“MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ".

FABIO ANDRÉS LÓPEZ MOLINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BÁSICAS
FLORENCIA – CAQUETÁ
2018

“MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ".

FABIO ANDRÉS LÓPEZ MOLINA

PROYECTO DE GRADO

Asesor Inicial:
Ingeniera, Lorena Suarez

Asesor Correcciones
Ingeniero, Jhon F. Quintero Tamayo

Director
Ingeniero, Alexander Larrahondo Nuñez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BÁSICAS
PROYECTO DE SEGURIDAD INFORMÁTICA II
FLORENCIA - CAQUETÁ
2018

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

INTRODUCCIÓN

El informe final del proyecto de grado denominado “MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ” que se muestra en este documento, tiene como objetivo general “Evaluar el cumplimiento de las políticas de Seguridad Informática y riesgos de la Armada Nacional de Colombia mediante Auditoría Interna de Seguridad informática en la Estación de Guardacostas Urabá”, se encuentra dividido en capítulos en los que se puede notar su evolución acorde a su desarrollo.

En el primer capítulo se realiza la definición del problema en el cual se exponen los recursos para contribuir a la seguridad informática con los que cuenta la Estación de Guardacostas y las posibles falencias que a primera vista se pueden encontrar en la misma, lo que nos lleva a la pregunta de investigación ¿Cómo fortalecer la aplicación de las políticas de seguridad informática de la Armada Nacional en la Estación de Guardacostas de Urabá?

El capítulo dos se justifica la realización del proyecto, teniendo en cuenta la gran importancia que tiene para las instituciones del Estado que sus activos informáticos, información y personal se encuentren debidamente protegidos y los últimos capacitados.

El objetivo general y los objetivos específicos se exponen en el capítulo tres, seguido del marco referencial en capítulo cuatro, que está compuesto por las normativas legales que avalan las políticas de Seguridad Informática de la Armada Nacional, las teorías que se configuran como el pilar fundamental del proyecto.

1 DEFINICIÓN DEL PROBLEMA

La estación de Guardacostas de Urabá es una Unidad Táctica de la Armada Nacional, que se encuentra ubicada en el municipio costero de Turbo Antioquia, entre sus responsabilidades principales está la protección de la vida humana a través del control del tráfico marítimo en el Golfo de Urabá, lo que conlleva enfrentar de manera directa el flagelo del narcotráfico y en consecuencia, su Recurso Humano debe estar adecuadamente capacitado y su Infraestructura Tecnológica protegida contra las actividades delictivas que buscan conocer, tergiversar, eliminar u ocultar la información que información que se maneja.

La Armada Nacional ha realizado inversiones en infraestructura y activos informáticos para la protección de la información y se han desarrollado políticas de seguridad informática[1]. Sin embargo, gran parte del personal que labora en la Estación de Guardacostas no está adecuadamente capacitado en temas como la utilización de contraseñas seguras, los riesgos que representa para la información ingresar a Internet e Intranet en los mismos equipos de cómputo donde se almacena información sensible y/o clasificada, y otras prácticas poco seguras.

En su gran mayoría, estos problemas se presentan por la falta de personal idóneo para realizar estas actividades de capacitación, por esta misma razón no se han implementado de manera adecuada las políticas de Seguridad Informática para las Fuerzas Militares ya que no cuentan con los equipos tecnológicos apropiados y la capacitación adecuada para el personal que labora en la Estación, Lo anterior genera riesgos para la seguridad de la información.

[1] FUERZAS MILITARES DE COLOMBIA. Directiva Permanente No. 200-12/2006 Políticas de Seguridad Informática PARA LAS F.F.M.M. FFMM. BOGOTA D.C. 84 p.

2 JUSTIFICACIÓN

Los organismos de Seguridad del Estado Colombiano, debido a sus funciones deben contar con los medios humanos y Tecnológicos adecuados para brindar seguridad a sus recursos informáticos, esto con el objetivo de mitigar los riesgos generados por ataques informáticos que puedan entorpecer el logro de sus Objetivos Estratégicos.

Se requiere de una intensiva socialización y sensibilización del personal que tripula las unidades para crear una asertiva conciencia de Seguridad informática. Aún hoy en día estamos enfrentando una época en la cual las personas se enfrentan a bruscos cambios de tipo tecnológico, es decir, tienen que adaptarse al uso de nuevas herramientas tanto Hardware como Software en sus actividades diarias y esto genera conflictos en muchos tripulantes que generan resistencia para afrontar nuevos retos. Es por esta razón que la capacitación del personal debe ser amplia y permanente, con el objetivo de inculcar un concepto amplio de las Políticas de Seguridad Informática y al final, la Estación de Guardacostas contará con un equipo de talento humano fortalecido y consiente de las amenazas de tipo informático, lo cual contribuye de manera directa al fortalecimiento de la Seguridad de la Información de la organización, a la protección de la confidencialidad, integridad y disponibilidad de la misma y por ende el cumplimiento de los Objetivos Estratégicos de la Organización.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Evaluar el cumplimiento de las políticas de Seguridad Informática y riesgos de la Armada Nacional de Colombia mediante Auditoría Interna de Seguridad informática en la Estación de Guardacostas Urabá.

3.2 OBJETIVOS ESPECÍFICOS

Identificar Deficiencias de seguridad informática mediante una auditoría interna en la Estación de Guardacostas Urabá.

Gestionar los riesgos encontrados en la auditoria mediante metodología Magerit.

Elaborar un informe técnico de Seguridad Informática para la Dirección de Tecnologías de la Información y las Comunicaciones de la Armada Nacional.

Capacitar al personal de la Estación de Guardacostas Urabá con el propósito de mejorar la aplicabilidad de las políticas de Seguridad Informática.

4 MARCO REFERENCIAL

4.1 MARCO LEGAL

4.1.1 Ley 57 de 1985[2]

Dentro de las referencias para el presente proyecto se ha decidido iniciar con la ley que ordena la publicidad de los actos y documentos oficiales, en este aspecto, las Fuerzas Militares y específicamente la Armada Nacional de Colombia está en la obligación de dar cumplimiento a esta ley constitucional. Por otra parte, también está obligado a proteger la reserva de los documentos que tienen carácter de reserva legal, como lo reza el artículo 13 de esta misma ley y tiene por objeto garantizar la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso en el marco de las labores de inteligencia y contrainteligencia que desarrolla la institución armada.

Estos temas también son tratados con más detalle en la Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones[3]. Más específicamente se ordena la creación centros de protección de datos de inteligencia y contrainteligencia en la Ley Estatutaria 1621 del 17 de abril de 2013 por medio de la cual se dictan medidas para que los organismos que desarrollan actividades de inteligencia y contrainteligencia puedan desarrollar su misión constitucional de manera adecuada y sin contravenir la misma constitución[4].

[2] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 57. (5, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. El Congreso. Bogotá, D.C., 1985. 6 p.

[3] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1712. (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. El Congreso. Bogotá, D.C., 2014. 314 p.

[4] COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". El Congreso. Bogotá, D.C., 2013. 17 p.

4.1.2 Conjunto de normas ISO/IEC 27000:2005.[5] La serie de normas ISO/IEC 27000 constituye un estándar para implementar y dar continuidad a un sistema de gestión de seguridad informática desarrollados por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) que proporcionan a las organizaciones grandes, medianas o pequeñas un ejemplo o una guía para realizar de la gestión de seguridad informática.
En esta serie de normas se recopila el porqué de la importancia de la implementación de un Sistema de Gestión de Seguridad de la información, se define su terminología, una pequeña introducción y una descripción de los pasos para el desarrollo, seguimiento, mantenimiento y potencialización de dicho sistema de gestión.

La norma principal de esta serie es la ISO/IEC 27001 en esta se recopilan todos los requisitos de un sistema de gestión de seguridad de la información, enumerando los objetivos de control y controles que se deben establecer en el sistema de gestión de los cuales, dependiendo de la actividad y tamaño de la organización, no se hace necesario acogerlos todos, pero se debe argumentar de manera veraz y verificable por qué, no se van a aplicar los controles excluidos.

La siguiente es la norma ISO/IEC 27002, es una norma de la familia que no es certificable y viene siendo una guía de buenas prácticas que realiza la descripción de 39 objetivos de control con 133 controles, agrupados en 11 dominios, igualmente aplicables a cualquier empresa interesada en asegurar la efectividad de su sistema de gestión de seguridad de su información.

Otra norma de esta familia, que tampoco es certificable es la ISO/IEC 27003 que se destaca por ser una guía con los aspectos más importantes a tener en cuenta a la hora de diseñar e implementar un SGSI, describe la manera de desarrollar el sistema desde su proyección hasta su implementación de la mano de una guía para conseguir la aprobación de la dirección.

Para determinar la eficacia del SGSI ya implementando la norma ISO/IEC 21004 proporciona una guía para el desarrollo de técnicas y métricas utilizadas para determinas dicha efectividad, esta norma igual que las dos anteriores no es certificable y actualmente se encuentra en proceso de actualización para su revisión.

La norma ISO/IEC 27001:2005 está genera una guía para la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión

[5] ISO27000.ES, El portal de ISO 27001 en Español. [en linea]. Madrid: Disponible en: http://www.iso27000.es/

de riesgos. También la norma ISO/IEC 27001:2005 se especifican los requisitos que deben llenar las entidades que realizan auditorias y certificación de sistemas de gestión de seguridad de la información.

Muchas otras normas se encuentran en proceso de actualización y desarrollo que entre otros tratan temas de gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores, gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones, gobierno corporativo de la seguridad de la información, SGSI orientada a organizaciones del sector financiero y de seguros, Cloud Computing, energía y más.

4.1.3 Políticas de seguridad informativa para las FFMM. Como una de las organizaciones más grandes del país, las fuerzas Militares de Colombia tienen la obligación de proteger la soberanía nacional y garantizar la seguridad de sus habitantes, para dar cumplimiento a esta misión hace uso de los recursos que ofrecen las TIC's para manejar los procesos Operativos y Administrativos de manera segura, eficaz y eficiente, para lo cual adopta algunas de las normas de la familia ISO/IEC27000 como marco de referencia para la proyección diseño e implementación de un robusto Sistema de Gestión de Seguridad de la Información.[6]
Este SGSI es de vital importancia, debido a que la información, al igual que la plataforma tecnológica que la soporta, son considerados de los activos estratégicos para las Fuerzas Militares por lo que la definición de un marco de control es primordial para brindar seguridad a los activos de información de las unidades que conforman la organización.

En este sentido y con la finalidad de establecer los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada se definen una serie de objetivos de implementación de la política de seguridad de la información para las Fuerzas Militares así:

- Proteger los recursos informáticos y tecnológicos utilizados para el procesamiento de la información, de las diferentes amenazas deliberadas o accidentales, internas o externas, buscando asegurar la confidencialidad, integridad, disponibilidad, trazabilidad de la información mediante la implementación de efectivos controles.

- Definir y establecer un modelo organizacional de Seguridad de la Información en el cual se instauran lo más acertadamente posible los roles y responsabilidades de los integrantes del grupo de implementación de la política.

6 FUERZAS MILITARES DE COLOMBIA. Directiva Permanente No. 200-12/2006 Políticas de Seguridad Informática PARA LAS F.F.M.M. FFMM. BOGOTA D.C. 84 p.

- Realizar las acciones pendientes a sensibilizar al personal en la aplicación de la política con el fin de mantener y mejorar de manera continua la cultura en seguridad de la información para minimizar los incidentes que atentan contra los pilares de la información.

- Coordinar con todas las organizaciones que interactúan con las Fuerzas Militares para lograr integralidad en la protección de la información y los activos informáticos y tecnológicos que la soportan.

- Coordinar con las jefaturas de las diferentes Fuerzas la adición presupuestal necesaria para la implementación, mantenimiento y mejoramiento del SGSI.[7]

En el desarrollo de las políticas de seguridad de la información de la Fuerzas Militares se establece la adopción de una metodología de análisis de riesgos de seguridad de la información con el objetivo de definir e implementar un tratamiento diferencial y especifico en cada una de las áreas operativas y administrativas de cada una de las unidades adscritas a las Fuerzas Militares.

Dentro el establecimiento de la política de seguridad informática se recomienda emplear una metodología basada en la norma ISO/IEC 27005 en su versión 2008 en la cual se establecen las siguientes actividades:

- La identificación de los activos informáticos y tecnológicos que posee la organización.

- Valoración del impacto que pueden generar la consolidación de los riesgos en los activos informáticos.

- Identificación de los escenarios en los que se generan amenazas y vulnerabilidades.

- Valoración de la probabilidad de ocurrencia de los escenarios de riesgo.

- Identificación de opciones para el tratamiento de los riesgos que sean valorados en un nivel en el que se puedan aceptar.

Para el desarrollo de las anteriores actividades se deben definir los procesos críticos en los cuales se debe aplicar el análisis de riesgos a través de entrevistas con los responsables de los activos y procesos mismos con el propósito de dar a

[7] MINISTERIO DE DEFENSA NACIONAL. Directiva Permanente N°. DIR2014-18 (19, Junio, 2014). Políticas de Seguridad de la Información para el Sector Defensa. MINDEFENSA. Bogotá D.C. 2014. 34 p.

conocer la metodología y realizar el levantamiento del inventario de los activos informáticos. Adicionalmente se debe nombrar un Comité de Seguridad de la información que se deberá reunir por los menos dos veces al año con el fin de evaluar la efectividad de los controles y los cambios significativos en la estructura organizacional.

En las misiones particulares que se emiten a las diferentes Jefaturas se encuentran:

- Promover el desarrollo de la cultura de seguridad de la información a través de campañas de sensibilización y concientización a todos los involucrados en cada uno de los procesos de la organización.

- Se deben gestionar los recursos financieros necesarios para proteger de manera adecuada los activos de información y realizar un adecuado y continuo mantenimiento del sistema de gestión de seguridad de la información.

- Se debe ordenar la inclusión de temas relacionados con seguridad de la información, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares.

- Siendo el tema un sistema de gestión se debe incluir en los planes de inspección de las departamentos y dependencias de toda la organización, revistas relacionadas con los aspectos de seguridad de la información, lo anterior teniendo en cuenta la transversalidad de todos los procesos.

- También se deben coordinar con las oficinas de Inspección delegadas de las Fuerzas la realización de auditorías al proceso del Sistema de Gestión de Seguridad de la Información.

- Las oficinas de tecnología deben implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información. Al igual que registra y mantiene la información requerida para auditar y evaluar la ejecución de los controles específicos.

- También debe definir, mantener y controlar la lista actualizada de software y aplicaciones tanto autorizadas como no autorizadas; así mismo, realizar el control y verificación de cumplimiento del licenciamiento software y aplicaciones asociadas.

Las oficinas cibernéticas de cada Fuerza y conjuntas desarrollaran estrategias, programas, proyectos y todas las actividades requeridas tendientes a garantizar la gestión de la ciberdefenza de los activos de información e informáticos de la organización.

De acuerdo con Christopher Hadnagy en su libro "Ingeniería Social el Arte del Hacking Personal" se define a la Ingeniería Social como "El acto de manipular a una persona para que lleve a cabo una acción que –puede ser o no- lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o lograr que se realice una determinada acción" [8]. En diferentes ramas de varias ciencias se puede decir que se utilizan elementos que pueden hacer parte de la Ingeniería Social para "manipular" a sus clientes, se puede hablar de la política en la que se aplica de principio a fin, el comercio, organizaciones de defensa y seguridad nacional que buscan persuadir a las personas para que realicen acciones que son beneficiosas para ellos mismos. También existen herramientas de la Ingeniería Social que son utilizadas por delincuentes que buscan que su víctima realice acciones que le perjudican. Aunque el resultado es muy diferente, el proceso puede ser similar.

Por otra parte María Gabriela Cortez Pinto en su trabajo de graduación que titula "Las vulnerabilidades humanas en relación a la seguridad informática para evitar la fuga de información confidencial en el departamento de recursos humanos de la Universidad Técnica de Ambato" concluye que "la única manera de combatir los ataques informáticos referentes a las vulnerabilidades humanas es la educación de los usuarios, para generar una cultura de concientización y seguridad en la relación establecida entre usuario y máquina."[9] Es por esto por lo que se deben buscar las maneras o metodologías más adecuadas para persuadir a los usuarios de poner en práctica de manera asertiva las recomendaciones y obligaciones que le son asignadas en las políticas de seguridad informática de su empresa.

En esta investigación también se analizó el estudio que realizaron Gabriela Torres y Diego Llanga en su tesis titulada "Estudio e Implementación de una metodología de Prevención de Intrusos para redes LAN" (Torres & Llanga, 2010) en el cual se refieren a las metodologías más utilizadas para desarrollar un Sistema de gestión de riesgos. Se realiza un análisis FODA de las propiedades cualitativas y cuantitativas de las metodologías; UNE 71504:2008, MAGERIT. Las

[8]HADNAGY, Christopher. Ingeniería Social: El arte del Hacking personal. Madrid: Editorial ANAYA MULTIMEDIA.,2011. 400 p.

[9] CORTEZ PINTO, Maria. Las vulnerabilidades humanas en relación a la seguridad informática para evitar la fuga de información confidencial en el departamento de recursos humanos de la Universidad Técnica de Ambato. Trabajo de Graduación para Ingeniero en Sistemas Computacionales e Informáticos. Ambato – Ecuador. Universidad Tecnico de Ambato. Facultad de Ingeniería en Sistemas Electrónica e Industrial. 2013. 209 p.

nomas; ISO 27005, ISO 27002. Este análisis es adecuado para la escogencia de la metodología adecuada a utilizar en El Autor.[10]

En un artículo publicado por la revista semana que titula “Las empresas colombianas no están preparadas para los ciberataques” en el cual se publica la cantidad alarmante de denuncias de delitos informáticos los cuales evidencian un incremento del 40% y generando pérdidas de alrededor de 500 millones de dólares. El panorama más desalentador es que el 43% de las empresas no cuentan con ninguna de clase de planes de contingencia contra ataques informáticos.[11]

4.2 MARCO TEÓRICO

El presente proyecto se lleva a cabo en la Estación de Guardacostas Urabá “Contralmirante José Augusto Matallana Rodríguez” ubicada en Avenida La Playa sector Punta Las Vacas en el municipio de Turbo, departamento Antioquia, está tripulada por personal de Oficiales, Suboficiales, Infantes de Marina Profesionales y Regulares y personal civil que en total suman 76 personas y realizan actividades de tipo administrativo y operativo. Para realizar las actividades administrativas este personal solo cuenta con 15 equipos de cómputo razón por la cual cada equipo es compartido con 4 personas en promedio. El tiempo destinado para el desarrollo del proyecto será de cuatro meses.

Para desarrollar las actividades para las que fue creado el cuerpo de guardacostas de la Armada Nacional entre las cuales se encuentra; contribuir a la defensa de la soberanía Nacional, labores de asistencia y rescate en el mar, proteger el medio marino contra la contaminación, Controlar y proteger la inmigración o emigración clandestinas y una de las más delicadas Controlar el tráfico marítimo.[12] Es de vital importancia propender por garantizar que la información alojada y tratada a través de los recursos informáticos esté disponible de manera constante sin alteraciones y lo más importante, manteniendo la debida confidencialidad.

[10] TORRES ANDAGANA, Gabriela y LLANGA SALCAN, Diego. Estudio e Implementación de una Metodología de Prevención de Intrusos para redes LAN. Tesis de Grado Ingeniero en Electrónica y computación. Riobamba – Ecuador.: Escuela Superior Politécnica de Chimborazo. Facultad De Informática y Electrónica. Escuela de Ingeniería Electrónica y Tecnología en Computación. 2010. 223 p.

[11] SEMANA. Las empresas colombianas no están preparadas para los ciberataques. [En linea]. Bogotá.: Semana.com. Disponible en: http://www.semana.com/tecnologia/articulo/las-empresas-colombianas-no-estan-preparadas-para-los-ciberataques/466430

[12] COLOMBIA. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. DECRETO 1874 (2, Agosto, 1979). Por el cual se crea el Cuerpo de Guardacostas y se dictan otras disposiciones. La Presidencia. Bogotá, D.C., 1979. 2 p.

4.2.1 Gestión de Riesgos. Una de las principales barreras a la aplicación de estas tecnologías computacionales en el sector de seguridad de una nación es la seguridad de la gran cantidad de datos sensibles que se manejan en las mismas. Estas organizaciones están obligadas constitucionalmente a salvaguardar la vida de los ciudadanos en cualquier tipo de actividad, es por esta razón que los estándares de seguridad que utilizan deben ser los mejores, por ende, es necesario implementar aplicaciones y metodologías con grandes restricciones para su utilización. Por esta razón El Autor busca el mejoramiento de las políticas de seguridad informática de la Estación.

La Gestión de Riesgos está encaminada a identificar de manera cualitativa y cuantitativa los riesgos que se presentan en los sistemas informativos, de la misma establecer la frecuencia con la cual ocurren y el impacto que pueden generar para posteriormente hacer la gestión de los riesgos con políticas y planes de contingencia para evitar que ocurran o atenuar su impacto. Para explicarlo mejor a continuación se hace claridad sobre los conceptos aquí utilizados.

AMENAZA: Es la probabilidad que tiene un desastre de ocurrir en un lapso dado, esta puede estar representada en una persona (hacker u operario falto de pericia), programa informático malicioso, o los factores climatológicos y desastres naturales.[13]

VULNERABILIDAD: Es una debilidad que puede tener el sistema, acuerdo Benavides Miriam y Solarte Francisco en el Modulo Riesgos y Control Informático se puede definir como " el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala. Se puede decir que la vulnerabilidad es inherente al sistema y es la posibilidad que una amenaza se materialice por el actuar de una persona, un programa o factor climático.[14]

SEGURIDAD DE LA INFORMACIÓN: Cada día se escucha hablar con mayor frecuencia de la seguridad de la información, seguridad informática, o en algunos casos información garantizada, aunque parezca y se usen comúnmente para referirse a lo mismo son términos diferentes, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Estas diferencias radican principalmente en el enfoque y las metodologías utilizadas.

[13]BENAVIDES RUANO, Miriam y SOLARTE SOLARTE, Francisco. Módulo riesgo y control informático. Pasto.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. 2012. 188 p.
[14] Ibid., p. 16

Para el caso de la seguridad de la información se refiere a salvaguardar la Confidencialidad, disponibilidad e integridad de la información y datos independientemente de la manera o el medio en el que se encuentren almacenados ya sean impresos físicamente en cualquier medio, electrónicos de diferentes clases como datos audio y video. Dependiendo de la actividad económica de la organización y de la clase de datos que se almacenen, en general la información es altamente sensible ya que hoy día existe legislación que protege los datos que los ciudadanos entregan a las organizaciones para conocimiento estrictamente de la organización misma y la pérdida o filtración de esta información tiene consecuencias legales, sin hablar de las económicas y la reputación de la organización.[15]

Por otra parte, la seguridad informática se encarga de proteger y gestionar los recursos de un sistema de información, tanto dispositivos como programas, para evitar que personal diferente a los encargados cambien la configuración de los sistemas valiéndose de diferentes técnicas, eso con el fin de cambiar o corromper de alguna manera la información allí contenida.

4.3 MARCO CONCEPTUAL

Se define la Seguridad Informática como el proceso de "asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió 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."[16]

Una organización implementa políticas de seguridad informática con el fin de proteger el activo más importante, que en la era contemporánea es la información.

Por otra parte existe un principio de la Ingeniería Social, es aquel que afirma que en un sistema informático de cualquier clase los usuarios internos y externos son el eslabón más débil de la cadena. Los delincuentes utilizan comúnmente cualquier medio de comunicación para engañar a las personas simulando, por ejemplo, ser un empleado de un banco o de una empresa, un compañero de

[15] Ibid., p. 34

[16] © Derecho.com. Manual Seguridad Básica Informática, ©Derecho.com FDL Licence. [En linea]. España.: Disponible en: http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/manual-seguridad-basico.pdf

trabajo, un técnico o un cliente y así obtener información de una persona o empresa.[17]

[17] AGUILERA LÓPEZ, Purificación. Seguridad Informática. 1 ed. Madrid: Editorial Editex. 2010. 240 p.

5 DISEÑO METODOLÓGICO

5.1 FASE 1, RECONOCIMIENTO DE LA INFRAESTRUCTURA INFORMÁTICA

En esta fase se identificarán los componentes de la infraestructura informática. Se realizará verificación de la arquitectura del sistema, todo el equipamiento informático, servicios subcontratados, las instalaciones Físicas y de Red. De manera paralela se desarrollará la auditoria Informática. Adicionalmente se iniciará el acercamiento capacitando al personal en los conceptos generales de Seguridad Informática.

5.2 FASE 2, CAPACITACIÓN DEL PERSONAL EN SEGURIDAD INFORMÁTICA.

Esta fase desarrollara desde el inicio del proyecto entrevistando al personal de la Estación de Guardacostas Urabá, con el fin de establecer cuál es su nivel de conocimiento de las políticas de seguridad informática de las Fuerzas Militares, para con ello, establecer un cronograma de capacitaciones con el fin de sensibilizar de manera adecuada al personal de la Estación. Se realizarán encuestas y entrevistas con las personas que tienen a su cargo el procesamiento y manejo de datos reservados de la organización, con el propósito de identificar el nivel de aplicación de las políticas de seguridad.

5.3 FASE 3. IDENTIFICACIÓN DE FACTORES DE RIESGO.

En esta fase se consolidan los datos recolectados de la aplicación de la metodología Magerit, también las acciones que ponen en alto riesgo (critico) el manejo de la información reservada.

5.4 FASE 4. ELABORACIÓN DE ACCIONES DE MEJORA.

Con los datos y conclusiones establecidas en las fases anteriores se establecen acciones de mejora para la correcta y oportuna aplicación de las políticas de

seguridad, teniendo en cuenta las razones expresadas por los usuarios y presentando alternativas para mejorar el uso de las políticas.

6 AUDITORIA INFORMÁTICA

Se llevó a cabo una auditoría interna de seguridad informática de acuerdo con lo establecido en las políticas de seguridad informática de las Fuerzas Militares e implementadas por la Armada Nacional y con el formato establecido para tal fin. En esta auditoria se siguieron los pasos que se describen a continuación:

6.1 PLANEAMIENTO DE LA AUDITORIA

En este primer paso se definieron y establecieron de forma clara las razones por las cuales se llevaba a cabo la auditoria informática en la Estación de Guardacostas Urabá por medio de una reunión en la que participan el señor comandante, Segundo comandante, los jefes de dependencias, encargado de Sistemas y el Vigía de seguridad informática de esta misma unidad. Se explica el propósito de la auditoria por medio de los objetivos de la siguiente manera:

- Verificar el cumplimiento de las políticas de Seguridad de la Informática de las Fuerzas Militares por parte de los integrantes de la estación de Guardacostas de Urabá.

- Propender por garantizar la integridad, confidencialidad y disponibilidad de la información mediante la aplicación adecuada de las recomendaciones y controles de seguridad establecidos en las Políticas de Seguridad de la Información de la Fuerzas Militares.

- Determinar la situación actual del área de informática de la Unidad y las actividades y esfuerzos necesarios para mejorar el cumplimiento de las políticas de seguridad informática.

- Visibilizar ante la Jefatura correspondiente los requerimientos tecnológicos y humanos técnicos para fortalecer la aplicación de las políticas de seguridad informática.

6.2 DESARROLLO DE LA AUDITORIA

El procedimiento de auditoría se inicia en las instalaciones que han sido asignadas al encargado de la oficina de Informática de la Estación de Guardacostas Urabá, se verifica el inventario de activos informáticos encontrando las hojas de vida de cada activo en forma digital, con la novedad que en estos documentos no se evidencian anotaciones de los trabajos realizados a los equipos, esto teniendo en cuenta que la mayoría de los equipos son obsoletos con modelos que datan desde del año 2002, entre los cuales se encontraron equipos de cómputo con sistemas operativos para los cuales la empresa desarrolladora, dejó de generar actualizaciones de seguridad cómo son: el sistema operativo Windows XP, también se encuentra equipos que están funcionando con aplicaciones también obsoletas como el Internet Explorer[18].

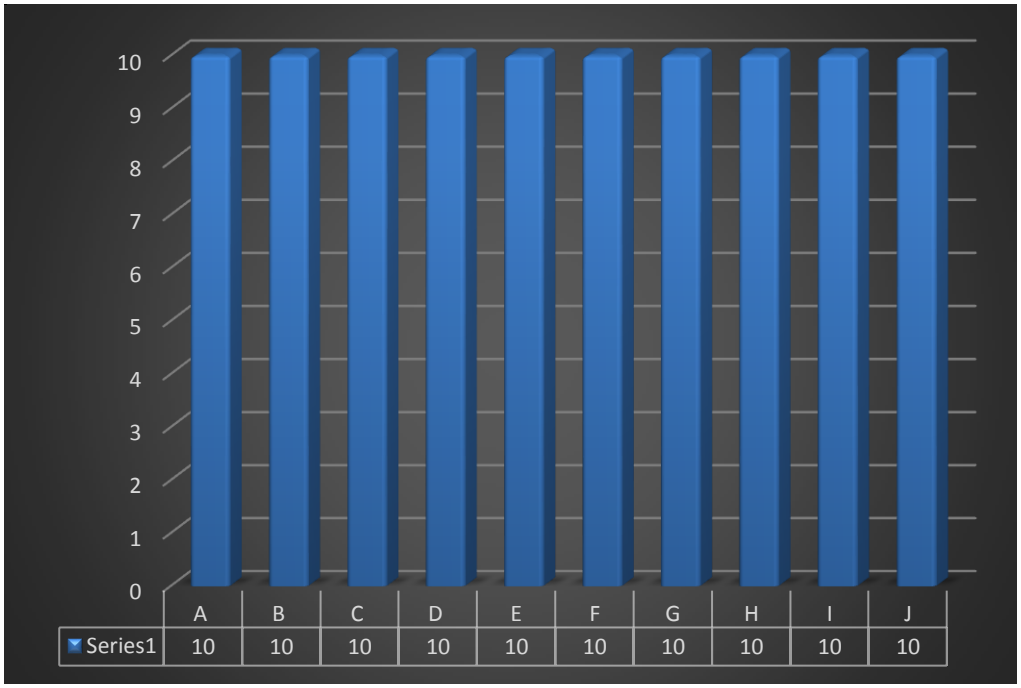
Continuando con el desarrollo de la auditoria se realiza la verificación inventario de equipos informáticos con los que cuenta la Unidad observando sus encargados con sus respectivos roles, perfiles y credenciales de manejo documental.

Una de las más importantes actividades de la auditoria es la aplicación del formato de verificación para usuarios finales, estipulada en los anexos de las Políticas de Seguridad Informática de las Fuerzas Militares, el cual asigna un puntaje a cada pregunta con el cual se le asigna una calificación final en la que se determina el nivel de aplicación de las políticas de seguridad de la información, arrojó los siguientes resultados:

A la pregunta: ¿Conoce las funciones del cargo que le fueron asignadas? Las personas seleccionadas en la encuesta respondieron afirmativamente como muestra la ilustración 1, lo cual demuestra gran compromiso del personal con sus cargos asignados y funciones adicionales.

[18] MICROSOFT. Se ha dejado de ofrecer soporte para Windows XP. [En linea]. Disponible en: https://www.microsoft.com/es-es/windowsforbusiness/end-of-xp-support

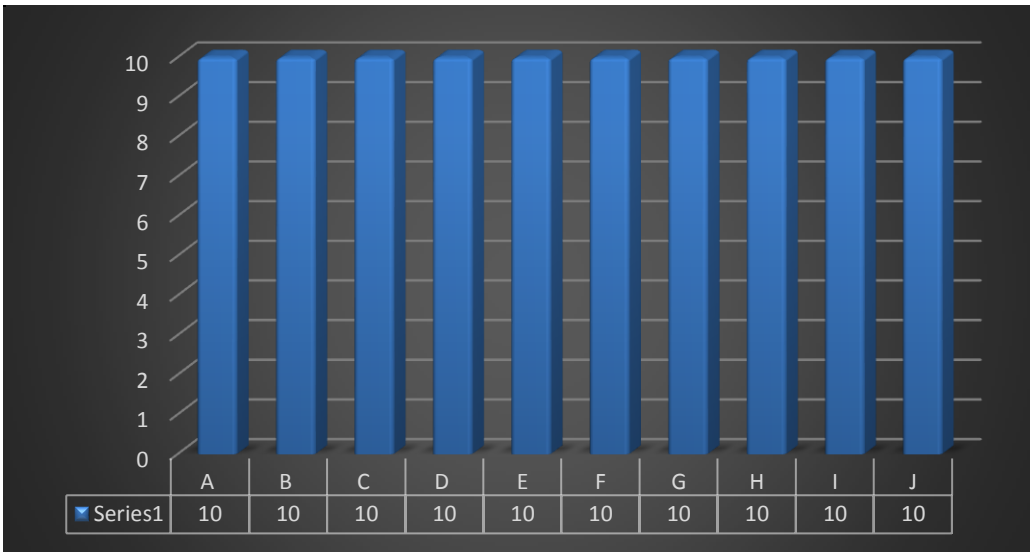
Ilustración 1. ¿Conoce las funciones del cargo que le fueron asignadas?



Fuente: El Autor.

A la pregunta: ¿conoce la política de seguridad informática en la armada nacional? (Mencione Alguna). El total de los encuestados respondió afirmativamente como se observa en la ilustración 2, pero en su gran mayoría, entiende las Políticas de Seguridad informática como la restricción a la utilización de dispositivos extraíbles en los terminales de cómputo y la promesa de reserva de la información que maneja, ignorando la integralidad de la política con todos los demás controles establecidos para asegurar la seguridad de la información, mostrando la falta de socialización adecuada y continua.

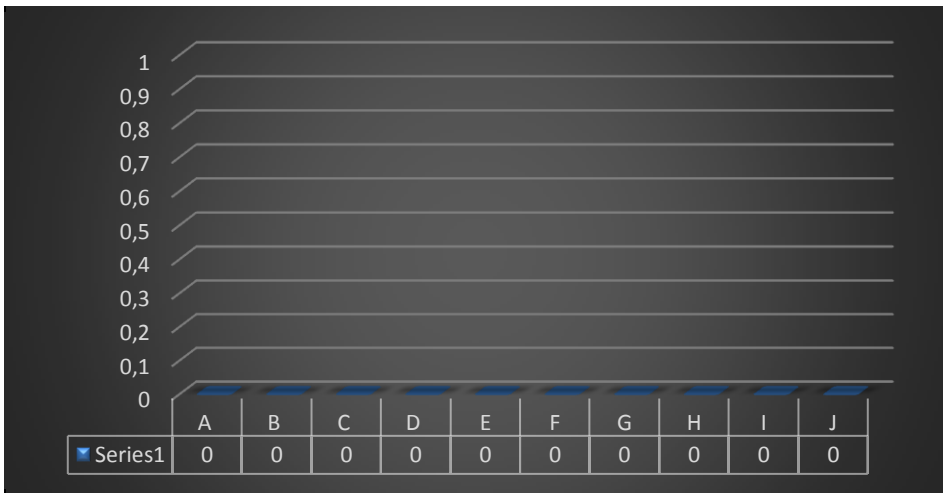
Ilustración 2. ¿Conoce la política de seguridad informática en la armada nacional?



Fuente: El Autor.

A la pregunta: ¿Ha firmado el formato de aceptación de políticas de seguridad informática para las FF.MM en su unidad actual?, los resultados fueron negativos en todos los encuestados. Debido a esto, se verificó con el encargado de realizar los formatos encontrando que no conocía la obligatoriedad del diligenciamiento de ese documento siempre que realizara presentación personal a trabajar en la Unidad, ya fuera militar o civil y sus labores fueran permanentes o temporales. Lo anterior se evidencia en la ilustración 3.

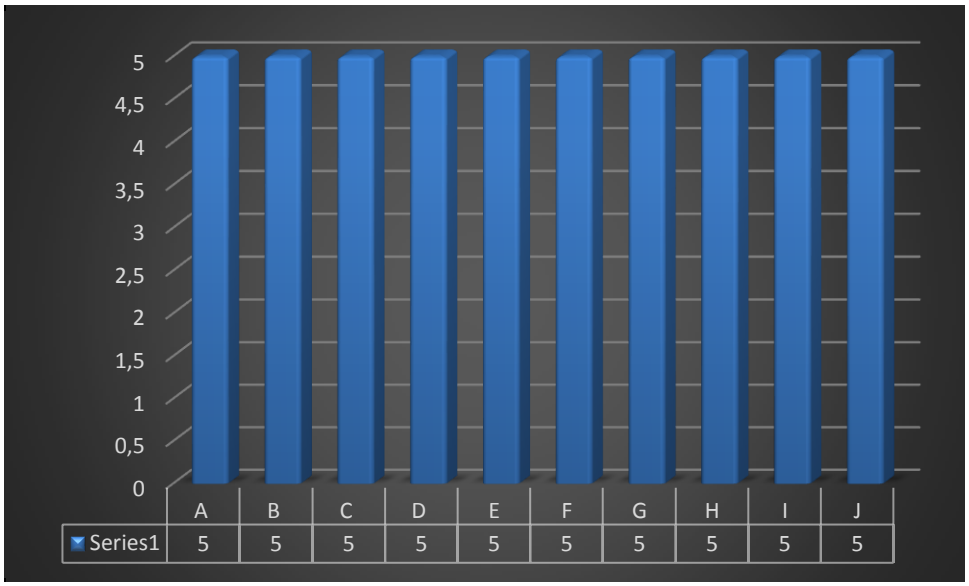
Ilustración 3. ¿Ha firmado el formato de aceptación de políticas de seguridad informática para las FF.MM en su unidad actual?



Fuente: El Autor.

En la pregunta: ¿Tiene tarjeta de manejo documental? (indique Grado de Clasificación) se pudo evidenciar que el documento de control se encontraba en una parte visible del área de trabajo de todos los usuarios como se evidencia en la siguiente ilustración.

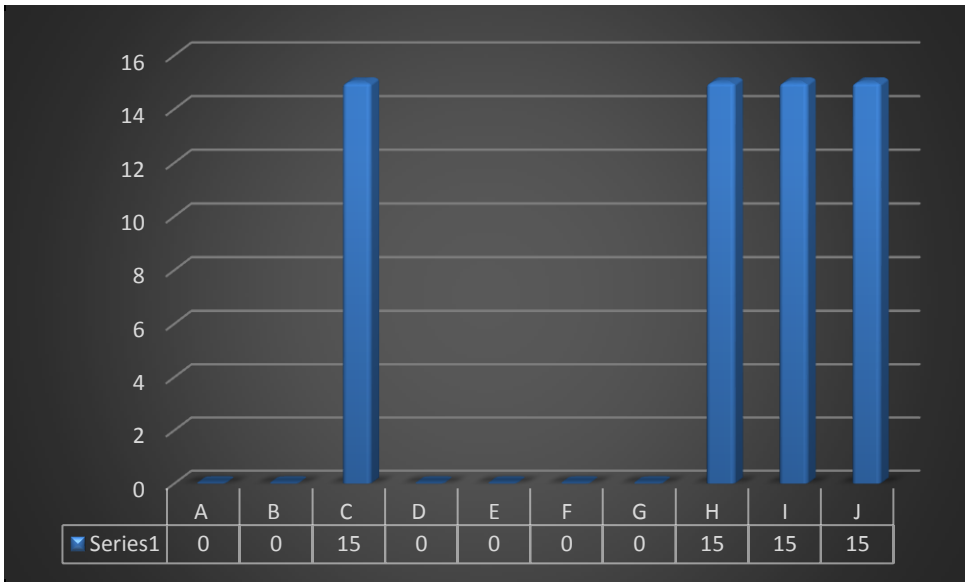
Ilustración 4. ¿Tiene tarjeta de manejo documental?



Fuente: El Autor.

Como continuación de la pregunta anterior se interroga: ¿Está vigente la tarjeta de manejo documental? (Verificar Tarjeta), y se encuentra que como aparece en la ilustración 5, el 60% de los encuestados no tiene actualizada su tarjeta de manejo documental, la cual debe ser actualizada de manera anual, en el momento en que el personal cambie de cargo o por orden del comandante de la Unidad al cambiar en algún sentido las funciones del cargo. Lo anterior por la necesidad de verificar si las nuevas funciones obligan al tripulante a manejar información con una clasificación diferente a la que venía manipulando.

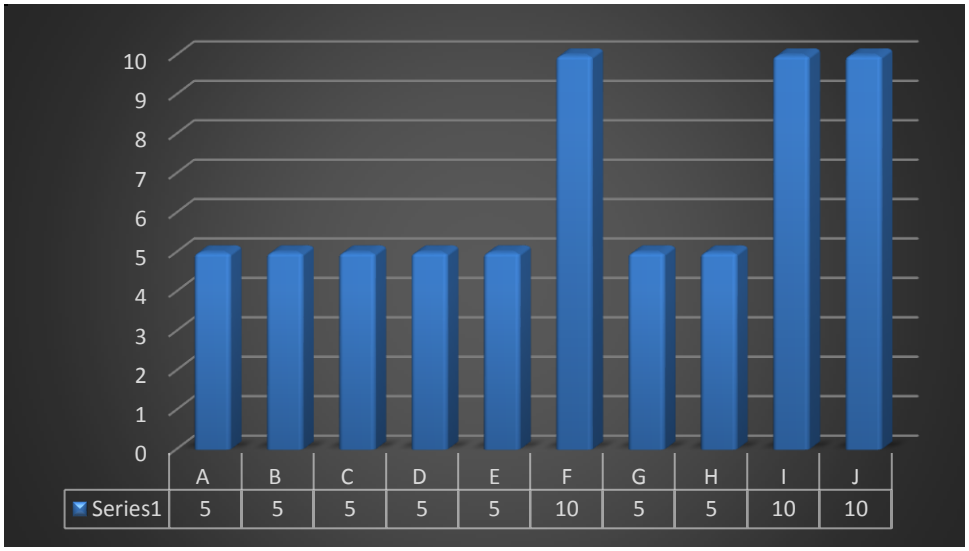
Ilustración 5. ¿Está vigente la tarjeta de manejo documental?



Fuente: El Autor.

Cuando se interroga al personal si por razones del servicio transporta información fuera de la institución en dispositivos personales y/o institucionales y se aclara que debe Marcar SÍ, si utiliza algún mecanismo de seguridad e indicar qué mecanismos, de lo contrario, marcar NO o Marque 0 si, SÍ transporta información sin mecanismo de seguridad. Se encontró que hace falta fortalecer la capacitación en seguridad informática, debido a que el personal que transporta información, que como se puede evidenciar en la ilustración 6, es relativamente poco. Confían la protección de su activo informático a la clave que solicita el sistema operativo que ofrece el dispositivo informático, lo cual genera altos riesgos a la confidencialidad, disponibilidad e integridad de la información que manejan debido a la facilidad con la que se pueden corromper estas claves.

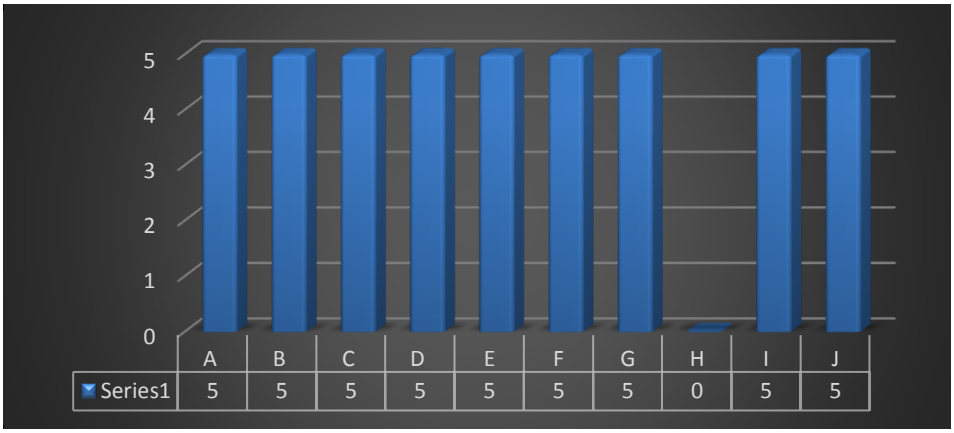
Ilustración 6. ¿Por razones del servicio transporta información fuera de la institución en dispositivos personales y/o institucionales?



Fuente: El Autor.

A la pregunta: ¿Conoce de los riesgos de transportar información fuera de la institución? (Indique dos (2)) el personal está consciente del riesgo de pérdida de información que se genera al exponer los activos informáticos a entornos poco seguros, más aún, teniendo en cuenta las características de la zona de Orden público en la que labora. Pero desconocen que existen otros riesgos asociados a la manipulación de activos informáticos con información clasificada en entornos poco seguros. En la ilustración 7 se evidencia el resultado de la encuesta.

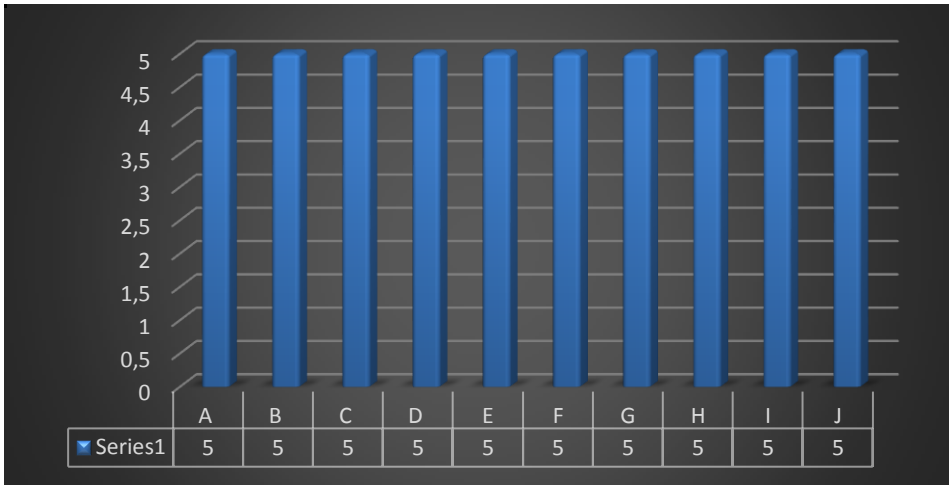
Ilustración 7. ¿Conoce de los riesgos de transportar información fuera de la institución?



Fuente: El Autor.

También se interroga al personal si tiene asignado algún activo informático para realizar sus funciones, además, se le pide Indicar cuántos equipos tiene asignados y como resultado se puede observar en la ilustración número 8 que tienen por lo menos en la mayoría de los casos un terminal de cómputo para realizar sus actividades, en los casos de los jefes de dependencia tiene dos y tres equipos contando teléfonos inteligentes y equipos de comunicación de voz cifrados.

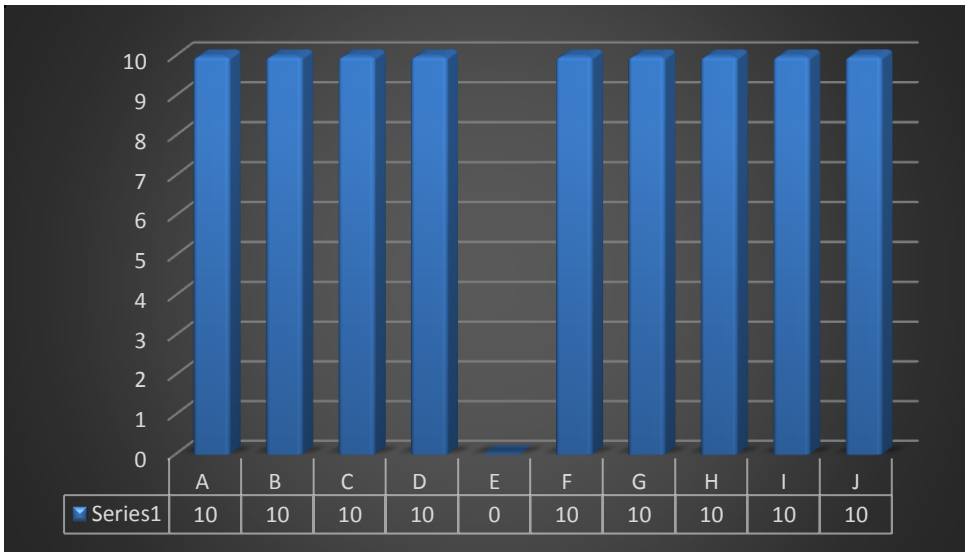
Ilustración 8. ¿Tiene asignado algún activo informático para realizar sus funciones?



Fuente: El Autor.

Cuando se verifica si corresponde el grado de clasificación del activo informático con el grado de clasificación de la tarjeta de manejo documental solo se observó un caso en el cual la tarjeta no manejo documental no correspondía con el grado de clasificación de la tarjeta de manejo documental mostrado en la ilustración 9.. Al realizar la verificación se pudo determinar que el equipo de cómputo había sido trasladado de otra dependencia y ya no contenía información con un grado alto de confidencialidad.

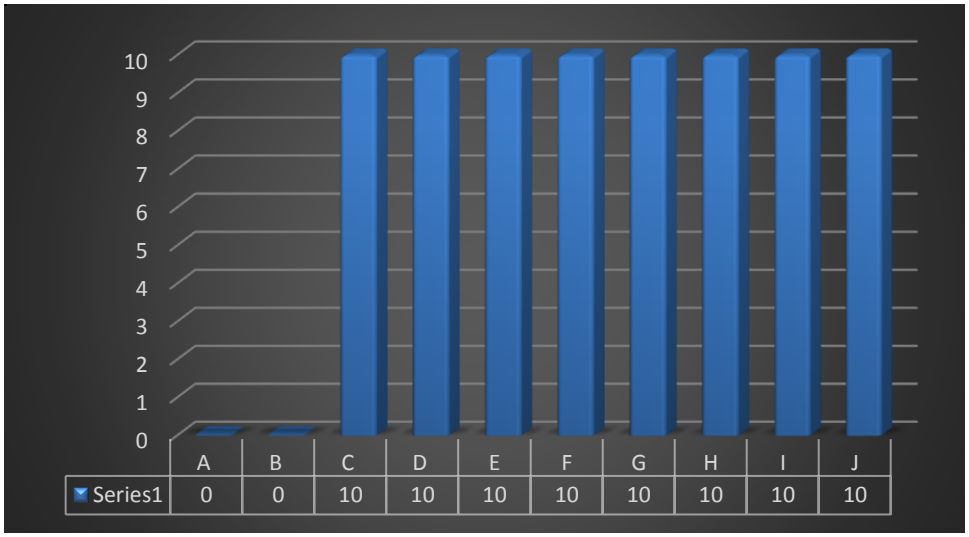
Ilustración 9. ¿Corresponde el grado de clasificación del activo informático con el grado de clasificación de la tarjeta de manejo documental?



Fuente: El Autor.

Se pregunta si el personal ha recibido información, capacitación o instrucciones referentes a seguridad de la información en un lapso igual o menor a un año y se encontró que la mayoría de las personas consultan los correos de los boletines informáticos que se genera desde el nivel central, pero carecen de capacitaciones que aclaren las dudas e informaciones generales que se envían en dichos correos. Los resultados de la pregunta se evidencian en la ilustración 10.

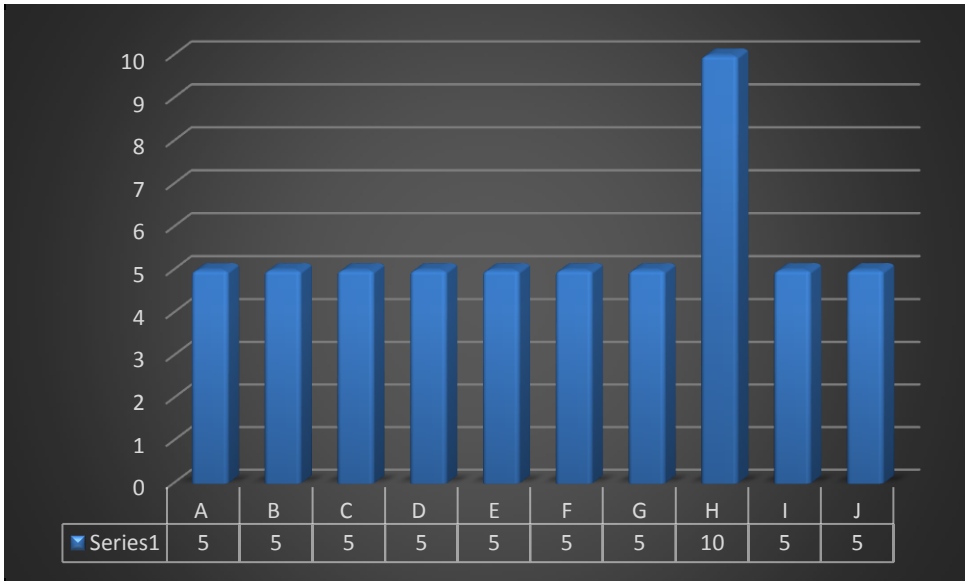
Ilustración 10. ¿Ha recibido información, capacitación o instrucciones referentes a seguridad informática?



Fuente: El Autor.

A la pregunta: ¿Almacena información institucional de clasificación reservado o superior en su computador? Solamente una persona indicó que manejaba este tipo de información y utilizaba mecanismos de seguridad para proteger la misma, pero se pudo evidenciar que el mecanismo de protección consiste en aplicar claves a los documentos planos que maneja, desconociendo los riesgos a los que queda expuesta la información aun con esas medidas. Como se puede apreciar en la ilustración 11 el 90% del personal encuestado aduce no manejar información de clasificación reservado o superior mientras que el restante 10% afirma que lo hace con aplicaciones de seguridad.

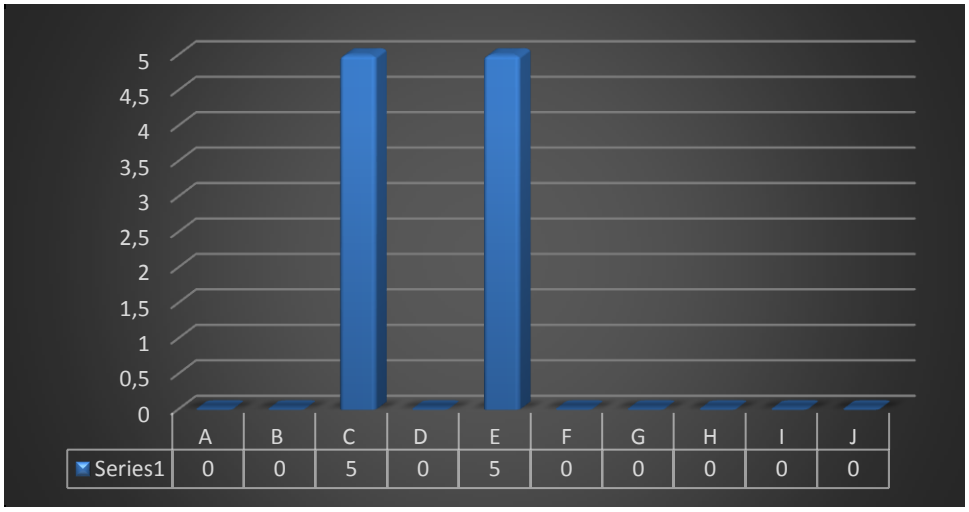
Ilustración 11. ¿Almacena información institucional de clasificación reservado o superior en su computador?



Fuente: El Autor.

Cuando se pregunta si el personal Almacena información personal en su computador o dispositivo informático institucionales evidencia de nuevo la falta de conocimiento profundo de las políticas de seguridad informática, debido a que un gran porcentaje almacena su información personal en equipos institucionales generando riesgos a la información de la organización, lo cual se puede apreciear en la ilustración 12.

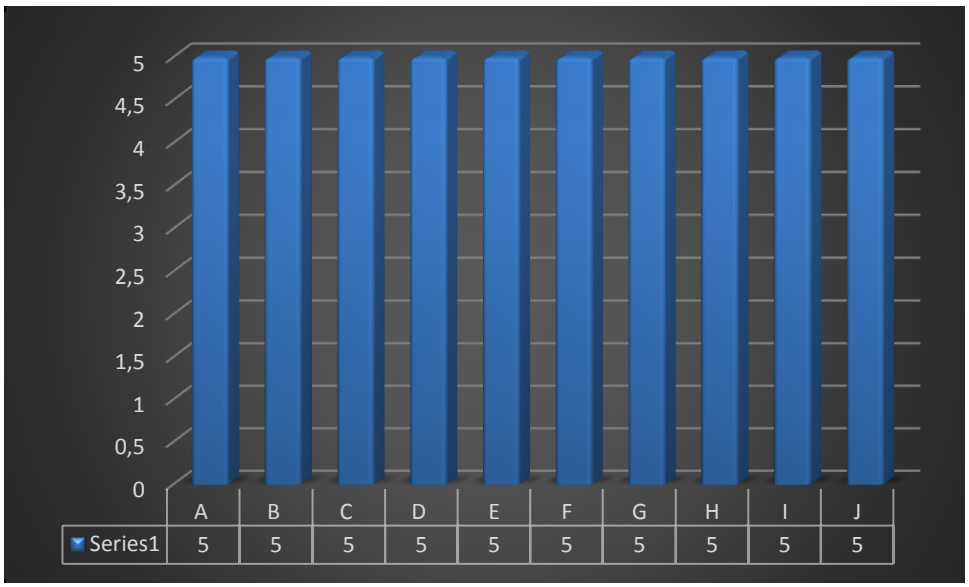
Ilustración 12. ¿Almacena información personal en su computador?



Fuente: El Autor.

Con respecto a la activación y utilización del correo electrónico la encuesta arroja como resultado que la totalidad del personal encuestado tiene asignado una cuenta de correo institucional, y es consecuencia de la obligatoriedad del personal a tener activo su correo electrónico institucional para realizar trámites de carácter laboral-personal. Lo anterior se puede apreciar en la ilustración 13

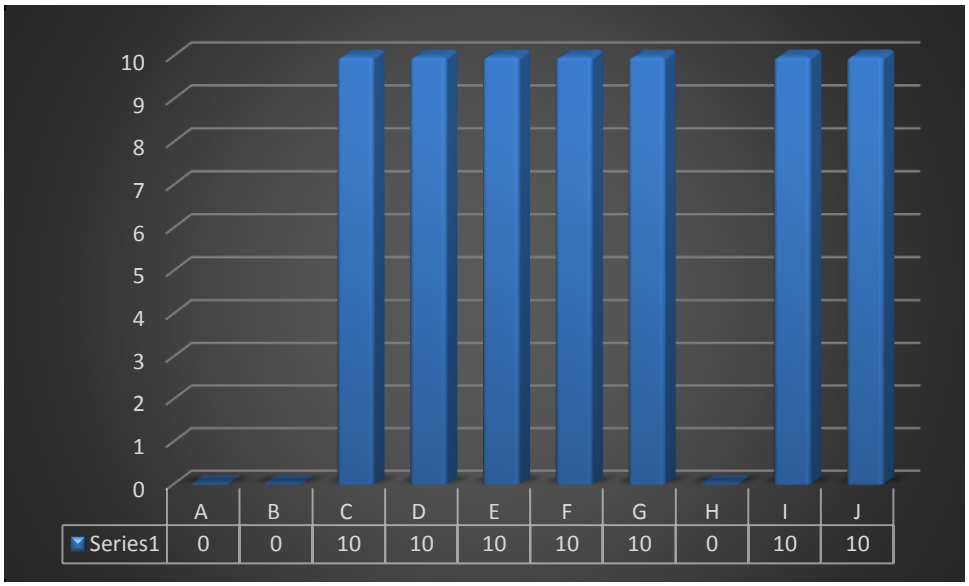
Ilustración 13. ¿tiene asignado cuenta de correo institucional?



Fuente: El Autor.

Cuando se le pregunta a los integrantes de la Estación de Guardacostas si realiza periódicamente backUp de la información y se Verifica dónde y cómo, se encuentra que una cantidad importante de personal aduce que no realiza backup de la información que genera y maneja, el porcentaje restante de personal aduce que si realiza copias de respaldo, pero los realiza de manera personal debido a que la unidad no cuenta con dispositivos para el almacenamiento de información y realizar los respectivos respaldos periódicos.

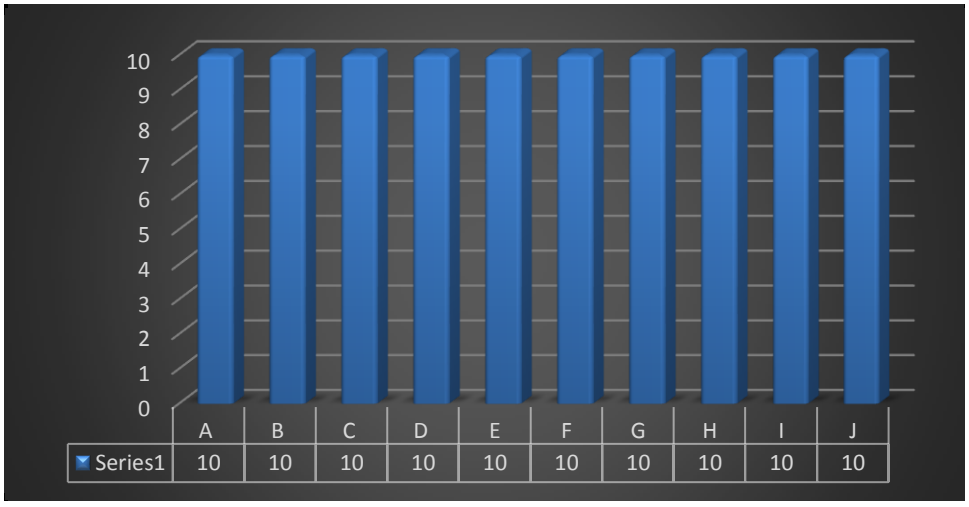
Ilustración 14. ¿Realiza periódicamente copias de respaldo de la información?



Fuente: El Autor.

También se le pregunta al personal si está autorizado para navegar en internet en los equipos institucionales, y se encuentra que hay personas que no conoce la diferencia entre internet e intranet, se explica esta diferencia y se les indica que en sus equipos sí es posible navegar en internet a través de un servidor de internet que se encuentra ubicado en un centro de datos a nivel central, el cual impide el acceso a páginas no autorizadas

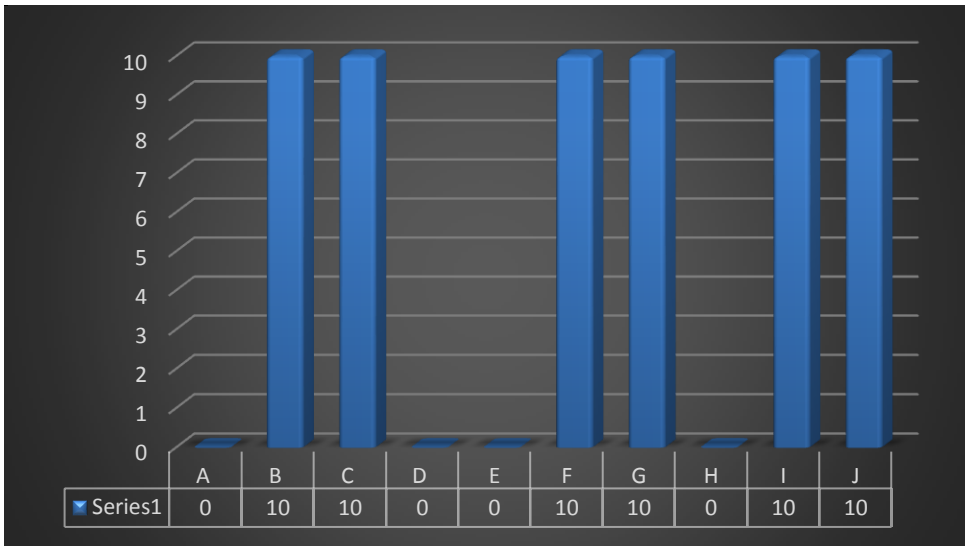
Ilustración 15. ¿Está autorizado para ingresar a internet?



Fuente: El Autor.

Se fue a otro punto en el que se encontró una falencia en la implementación de las políticas de seguridad informática de las Fuerzas Militares una cantidad considerable de personal no cambia sus contraseñas, aducen en la mayoría de ocasiones que se debe a que sus equipos son compartidos con las demás personas que trabajan en la oficina por lo cual no se realiza cambio periódico de contraseña, y las personas que realizan cambio de contraseña no la realizan de manera periódica.

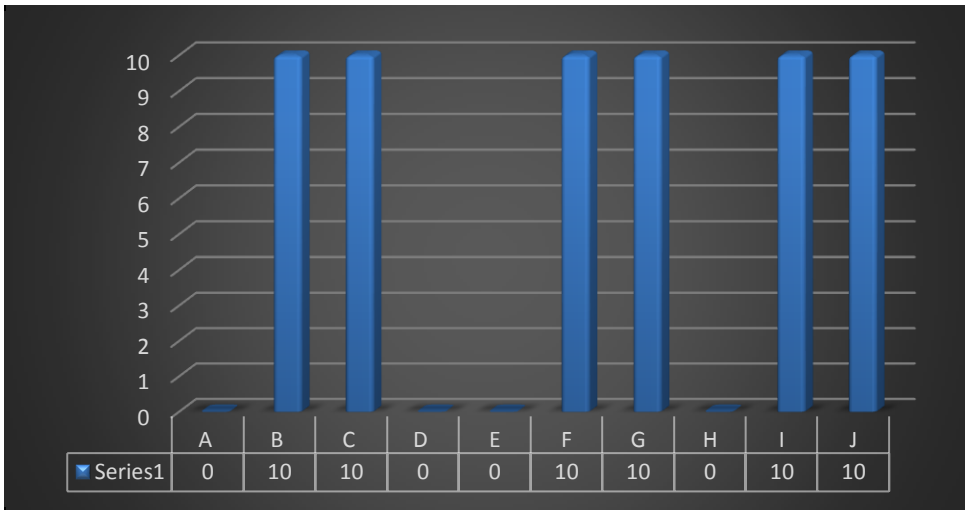
Ilustración 16. ¿Cambia periódicamente sus claves de acceso al computador y al correo electrónico?



Fuente: El Autor.

Se verificaron varios terminales informáticos y se encontró las claves hace un lapso extenso no se cambian, lo que genera riesgos para la seguridad de la información que en estos se almacena.

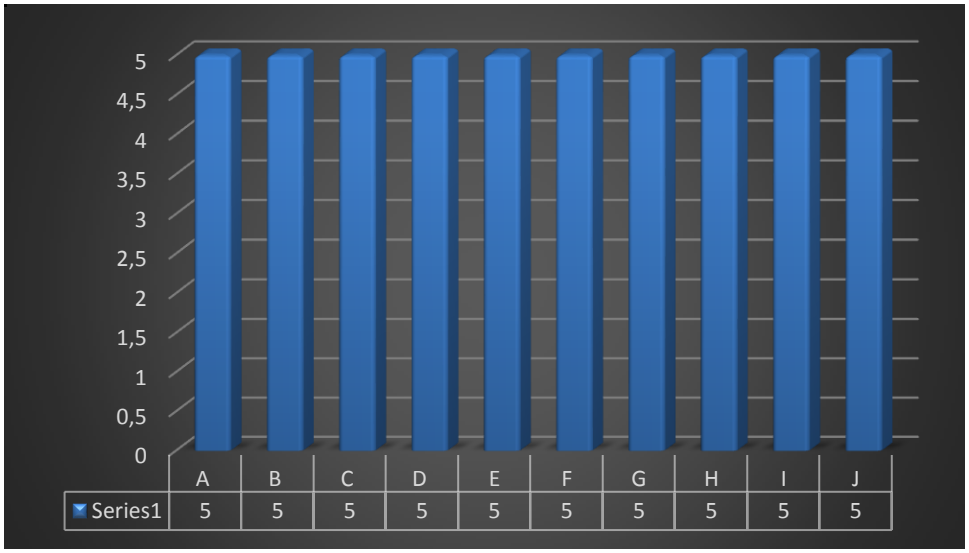
Ilustración 17. ¿El cambio de clave de acceso es menor a un mes?



Fuente: El Autor.

También se encontró que la totalidad de los computadores institucionales verificados tienen activada el bloqueo automático como se puede apreciar en la ilustración 18..

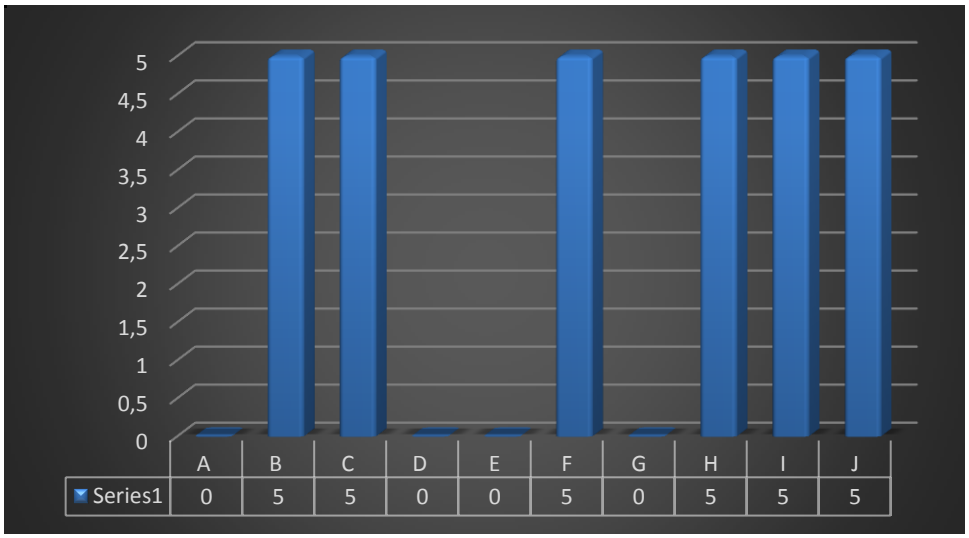
Ilustración 18. ¿tiene activo el bloqueo automático del computador?



Fuente: El Autor.

Las personas aducen que no apagan los computadores cuando se ausenta del recinto porque Generalmente hay personas que están esperando su turno para utilizarlo y realizar sus labores lo que se evidencia en la ilustración siguiente.

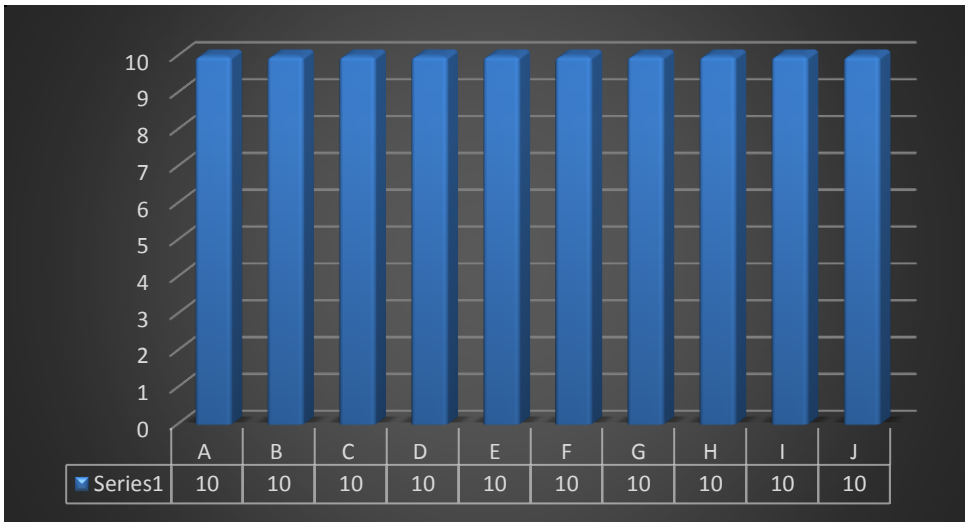
Ilustración 19. ¿bloquea o apaga su computador en horas de almuerzo?



Fuente: El Autor.

Se verificó que todos los equipos de cómputo tuvieran bloqueado el acceso a dispositivos removibles, y se pudo evidenciar que este procedimiento se realiza por medio de la consola de antivirus que es administrada en el nivel central, lo cual queda evidenciado en la ilustración 20 donde se aprecia que la totalidad de los equipos tienen bloqueado el acceso a dispositivos removibles. Sin embargo, es necesario realizar capacitación al personal en uso apropiado del correo electrónico institucional para compartir archivos.

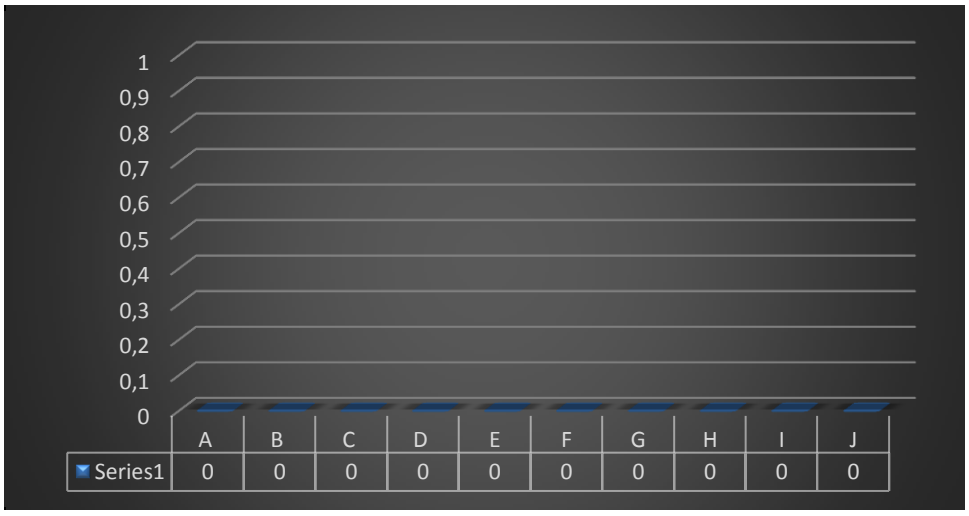
Ilustración 20. ¿Tiene bloqueados los dispositivos removibles del computador?



Fuente: El Autor.

En esta pregunta se evidencia el déficit de equipos informáticos que tiene la estación, por lo cual, dentro de las recomendaciones se va a solicitar a la jefatura la adquisición de los equipos informáticos necesarios para dar cumplimiento a las políticas de seguridad informática ordenadas por el alto mando.

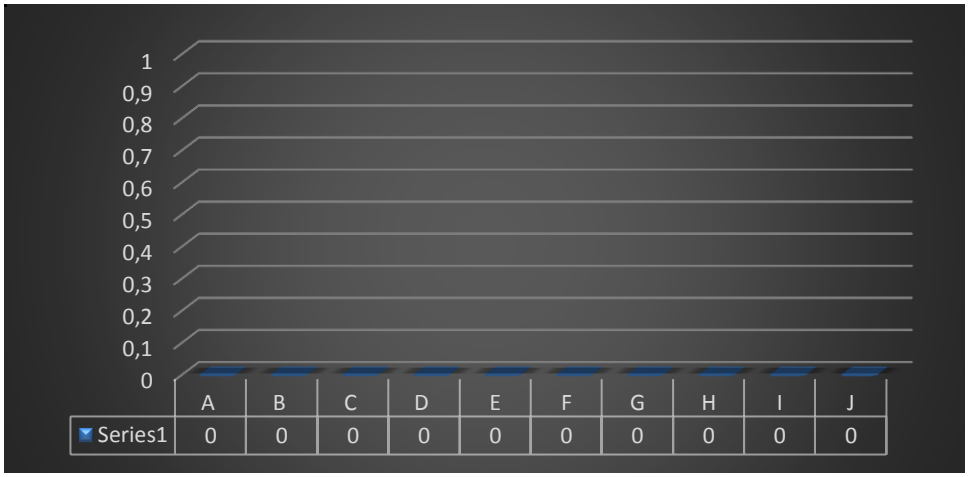
Ilustración 21. ¿comparte su activo informático con otro funcionario de la institución?



Fuente: El Autor.

Como en la pregunta anterior en esta también se evidencia la falta de equipos informáticos para el desarrollo de las actividades laborales del personal. En la ilustración 22 queda esto comprobado.

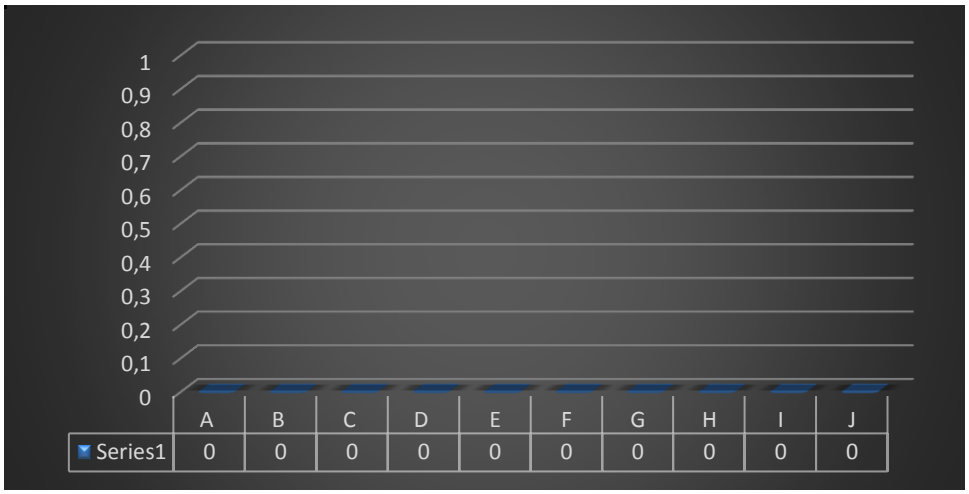
Ilustración 22. ¿Ha tenido que emplear o emplea actualmente algún activo informático personal para realizar funciones institucionales?



Fuente: El Autor.

En la ilustración 23 se evidencia que igual que en las dos preguntas anteriores en esta ocasión también, la falta de equipos informáticos para el personal genera incumplimiento de las políticas de seguridad informática con los riesgos que conlleva estos, se sugiere al personal hacer uso del correo institucional como una alternativa para guardar la información institucional.

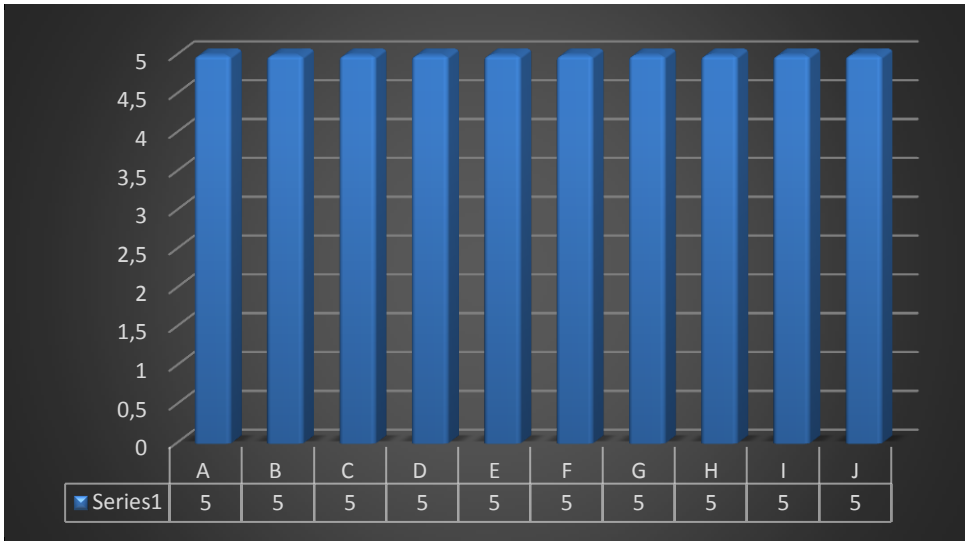
Ilustración 23. ¿Almacena información institucional en equipos personales?



Fuente: El Autor.

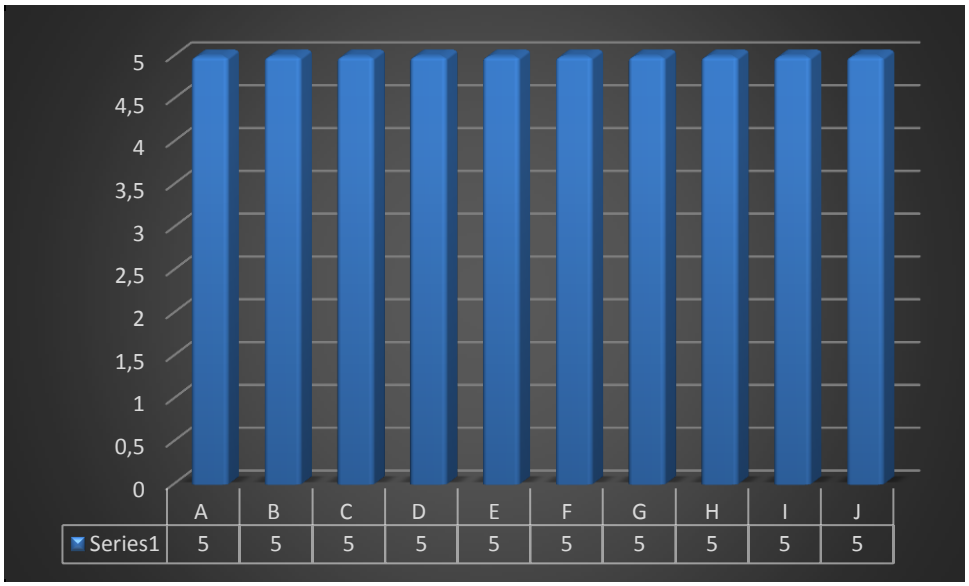
Se encontró que todos los equipos tienen la consola de antivirus actualizada desde el nivel central y los resultados se ven reflejados en las ilustraciones 24 y 25.

Ilustración 24. ¿Tiene antivirus licenciado el equipo asignado?



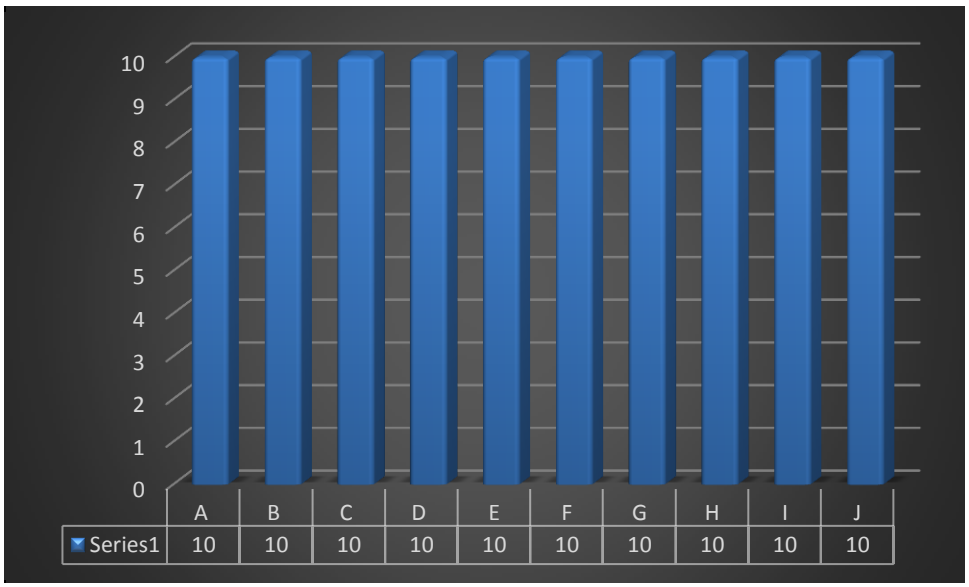
Fuente: El Autor.

Ilustración 25. ¿La fecha de actualización del antivirus es menor a 15 días?



Fuente: El Autor.

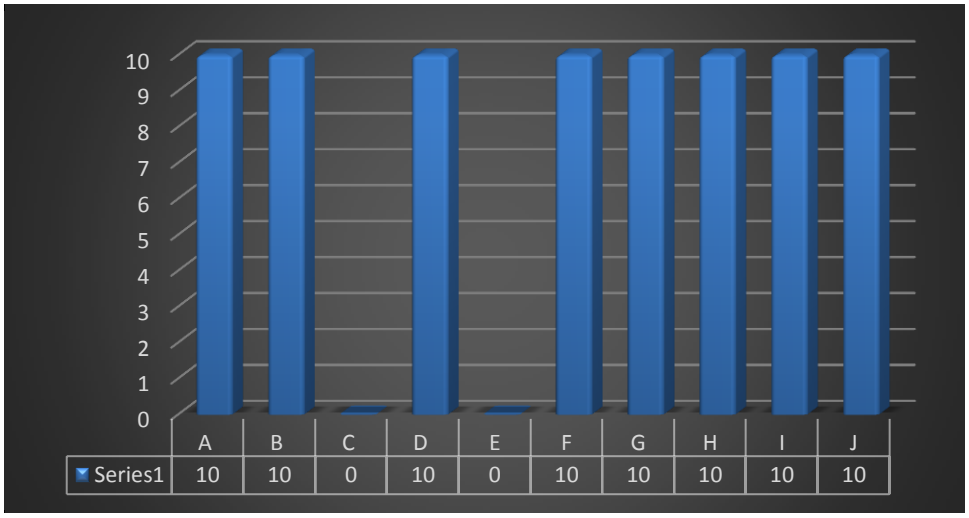
Ilustración 26. ¿Conoce los procedimientos para reportar los incidentes informáticos?



Fuente: El Autor.

Al preguntar al personal si conoce los números de contacto para reportar incidentes informáticos como se aprecia en la ilustración 27 se puede determinar que la mayor parte del personal tiene claro a quien reportar estas novedades.

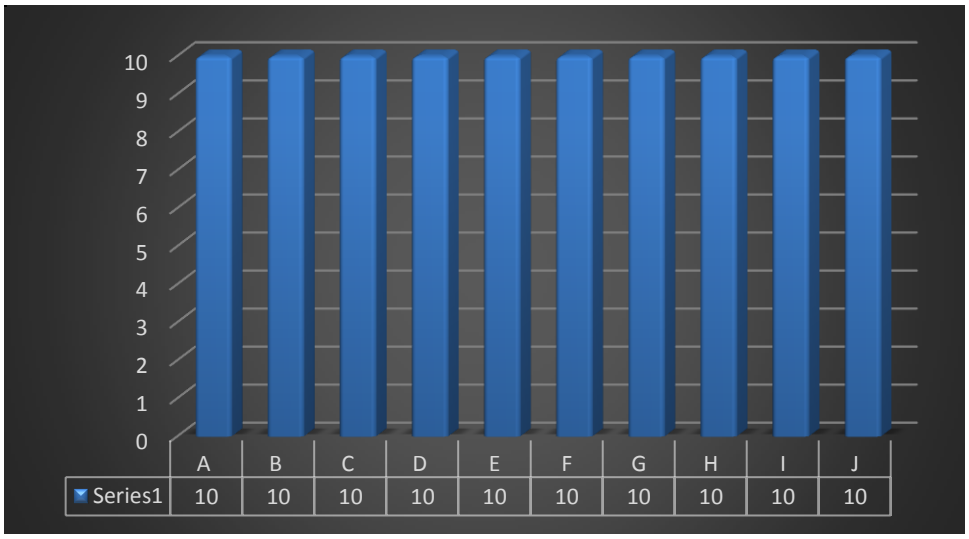
Ilustración 27. ¿conoce algún número de extensión o teléfono para reportar ataques o incidentes informáticos?



Fuente: El Autor.

En la ilustración 28 también se puede evidenciar que la totalidad de personal encuestado tiene claro cuál es el personal encargado de la seguridad informática en la Unidad.

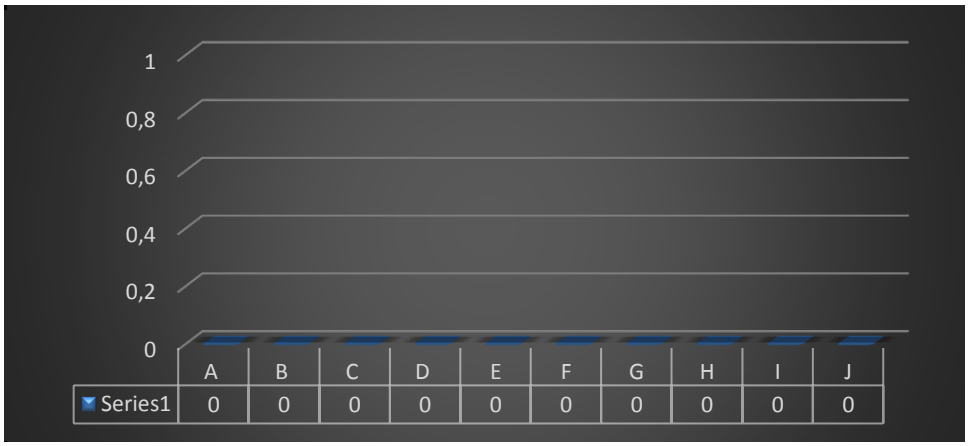
Ilustración 28. ¿Conoce al personal encargado de la seguridad informática en su Unidad?



Fuente: El Autor.

En la ilustración 29. se puede ver que el personal tiene claro la restricción existente para enviar información por internet, la mayoría aduce que utilizan el correo electrónico institucional para compartir la información institucional.

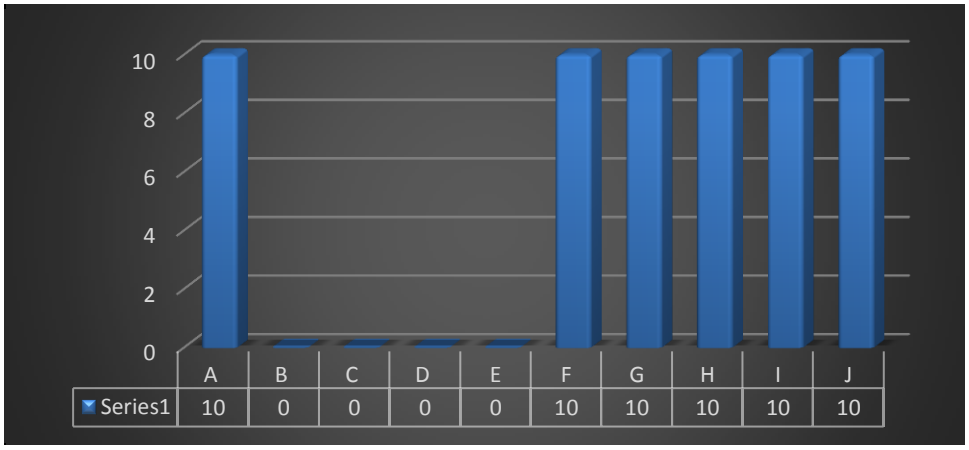
Ilustración 29. ¿Por funciones de su trabajo envía información a través de internet?



Fuente: El Autor.

La ilustración 30 indica que el personal conoce obligatoriedad de utilizar software de cifrado para enviar información clasificada vía internet y conoce el procedimiento ya que el software autorizado y entregado por el alto mando es operado por personal idóneo y capacitado para tal fin.

Ilustración 30. ¿Utiliza software de cifrado para enviar información clasificada vía internet?



Fuente: El Autor.

7 APLICACIÓN DE LA METODOLOGÍA MAGERIT

7.1 RAZÓN SOCIAL DE LA EMPRESA

Estación de Guardacostas Urabá “Contralmirante José Augusto Matallana Rodríguez”

7.2 TIPO DE ENTIDAD

La estación de Guardacostas de Urabá es una Unidad Táctica de la Armada Nacional que se encuentra ubicada en el municipio costero de Turbo Antioquia, dentro de sus responsabilidades está el control del tráfico marítimo en el Golfo de Urabá lo que conlleva enfrentar de manera directa el flagelo del narcotráfico. En consecuencia, su Recurso Humano y su Infraestructura Tecnológica deben estar adecuadamente capacitados y protegidos contra las actividades delictivas que buscan conocer, tergiversar, ocultar o eliminar la información que esta maneja.

7.3 FUNCIONES PRINCIPALES DE LA ESTACIÓN DE GUARDACOSTAS

- Contribuir a la defensa de la soberanía nacional.
- Controlar la pesca.
- Colaborar con la Dirección General de Aduanas en la represión del contrabando.
- Efectuar labores de asistencia y rescate en el mar.
- Proteger el medio marino contra la contaminación.
- Proteger a los buques y a sus tripulaciones de acuerdo al derecho internacional.
- Controlar y prevenir la inmigración o emigración clandestinas.
- Contribuir al mantenimiento del orden interno.
- Proteger los recursos naturales.
- Colaborar en las investigaciones oceanográficas e hidrográficas.
- Controlar el tráfico marítimo.
- Colaborar en todas aquellas actividades que los organismos del Estado realicen en el mar.
- Colaborar con los particulares en las actividades legítimas que realicen en el mar.

- Las demás que le señalen la ley y los reglamentos. [19]

La Estación de Guardacostas Urabá es una Unidad Táctica Operacional que depende del Cuerpo de Guardacostas de Colombia, el cual a su vez dependiente de la Armada Nacional, para el cumplimiento de las funciones antes mencionadas, la cual está conformada por las unidades a flote y el equipo asociado que se adquiera y destine para el cumplimiento de las mismas funciones de acuerdo con el programa elaborado por el comando de la Armada y aprobadas por los Ministros de Hacienda y Crédito Público, Defensa Nacional y Agricultura

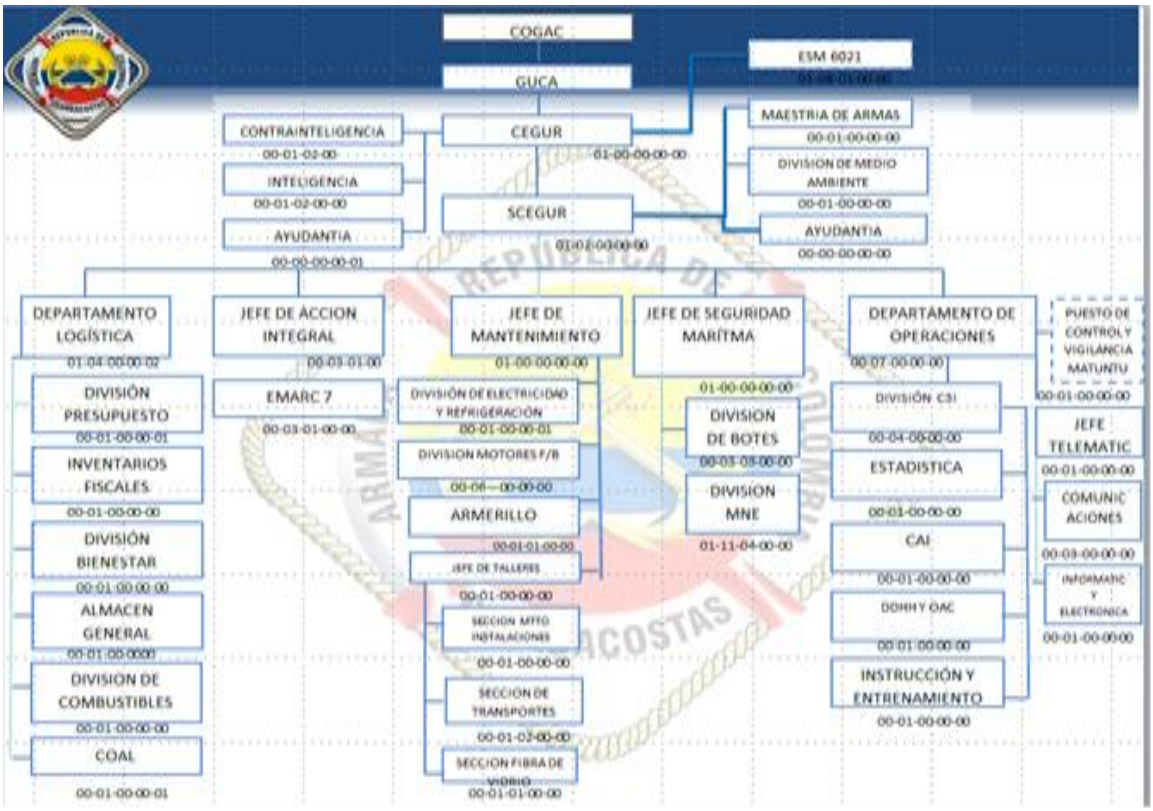
7.4 UBICACIÓN DE LA EMPRESA

La Estación de Guardacostas Urabá “Contralmirante José Augusto Matallana Rodríguez” se encuentra ubicada en Avenida “La Playa” sector Punta Las Vacas en el municipio de Turbo, departamento Antioquia, está tripulada por personal de Oficiales, Suboficiales, Infantes de Marina Profesionales y Regulares y personal civil que en total suman 76 personas y realizan actividades de tipo administrativo y operativo. Para realizar las actividades administrativas este personal solo cuenta con 15 equipos de cómputo razón por la cual cada equipo es compartido con 4 personas en promedio.

[19] Ibid., p. 1

7.5 ORGANIGRAMA DE LA EMPRESA

Ilustración 31. Organigrama de la Empresa



Fuente: Departamento de Personal de la Estación de Guardacostas Urabá

7.6 ÁREA ENCARGADA DE LA TECNOLOGÍA

Dependiente del área de Tecnologías de la información y las Comunidades se encuentra el Jefe Sistemas y Seguridad Informática de la Estación que cual desempeña normalmente las siguientes funciones:

- Informar al comando cualquier novedad que se presente con los activos informáticos.

- Efectuar revistas sanitizacion acuerdo directivas vigentes.

- Mantener en funcionamiento las redes LAN servicios Intranet.

- Asesorar al personal de la Unidad en lo relacionado con el uso adecuado de los recursos telemáticos asignados para el desarrollo de las operaciones y actividades administrativas.

- Atender permanentemente Pruebas Videoconferencias.

- Atender problemas relacionados con el funcionamiento de los equipos de cómputo y redes de datos ubicados en las diversas áreas administrativas de la Unidad.

- Difundir de manera clara y oportuna las políticas de seguridad informática y protección de la información que se encuentra en medios digitales.

- Realizar mantenimiento preventivo y correctivo de los sistemas informáticos y operativos (hardware y software) acuerdo plan semanal de trabajos.

- Asesorar, difundir e instruir sobre las nuevas herramientas de desarrollo y recursos informáticos implementados y puestos al servicio del personal de la Institución.

- Velar porque todo el personal de la Unidad haga uso correcto de los sistemas de intercambio de información autorizados por medio de la creación de las cuentas de correo Institucional.

- Coordinar, organizar, dirigir y controlar la ejecución de los programas implementados en red y programas específicos.

7.7 INVENTARIO DE EQUIPOS INFORMÁTICOS

Tabla 1. Inventario de Equipos Informáticos

ELEMENTO	MARCA	MODELO	SERIE
CPU	DELL	OPTIPLEX 780	9547
CPU	JANUS	SIN MODELO	12033182163
CPU	JANUS	SIN MODELO	12033182282
MONITOR	LG	E195ls-Bn	111lten28804
MONITOR	LG	E195ls-Bn	111ltgc28799

Tabla 1. (Continuación)

ELEMENTO	MARCA	MODELO	SERIE
CPU	DELL	OPTIPLEX 740	12ph7f1
MONITOR	SAMSUNG	S19a300b	2bbnm9nb509199y
PC PORTÁTIL	HP	PROBOOK 4720S	2ce04613pn
MONITOR	HP	SIN MODELO	6cm22912qq
MONITOR	HP	LV1911	6cm2291302
IMPRESORA	HP	OFFICEJET	Ccab06210020t4
IMPRESORA	HP	Deskjet 2050	Cn1a13n0c1
IMPRESORA	HP	DESKJET 3050	Cn1bg43631
IMPRESORA	HP	DESKJET 3050	Cn1bg437vg
IMPRESORA	HP	DESKJET 2515	Cn3183jj74
MONITOR	SIN MARCA	SIN MODELO	Cng54603f6
IMPRESORA	HP	LASERJET M1132MPF	Cng9ccvnz8
IMPRESORA	HP	LASERJET M1132MFP	Cng9ccvnzv
CPU	DELL	OPTIPLEX 780	Dcneif
CPU	DELL	OPTIPLEX 740	F1ph7f1
IMPRESORA	EPSON	Lx-300+Ii	G8dy067262
CPU	DELL	OPTIPLEX 740	J2ph7f1
PC PORTÁTIL	HP COMPAC	6710B	L0210-0044
MONITOR	DELL	17bfpb	Mx-0xw368-46634-78f-104u
CPU	HP COMPAC	Dc5850	Mxj847032m
CPU	HP	SIN MODELO	Mxl2140rst
MONITOR	DELL	SIN MODELO	Mx-Op513r-70715-08t-1zgs
MONITOR	DELL	E178fdb	Mx-Oxw368-46634-78f-127u
SWICH	D-LINK	Des-1024a	Qb3r1b3000281
MONITOR	VIZTA	SIN MODELO	Rabwf118004518
SWICH	CISCO	2800	SIN MODELO
IMPRESORA	RICOH	AFICIO MP 201	W3058602815
IMPRESORA	RICOH	Aficio Mp 301	W913p604042
CPU	COMPAC	SIN MODELO	Xcog2092111252
PC PORTATIL	HP COMPAC	6710B	SIN SERIE
CPU	ARGON	SIN MODELO	SIN SERIE

Fuente: El autor

7.8 INVENTARIOS DE ACTIVOS:

Tabla 2. Inventario de Equipos

TIPO DE ACTIVO	IDENTIFICACIÓN DE ACTIVO
Hardware [HW]	[print]Impresora Comando [print]Impresora Logística

TIPO DE ACTIVO	IDENTIFICACIÓN DE ACTIVO
	[print]Impresora Telemática [print]Impresora Operaciones [ipphone] Teléfono IP Ayudante Comando [ipphone] Teléfono IP logística [ipphone] Teléfono IP Telemática [ipphone] Teléfono IP Operaciones [ipphone] Teléfono IP C3I [mobile] PC Comando [mobile] PC Telemática [pc] PC Ayudante Comando [pc] PC Jefe Personal [pc] PC secretaria Logística [pc] PC Logística
Hardware [HW]	[pc] PC Seguridad Marítima [pc] PC Almacén [pc] PC Telemática [pc] PC RAdio [pc] PC Operaciones [pc] PC Planes [pc] PC C3I [switch]SWICH LAN (03) Access point Equipos de usuarios
Software [SW]	Sistema Operativo Windows 7 Profesional Micorsoft Office 2010 profesional W-XP
Comunicaciones [COM]	[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] comunicaciones radio [wifi] red inalámbrica

Tabla 2. (Continuación)

TIPO DE ACTIVO	IDENTIFICACIÓN DE ACTIVO
Comunicaciones [COM]	[LAN] red local [Internet] Internet
[Media] Soportes de información	[printed] material impreso
[AUX]Equipos auxiliares	Sistema de vigilancia CCTV Sistema de extinción de incendios [ups] UPS Operaciones [ups] UPS Telemática [ups] sistemas de alimentación ininterrumpida [gen] generadores Principal [ac] equipos de climatización varios [cabling] cableado [wire] cable eléctrico

	[fiber] fibra óptica
[P]Personal	[ui] Comandante [ui] Jefe de personal [ui] Ayudante Comando
[P]Personal	[ui] Jefe de Operaciones [ui] Jefe de Logística [ui] Jefe de Acción Integral [ui] Jefe de Inteligencia y Contrainteligencia [ui] Jefe de Seguridad Marítima [adm] Jefe Sistemas

Fuente: El Autor

7.9 VALORACIÓN DE LOS ACTIVOS

Para realizar la valoración de activos es necesario identificar los criterios y las dimensiones de la valoración que se realizará, por lo tanto, se definen las siguientes tablas que recomienda el libro 2 de la metodología MAGERIT.

Tabla 3. Criterio de Valoración

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave

Tabla 3. (Continuación)

9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	despreciable	Irrelevante a efectos prácticos

Fuente: Magerit

7.9.1 Dimensiones de valoración

Tabla 4. Dimensiones de Valoración

VALOR	DIMENSIÓN
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad

[A]	Autenticidad
[T]	Trazabilidad

Fuente: Magerit

7.10 VALORACIÓN DE ACTIVOS

Tabla 5. Valoración de Activos

TIPO DE ACTIVO	ACTIVO	[D]	[I]	[C]	[A]	[T]
Hardware [HW]	[print]Impresora Comando	5	2	6	3	3
	[print]Impresora Logística	5	2	6	3	3
	[print]Impresora Telemática	5	2	6	3	3
	[print]Impresora Operaciones	5	2	6	3	3
	[ipphone] Teléfono IP Ayudante Comando	4	2	8	5	2
	[ipphone] Teléfono IP logística	3	2	6	4	2

Tabla 5. (Continuación)

TIPO DE ACTIVO	ACTIVO	[D]	[I]	[C]	[A]	[T]
Hardware [HW]	[ipphone] Teléfono IP Telemática	4	2	8	5	2
	[ipphone] Teléfono IP Operaciones	4	2	8	5	2
	[ipphone] Teléfono IP C3I	4	2	8	5	2
	[mobile] PC Comando	10	8	8	10	8
	[mobile] PC Telemática	7	4	4	4	4
	[pc] PC Ayudante Comando	5	3	7	10	7
	[pc] PC Jefe Personal	10	8	8	10	8
	[pc] PC secretaria Logística	5	3	7	10	7
	[pc] PC Logística	5	3	7	10	7

	[pc] PC Seguridad Marítima	5	3	7	10	7
	[pc] PC Almacén	5	3	7	10	7
	[pc] PC Telemática	10	8	8	10	8
	[pc] PC RAdio	10	9	10	10	8
	[pc] PC Operaciones	10	9	10	10	8
	[pc] PC Planes	10	9	10	10	8
	[pc] PC C3I	10	9	10	10	8
	[switch] SWICH LAN (03)	10	10	10	10	2
	[switch] CRIPTO	10	9	10	10	8
	Access point	5	3	7	10	7
Software [SW]	Sistema Operativo Windows 7 Profesional	10	5	8	9	9
	Micorsoft Office 2010 profesional	9	6	6	6	8
Comunicaciones [COM]	[PSTN] red telefónica	5	5	6	4	2
	[ISDN] rdsi (red digital)	9	10	10	10	9
	[X25] X25 (red de datos)	5	5	6	4	2
	[ADSL] ADSL	5	5	6	4	2
	[pp] punto a punto	5	5	6	4	2
	[wifi] red inalámbrica	4	3	2	4	2
	[LAN] red local	9	10	10	10	9
	RAD	9	10			

Tabla 5. (Continuación)

TIPO DE ACTIVO	**ACTIVO**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
	[Internet] Internet	5	5	6	4	2
[Media] Soportes de información	[printed] material impreso	10	9	9	10	8
[AUX]Equipos auxiliares	Sistema de vigilancia CCTV	8	8	7	7	6
	Sistema de extinción de incendios	10				
	[ups] UPS Operaciones	10	8			
	[ups] UPS Telemática	10	8			
	[gen] generadores Principal	9	7			
	[ac] equipos de climatización varios	6	5			

	[cabling] cableado	9	7			
	[wire] cable eléctrico	9	7			
	[fiber] fibra óptica	10				
[P] Personal	[ui] Comandante	10	8	0	9	10
	[ui] Jefe de personal	9	8	0	9	10
	[ui] Ayudante Comando	8	8	0	9	10
	[ui] Jefe de Operaciones	8	8	0	9	10
	[ui] Jefe de Logística	8	9	0	9	10
	[ui] Jefe de Acción Integral	7	10	0	9	10

Fuente: El autor

7.11 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia entregada por el software PILAR 5.2.9[20]

Tabla 6. Degradación de Valor

DEGRADACIÓN DE VALOR	
MA	Muy Alto
A	Alto
M	Media
B	Baja
MB	Muy baja

Fuente: Herramienta Pilar

[20] Tomado de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Tabla 7. Probabilidad de Ocurrencia

PROBABILIDAD DE OCURRENCIA	
CS	Casi seguro
MA	Muy alto
P	Posible
PP	Poco Probable
MB	Siglos
MR	Muy rara
0	

Fuente: El Autor

Tabla 8. Identificación y Valoración de Amenazas

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
[print] En General	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.3] Contaminación medioambiental	P.P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	A	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA	M	-	-	-	-
	[A.11] Acceso no autorizado	P	-	A	A	-	-
	[A.23] Manipulación del hardware	MA	A	-	A	-	-
[ipphone] En General	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.3] Contaminación medioambiental	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	MA	-	A	A	-	-
	[A.23] Manipulación del hardware	A	A	-	A	-	-
[mobile] PC Comando	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-

Tabla 8. (Continuación)

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
[mobile] PC Comando	[I.3] Contaminación medioambiental	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	MA	-	A	A	-	-
	[A.23] Manipulación del hardware	A	A	-	A	-	-
	[E.25] Robo	A	MA		MA		
	[E.24] Caída del sistema por agotamiento de recursos	P	A				
[mobile] PC Telemática	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.3] Contaminación medioambiental	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	MA	-	A	A	-	-
	[A.23] Manipulación del hardware	A	A	-	A	-	-
	[E.25] Robo	A	MA		MA		
	[E.24] Caída del sistema por agotamiento de recursos	P	A				
Equipos de usuarios	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	PP	-	M	M	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-

Tabla 8. (Continuación)

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
Equipos de usuarios	[I.*] Desastres industriales	PP	B	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Uso no previsto	A	M	A	A	-	-
Sistema Operativo Windows 7 Profesional	[I.5] Avería e origen físico o lógico	P	M	-	-	-	-
	[E.1] Errores de los usuarios	MA	A	A	A	-	-
	[E.8] Difusión de software dañino	P	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (Software)	B	-	A	-	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	B	-	-	-
[switch] SWICH LAN (03)	[E.2] Errores del administrador	P	-	-	A	A	-
	[E.8] Difusión de software dañino	P	-	A	A	A	-
	[E.9] Errores de [re-]encaminamiento	PP	A	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	-	-	A	-	-
	[A.11] Acceso no autorizado	P	-	A	A	-	-
Access point	[N.1] Fuego	PP	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	[A.11] Acceso no autorizado	PP	-	B	B	-	-

Tabla 8. (Continuación)

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
[COM] Comunicaciones	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	PP	-	M	M	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.*] Desastres industriales	PP	B	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[A.7] Uso no previsto	A	M	A	A	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
	[E.19] Fugas de información	P			A		
	[E.18] Destrucción de información	PP	M				
	[E.15] Alteración accidental de la información	P		A			
	[I.8] Fallo de servicios de comunicaciones	P	A				
[Media] Soportes de información	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	PP	-	M	M	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.*] Desastres industriales	PP	B	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
	[I.3] Contaminación mecánica	P	M	-	-	-	-
	[I.10] Degradación de los soportes de almacenamiento de la información	P	A	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Uso no previsto	P	M	A	A	-	-
	[E.1] Errores de los usuarios	P	M	M	A		
	[E.18] Destrucción de información	PP	A				
	[A.15] Modificación deliberada de la información	P		M			

Tabla 8. (Continuación)

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
Sistema de vigilancia CCTV	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	PP	-			-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.*] Desastres industriales	PP	B	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[A.7] Uso no previsto	A	M	A	A	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
	[E.19] Fugas de información	PP					
	[E.18] Destrucción de información	PP	M				
	[E.15] Alteración accidental de la información	P		A			
	[I.8] Fallo de servicios de comunicaciones	P	A				
[ui] Comandante	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.7] Deficiencias en la organización	P	M				
[ui] Jefe de Operaciones	[E.19]Fugas de información	P	M	A	A		
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.7] Deficiencias en la organización	P	M				
[ui] Jefe de Acción Integral	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[E.7] Deficiencias en la organización	P	M				
	[E.19] Fugas de información	PP			B		

Tabla 8. (Continuación)

ACTIVO	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
[ui] Jefe de Logística	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[E.7] Deficiencias en la organización	P	M				
[ui] efe de Inteligencia y contrainteligencia	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
[ui] Jefe de Manteniemiento	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
[ui] Jefe de Personal	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
[ui] Jefe de Operaciones	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.19]Fugas de información	P	M	A	A		
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
Responsable Sistemas de Información	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-
	[E.19] Fugas de información	P	M	A	A		
	[E.28] Indisponibilidad del personal	P	M	M	M	-	-
	[A.29] Extorsión	PP	M	M	M	-	-
	[A.30] Ingeniería social (picaresca)	MA	A	A	B	-	-

Fuente: El Autor

7.12 IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS

Como se pudo observar en la descripción de elementos estos componentes implican riesgos menores, a los que bastará aplicar globalmente medidas básicas de seguridad práctica y tomar medidas para capacitar de manera adecuada el personal.

Tabla 9. Identificación y Valoración de Salvaguardas

SALVAGUARDAS	DIMENSIÓN	EVALUACIÓN
Control de acceso	[I], [C], [A_S]	50%
Registro de actuaciones	[D], [T_S]	75%
Copias de seguridad de los datos (backup)	[I], [C], [A_S], [D]	75%
Registro y auditoría	[A_S]	25%
Cifrado de la información	[C]	75%
Copias de seguridad (backup)	[D]	80%
Se aplican perfiles de seguridad	[I] [C]	50%
Cambios (actualizaciones y mantenimiento)	[D]	50%
Puntos de interconexión: conexiones entre zonas de confianza	[I] [C]	50%
Protección criptográfica del contenido	[C]	50%
Limpieza de Contenidos		

Fuente: El Autor

7.13 PLAN DE MEJORAMIENTO

Dentro de los hallazgos más importantes se encontró que el personal no tiene conocimiento adecuado de las políticas de seguridad informática de las Fuerzas Militares, lo que conlleva al aumento del riesgo que se materialicen las diferentes amenazas que afectan los activos informáticos y la información que almacenan y

manejan. Con el objetivo de mitigar estos riesgos se elabora el plan de actividades que a continuación se expone.

Tabla 10. Plan de Mejoramiento

OBJETIVO	ACTIVIDAD	RESPONSABLE	PRODUCTO	FECHA INICIAL	FECHA FINAL
Reforzar los conocimientos del personal en las obligaciones que tienen para dar cumplimiento a las políticas de seguridad informática.	Desarrollar actividades de capacitación del personal en las Políticas de Seguridad informática de la Armada Nacional	Encargado del Área de Sistemas	Listados de asistencia a la capacitación	06-03-17	10-04-17
Realizar la verificación y actualización de las promesas de reserva, tarjetas de manejo documental y formato de aceptación y cumplimiento de las políticas de seguridad informática.	Se verificarán los formatos buscando su actualización de acuerdo al establecido en el aplicativo web.	Jefe del departamento de contrainteligencia	Informe de la actividad desarrollada.	12-04-17	17-04-17
Dar a conocer a la jefatura las necesidades en terminales de computo que tiene la Unidad	Elaborar un informe a la jefatura solicitando los equipos faltantes y novedades encontradas.	Jefe de Telemática	Oficio a la jefatura	03-05-17	03-05-17

Fuente: El Autor

Con el objetivo de prevenir, detectar o neutralizar las amenazas, vulnerabilidades y riesgos que puedan afectar los activos informáticos que almacenan y manejan los datos o la información clasificada, información pública reservada e información pública clasificada, se determinó la realización de una serie de capacitaciones con el fin de fortalecer los puntos más vulnerados en esta estación de Guardacostas como son:

- La verificación y actualización del formato de aceptación de políticas de seguridad informática para las FF.MM con las instrucciones correspondientes para establecer la comunicación continua y expedita entre los departamentos de Logística, personal y el encargado de la seguridad Informática para actuar de manera inmediata en el caso de contratación, ingreso o cambio de personal que labora en las instalaciones, esta tarea debe ser dirigida y controlada por el segundo comandante de la unidad. Estas recomendaciones también aplican para la verificación, elaboración y actualización de las tarjetas de manejo documental.

- Como aporte integral a las políticas de seguridad informática se programó la realización de capacitaciones de 30 minutos, tres días a la semana durante cinco semanas con el objetivo de involucrar a la mayor cantidad de personal teniendo en cuenta la falta de disponibilidad del personal y la rotación del mismo, debido al cumplimiento de los diferentes servicios. En estas capacitaciones se informó y sensibilizó al personal en la aplicación de los controles y acciones para fortalecer la protección de la información y los activos informáticos que la soportan.

- Se recomienda al encargado de informática de la Unidad, crear usuarios en los equipos de cómputo con el fin de fortalecer el principio de compartimentación de la información y por ende la confidencialidad de la misma entre los diferentes usuarios de un mismo terminal de trabajo.

- Se elevó un informe a la jefatura correspondiente informando las novedades encontradas y solicitando el apoyo con la renovación de los equipos informáticos de la Estación y la asignación de nuevos equipos que suplan las necesidades existentes.

- Se incluye en el plan de actividades mensuales de la estación capacitación al personal realizando reentrenamiento en los temas de las políticas de seguridad informática. Igualmente nombrar mensualmente un tripulante de la estación para realizar una inspección de los temas más críticos en la seguridad de la información.

8 CONCLUSIONES

- Con el desarrollo de este proyecto se lograron identificar las deficiencias de seguridad informática en la Estación de Guardacostas mediante la aplicación de la auditoria. Lo anterior permite aumentar el grado de protección de los datos e información que utiliza la institución para alcanzar el logro de los objetivos estratégicos que aportan a la consolidación del desarrollo marítimo de la nación.

- Mediante la aplicación de la metodología Magerit se logró visibilizar ante el Comando de la Estación la importancia de gestionar de manera adecuada, sistemática y permanente los riesgos informáticos encontrados mediante la auditoria para con ello mejorar en gran medida la seguridad de los activos informáticos y la información que estos procesan y almacenan.

- Con el informe elevado ante la Dirección de Tecnologías de la información y las Comunicaciones de la Armada Nacional que se puede verificar en el anexo A. de este documento, se espera mejorar ostensiblemente la aplicación de las políticas de seguridad informática de las Fuerzas Militares acogidas por la Armada Nacional, con la dotación de nuevas terminales informáticas con tecnología de punta que impactarán no solo en los pilares fundamentales de la Seguridad Informática sino también en el desempeño y eficiencia de las personas en el desarrollo de sus labores cotidianas.

- La seguridad Informática es un tema que se debe abordar con mucho tacto a la hora de capacitar a cualquier clase de personal, en este proyecto se inició el proceso de capacitación del personal con el tema “Seguridad informática personal y en redes sociales” lo cual generó muy buena acogida en la mayoría del público asistente, ya que se abordó el tema con ayudas multimedia que atraían jocosamente al personal. Luego se socializó al personal la seguridad

en las compras y transacciones a través de internet para finalmente introducirlos de lleno en el tema de la seguridad informática organizacional. Evidencia de este grupo de capacitaciones se publica en el anexo B. con los formatos de listados de asistencia que fueron editados ocultando la información que la Institución considera como Publica Reservada.

9 RECOMENDACIONES

- Con el propósito de dar continuidad al proceso de concientización en seguridad informática en la Estación de Guardacostas se recomienda que, dentro de las proyecciones de traslados de personal, se soliciten tripulantes con las capacidades cognitivas y actitud proactiva para dar continuidad al sistema de gestión de seguridad informática y propender por su mejora continua.

- Igualmente es importante realizar la verificación del plan de mejoramiento propuesto en este proyecto con el fin de calificar su impacto en la protección de los activos informáticos y la información, esto con el fin de modificarlo o ampliarlo, dependiendo de los resultados obtenidos.

- Se debe realizar seguimiento riguroso al informe técnico realizado a la Dirección de Tecnologías de la información y la Comunicaciones de la Armada Nacional, buscando una gestión eficaz de la dirección en la asignación de los recursos solicitados. Se recomienda que este seguimiento se realice mensualmente recabando el informe enviado.

- Teniendo en cuenta la rotación del personal en la Unidad se solicita que se incluya en la instrucción y entrenamiento anual las capacitaciones y realimentaciones de las policitas de seguridad Informática de la Armada Nacional.

BIBLIOGRAFÍA

© Derecho.com. Manual Seguridad Básica Informática, ©Derecho.com FDL Licence. [En linea]. España.: Disponible en: http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/manual-seguridad-basico.pdf

AGUILERA LÓPEZ, Purificación. Seguridad Informática. 1 ed. Madrid: Editorial Editex. 2010.

BENAVIDES RUANO, Miriam y SOLARTE SOLARTE, Francisco. Módulo riesgo y control informático. Pasto.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. 2012.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". El Congreso. Bogotá, D.C., 2013.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1712. (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. El Congreso. Bogotá, D.C., 2014.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 57. (5, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. El Congreso. Bogotá, D.C., 1985.

COLOMBIA. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. DECRETO 1874 (2, Agosto, 1979). Por el cual se crea el Cuerpo de Guardacostas y se dictan otras disposiciones. La Presidencia. Bogotá, D.C., 1979.

CORTEZ PINTO, Maria. Las vulnerabilidades humanas en relación a la seguridad informática para evitar la fuga de información confidencial en el departamento de recursos humanos de la Universidad Técnica de Ambato. Trabajo de Graduación para Ingeniero en Sistemas Computacionales e Informáticos. Ambato – Ecuador. Universidad Tecnico de Ambato. Facultad de Ingeniería en Sistemas Electrónica e Industrial. 2013.

FUERZAS MILITARES DE COLOMBIA. Directiva Permanente No. 200-12/2006 Políticas de Seguridad Informática PARA LAS F.F.M.M. FFMM. BOGOTÁ D.C. 2006.

HADNAGY, Christopher. Ingeniería Social: El arte del Hacking personal. Madrid: Editorial ANAYA MULTIMEDIA.,2011.

MICROSOFT. Se ha dejado de ofrecer soporte para Windows XP. [En línea]. Disponible en: https://www.microsoft.com/es-es/windowsforbusiness/end-of-xp-support

SEMANA. Las empresas colombianas no están preparadas para los ciberataques. [En linea]. Bogotá.: Semana.com. Disponible en: http://www.semana.com/tecnologia/articulo/las-empresas-colombianas-no-estan-preparadas-para-los-ciberataques/466430

SO27000.ES, El portal de ISO 27001 en Español. [en linea]. Madrid: Disponible en: http://www.iso27000.es/

TORRES ANDAGANA, Gabriela y LLANGA SALCAN, Diego. Estudio e Implementación de una Metodología de Prevención de Intrusos para redes LAN. Tesis de Grado Ingeniero en Electrónica y computación. Riobamba – Ecuador.: Escuela Superior Politécnica de Chimborazo. Facultad De Informática y Electrónica. Escuela de Ingeniería Electrónica y Tecnología en Computación. 2010.

ANEXO A. Informe Técnico a DITIC

INFORME TÉCNICO

Se realiza el presente informe técnico soportado en el análisis de riesgos realizado a la estación de Guardacostas Urabá en el marco del desarrollo de la auditoría de seguridad informática a la entidad mencionada. Se consideran los resultados de las encuestas que generan riesgo crítico para los activos informáticos de la Unidad.

Teniendo en cuenta lo anterior, se analizan los resultados de la pregunta "¿Ha firmado el formato de aceptación de políticas de seguridad informática para las FF.MM en su unidad actual?". En los que se encuentra que ninguno de los encuestados conocen o han diligenciado dicho formato (Formato Declaración de Aceptación y Compromiso de Cumplimiento Políticas de Seguridad de la Información para las FF.MM en la ARC INNA-FT-110-JINA-V01) como se ordena en la Directiva Permanente 009 del 20 de abril de 2015. El diligenciamiento del formato mencionado es muy importante, ya que en este se informa la obligatoriedad del conocimiento y aceptación de las políticas de seguridad Informática y las repercusiones disciplinarias, Administrativas y penales a las cuales está expuesto en caso de no dar cumplimento a las políticas mencionadas. Se verificó con el encargado de realizar los formatos encontrando que no conocía la obligatoriedad del diligenciamiento de ese documento siempre que realizara presentación personal a trabajar en la Unidad, ya fuera militar o civil y sus labores fueran permanentes o temporales.

Los resultados de la pregunta: "¿Está vigente la tarjeta de manejo documental?" los resultados obtenidos muestran que solo el 40% de los encuestados tiene actualizado el documento, y visto que está ordenado en la Directiva Permanente 001 del Comando de la Armada Nacional de fecha 12 de enero de 2017. Se le informa al personal la importancia de mantener actualizada la tarjeta de manejo documental, considerando que la misma se elabora después de un análisis de las funciones que desempeña el tripulante y el grado de clasificación que puede conocer. Lo anterior con el objetivo de garantizar el principio de compartimentación que busca proteger la confidencialidad de la información. Buscando subsanar esta novedad a futuro, el encargado de la sección de

Contrainteligencia estableció como control, elaborar un plan de trabajo para la verificación mensual de las tarjetas de manejo documental.

Otra forma en la que se pone en riesgo la información de la Institución es trasportándola en activos informáticos no autorizados o sin las medidas de seguridad necesarias. Cuando se le preguntó al personal si: ¿Por razones del servicio transporta información fuera de la institución en dispositivos personales y/o institucionales?, se encontró que el 70% del personal encuestado trasporta información institucional fuera del entorno seguro y no utilizan herramientas adecuadas para proteger la información, lo cual indica que hace falta fortalecer la capacitación en seguridad informática, debido a que el personal que transporta información institucional reservada en sus activos informáticos aduciendo que no contaban con un activo informático institucional apropiado.
Buscando subsanar esta novedad, se le explico al personal que eran responsables de la seguridad de la información que generan o manejan y deben ceñirse a las normas establecidas en la Directiva Permanente 009 del 20 de abril de 2015.

En la pregunta: ¿Ha recibido información, capacitación o instrucciones referentes a seguridad informática?, a pesar que el 80% de la muestra manifiesta haber recibido capacitación en temas de Seguridad Informática, los mismos manifiestan que los boletines informáticos los recibieron por medio del correo electrónico institucional, generados desde el nivel central, pero carecen de actividades de sensibilización o capacitaciones que aclaren las dudas e informaciones generales que se envían en dichos correos. Para mejorar lo anterior se desarrollaron capacitaciones con el ánimo de mejorar la realimentación de la información enviada al correo institucional.

En la pregunta ¿Almacena información personal en su computador Institucional?, solamente una persona indicó que manejaba este tipo de información y utilizaba mecanismos de seguridad para proteger la misma, pero se pudo evidenciar que el mecanismo de protección consiste en aplicar claves a los documentos planos que maneja, lo anterior evidencia desconocimiento general de las políticas de seguridad informática de las Fuerzas Militares. Se realizó una sensibilización al personal sobre los riesgos para la información Institucional y para el desempeño del activo Informático que implica manejar información personal como videos, música entre otros, tales como los derechos de autor de este tipo de archivos.

Cuando se le pregunta al personal si: ¿Realiza periódicamente copias de respaldo de la información? se encuentra que el 30% del personal aduce que no realiza respaldo de la información que genera y maneja, el porcentaje restante de personal indica que si realiza copias de respaldo, pero los realiza de manera personal debido a que la unidad no cuenta con dispositivos para el almacenamiento de información y realizar los respectivos respaldos periódicos. Este tema que el Autor considera muy delicado, fue tratado directamente con el Comandante de la Estación, con el fin de exponer la situación al alto mando, buscando los recursos necesarios para la adquisición de los activos necesario para realizar los respaldos de información como lo indican las políticas de Seguridad Informática para las Fuerzas Militares.

El cambio periódico de las claves de acceso a los activos informáticos y aplicaciones institucionales es otra novedad encontrada, la cual se le reporta a la Jefatura encargada, buscando que desde el nivel central se tomen las medidas técnicas tendientes a realizar las solicitudes de cambio de contraseña de manera automática. A nivel local se le realizan las recomendaciones pertinentes al encargado de la sección de telemática de la unidad como implementar un servidor de controlador de dominio con el propósito de administrar el acceso a los diferentes activos informáticos con los que cuenta la unidad además de sensibilizar al personal de la unidad para que realicen buenas practicas del uso de mencionados activos.

Otra novedad encontrada es el déficit de equipos de cómputo en la unidad, por lo cual un equipo de cómputo es compartido por cuatro personas. De la anterior situación se puso en conocimiento a la jefatura encargada. A nivel local se dieron las recomendaciones al encargado de la sección de telemática para que genere usuarios para cada tripulante en los diferentes equipos de cómputo, permitiendo tener control de la trazabilidad de las actividades efectuadas por cada usuario desde un mismo activo.

El envío de información a través de internet también es un riesgo para la información que se maneja en la Unidad, razón por la cual se sensibiliza al personal para que evite realizar estas acciones y recurra a los canales y herramientas autorizadas para estos fines, igualmente generar bloqueos a nivel de red con el propósito de evitar el uso de correos comerciales para el trámite de información institucional.

CONCLUSIONES

Se evidencia que se tienen controles establecidos, pero no se están gestionando a cabalidad, ya que con base a la muestra recolectada se observó que se deben implementar nuevos mecanismos que permitan garantizar la integridad, confidencialidad y disponibilidad de la información institucional.
Se debe gestionar con el nivel central para que asigne personal idóneo a ocupar los cargos de Oficial de Seguridad Informática y Coordinador de telemática y a corto plazo capacitar al personal que se encuentra en el momento desempeñándose en estos cargos.

Equipos, la institución debe contemplar en su plan de compras la adquisición del material necesario para que los funcionarios de la Estación de Guardacostas puedan desarrollar sus actividades adecuadamente.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ARMADA NACIONAL
ESTACIÓN DE GUARDACOSTAS URABÁ

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

No. 315 MDN-CGFM-CARMA-SECAR-JONA-COGAC-CGUCA-CEGUR-JDO-29.57

Turbo (Antioquia), 15 MAY 2017

Señor Capitán de Navío
ALVARO JOSÉ CERMEÑO PETRO
Director Tecnologías de la Información y las Comunicaciones.
Carrera 54 No. 26-25 CAN
Bogotá D.C.

Asunto: Solicitud Asignación Computadores

Con toda atención, me dirijo al señor capitán de Navío Director Tecnologías de la Información y las Comunicaciones con el fin de solicitarle apoyo con la asignación de equipos de cómputo para esta unidad, en consideración a lo que seguidamente expongo:

- [redacted]
- La falta de equipos de trabajo genera lentitud en el desarrollo de las actividades administrativas.
- Otro factor importante son los riesgos para la información que genera la falta de equipos de cómputo, ya que en el afán de acertar en el cumplimento de sus labores, el personal hace uso de sus equipos personales, lo cual vulnera las Políticas de Seguridad Informática de la Armada Nacional.

Respetuosamente,

Capitán de Corbeta DIEGO ALEJANDRO GIL BARÓN
Comandante Estación de Guardacostas Urabá

Vo. Bo. TK González Emmanuel
JDO
Elaboró: S3 López Fabio
Revisó: SJT Mejia Franklin

"Protegemos el azul de la Bandera"
Línea anticorrupción Armada Nacional 01 8000 11 69 69 – 24 Horas
Avenida la Playa Sector Punta las vacas – 3692000 ext. 11461/2
www.armada.mil.co cegur@armada.mil.co

GEDOC-FT-001-AYGAR-V07

ANEXO B. Listados de asistencia a capacitaciones S.I.

ARMADA NACIONAL REPUBLICA DE COLOMBIA	**FORMATO LISTADO DE ASISTENCIA**	
	Proceso: Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
Código: DIREST-FT-001-JEPLAN-V05	**Rige a partir de:** 10/03/2015	Página 1 de 1

Objetivo: Prevenir al personal en los tecnicos de ingeniería básal molicosa para extraer información.

Moderador: SJ Lopez Molino Fabio Andrés **Fecha:** 08 marzo 2017. **Hora:** 1000R.

Tipo: Capacitación ☒ Reunión ☐ Otro ☐ Cual? **Guarnición:** Tuibo **Proceso:** Operaciones Navales

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							6-2.
14							Emzabala.
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL REPUBLICA DE COLOMBIA	**FORMATO LISTADO DE ASISTENCIA**	
	Proceso: Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
Código: DIREST-FT-001-JEPLAN-V05	**Rige a partir de:** 10/03/2015	Página 1 de 1

Objetivo: Realizar capacitación al personal en los cordados. con la información que recibe en el correo electrónico

Moderador: S3 López Molina Fabio Andrés **Fecha:** 24 Febrero 2017. **Hora:** 0800R.

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Turbo **Proceso:** Operaciones Navales

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

Código: DIREST-FT-001-JEPLAN-V05	**Proceso:** Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
	Rige a partir de: 10/03/2015	Página 1 de 1.

Objetivo: Realizar inducción a los Políticos de Seguridad Informática de las FFMM.

Moderador: Sg Lopez Molina. Fabio Andres **Fecha:** 17 Febrero 2017. **Hora:** 0830 OR.

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Tulua **Proceso:** Operaciones Navales

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

Código: DIREST-FT-001-JEPLAN-V05	**Proceso:** Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
	Rige a partir de: 10/03/2015	Página 1 de 1

Objetivo: Complementación Instrucción políticas de Seguridad Informatica

Moderador: CS López Molino Fabio Andrés **Fecha:** 05 mayo 2019. **Hora:** 1400 R.

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Tolú **Proceso:** Operaciones Navales.

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							Evaluada.
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

	Proceso: Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
Código: DIREST-FT-001-JEPLAN-V05	**Rige a partir de:** 10/03/2015	Página 1 de 1

Objetivo: Recomendaciones de seguridad en la navegación en paginas web.

Moderador: SJ López Molina Fabio Andrés **Fecha:** 06 abril 2017. **Hora:** 0800H.

Tipo: Capacitación ☒ Reunión ☐ Otro ☐ Cual? **Guarnición:** Tuba **Proceso:** Operaciones Navales.

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

Código: DIREST-FT-001-JEPLAN-V05	**Proceso:** Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
	Rige a partir de: 10/03/2015	Página 1 de 1

Objetivo: Recomendaciones de Seguridad en el manejo de redes sociales.

Moderador: S3 Lopez Molmo. Fabio Andres **Fecha:** 30 marzo 2017. **Hora:** 0800R.

Tipo: Capacitación ☒ Reunión ☐ Otro ☐ Cual? **Guarnición:** Tuba **Proceso:** Operaciones Navales

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

	Proceso: Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
Código: DIREST-FT-001-JEPLAN-V05	**Rige a partir de:** 10/03/2015	Página 1 de 1

Objetivo: Informar al personal los riesgos a los que expone la información al usar los PC de la unidad

Moderador: S3 Lic. Molina Fabio Andrés **Fecha:** 24 mayo 2017. **Hora:** 1000 H.

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Cúcuta **Proceso:** Operaciones Navales.

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL
REPUBLICA DE COLOMBIA

FORMATO LISTADO DE ASISTENCIA

Proceso: Direccionamiento Estratégico Armada Nacional | **Autoridad:** JEPLAN

Código: DIREST-FT-001-JEPLAN-V05 | **Rige a partir de:** 10/03/2015 | Página 1 de 1

Objetivo: Realizar capacitación en Inteligencia de la Información

Moderador: Soldado Liliana Fabio Andrés **Fecha:** 17 marzo 2017 **Hora:** 0800R

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Tolú **Proceso:** Operaciones Navales.

Nº	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

ARMADA NACIONAL REPUBLICA DE COLOMBIA	**FORMATO LISTADO DE ASISTENCIA**	
	Proceso: Direccionamiento Estratégico Armada Nacional	**Autoridad:** JEPLAN
Código: DIREST-FT-001-JEPLAN-V05	**Rige a partir de:** 10/03/2015	Página 1 de 1

Objetivo: Correcta Manera de almacenar la información para la realización de los respaldos.

Moderador: S3 López Medina Fabio Andrés **Fecha:** 13 marzo 2017 **Hora:** 1400H

Tipo: Capacitación [X] Reunión [ ] Otro [ ] Cual? **Guarnición:** Tuba **Proceso:** Operaciones Navales.

N°	GRADO	APELLIDOS Y NOMBRES	DEPENDENCIA	CEDULA	CELULAR	E-MAIL	FIRMA
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							Ejecutada.
15							
16							
17							
18							
19							
20							

RESUMEN ANALÍTICO ESPECIALIZADO	
TITULO	MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ
AUTOR	LÓPEZ MOLINA, Fabio Andrés
PALABRAS CLAVE	Seguridad Informática, Auditoria, Metodología de Análisis de Riesgos, Integridad, Confidencialidad, Disponibilidad, No repudio, Amenazas a la Información, Activos Informáticos.
DESCRIPCIÓN	En este documento se describen las actividades que se llevaron a cabo en el desarrollo de una auditoría de Seguridad Informática a una Estación de Guardacostas de la Armada Nacional, con el propósito de mejorar la aplicabilidad de las políticas de Seguridad Informática para lo cual también se aplicó una metodología de Gestión de Riesgos que dio origen a un plan de mejoramiento que a su vez busca garantizar el cumplimiento de los controles de Seguridad.
FUENTES BIBLIOGRÁFICAS	© Derecho.com. Manual Seguridad Básica Informática, ©Derecho.com FDL Licence. [En linea]. España.: Disponible en: http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/manual-seguridad-basico.pdf AGUILERA LÓPEZ, Purificación. Seguridad Informática. 1 ed. Madrid: Editorial Editex. 2010. BENAVIDES RUANO, Miriam y SOLARTE SOLARTE, Francisco. Módulo riesgo y control informático. Pasto.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. 2012. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". El Congreso. Bogotá, D.C., 2013. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1712. (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. El Congreso. Bogotá, D.C., 2014. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 57. (5, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. El Congreso. Bogotá, D.C., 1985. COLOMBIA. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. DECRETO 1874 (2, Agosto, 1979). Por el cual se crea el Cuerpo de Guardacostas y se dictan otras disposiciones. La Presidencia. Bogotá, D.C., 1979. CORTEZ PINTO, Maria. Las vulnerabilidades humanas en relación a la seguridad informática para evitar la fuga de información confidencial en el departamento de recursos humanos de la Universidad Técnica de Ambato. Trabajo de Graduación para Ingeniero en Sistemas Computacionales e

	Informáticos. Ambato – Ecuador. Universidad Tecnico de Ambato. Facultad de Ingeniería en Sistemas Electrónica e Industrial. 2013. FUERZAS MILITARES DE COLOMBIA. Directiva Permanente No. 200-12/2006 Políticas de Seguridad Informática PARA LAS F.F.M.M. FFMM. BOGOTA D.C. 2006. HADNAGY, Christopher. Ingeniería Social: El arte del Hacking personal. Madrid: Editorial ANAYA MULTIMEDIA.,2011. SEMANA. Las empresas colombianas no están preparadas para los ciberataques. [En linea]. Bogotá.: Semana.com. Disponible en: http://www.semana.com/tecnologia/articulo/las-empresas-colombianas-no-estan-preparadas-para-los-ciberataques/466430 SO27000.ES, El portal de ISO 27001 en Español. [en linea]. Madrid: Disponible en: http://www.iso27000.es/ TORRES ANDAGANA, Gabriela y LLANGA SALCAN, Diego. Estudio e Implementación de una Metodología de Prevención de Intrusos para redes LAN. Tesis de Grado Ingeniero en Electrónica y computación. Riobamba – Ecuador.: Escuela Superior Politécnica de Chimborazo. Facultad De Informática y Electrónica. Escuela de Ingeniería Electrónica y Tecnología en Computación. 2010.
CONTENIDO	El presente es el resumen de un informe final del Proyecto de Seguridad Informática denominado “MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ” como objetivo general “Evaluar el cumplimiento de las políticas de Seguridad Informática y riesgos de la Armada Nacional de Colombia mediante Auditoría Interna de Seguridad informática en la Estación de Guardacostas Urabá”, y como objetivos específicos; Identificar Deficiencias de seguridad informática mediante una auditoría interna, Gestionar los riesgos encontrados en la auditoria mediante metodología Magerit, elaborar un informe técnico de Seguridad Informática para la Dirección de Tecnologías de la Información y las Comunicaciones de la Armada Nacional y como componente practico principal: Capacitar al personal de la Estación de Guardacostas Urabá con el propósito de mejorar la aplicabilidad de las políticas de Seguridad Informática. En el primer capítulo se realiza la definición del problema en la cual se exponen los recursos para contribuir a la seguridad informática con los que cuenta la Estación de Guardacostas y las posibles falencias que a primera vista se pueden encontrar en la misma lo que nos lleva a la pregunta de investigación ¿Cómo fortalecer la aplicación de las políticas de seguridad informática de la Armada Nacional en la Estación de Guardacostas de Urabá? El capítulo dos se justifica la realización del proyecto teniendo en cuenta la gran importancia que tiene para las instituciones del Estado que sus activos informáticos, información y personal se encuentren debidamente protegidos

	y capacitados respectivamente. En el capítulo se desarrolla la auditoría de Seguridad informática verificando la aplicación de los controles que ordenan las Políticas de Seguridad Informática de la institución de acuerdo a los formatos establecidos dentro de su Sistema de Gestión de Seguridad Informática. Seguidamente se aplica la metodología para la gestión de Riesgos Denominada “MAGERIT” con el objetivo de determinar un plan de mejoramiento que permita mitigar los riesgos más inminentes y que puedan generar un impacto negativo en la seguridad de la información.
METODOLOGÍA	Por la naturaleza práctica de este proyecto no se utilizó una metodología en particular.
CONCLUSIONES	Con el desarrollo de este proyecto se lograron identificar las deficiencias de seguridad informática permitiendo aumentar la protección de los datos e información que utiliza la institución. Mediante la aplicación de la metodología Magerit se logró visibilizar ante el Comando de la Estación la importancia de gestionar de manera adecuada, sistemática y permanente los riesgos informáticos La seguridad Informática es un tema que se debe abordar con mucho tacto a la hora de capacitar al personal, se debe primero sensibilizar el tema en lo personal y luego pasar al campo empresarial.
FECHA	28 mayo de 2017

RESUMEN ANALÍTICO ESPECIALIZADO	
TITULO	MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ESTACIÓN DE GUARDACOSTAS URABÁ
AUTOR	LÓPEZ MOLINA, Fabio Andrés
PALABRAS CLAVE	Seguridad Informática, Auditoria, Metodología de Análisis de Riesgos, Integridad, Confidencialidad, Disponibilidad, No repudio, Amenazas a la Información, Activos Informáticos.
DESCRIPCIÓN	En este documento se describen las actividades que se llevaron a cabo en el desarrollo de una auditoría de Seguridad Informática a una Estación de Guardacostas de la Armada Nacional, con el propósito de mejorar la aplicabilidad de las políticas de Seguridad Informática para lo cual también se aplicó una metodología de Gestión de Riesgos que dio origen a un plan de mejoramiento que a su vez busca garantizar el cumplimiento de los controles de Seguridad.
FUENTES BIBLIOGRÁFICAS	© Derecho.com. Manual Seguridad Básica Informática, ©Derecho.com FDL Licence. [En linea]. España.: Disponible en: http://cefire.edu.gva.es/file.php/1/Comunicacion_y_apertura/B1_Navegacion_Internet/manual-seguridad-basico.pdf AGUILERA LÓPEZ, Purificación. Seguridad Informática. 1 ed. Madrid: Editorial Editex. 2010. BENAVIDES RUANO, Miriam y SOLARTE SOLARTE, Francisco. Módulo riesgo y control informático. Pasto.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. 2012. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". El Congreso. Bogotá, D.C., 2013. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1712. (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. El Congreso.

	Bogotá, D.C., 2014. COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 57. (5, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. El Congreso. Bogotá, D.C., 1985. COLOMBIA. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. DECRETO 1874 (2, Agosto, 1979). Por el cual se crea el Cuerpo de Guardacostas y se dictan otras disposiciones. La Presidencia. Bogotá, D.C., 1979. CORTEZ PINTO, Maria. Las vulnerabilidades humanas en relación a la seguridad informática para evitar la fuga de información confidencial en el departamento de recursos humanos de la Universidad Técnica de Ambato. Trabajo de Graduación para Ingeniero en Sistemas Computacionales e Informáticos. Ambato – Ecuador. Universidad Tecnico de Ambato. Facultad de Ingeniería en Sistemas Electrónica e Industrial. 2013. FUERZAS MILITARES DE COLOMBIA. Directiva Permanente No. 200-12/2006 Políticas de Seguridad Informática PARA LAS F.F.M.M. FFMM. BOGOTA D.C. 2006. HADNAGY, Christopher. Ingeniería Social: El arte del Hacking personal. Madrid: Editorial ANAYA MULTIMEDIA.,2011. SEMANA. Las empresas colombianas no están preparadas para los ciberataques. [En linea]. Bogotá.: Semana.com. Disponible en: http://www.semana.com/tecnologia/articulo/las-empresas-colombianas-no-estan-preparadas-para-los-ciberataques/466430 SO27000.ES, El portal de ISO 27001 en Español. [en linea]. Madrid: Disponible en: http://www.iso27000.es/ TORRES ANDAGANA, Gabriela y LLANGA SALCAN, Diego. Estudio e Implementación de una Metodología de Prevención de Intrusos para redes LAN. Tesis de Grado Ingeniero en Electrónica y computación. Riobamba – Ecuador.: Escuela Superior Politécnica de Chimborazo. Facultad De Informática y Electrónica. Escuela de Ingeniería Electrónica y Tecnología en Computación. 2010.
CONTENIDO	El presente es el resumen de un informe final del Proyecto de Seguridad Informática denominado “MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA

	ESTACIÓN DE GUARDACOSTAS URABÁ" como objetivo general "Evaluar el cumplimiento de las políticas de Seguridad Informática y riesgos de la Armada Nacional de Colombia mediante Auditoría Interna de Seguridad informática en la Estación de Guardacostas Urabá", y como objetivos específicos; Identificar Deficiencias de seguridad informática mediante una auditoría interna, Gestionar los riesgos encontrados en la auditoria mediante metodología Magerit, elaborar un informe técnico de Seguridad Informática para la Dirección de Tecnologías de la Información y las Comunicaciones de la Armada Nacional y como componente practico principal: Capacitar al personal de la Estación de Guardacostas Urabá con el propósito de mejorar la aplicabilidad de las políticas de Seguridad Informática. En el primer capítulo se realiza la definición del problema en la cual se exponen los recursos para contribuir a la seguridad informática con los que cuenta la Estación de Guardacostas ya las posibles falencias que a primera vista se pueden encontrar en la misma lo que nos lleva a la pregunta de investigación ¿Cómo fortalecer la aplicación de las políticas de seguridad informática de la Armada Nacional en la Estación de Guardacostas de Urabá? El capítulo dos se justifica la realización del proyecto teniendo en cuanta la gran importancia que tiene para las instituciones del Estado que sus activos informáticos, información y personal se encuentren debidamente protegidos y capacitados respectivamente. En el capítulo se desarrolla la auditoría de Seguridad informática verificando la aplicación de los controles que ordenan las Políticas de Seguridad Informática de la institución de acuerdo a los formatos establecidos dentro de su Sistema de Gestión de Seguridad Informática. Seguidamente se aplica la metodología para la gestión de Riesgos Denominada "MAGERIT" con el objetivo de determinar un plan de mejoramiento que permita mitigar los riesgos más inminentes y que puedan generar un impacto negativo en la

	seguridad de la información.
METODOLOGÍA	Por la naturaleza práctica de este proyecto no se utilizó una metodología en particular.
CONCLUSIONES	Con el desarrollo de este proyecto se lograron identificar las deficiencias de seguridad informática permitiendo aumentar la protección de los datos e información que utiliza la institución. Mediante la aplicación de la metodología Magerit se logró visibilizar ante el Comando de la Estación la importancia de gestionar de manera adecuada, sistemática y permanente los riesgos informáticos La seguridad Informática es un tema que se debe abordar con mucho tacto a la hora de capacitar al personal, se debe primero sensibilizar el tema en lo personal y luego pasar al campo empresarial.
FECHA	28 mayo de 2017