envío y recepción de mail
1.2.2.3	2	No es suficiente la frecuencia de escaneado de las unidades de las computadores
1.2.2.4	1	No se generan discos de recuperación
1.3.5.4	1	Control de información que bajan los usuarios de la Web
1.6.1.4	1	Utilidad auditoria para rastreo de acciones
1.6.1.5	1	Históricos generados
1.6.2.1	3	Control de acceso
3.1.1	3	Versión y parches del IIS
3.1.2	2	Versiones actuales del IIS; ACL y directorios
3.1.3	2	Habilitación del log del IIS
3.1.4	3	WebDav ntdll.dll en IIS
3.1.5	2	Aplicaciones de muestra en directorios iissamples, iishelp y msadc
3.2.1	3	Versión y parches del SQL Server
3.2.2	2	Log autenticación servidor SQL
3.2.3	2	Cuenta SA, contraseña
3.3.1	3	Autenticación, algoritmo usado
3.3.2	3	Archivo hashes LM, habilitación autenticación a través de la red
3.4.1	3	Versión y parches del Internet Explorer
3.4.2	2	Nivel seguridad del IE
3.5.1	3	Uso SMB, conectividad NetBios
3.5.2	2	Sesión nula, registro anónimo
3.5.3	3	Acceso remoto al registry
3.5.4	3	rpc y parches
3.6.1	3	Versión y parches del MDAC
3.6.2	2	Archivo msadcs.dll con windows e IIS
3.6.3	1	Versión y SP del Jet Engine
3.7.1	3	Habilitación del Windows Scripting Host
3.7.2	1	Forma de ejecución de scripts
3.8.1	2	Ventana de vista previa del Outlook
3.8.2	1	Restricción zona de seguridad del Outlook
3.9.1.	3	Puertos de aplicaciones transmisión de datos
3.9.2	2	Existencia en disco de archivos de transmisión de datos
3.10.1	2	Versión y puertos habilitados del SNMP
3.10.2	3	Nombres comunidad por default del SNMP
3.10.3	2	Chequeo registros MIB del SNMP
3.11.1	3	Registros bajo SecurePipeServers
3.12.1	3	Registro Winlogon
3.12.2	2	Registro LanMan Print Services, para no poder agregar drivers impresión
3.12.3	2	Registro Subsystems, OS/2 y Posix
3.12.4	2	Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema
3.12.5	2	Registro Session Manager, atributos recursos compartidos, borrado archivo páginas

3.14.1	2	Uso del passfilt.dll
3.14.2	1	Uso del syskey.exe
3.15.1	3	Se usa FAT
3.15.2	2	Grupos Everyone (Todos) y/o Usuarios controlados
3.16.1	2	Logs en Event Viewer
3.16.2	1	Nombres existentes en registro HKLM\System\CurentControlSet\Control\Lsa
3.17.1	2	Existencia y/o restricciones de acceso de archivos ejecutables de cuidado
3.17.2	1	Ubicación de los archivos ejecutables de cuidado
3.17.3	2	Existencia del programa rollback.exe
3.18.1	2	Existencia de c:\windows\system32\os2 y subdirectorios
3.18.2	2	Archivos del os2 y posix en c:\windows\system32
3.18.3	1	Registros os2 subsystem for windows

En la Tabla 31 se describe las amenazas y vulnerabilidades verificadas de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Servidor de Administración.

Tabla 31 Amenazas vs. Vulnerabilidades verificadas Servidor Administración (Activo 3.1).
Fuente: Autor.

	Amen.	2.18	2.23	2.24	4.5	4.16	5.13	5.18	5.21	5.29
Vulner.	**Nivel**	**2**	**2**	**3**	**4**	**1**	**4**	**3**	**4**	**3**
1.1.4.3	3		X							
1.2.2.1	3						X	X		
1.2.2.3	2						X	X		
1.2.2.4	1						X			
1.3.5.4	1	X								
1.6.1.4	1								X	
1.6.1.5	1								X	
1.6.2.1	3				X					
3.1.1	3			X						
3.1.2	2			X						
3.1.3	2			X						
3.1.4	3			X						
3.1.5	2			X						
3.2.1	3			X						
3.2.2	2			X						

3.2.3	2			X						
3.3.1	3			X						X
3.3.2	3			X						
3.4.1	3			X						
3.4.2	2			X						
3.5.1	3			X						
3.5.2	2			X						
3.5.3	3			X						
3.5.4	3			X						
3.6.1	3			X						
3.6.2	2			X						
3.6.3	1			X						
3.7.1	3			X						
3.7.2	1			X						
3.8.1	2			X						
3.8.2	1			X						
3.9.1.	3			X						
3.9.2	2			X						
3.10.1	2			X						
3.10.2	3			X						
3.10.3	2			X						
3.11.1	3			X						
3.12.1	3			X		X				
3.12.2	2			X						
3.12.3	2			X						
3.12.4	2			X						
3.12.5	2			X						
3.14.1	2			X						
3.14.2	1			X						
3.15.1	3			X						
3.15.2	2			X						
3.16.1	2			X						
3.16.2	1			X						
3.17.1	2			X						X
3.17.2	1			X						
3.17.3	2			X						
3.18.1	2			X						
3.18.2	2			X						
3.18.3	1			X						

En la Tabla 32 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones

del Comando Conjunto de las FF.AA como son: Servidor de BDD.

Tabla 32 Cruce de las Amenazas y las vulnerabilidades Servidor de BDD (Activo 3.1).
Fuente: Autor.

Amenaza			Vulnerabilidades					
No.	**Div.**	**Descripción**						
2.18	2	Reducción de la velocidad de transmisión o ejecución de datos	1.3.5.4					
2.23	2	Planificación inadecuada de los dominios	3.1.1	3.1.2	3.1.3	3.1.4	3.1.5	3.3.1
			3.3.2	3.4.1	3.4.2	3.6.1	3.6.2	3.7.1
2.24	3	Protección inadecuada del sistema Windows	3.7.2 3.12.4 3.16.2	3.8.2 3.12.5 3.18.1	3.10.1 3.14.1 3.18.2	3.10.2 3.14.2 3.18.3	3.12.1 3.15.2	3.12.3 3.16.1
4.5	4	Diversidad de posibilidades de acceso a sistemas de TI en red						
4.16	1	Reconocimiento automático del DVD-ROM	3.12.1					
5.13	4	Virus de computador	1.2.2.1					
5.18	3	Macrovirus	1.2.2.1					
5.21	4	Mal uso de los derechos de administrador en sistemas Windows	1.6.1.4	1.6.1.5				
5.29	3	Adquisición no autorizada de derechos de administrador con Windows	3.3.1					

En la Tabla 33 se describe las vulnerabilidades potenciales que pueden afectar al Servidor de BDD del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 33 Vulnerabilidades Potenciales del Servidor de BDD (Activo 3.1).
Fuente: Autor.

Nro.	Nivel	Descripción
1.1.4.3	3	Mecanismos de control de acceso interno
1.2.2.1	3	No está habilitado para envío y recepción de mail
1.2.2.3	2	No es suficiente la frecuencia de escaneado de las unidades de las computadores
1.2.2.4	1	No se generan discos de recuperación
1.3.5.4	1	Control de información que bajan los usuarios de la Web
1.6.1.4	1	Utilidad auditoría para rastreo de acciones
1.6.1.5	1	Históricos generados
1.6.2.1	3	Control de acceso
3.1.1	3	Versión y parches del IIS
3.1.2	2	Versiones del IIS; ACL y directorios
3.1.3	2	Habilitación del log del IIS
3.1.4	3	WebDav ntdll.dll en IIS
3.1.5	2	Aplicaciones de muestra en directorios iissamples, iishelp y msadc
3.2.1	3	Versión y parches del SQL Server
3.2.2	2	Log autenticación servidor SQL
3.2.3	2	Cuenta SA, contraseña
3.3.1	3	Autenticación, algoritmo usado
3.3.2	3	Archivo hashes LM, habilitación autenticación a través de la red
3.4.1	3	Versión y parches del Internet Explorer
3.4.2	2	Nivel seguridad del Internet Explore
3.5.1	3	Uso SMB, conectividad NetBios
3.5.2	2	Sesión nula, registro anónimo
3.5.3	3	Acceso remoto al registry
3.5.4	3	rpc y parches
3.6.1	3	Versión y parches del MDAC
3.6.2	2	Archivo msadcs.dll con windows e IIS
3.6.3	1	Versión y SP del Jet Engine
3.7.1	3	Habilitación del Windows Scripting Host
3.7.2	1	Forma de ejecución de scripts
3.8.1	2	Ventana de vista previa del Outlook/Outlook Express
3.8.2	1	Restricción zona de seguridad del Outlook Express
3.9.1	3	Puertos de aplicaciones P2P
3.9.2	2	Existencia en disco de archivos propios de P2P
3.10.1	2	Versión y puertos habilitados del SNMP
3.10.2	3	Nombres comunidad por default del SNMP
3.10.3	2	Chequeo registros MIB del SNMP
3.11.1	3	Registros bajo SecurePipeServers
3.12.1	3	Registro Winlogon
3.12.2	2	Registro LanMan Print Services, para no poder agregar drivers impresión
3.12.3	2	Registro Subsystems, OS/2 y Posix
3.12.4	2	Registro bajo EventLog, para que no se vean los logs de aplicaciones y sistema
3.12.5	2	Registro Session Manager, atributos recursos compartidos, borrado archivo páginas

3.14.1	2	Uso del passfilt.dll
3.14.2	1	Uso del syskey.exe
3.15.1	3	Se usa FAT
3.15.2	2	Grupos Everyone (Todos) y/o Usuarios controlados
3.16.1	2	Logs en Event Viewer
3.16.2	1	Nombres existentes en registro HKLM\System\CurentControlSet\Control\Lsa
3.17.1	2	Existencia y/o restricciones de acceso de archivos ejecutables de cuidado
3.17.2	1	Ubicación de los archivos ejecutables de cuidado
3.17.3	2	Existencia del programa rollback.exe
3.18.1	2	Existencia de c:\windows\system32\os2 y subdirectorios
3.18.2	2	Archivos del os2 y posix en c:\windows\system32
3.18.3	1	Registros os2 subsystem for windows

En la Tabla 34 se describe las amenazas y vulnerabilidades verificadas de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Servidor de BDD.

Tabla 34 Amenazas vs. Vulnerabilidades verificadas Servidor de BDD (Activo 3.1).

Fuente: Autor.

	Amen.	2.18	2.24	4.16	5.13	5.18	5.21	5.29
Vulner.	**Nivel**	**2**	**3**	**1**	**4**	**3**	**4**	**3**
1.1.4.3	3							
1.2.2.1	3							
1.2.2.3	2							
1.2.2.4	1				X	X		
1.3.5.4	1	X						
1.6.1.4	1						X	
1.6.1.5	1						X	
1.6.2.1	3							
3.1.1	3		X					

3.1.2	2		X					
3.1.3	2		X					
3.1.4	3		X					
3.1.5	2		X					
3.2.1	3							
3.2.2	2							
3.2.3	2							
3.3.1	3		X					X
3.3.2	3		X					
3.4.1	3		X					
3.4.2	2		X					
3.5.1	3							
3.5.2	2							
3.5.3	3							
3.5.4	3							
3.6.1	3							
3.6.2	2		X					
3.6.3	1							
3.7.1	3		X					
3.7.2	1		X					
3.8.1	2							
3.8.2	1		X					
3.9.1	3							
3.9.2	2							
3.10.1	2		X					
3.10.2	3		X					
3.10.3	2							
3.11.1	3							
3.12.1	3		X	X				
3.12.2	2							
3.12.3	2		X					
3.12.4	2		X					
3.12.5	2		X					
3.14.1	2		X					
3.14.2	1		X					
3.15.1	3							
3.15.2	2		X					
3.16.1	2		X					
3.16.2	1		X					
3.17.1	2							
3.17.2	1							
3.17.3	2							
3.18.1	2		X					
3.18.2	2		X					
3.18.3	1		X					

En la Tabla 35 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Equipos de Seguridad Perimetral.

Tabla 35 Cruce de las Amenazas y las vulnerabilidades Equipos de Seguridad Perimetral (Activo 3.5).
Fuente: Autor.

AMENAZAS			Vulnerabilidades					
Nro.	Div.	Descripción						
2.17	4	Pérdida de confidencialidad de datos sensibles de la red a proteger	2.1.1 2.6.2 2.8.9 2.10.4 2.11.8 2.12.1	2.2.2 2.6.3 2.8.10 2.11.2 2.11.9 2.12.2	2.2.3 2.8.2 2.9.1 2.11.3 2.11.11 2.14.1	2.3.3 2.8.3 2.9.3 2.11.4 2.11.12	2.5.1 2.8.5 2.9.4 2.11.6 2.11.14	2.6.1 2.8.6 2.10.1 2.11.7 2.11.15
3.10	4	Exportación incorrecta de sistemas de archivos bajo Linux	2.1.1	2.4.2	2.6.4	2.13.1		
3.11	4	Configuración impropia del sendmail	1.4.3.1	2.7.1	2.8.11	2.11.5		
4.1	2	Interrupciones en la fuente de energía	1.4.3.1	2.4.1	2.8.7	2.11.10		
4.13	4	Autenticación faltante o de pobre calidad	2.2.1	2.4.3	2.8.8			
5.30	1	Sabotaje	1.4.3.1	2.9.4				

En la Tabla 36 se describe las vulnerabilidades potenciales que pueden afectar a los Equipos de Seguridad Perimetral del

Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA.

Tabla 36 Vulnerabilidades Potenciales de los Equipos de Seguridad Perimetral (Activo 3.5).
Fuente: Autor.

Nro.	Nivel	Descripción
1.4.3.1	2	Gestión de fallas dispositivos externos al funcionamiento del equipamiento TI
2.1.1	2	Servicios habilitados innecesarios
2.2.1	2	Instalación/ISC, versión y parches Bind
2.2.2	2	Actualización dinámica del DNS
2.2.3	2	Demonio named habilitado en servidores no DNS
2.3.1	3	RPC habilitado
2.3.3	2	Servicios RPC que se pueden explotar
2.4.1	2	Versión SNMP y puertos habilitados
2.4.2	3	Nombres comunidad SNMP por default
2.4.3	2	Chequeo registros MIB del SNMP
2.5.1	1	Instalación y versión ssh
2.6.1	3	Versión NIS
2.6.2	3	Ubicación password del root con NIS
2.6.3	2	Versión NFS
2.6.4	3	Configuración archivo export y montaje de sistema de archivos NFS
2.7.1	1	Versión Open SSL
2.8.1	3	Habilitación y funcionalidad anónima ftp
2.8.2	3	Sin uso de password en el modo de subida ftp
2.8.3	3	No hay restricciones y mecanismos para direcciones IP o dominios en ftp
2.8.5	3	Especificación de las cuentas administrativas en archivo ftpusers
2.8.6	3	No hay diferenciación archivos contraseñas ftp con los del Sistema Operativo
2.8.7	2	Permisos y propietarios del raíz y subdirectorios etc y bin del ftp anónimo
2.8.8	2	Permisos y propietarios de archivos de subdirectorios etc y bin
2.8.9	2	Permisos y propietarios directorio home ~ftp/
2.8.10	3	Existencia de archivos .rhosts y .forward
2.8.11	3	Restricciones de escritura para everyone en directorios ftp y sus archivos
2.9.1	2	Hay cuentas extras con UID 0, o sin contraseñas en el archivo passwd
2.9.2	3	tftp habilitado
2.9.3	3	tftp necesario pero sin precauciones de acceso restringido

2.9.4	2	No se usa un programa para mejorar la elección de contraseñas
2.10.1	2	Permisos y propietarios no adecuados en archivos de servicios de red
2.10.2	2	Cron acepta usuarios ordinarios
2.10.3	3	Se puede registrar como root en la consola en forma remota
2.10.4	3	Terminales no adecuados en el archivo de terminal seguro
2.11.1	2	Archivos .exrc no justificados
2.11.2	2	Archivos .forward en directorios home de usuarios
2.11.3	2	Umask inadecuado de algunos programas
2.11.4	2	Restricciones de acceso no adecuadas en algunos archivos bajo /etc
2.11.5	3	Escritura indebida de los archivos log
2.11.6	2	Características extendidas (inmutabilidad y sólo anexado) no habilitadas
2.11.7	2	Inadecuados permisos, propiedad y grupo de /vmunix
2.11.8	3	Archivos que no debieran ser propiedad sino de root, y /tmp que no tiene el sticky-bit
2.11.9	3	Archivos o directorios no esperados que son escribibles por cualquiera
2.11.10	2	Archivos que no debieran tener seteados el bit SUID o SGID
2.11.11	2	Umask inadecuado de algunos usuarios
2.11.12	2	Archivos ordinarios en el directorio /dev
2.11.13	2	Archivos especiales fuera de /dev
2.11.14	2	Archivos ejecutables y sus directorios ascendentes escribibles por grupos o cualquiera
2.11.15	2	Archivos sin propietarios
2.12.1	3	No se han definido los archivos log adecuados para seguridad
2.12.2	2	No se usan las extensiones de seguridad de Linux para los archivos log
2.13.1	2	Inadecuados permisos y propiedad del archivo /etc/export
2.14.1	3	Parches y actualizaciones Linux

En la Tabla 37 se describe las amenazas y vulnerabilidades verificadas de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA como son: Equipos de Seguridad Perimetral.

Tabla 37 Amenazas vs. Vulnerabilidades verificadas Para los Equipos de Seguridad Perimetral (Activo 3.5).
Fuente: Autor.

	Amen.	2.17	3.10	3.11	4.1	4.13	5.30
Vulner.	**Nivel**	**4**	**4**	**4**	**2**	**4**	**1**
1.4.3.1	2			X	X		X
2.1.1	2	X	X				
2.2.1	2					X	
2.2.2	2	X					
2.2.3	2	X					
2.3.1	3						
2.3.3	2	X					
2.4.1	2				X		
2.4.2	3		X				
2.4.3	2					X	
2.5.1	1	X					
2.6.1	3	X					
2.6.2	3	X					
2.6.3	2	X					
2.6.4	3		X				
2.7.1	1			X			
2.8.1	3						
2.8.2	3	X					
2.8.3	3	X					
2.8.5	3	X					
2.8.6	3	X					
2.8.7	2				X		
2.8.8	2					X	
2.8.9	2	X					
2.8.10	3	X					
2.8.11	3			X			
2.9.1	2	X					
2.9.2	3						
2.9.3	3	X					
2.9.4	2	X					X
2.10.1	2	X					
2.10.2	2	X					
2.10.3	3	X					
2.10.4	3	X					
2.11.1	2						
2.11.2	2	X					
2.11.3	2	X					
2.11.4	2	X					
2.11.5	3			X			
2.11.6	2	X					
2.11.7	2	X					
2.11.8	3	X					
2.11.9	3	X					
2.11.10	2				X		

2.11.11	2	X					
2.11.12	2	X					
2.11.13	2						
2.11.14	2	X					
2.11.15	2	X					
2.12.1	3	X					
2.12.2	2	X					
2.13.1	2		X				
2.14.1	3	X					

4.6 Análisis del Riesgo, Valoración y Evaluación

El análisis del riesgo tiene como objetivo identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

La referencia [6] señala que “los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que las amenazas y vulnerabilidades relacionadas se junten y causen un incidente”.

Para realizar el cálculo del riesgo se utilizará la matriz de riesgo de la metodología de CRAMM que se describe en la Tabla 38.

Tabla 38 Matriz de Riesgo.
Fuente: [8]

Amenaza		Muy Baja			Baja			Media			Alta			Muy Alta		
Vulnerabilidad		Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta
Activo	**1**	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	2	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Riesgos	
Nivel	**Valor**
Muy Bajo	1
Bajo	2
Medio bajo	3
Medio	4
Medio alto	5
Alto	6
Muy Alto	7

Amenazas	
Nivel	**Valor**
Muy Baja	1
Baja	2
Media	3
Alta	4
Muy Alta	5

Vulnerabilidades	
Nivel	**Valor**
Baja	1
Media	2
Alta	3

Para el cálculo de riesgo de un activo utilizando la matriz de la **Tabla 39**, se requiere los valores de la **Tabla 18** Activos Primarios Clasificados definidos en 7 clases y 10 niveles (1 -10); los valores de las amenazas definidas en la **Tabla 19** clasificadas en 5 tipos y 5 niveles de amenazas (1 - 5); y, los valores de las vulnerabilidades definidas en la **Tabla 21**

clasificadas en 4 tipos y 3 niveles de vulnerabilidades (1 - 3). Con esta información reemplazaremos en la matriz y determinamos el nivel del riesgo para este activo el mismo que tendrá un valor de (1 – 7).

Utilizando la matriz de riesgo en la Tabla 39 se presenta el cálculo del riesgo para los activos: Centro Principal de Procesamiento.

Tabla 39 Niveles particulares de riesgo para el Centro Principal de Procesamiento. Activo 1.1
Fuente: Autor.

	Amen.	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	2.1	2.2	2.4	2.10	2.11	5.4	5.5	5.29
Vulner.	**Nivel**	4	2	4	3	2	2	2	2	2	4	5	3	3	2	3	5	1
1.2.3.1	1										6							
1.2.4.1	1										6							
1.4.1.1	2															6		5
1.4.1.2	1																	4
1.4.3.1	2			6		5												
1.4.4.1	1														5			
1.4.4.2	1				5													
1.4.4.3	1						5										7	4
1.4.4.4	1							5	5	5							7	4
1.4.4.5	2			5														
1.5.1.1	1													5				
1.5.1.4	2										6							
1.5.2.1	3											7						
1.6.1.1	2												6					
1.6.1.2	1												5					
1.6.1.3	2												6					
1.6.1.4	1												5					
1.6.1.5	1												5					
1.7.1.1	2		6															
1.7.1.2	1		6															
1.7.1.3	2		6															
1.7.1.4	2		6															
1.7.2.1	3		7															
1.7.2.2	2		6															
1.7.2.3	2		6															
1.7.2.4	2		6															

En la Tabla 40 se presenta el resumen de las amenazas para el activo Centro Principal de Procesamiento.

Tabla 40 Resumen efectos de las amenazas para el Centro Principal de Procesamiento.
Fuente: Autor.

Nro.	Nivel	Descripción	Cantidad Vulnerab. Potenc.	Máximo riesgo
1,2	4	Fallas de los sistemas de TI	8	7
1,3	2	Rayos	1	5
1,4	4	Incendio	1	6
1,5	3	Inundación	1	5
1,6	2	Cables quemados	1	5
1,7	2	Polvo y suciedad	1	5
1,8	2	Efectos de catástrofes en el ambiente	1	5
1,9	2	Problemas causados por grandes eventos públicos	1	5
1,1	2	Tormentas	1	5
2,1	4	Falta o insuficiencia de reglas de seguridad en general	3	6
2,2	5	Conocimiento insuficiente de documentos sobre reglas y procedimientos	1	7
2,4	3	Monitoreo insuficiente de las medidas de seguridad TI	5	6
2,1	3	Dimensionamiento insuficiente de redes y centro de cómputo	1	5
2,11	2	Documentación insuficiente del cableado	1	5
5,4	3	Robo	1	6
5,5	5	Vandalismo	2	7
5,29	1	Sabotaje	4	5

En conclusión, el Centro Principal de Procesamiento tiene un nivel de riesgo promedio de 5,59 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 34 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

Utilizando la matriz de riesgo en la Tabla 41 se presenta el cálculo del riesgo para los activos: Servidor de Producción.

Tabla 41 Niveles particulares de riesgo Servidor de Producción Activo 3.1
Fuente: Autor.

	Amen.	2,1	2,3	2,18	2,19	2,2	2,21	3,3	3,15	4,4	4,14	5,12	5,13	5,18
Vulner.	**Nivel**	**4**	**2**	**3**	**3**	**2**	**4**	**4**	**3**	**5**	**4**	**3**	**4**	**3**
1.1.1.2	2							5						
1.1.1.3	2							5						
1.2.2.1	3												6	5
1.2.2.3	2											5	5	
1.2.2.4	1												5	
1.2.3.1	1													
1.2.3.3	1					4			4					
1.2.5.1	3								5					
1.3.2.1	1										5			
1.3.2.2	3										6			
1.3.2.3	2													
1.3.3.1	1										5			
1.3.3.2	1										5			
1.3.3.3	2										5			
1.3.3.4	1										5			
1.3.4.1	2										5			
1.3.4.2	1													
1.3.4.3	1										5			
1.3.4.4	1										5			
1.3.5.1	2			5							5			
1.3.5.2	1			4							5			
1.3.5.3	2										5			
1.3.5.4	1					4		5						
1.3.6.1	1			4										
1.3.6.3	1			4					4					
1.3.6.4	2													
1.3.7.3	1			4										
1.3.7.6	1			4										
1.3.7.7	1						5							
1.3.7.8	1									5				
1.4.5.2	1				4									
1.5.1.3	1													
1.6.3.1	1		4											
1.6.3.2	1		4											
1.6.3.3	1		4											
1.7.3.1	1								4					
1.7.3.2	2								5					
1.7.3.3	2								5					
1.7.4.1	3													
1.7.4.2	3	6						6						
1.7.4.3	1							5						
1.7.4.4	2							5						
1.7.4.5	3							6						
1.7.4.6	3							6						

En la Tabla 42 se presenta el resumen de las amenazas para el activo Servidor de Producción.

Tabla 42 Resumen efectos de las amenazas para Servidor de Producción. Activo 3.1
Fuente: Autor.

Nro.	Nivel	Descripción	Cantidad Vulnerab. Potenc.	Máximo riesgo
2,1	4	Falta o insuficiencia de reglas de seguridad en general	1	6
2,3	2	Recursos incompatibles o inadecuados	3	4
2,18	3	Procedimientos faltantes o inadecuados para test y liberación de software	6	5
2,19	3	Documentación faltante o inadecuada	1	4
2,2	2	Violación de derechos de autor	2	4
2,21	4	Prueba de software con datos de producción	1	5
3,3	4	No cumplimiento con las medidas de seguridad TI.	8	6
3,15	3	Errores en la configuración y operación	6	5
4,4	5	Reconocimiento de vulnerabilidades en el software	1	5
4,14	4	Vulnerabilidades o errores de software	12	6
5,12	3	Caballos de Troya	1	5
5,13	4	Virus de computador	3	6
5,18	3	Macrovirus	1	5

En conclusión, el activo 3.1 Servidor de Producción tiene un nivel de riesgo promedio de 5,10 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 46 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

En la Tabla 43 utilizando la matriz de riesgo se presenta el cálculo del riesgo para los activos: Servidor de Administración.

Tabla 43 Niveles particulares de riesgo para el Servidor de Administración (Activo 3.1)
Fuente: Autor.

	Amen.	2,18	2,23	2,24	4,5	4,16	5,13	5,18	5,21	5,29
Vulner.	**Nivel**	**2**	**2**	**3**	**4**	**1**	**4**	**3**	**4**	**3**
1.1.4.3	3		6							
1.2.2.1	3						7	6		
1.2.2.3	2						7	6		
1.2.2.4	1						6			
1.3.5.4	1	5								
1.6.1.4	1								6	
1.6.1.5	1								6	
1.6.2.1	3				7					
3.1.1	3			6						
3.1.2	2			6						
3.1.3	2			6						
3.1.4	3			6						
3.1.5	2			6						
3.2.1	3			6						
3.2.2	2			6						
3.2.3	2			6						
3.3.1	3			6						6
3.3.2	3			6						
3.4.1	3			6						
3.4.2	2			6						
3.5.1	3			6						
3.5.2	2			6						
3.5.3	3			6						
3.5.4	3			6						
3.6.1	3			6						
3.6.2	2			6						
3.6.3	1			6						
3.7.1	3			6						
3.7.2	1			6						
3.8.1	2			6						
3.8.2	1			6						
3.9.1	3			6						
3.9.2	2			6						
3.10.1	2			6						
3.10.2	3			6						
3.10.3	2			6						
3.11.1	3			6						
3.12.1	3			6		6				
3.12.2	2			6						
3.12.3	2			6						
3.12.4	2			6						
3.12.5	2			6						
3.14.1	2			6						
3.14.2	1			6						
3.15.1	3			6						

3.15.2	2			6						
3.16.1	2			6						
3.16.2	1			6						
3.17.1	2			6						6
3.17.2	1			6						
3.17.3	2			6						
3.18.1	2			6						
3.18.2	2			6						
3.18.3	1			6						

En la Tabla 43 se presenta el resumen de las amenazas para el activo Servidor de Administración.

Tabla 44 Resumen efectos de las amenazas Servidor de Administración (Activo 3.1).
Fuente: Autor.

Nro.	Nivel	Descripción	Cantidad Vulnerab. Potenc.	Máximo riesgo
2,18	2	Reducción de la velocidad de transmisión o ejecución de datos	1	5
2,23	2	Planificación inadecuada de los dominios	1	6
2,24	3	Protección inadecuada del sistema Windows	46	6
4,5	4	Diversidad de posibilidades de acceso a sistemas TI en red	1	7
4,16	1	Reconocimiento automático del DVD-ROM	1	6
5,13	4	Virus de computador	3	7
5,18	3	Macrovirus	2	6
5,21	4	Mal uso de los derechos de administrador en sistemas Windows	2	6
5,29	3	Adquisición no autorizada de derechos de administrador con Windows	2	6

En conclusión, el activo 3.1, Servidor de Administración tiene un nivel de riesgo promedio de 6,11 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 59 y los niveles de protección

son: para la confidencialidad es alto, para la integridad medio y la disponibilidad es alta.

Utilizando la matriz de riesgo en la Tabla 45 se presenta el cálculo del riesgo para los activos: Servidor de Base de Datos.

Tabla 45 Niveles particulares de riesgo para el Servidor de Base de Datos (Activo 3.1).
Fuente: Autor.

	Amenaza	2,2	2,2	4,2	5,1	5,2	5,2	5,3
Vulnerabilidad	**Nivel**	**2**	**3**	**1**	**4**	**3**	**4**	**3**
1.1.4.3	3							
1.2.2.1	3							
1.2.2.3	2							
1.2.2.4	1				6	6		
1.3.5.4	1	5						
1.6.1.4	1						6	
1.6.1.5	1						6	
1.6.2.1	3							
3.1.1	3		6					
3.1.2	2		6					
3.1.3	2		6					
3.1.4	3		6					
3.1.5	2		6					
3.2.2	2							
3.2.3	2							
3.3.1	3		6					6
3.3.2	3		6					
3.4.1	3		6					
3.4.2	2		6					
3.5.1	3							
3.5.2	2							
3.5.3	3							
3.5.4	3							
3.6.1	3							
3.6.2	2		6					
3.6.3	1							
3.7.1	3		6					
3.7.2	1		6					
3.8.1	2							
3.8.2	1		6					
3.9.1	3							
3.9.2	2							
3.10.1	2		6					

3.10.2	3		6					
3.10.3	2							
3.11.1	3							
3.12.1	3		6	6				
3.12.2	2							
3.12.3	2		6					
3.12.4	2		6					
3.12.5	2		6					
3.14.1	2		6					
3.14.2	1		6					
3.15.1	3							
3.15.2	2		6					
3.16.1	2		6					
3.16.2	1		6					
3.17.1	2							
3.17.2	1							
3.17.3	2							
3.18.1	2		6					
3.18.2	2		6					
3.18.3	1		6					

En la Tabla 46 se presenta el resumen de las amenazas para el activo Servidor de Base de Datos.

Tabla 46 Resumen efectos de las amenazas Servidor de Base de Daros (Activo 3.1).

Fuente: Autor.

Nro.	Nivel	Descripción	Cantidad Vulnerab. Potenc.	Máximo riesgo
2,18	2	Reducción de la velocidad de transmisión o ejecución debido a funciones de trasmisión de datos	1	5
2,24	3	Protección inadecuada del sistema Windows	27	6
4,16	1	Reconocimiento automático del DVD-ROM	1	6
5,13	4	Virus de computador	1	6
5,18	3	Macrovirus	1	6
5,21	4	Mal uso de los derechos de administrador en sistemas Windows	2	6
5,29	3	Adquisición no autorizada de derechos de administrador con Windows	1	6

En conclusión, el activo 3.1, Servidor de Base de Datos tiene un nivel de riesgo promedio de 5,86 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 34 y los niveles de protección son: para la confidencialidad es alto, para la integridad medio y la disponibilidad es alta.

Utilizando la matriz de riesgo en la Tabla 47 se presenta el cálculo del riesgo para los activos: Equipos de Seguridad Perimetral.

Tabla 47 Niveles particulares de riesgo para Equipos de Seguridad Perimetral (Activo 3.5).
Fuente: Autor.

	Amen.	2,17	3,1	3,11	4,1	4,13	5,3
Vulner.	**Nivel**	**4**	**4**	**4**	**2**	**4**	**1**
1.4.3.1	2			7	6		5
2.1.1	2		7				
2.2.1	2					7	
2.2.2	2	7					
2.2.3	2	7					
2.3.1	3						
2.3.3	2	7					
2.4.1	2				6		
2.4.2	3		7				
2.4.3	2					7	
2.5.1	1	6					
2.6.1	3	7					
2.6.2	3	7					
2.6.3	2	7					
2.6.4	3		7				
2.7.1	1			6			
2.8.1	3						
2.8.2	3	7					
2.8.3	3	7					
2.8.5	3	7					
2.8.6	3	7					
2.8.7	2				6		
2.8.8	2					7	

2.8.9	2	7					
2.8.10	3	7					
2.8.11	3			7			
2.9.1	2	7					
2.9.2	3						
2.9.3	3	7					
2.9.4	2	7					5
2.10.1	2	7					
2.10.2	2	7					
2.10.3	3	7					
2.10.4	3	7					
2.11.1	2						
2.11.2	2	7					
2.11.3	2	7					
2.11.4	2	7					
2.11.5	3	7					
2.11.6	2	7					
2.11.7	2	7					
2.11.8	3	7					
2.11.9	3	7					
2.11.10	2				6		
2.11.11	2	7					
2.11.12	2	7					
2.11.13	2						
2.11.14	2	7					
2.11.15	2	7					
2.12.1	3	7					
2.12.2	2	7					
2.13.1	2		7				
2.14.1	3	7					

En la Tabla 48 se presenta el resumen de las amenazas para el activo Equipos de Seguridad Perimetral.

Tabla 48 Resumen efectos de las amenazas Equipos de Seguridad Perimetral (Activo 3.5).
Fuente: Autor.

Nro.	Nivel	Descripción	Cantidad Vulnerab. Potenc.	Máximo riesgo
2,17	4	Pérdida de confidencialidad de datos sensibles de la red a proteger	34	7
3,1	4	Exportación incorrecta de sistemas de archivos bajo Linux	4	7
3,11	4	Configuración impropia del sendmail	4	7
4,1	2	Disrupciones en la fuente de energía	4	6
4,13	4	Autenticación faltante o de pobre calidad	3	7
5,3	1	Sabotaje	2	5

En conclusión, el activo 3.5, Equipos de Seguridad Perimetral tiene un nivel de riesgo promedio de 6,50 sobre 7, el total de cruces encontrado para las amenazas y vulnerabilidades fue de 52 y los niveles de protección son: para la confidencialidad es medio, para la integridad medio y la disponibilidad es alta.

4.7 Identificar y Evaluar las Opciones para el Tratamiento del Riesgo

Una vez efectuados el análisis y la evaluación del riesgo, se debe decidir cuáles acciones se deben tomar con esos activos que están sujetos a riesgos y estas decisiones deberán ejecutarse, identificando y planificando las actividades con claridad y distribuir las responsabilidades a los encargados de los activos, estimar los requerimientos de los recursos, el conjunto de entregables, fechas críticas y la supervisión del progreso.

Según la Norma ISO/IEC 27002:2013 las opciones posibles para el tratamiento de riesgos son: (a) Aplicar controles apropiados. (b) Aceptar riesgos consistente y objetivamente. (c) Evitar los riesgos. (d) Transferir los riesgos. De las opciones propuestas por la norma se decidió tomar las 2 primeras, por lo que en este caso de estudio los riesgos serán controlados o asumidos.

En el **Anexo J** se presentan los procedimientos correspondientes al control A.16.1.2 Reporte de eventos de seguridad de la información, control A.9.2.4 Gestión de información secreta de autenticación de usuarios, control A.9.3.1 Uso de información secreta de autenticación, control A.9.4.3 Sistema de Gestión de contraseñas.

4.8 Seleccionar los Objetivos de Control y Controles para el Tratamiento del Riesgo

Los resultados del análisis y la evaluación del riesgo del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., requieren ser revisados con regularidad para visualizar cualquier modificación.

Luego del proceso de identificación de las opciones de tratamiento de riesgo y de haber evaluado estos riesgos, del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., deberá asignar

los recursos y las acciones correspondientes para implementar las decisiones de la gestión del riesgo que deben iniciar y decidir cuáles objetivos de control y controles escoger para el tratamiento del riesgo y preparar la declaración de aplicabilidad, como se ilustra en la Tabla 49, el cual es un documento muy importante del Sistema de Gestión de Seguridad de la Información.

Tabla 49 Plan de tratamiento del riesgo.
Fuente: Autor.

Áreas	Actividades	Control	Activo	Fecha de Culminación	Responsable
DTIC'S	Elaborar procedimientos para el sistema de administración de contraseñas, uso de contraseñas y administración de contraseñas de usuarios.	A.11.2.3	Seguridad Informática	15/01/2018	Departamento de Seguridad e Investigación
	Realizar controles de cambios cuando ocurra alguna variación en los recursos o en los sistemas de la DTIC'S	A.12.1.2	Recursos Informáticos	Cada vez que ocurra un cambio	Departamento de Plataformas Tecnológicas
	Realizar estadísticas del crecimiento de los sistemas de la DTIC'S a fin de hacer proyecciones de los requisitos de la capacidad futura de los servidores	A.12.1.3	servicios	Semestral	Departamento de Servicios

	Instalar antivirus y actualizarlos constantemente para mitigar el riesgo del código malicioso	A.12.2.1	Soporte de Hardware y Software	Semanalmente	Departamento de Plataformas Tecnológicas
	Elaborar un programa de capacitación para la detección y prevención de código malicioso.	A.12.2.1	Seguridad e investigación	15/02/2018	Departamento de Plataformas Tecnológicas
	Realizar las copias de seguridad de la información según la política de seguridad acordada.	A.12.3.1	Base de Datos y Servidores	Semanalmente	Departamento de Plataformas Tecnológicas
	Elaborar registro de las fallas detectada en los sistemas y en la infraestructura.	A.12.4.3	Recursos Informáticos	Regularmente	Departamento de Plataformas Tecnológicas
	Elaborar las políticas de control de acceso a los sistemas de la DTIC'S	A.9.1.1	Base de Datos y Servidores	15/02/2018	Departamento de Seguridad e Investigación
	Elaborar procedimientos de selección y uso de contraseñas	A.9.3.1	Seguridad Informática	15/01/2018	Departamento de Seguridad e Investigación
	Elaborar un plan para la realización de auditorías de sistemas que conlleve a minimizar el riesgo de interrupciones en los procesos administrativos.	A.12.7.1	Software y Plataformas Tecnológicas	30/06/2018	DTIC'S
	Elaborar un programa detallado de capacitación para el manejo de los sistemas de la DTIC'S.	A.7.2.2	Servicios	30/03/2018	Departamento de Seguridad e Investigación
	Elaborar un documento de la política de seguridad de la información	A.5.1.1	Seguridad Informática	30/11/2018	Departamento de Seguridad e Investigación

	Elaborar políticas para que los usuarios ejerciten buenas prácticas en la selección y uso de claves.	A.9.3.1 A.9.4.3	Seguridad Informática	15/02/2018	Departamento de Seguridad e Investigación
	Elaborar políticas definidas para la asignación de responsabilidades en la protección de activos de información así como de seguridad de información.	A.6.1.1	Seguridad e Investigación	15/02/2018	DTIC'S
	Se debe organizar y mantener actualizada la cadena de contactos (Interno o Externo) con el mayor detalle posible identificando los requisitos de seguridad antes de dar acceso a la información.	A.15.1.2	Seguridad Informática	30/01/2018	Departamento de Seguridad e Investigación

4.9 Obtener la Aprobación por parte de la Dirección de los Riesgos Residuales Propuestos

Según la [5], el riesgo residual es: "El riesgo remanente después del tratamiento del riesgo". En el paso anterior Selección de Objetivos de Control y Controles, se propusieron salvaguardas para los riesgos detectados y clasificados como importantes.

La aplicación de estos controles persigue llevar el riesgo a niveles aceptables, permitiendo un margen de error Riesgo Residual, el cual debe ser conocido y aprobado por el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., por lo cual se hace necesario que en el Diseño de un Sistema de Gestión de Seguridad de la Información, la Dirección apruebe el Riesgo Residual no cubierto, la aprobación se puede conseguir por medio de la firma del documento “Matriz de Gestión de Riesgo, Controles Recomendados y Estimados” y la firma del siguiente documento:

Comando Conjunto de las Fuerzas Armadas
Dirección de Tecnologías de la Información y Comunicaciones
Quito

APROBACIÓN DEL RIESGO RESIDUAL

DECLARACIÓN

A través del siguiente documento se aprueba el “Riesgo Residual” no cubierto en la implantación de los controles sugeridos como resultado de la Evaluación del Riesgo para el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

A los ___ días del mes de _____ del 2017.

Director de DTIC’S del Comando Conjunto de las FF.AA.
Firma autorizada

CAPÍTULO 5

PROPUESTA DE IMPLEMENTACIÓN Y OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

5.1 Obtener la Autorización de la Dirección para Implementar y Operar el SGSI.

Es necesario garantizar la puesta en marcha de Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., con el compromiso de la Dirección de facilitar los recursos necesarios para la implementación de los controles propuestos.

En este caso de estudio, el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA, tiene la competencia para autorizar los recursos necesarios para la implementación y operación del SGSI.

La autorización para implementación del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. se puede lograr a través de la firma del documento “Enunciado de Aplicabilidad” por parte del “Director de la DTIC’S” con competencia para ello y la firma del siguiente documento:

Comando Conjunto de las Fuerzas Armadas
Dirección de Tecnologías de la Información y Comunicaciones
Quito

AUTORIZACIÓN DE IMPLEMENTACIÓN Y OPERACIÓN

RESOLUCIÓN No. _____

El _____ del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., en Sesión No. _____, Ordinaria, celebrada el día ____ de _____ del año _____, en uso de las atribuciones legales y reglamentarias que le confiere la ley AUTORIZÓ la IMPLEMENTACIÓN Y OPERACIÓN DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS DEL ECUADOR.

Director de DTIC'S del Comando Conjunto de las FF.AA.
Firma autorizada

En el **Anexo K** se presenta un cronograma de cuarenta y cuatro (44) semanas para implementar el Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

5.2 Declaración de Aplicabilidad

La declaración de aplicabilidad, como lo exige el ISO/IEC 27001:2013 es un excelente registro de los últimos controles establecidos. Tiene como finalidad la observancia de todos los controles de seguridad propuestos en la norma ISO/IEC 27001:2013, con la justificación de su inclusión o exclusión.

El uso de la declaración de aplicabilidad es muy apropiado para mantener un registro actualizado de los últimos controles instaurados en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., en la Tabla 50 se tiene una ilustración de la declaración de aplicabilidad.

Tabla 50 Declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información.

Fuente: Autor.

Objetivos de control	Controles	Aplicabilidad		Justificación
		SI	NO	
A.5.1. Gestión de la Gerencia de la Seguridad de la información	A.5.1.1	X		Es necesario establecer las políticas de seguridad para los sistemas de información, ya que manejan la información vital de la DTIC'S. Es necesario revisar periódicamente las políticas de seguridad para asegurar que se mantengan adecuadas.
	A.5.1.2	X		
A.6.1 Organización interna	A.6.1.1	X		Es necesario tener controles y políticas para el manejo de la seguridad de la información dentro de la DTIC'S.
	A.6.1.2	X		
	A.6.1.3	X		
	A.6.1.4	X		
	A.6.1.5	X		
A.7.1 Antes de Reclutarlo	A.7.1.1	X		La DTIC'S verificará los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.
	A.7.1.2	X		
	A.7.2.2	X		
A.8.1 Responsabilidades de los Activos	A.8.1.1	X		La DTIC'S identificará los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos
	A.8.1.2	X		
	A.8.1.3	X		
	A.8.1.4	X		
A.8.2 Clasificación de la Información	A.8.2.1	X		La información de la DTIC'S debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.
	A.8.2.2	X		
	A.8.2.3	X		
A.9.1 Requisitos del Negocio Sobre Control de Acceso	A.9.1.1	X		Los usuarios de la DTIC'S deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.
	A.9.1.2	X		
A.9.2 Gestión del Acceso al Usuario	A.9.2.1	X		La DTIC'S implementará un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.
	A.9.2.2	X		
	A.9.2.3	X		
	A.9.2.4	X		
	A.9.2.5	X		
	A.9.2.6	X		

A.10.1 Controles de Criptografía	A.10.1.1	X		Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida
	A.10.1.2	X		
A.11.1 Áreas Seguras	A.11.1.1	X		Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.
	A.11.1.2	X		
	A.11.1.3	X		
A.11.2 Equipos	A.11.2.1	X		Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.
	A.11.2.2	X		
A.12.1 Procedimientos y responsabilidades operaciones	A.12.1.1	X		Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.
	A.12.1.2		X	
A.12.3 Backup	A.12.3.1	X		Se debe tomar y poner a prueba de manera regular, el back up de copias de la información, software e imágenes del sistema, de acuerdo a la política de back up de la organización.
A.12.7 Consideraciones de las Auditorias de los Sistemas de Información	A.12.7.1	X		Se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio.
A.13.1 Gestión de la Seguridad en las Redes	A.13.1.1	X		Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.
	A.13.1.2	X		
	A.13.1.3	X		
A.13.2 Transferencia de la Información	A.13.2.1	X		Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.
	A.13.2.2	X		
	A.13.2.3	X		
	A.13.2.4	X		

A.14.1 Requisitos de Seguridad de los Sistemas de Información	A.14.1.1	X		Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes
	A.14.1.2	X		
	A.14.1.3	X		
A.15.1 Seguridad de la Información en la Relación con los Proveedores	A.15.1.1	X		Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.
	A.15.1.2	X		
	A.15.1.3	X		
A.16.1 Gestión de los Incidentes de la Seguridad de la Información y su Mejora	A.16.1.1	X		Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.
	A.16.1.2	X		
	A.16.1.3	X		
	A.16.1.4	X		
A.17.1 Continuidad de la Seguridad de la Información	A.17.1.1	X		La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa
	A.17.1.2	X		
	A.17.1.3	X		
A.18.1 Cumplimiento de los Requisitos Legales y Contractuales	A.18.1.1		X	Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software
	A.18.1.2	X		
	A.18.1.3	X		
	A.18.1.4	X		
	A.18.1.5	X		

CAPÍTULO 6

ANÁLISIS DE RESULTADOS DEL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA.

Los resultados obtenidos se derivan del desarrollo del Diagóstico y del Diseño de un Sistema de Gestión de Seguridad de la Información que fueron definidas para dar cumplimiento a los objetivos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

6.1 Análisis del Alcance el SGSI.

La determinación del alcance de un Sistema de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., ha sido realizada tomando en cuenta la norma ISO 27001, [5].

Para determinar el alcance del Sistema de Seguridad de la Información se tomó en cuenta los siguientes aspectos tanto internos como externos, como se describe en la Cláusula 4.1 de la norma a fin de conocer mejor los procesos el Departamento de Informática e Identificar las partes interesadas, de acuerdo a la cláusula 4.2

Se realizó el análisis de interfaces y dependencias, verificando las interrelaciones entre lo que ocurre dentro del Sistema de Gestión de Seguridad de la Información y el mundo externo, incluyendo también información respecto a la ubicación de la DTIC'S y las unidades organizativas que integran.

El alcance abarca el análisis y diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA. utilizando la norma ISO 27001:2013, dirigidos a procesos, activos y riesgos, cumpliendo con los estándares,

procedimientos, normas y medidas, para asegurar la integridad, dispinibilidad y confidencialidad de la información, [5].

6.2 Análisis de las Políticas y Objetivos de Seguridad

La DTIC'S estableció una política de seguridad para apoyar al Diseño del Sistema de Seguridad de Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

Se desarrolló las Políticas de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., que contienen políticas, normas y lineamientos que regirán la seguridad de la información y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información.

Para minimizar al máximo los riesgos asociados con la seguridad de la información, se debe realizar el cumplimiento de las políticas de seguridad de la información por parte todos los colaboradores y de terceros que tienen relación alguna con la entidad, por lo cual es necesario que la política del sistema de gestión de seguridad de la información sea impulsada por la alta directiva para alcanzar este propósito.

Es necesario hacer conocer al personal del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., el propósito de las políticas de seguridad de la información antes de su aplicación, con el objetivo de que los usuarios y terceros comprendan como estas políticas ayudan a proteger la confidencialidad, integridad y disponibilidad de la información.

Las Políticas de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se basa en los objetivos de control y controles definidos en el Anexo A de la Norma ISO/IEC 27001:2013, de acuerdo como se describe en la Tabla 51.

Tabla 51 Objetivo de Control y Controles.
Fuente: Autor.

ANEXO A NORMA ISO 27001:2013	
A.5.	Política General de Seguridad de la Información
A.6.	Organización de Seguridad de la Información
A.7.	Seguridad de los Recursos Humanos
A.8.	Gestión de Activos
A.9.	Control de Acceso
A.10.	Criptografía
A.11.	Seguridad Física y del Entorno
A.12.	Seguridad de las Operaciones
A.13.	Seguridad de las Comunicaciones
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas
A.15.	Relaciones con los Proveedores
A.16.	Gestión de Incidentes de Seguridad de la Información
A.17.	Seguridad de la Información en la Continuidad del Negocio
A.18.	Cumplimiento de Requisitos Legales y Contractuales

Las Políticas de Seguridad de la Información definidas, son de obligatorio cumplimiento por todos los colaboradores y terceros que laboran o presten sus servicios en el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., la documentación de esta política, se presenta en el **Anexo H**.

6.3 Análisis de los Procedimientos y Controles del SGSI

En el Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., una vez efectuados el análisis y la evaluación del riesgo, se debe decidir cuáles acciones se deben tomar o que procedimientos se debe realizar con esos activos que están sujetos a riesgos y estas decisiones deberán ejecutarse, identificando y planificando las actividades con claridad, el cual se deberá distribuir las responsabilidades a los encargados de los activos, estimar los requerimientos de los recursos, el conjunto de entregables, fechas críticas y la supervisión del progreso.

Según la Norma ISO/IEC 27001:2013, los objetivos de control y controles de para el Diseño del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando

Conjunto de las FF.AA., se extrae directamente del Anexo A de la Norma y están alineados a aquellos detallados en el ISO/IEC 27001:2013, Cláusulas del 5 al 18, [5].

En el **Anexo J** se presentan los procedimientos correspondientes al control A.16.1.2 Reporte de eventos de seguridad de la información, control A.9.2.4 Gestión de información secreta de autenticación de usuarios, control A.9.3.1 Uso de información secreta de autenticación, control A.9.4.3 Sistema de Gestión de contraseñas, [5].

6.4 Análisis de la Declaración de Aplicabilidad

Para realizar la Declaración de la Aplicabilidad en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., de acuerdo a lo que establece la norma ISO/IEC 27001:2013, se tomó en cuenta el numeral 6.1.3 “Tratamiento de los riesgos de la Seguridad de la Información”, el literal d) “Elaborar una Declaración de Aplicabilidad que contiene los controles necesarios” y la argumentación de las inclusiones, si se aplicarán o no así como la argumentación de las exclusiones de cada uno de los 35 objetivos de control y 114 controles del Anexo A.

La declaración de aplicabilidad, es un excelente registro de los últimos controles establecidos, tiene como finalidad la observancia de todos los controles de seguridad propuestos en la norma ISO/IEC 27001:2013, con la justificación de su inclusión o exclusión, [5].

Para mantener un registro actualizado de los últimos controles instaurados, es necesario el uso de la declaración de aplicabilidad en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

6.5 Análisis de la Evaluación de Riesgos

Para realizar la evaluación del riesgo del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., es necesario determinar el cálculo de los riesgos de seguridad de información que incluye el análisis y la evaluación del riesgo, la metodología para el análisis de riesgo será: 1) Identificar los activos dentro del alcance del SGSI y los dueños de esos activos; 2) Identificar las amenazas a esos activos; 3) Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas; y, 4) Identificar los impactos que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener sobre los activos.

Esta metodología establece los elementos y lineamientos para la valoración y el tratamiento de los Riesgos de Seguridad de la Información de la Entidad, para lo cual, se tuvo en cuenta los requerimientos establecidos en los numerales 6.1.2 Valoración de riesgos de la seguridad de la información[7] y 6.1.3 Tratamiento de riesgos de la seguridad de la información[8] de la norma ISO\IEC 27001:2013.

La norma ISO/IEC 27001:2013, describe un enfoque más amplio para la valoración de los riesgos, ya que no limita la identificación de los riesgos a partir de la identificación de los activos, amenazas y vulnerabilidades, pero para valorar los riesgos de tecnología, es necesario realizar el proceso de clasificar los activos de información para determinar su criticidad y nivel de protección y así poder identificar los riesgos de seguridad asociados y de esta forma realizar un análisis para determinar los mecanismos más convenientes para protegerlos de acuerdo a la Tabla 52.

[7] Norma ISO/IEC 27001:2013, Pág. 4
[8] Norma ISO/IEC 27001:2013, Pág. 5

Tabla 52 Identificación de los activos.
Fuente: Autor.

NOMBRE	DESCRIPCIÓN
IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACIÓN	• Identificar los activos de información • Determinar el tipo de activo • Identificar los dueños de los riesgos • Identificar el responsable del activo • Identificar el contenedor del activo • Valorar los activos • Determinar el valor de criticidad del activo • Establecer el nivel de criticidad del activo • Determinar los activos para la valoración de riegos
IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACIÓN VALORACIÓN DE RIESGOS	• Identificar de amenazas y vulnerabilidades • Analizar el riesgo inherente • Mapa de calor • Elaborar Matriz de Riesgo Inherente • Evaluar controles existentes para mitigar los riesgos • Determinar Riesgo Residual • Elaborar Matriz de Riesgo Residual • Establecer opciones y/o planes de tratamiento de riesgos

En el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se identificaron los activos vitales, generando un listado de los mismos, en el cual se asignó y clasificó a cada uno de los activos por su nivel de importancia (escala 1 – 10), siendo el valor de 10 como el activo de mayor importancia y agrupados en 06 clases de activos, como se detalla en la Tabla 53.

Tabla 53 Activos clasificados.
Fuente: Autor.

ACTIVOS CLASIFICADOS	
Clase 1 – Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones
Clase 2 – Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Clase 3 – Equipos informáticos	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Clase 4 – Software	Programas, aplicativos, desarrollos, software base, sistema de información
Clase 5 – Servicios	Contempla servicios prestados por el sistema
Clase 6 – Datos / Información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad.

Identificación de Amenazas

Para la identificación de amenazas de los activos de información, en la Tabla 54 se muestra una clasificación de 5 tipos de amenazas y 5 niveles de amenazas que afectan a los activos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., se debe tomar en cuenta que una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

Tabla 54 Amenazas definidas.
Fuente: Autor.

AMENAZAS DEFINIDAS			
Tipo		**Niveles de Amenazas**	
1.- Fuerza Mayor		Muy Baja	1
2.- Deficiencias organizacionales		Baja	2
3.- Fallas humanas		Media	3
4.- Fallas técnicas		Alta	4
5.- Actos deliberados		Muy alta	5

Utilizando las amenazas clasificadas, se procedió a realizar un cruce de las amenazas y los activos, para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.

Identificación de Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización, se clasificó en 04 tipos de vulnerabilidades como se indica en la Tabla 55.

Tabla 55 Tipos de Vulnerabilidades.
Fuente: Autor.

TIPOS DE VULNERABILIDADES
Tipo 1: física, organizacionales y operacionales
Tipo 2: técnica para plataforma Linux
Tipo 3: técnica para plataforma Windows
Tipo 4: técnica de otros dispositivos

Con las vulnerabilidades clasificadas en el Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA., se procedió a verificar cada una de ellas con los activos, de acuerdo a como se indica en el **Anexo I**.

Cálculo de Amenazas y Vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades, es necesario verificar la posibilidad de que puedan juntarse y causar un riesgo. En la Tabla 23 se describe los cruces de las amenazas y vulnerabilidades para obtener el nivel de riesgo de los activos más importantes del Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA., como son el Centro Principal de Procesamiento; Servidor de Producción; Servidor de Administración; Servidor de Base de Datos; y, Equipos de Seguridad Perimetral.

Análisis de Riesgo Valoración y Evaluación

El análisis del riesgo es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir, tiene como objetivo identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

Para realizar el cálculo del riesgo en Departamento de Informática de la Dirección de Tecnologías de la información y Comunicaciones del Comando Conjunto de las FF.AA., se utilizaron la matriz de riesgo de la metodología de Cramm que se describe en la Tabla 39.

Para el cálculo de riesgo de un activo utilizando la matriz de la **Tabla 39**, se requiere los valores de la **Tabla 18** Activos Primarios Clasificados definidos en 7 clases y 10 niveles (1 -10); los valores de las amenazas definidas en la **Tabla 19** clasificadas en 5 tipos y 5 niveles de amenazas (1 - 5); y, los valores de las vulnerabilidades definidas en la **Tabla 21** clasificadas en 4 tipos y 3 niveles de vulnerabilidades (1 - 3). Con esta información reemplazaremos en la matriz y determinamos el nivel del riesgo para este activo el mismo que tendrá un valor de (1 – 7), [8].

Los resultados obtenidos del análisis y evaluación de los riesgos se describen en la Tabla 56, los mismos que permiten aplicar los métodos para el tratamiento de los riesgos, evaluarlos y preparar planes para este tratamiento y ejecutarlos.

Tabla 56 Resultados del análisis de riesgo.
Fuente: Autor.

Activo	Nivel de riesgo	Cruce de amenazas y vulnerabilidades	Niveles de Protección		
			Confidenc.	Integrid.	Disponibilid.
1.1 Centro Principal de Procesamiento	5,59	34	Medio	Medio	Alto
3.1 Servidor de Producción	5,10	46	Medio	Medio	Alto
3.1 Servidor de Administración	6,11	59	Alto	Medio	Alto
3.1 Servidor de BDD	5,86	34	Alto	Medio	Alto
3.5 Equipos de Seguridad Perimetral	6,50	52	Medio	Medio	Alto

6.6 Análisis del Plan del Tratamiento de Riesgos

Es necesario revisar con regularidad los resultados del análisis y la evaluación del riesgo del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., para visualizar cualquier modificación que se requiera.

Para realizar el Plan del tratamiento de riesgos[9] se utilizó la Norma ISO/IEC 27001:2013, numeral 6.1.3, literal e) Formular el tratamiento de los riesgos de seguridad de la información; y, literal f) Hacer que los poseedores del riesgos aprueben el plan de del tratamiento de riesgos

[9] Norma ISO/IEC 27001:2013, Pág. 5

de la seguridad de la información y acepten los riesgos residuales de la seguridad de la información, [5].

El Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., deberá conservar la información documentada acerca del proceso de tratamiento de los riesgos de la seguridad de la información de acuerdo a lo que describe la norma.

Se debe asignar los recursos y las acciones correspondientes para implementar las decisiones de la gestión del riesgo que deben iniciar y decidir cuáles objetivos de control y controles escoger para el tratamiento del riesgo y preparar la declaración de aplicabilidad, como se ilustra en la Tabla 49, el cual es un documento muy importante del Sistema de Gestión de Seguridad de la Información.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., actualmente no disponen de un Sistema de Gestión de Seguridad de la Información para resguardar los activos de información que posee, lo que dificulta mantener resguardada la información de acuerdo a las normas de la ISO 27001:2013.

2. En el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.,

se realizó una encuesta a 51 personas, para determinar cómo se encuentra la seguridad de la información en función a los objetivos definidos aplicando un cuestionario estructurado con preguntas cerradas que cubren todos los aspectos de riesgos, incluso las amenazas a la confiabilidad, integridad y la disponibilidad de la información y están basadas en los objetivos de control de la ISO 27001:2013, que contiene 44 ítems relacionados a 25 indicadores utilizando el método Alpha de Crombrach para determinar la validez del instrumento, lo que permitió trabajar con información de alta confiabilidad debido a que el resultado fue de 0,96.

3. Se realizó el levantamiento de información por observación directa utilizando como guía la norma ISO/IEC 27001:2013, en la cual se encuentran 14 cláusula, 25 objetivos de control y 44 controles en base a los requerimientos del Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., lo que permitió identificar los activos de información así como el diagnóstico de seguridad de estos activos de acuerdo a los objetivos de control y controles revisados.

4. Se realizó el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando

Conjunto de las FF.AA.; así como la identificación del riesgo, identificación de las amenazas y vulnerabilidades; el cálculo del riesgo; tratamiento de riesgo; y, revisión de los riesgos y reevaluación de los activos de información.

Recomendaciones

1. Realizar la implementación del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., que permitirá resguardar los activos de información que posee la institución, a fin de mantener la información de acuerdo a las normas de la ISO 27001:2013 y continuar con la implementación.

2. Utilizar el método Alpha de Crombrach para determinar la validez del instrumento para futuras actualizaciones e investigaciones referentes al Sistema de Gestión de Seguridad de la Información el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., la misma que permitirá medir la confiabilidad de la información con la que se va a

trabajar para monitorear y revisar el Sistema de Gestión de Seguridad de la Información.

3. Revisar y actualizar periódicamente el Anexo F donde se encuentran los objetivos de control y controles listados en la Tabla A.1 de la norma ISO/IEC 27001:2013, en base a los requerimientos del Comando Conjunto de las Fuerzas Armadas y de acuerdo a lo que dispone en seguridad de la información para el levantamiento de la información del Sistema de Gestión de Seguridad de la Información, la misma que permitirá identificar y actualizar los activos de información así como el diagnóstico de seguridad de estos activos.

4. Utilizar y aplicar la información que se generó en el Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA.; aplicando la norma ISO 27001:2013, para realizar la implementación del Sistema de Gestión de Seguridad de la Información para Instituciones Militares, lo que permitirá gestionar eficientemente la accesibilidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información, minimizando los riesgos de seguridad de la información.

BIBLIOGRAFÍA

[1] PUCE, «http://es.slideshare.net/juankytascaz/juan-toca-pdf-28022637,» 21 Ago 2013. [En línea]. Available: http://es.slideshare.net/juankytascaz/juan-toca-pdf-28022637. [Último acceso: 03 Feb 2016].

[2] FGE, «http://www.metroecuador.com.ec/noticias/fiscalia-registra-1-026-denuncias-por-delitos-informaticos-en-ecuador/rUrokw---SvYDq0dbtKlVM/,» 23 Nov 2015. [En línea]. Available: http://www.metroecuador.com.ec. [Último acceso: 7 Jun 2016].

[3] SENAIN, «http://www.andes.info.ec/es/noticias/secretaria-inteligencia-ecuador-ratifica-sus-instalaciones-combate-unicamente-crimen,» 27 Jul 2015. [En línea]. Available: http://www.andes.info.ec. [Último acceso: 12 Abr 2016].

[4] D.G.P. COGMAR-INF-002-2010-O, « Directiva de Seguridad de la Información. Es una infraestructura de intranet que utiliza las Fuerzas Armadas,» 2010.

[5] ISO/IEC 27001:2013, *Estándar Internacional,* 2013.

[6] A. Alexander, Diseño de un Sistema de Seguridad de la Información, óptica ISO 27001:2005, Bogotá, D.C.- Colombia: Alfaomega Colombiana S.A., 2007.

[7] A. S. Tanenbaum, Redes de Computadoras, Mexico: Pearson Education, 2003.

[8] CRAMM, «CCTA Risk Analysis and Management Method (CRAMM),» Version 5.0, 2003.

[9] ISO/IEC 27001:2005, *Estándar Internacional,* 2005.

[10] ISO /IEC 17779:2005, *Código de Práctica para la Gestión de Seguridad de la Información,* 2005.

[11] INEN, «Código de Práctica para la Gestión de la Seguridad de la Información,» de *Tecnologías de la Información - Técnicas de Seguridad - Código de Práctica para la Gestión de la Seguridad de la Información*, Quito, NTE INEN, 2009.

[12] D.G.P. COGMAR-INF-002-2010-O, *Directiva General Permanente,* Quito, Pichincha: Armada del Ecuador, 2010.

[13] COMACO, *Manual de Elaboración de Documentación de las Fuerzas Armadas.,* Quito, Pichincha: COMACO, 2008.

[14] COMACO, *Estatuto Orgánico por Procesos,* Aquito, Pichincha: COMACO, 2012.

[15] R. Hernández, Metodología de la Investigación, Mexico D.F.: McGraw-Hill, 2003.

[16] B. B. Mendenhall, Introducción a la Probabilidad Estadística, Mexico, D.F.: Cengage Learning Editores, S.A. de C.V.,, 2010.

[17] L Hurdado y Toro G.J., Paradigmas y Métodos de Investigación, Valencia - España: Editorial Espíteme, 2001.

[18] ESPE, *Tesis Manual de procedimientos para ejecutar la auditoria informática en la Armada del Ecuador,* Quito, Pichincha: ESPE / SANGOLQUÍ, 2005.

[19] V. De Freitas, Análisis y Evaluación del Riesgo de la Información: Caso de estudio Universidad Simón Bolívar. Enlace:Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1), 43-55, 2009.

[20] International Organitation for Standardization: ISO 27001 - information security management, «ISO/IEC 27001 - Information security management,» 2013. [En línea]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Último acceso: 01 05 2016].