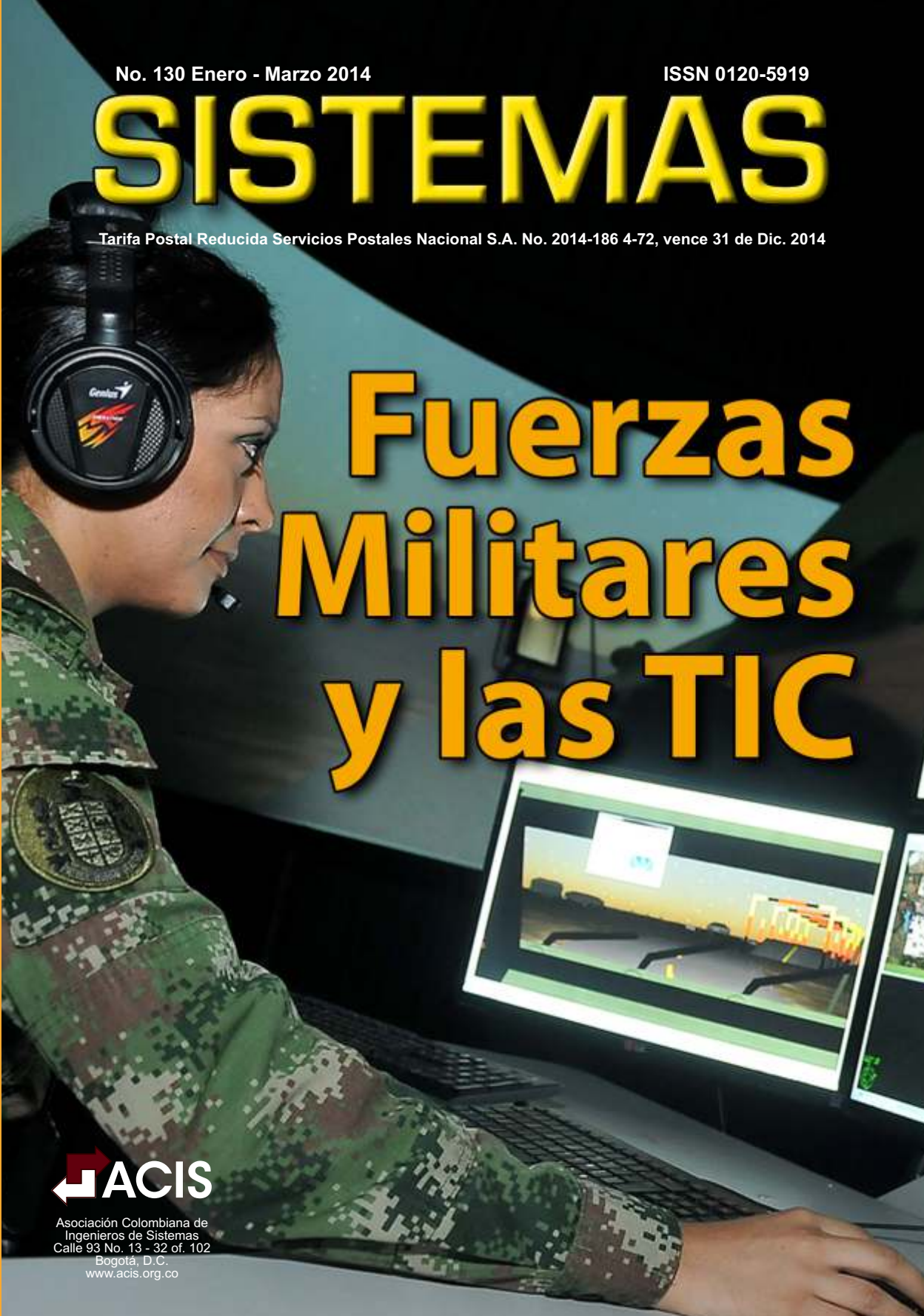
No. 130 Enero - Marzo 2014 ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2014-186 4-72, vence 31 de Dic. 2014



Fuerzas Militares y las TIC

ACIS
Asociación Colombiana de Ingenieros de Sistemas
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

INSCRIPCIONES ABIERTAS

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD
Otorgada por el Ministerio de Educación Nacional.

Resolución 12773 del 19 de septiembre de 2013

UNIVERSIDAD EAN

PROGRAMAS PRESENCIALES

Carrera Profesional en Ingeniería de Producción
Acreditación Internacional ABET
Acreditación de Alta Calidad MEN*

Carrera Profesional en Ingeniería Ambiental

Carrera Profesional en Ingeniería de Sistemas[1]
Acreditación de Alta Calidad MEN*

Especialización en Gerencia Estratégica del Diseño

Especialización Gerencia de Tecnología

Especialización Gerencia Informática

Especialización Gerencia de Proyectos
Certificación de los cursos avalados por el PMI.

Maestría en Innovación
Doble Titulación Internacional:
Universidad EAN / Universidad Antonio de Nebrija, Madrid - España.

Maestría en Gestión de Proyectos
Doble Titulación Internacional:
Universidad EAN / Universidad de Quebec, Canadá.
Certificación de los cursos avalados por el PMI.

Doctorado en Gerencia de Proyectos

PROGRAMAS VIRTUALES

Carrera Profesional en Ingeniería de Producción

Carrera Profesional en Ingeniería de Sistemas

Especialización en Gestión de Sistemas y Tecnologías de la Información en la Empresa
(A Distancia, con opción de Doble Titulación Internacional)
Convenio: Universidad EAN Universidad Politécnica de Madrid, España (CEPADE)

1 Con opción de Doble Titulación Internacional Universidad EAN – Universidad de Quebec - Canadá
*Acreditación de Alta Calidad otorgada por el Ministerio de Educación Nacional.

17 *Carreras Profesionales*
8 Presenciales y 9 Virtuales

32 *Especializaciones*
22 Presenciales y 10 Virtuales

10 *Maestrías*
Con opción de doble titulación internacional

3 *Doctorados*

www.ean.edu.co

@UniversidadEAN /UniversidadEANColombia /universidadean /PortalUEAN

Centro de Contacto en Bogotá: +(57-1) 593 6464
Línea gratuita nacional: 01 8000 93 1000
E-mail: informacion@ean.edu.co
El Nogal: Cra. 11 No. 78-47
Bogotá D.C. // Colombia, Suramérica

Con el reconocimiento de alta calidad académica por parte de dos de las más prestigiosas acreditadoras internacionales con sede en los Estados Unidos.

ABET otorga la acreditación internacional de calidad al programa de Ingeniería de Producción.

Accredited ABET Engineering Accreditation Commission

ACBSP ACCREDITED

Personería Jurídica Resolución 2898, Mayo 16 – 69 Min Justicia. Institución de Educación Superior sujeta a inspección y vigilancia por el Ministerio de Educación Nacional. Códigos SNIES con registro calificado números: 102777, 54451, 101871, 54013, 4320, 1985, 102961, 1984, 52422, 52084, 54374, 102139, 102126.

En esta edición

Editorial 4

Fuerzas Militares y las TIC

En esta edición, como en otras, la revista incursiona en diferentes ambientes con el propósito de mostrar a los lectores el uso y alcance de las Tecnologías de Información y Comunicaciones –TIC-. De ahí, haberlas escogido como tema central en este número.

Más allá de las TIC en Mindefensa* 8

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia –colCERT- y la Dirección de Ciencia, Tecnología e Innovación –Ctel-, se pronunciaron en torno a varias inquietudes.

Columnista Invitado 14

Desarrollo tecnológico: un desafío hacia la independencia estratégica

La innovación revoluciona los procesos que antes se adelantaban de manera tradicional, y genera mejoras sustanciales en los niveles estratégico, operacional y táctico. Nuestro compromiso es asentar un modelo tecnológico, que con posteridad, pueda tener aplicación dual y que repercuta en la consolidación del país como un referente en ciencia y tecnología.

Cara y Sello 22

Sector Defensa y TI. Sistemas de investigación

Comando General, Ejército, Fuerza Aérea Colombiana (FAC) y Policía Nacional acudieron a la cita para debatir en torno a las Tecnologías de Información y Comunicaciones TIC.

Uno 44

Educación, promotora del crecimiento y calidad académica de la Fuerza Pública Colombiana

El presente artículo pretende ofrecer un contexto de lo adelantado en materia de política educativa en el Ministerio de Defensa Nacional, a fin de unificar los procesos educativos de formación, capacitación y entrenamiento. Actividades realizadas dentro de las escuelas y centros de formación de las Fuerzas Armadas y la Policía Nacional, en búsqueda de la profesionalización del servicio y la excelencia académica de los hombres y mujeres que las conforman.

Dos 51

Ciencia y Tecnología en el Ejército Nacional de Colombia

El presente artículo muestra el contexto en el que se desarrollan las actividades de investigación y desarrollo tecnológico (I+D+i) en el sector defensa, con el propósito de dar a conocer las prácticas y resultados obtenidos de estas actividades.

Tres 59

Fuerzas Armadas de Colombia, grados y jerarquías

Recuento contextual y gráfico de las insignias y grados en las Fuerzas Armadas.

Publicación de la Asociación Colombiana de
Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del
Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales
Nacional S.A. No. 2014-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Dirección General
Francisco Rueda Fajardo

Consejo de Redacción
Julio López M.
María Esperanza Potes L.
Gabriela Sánchez A.
Jeimy J. Cano
Manuel Dávila S.

Editor Técnico
Manuel Dávila S.

Editora
Sara Gallardo M.

Junta Directiva ACIS
2013-2014

Presidente
Jaime García Cepeda
Secretaria
Martha Elena Frías Díaz
Tesorero
Edgar Ruíz Dorantes
Vocales
Jorge A. Quiroga Gutiérrez
Ricardo Munévar Molano
Camilo Rodríguez Acosta

Directora Ejecutiva
Beatriz E. Caicedo R.

Foto Carátula
Mindefensa

Diseño y diagramación
Bruce Garavito

Impresión
Javegraf

Los artículos que aparecen en esta edición no reflejan necesariamente el pensamiento de la Asociación. Se publican bajo la responsabilidad de los autores.

Enero-Abril 2014
Calle 93 No.13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

NASCO
NACIONAL DE COMPUTADORES S.A.

APOYA ESTA PUBLICACIÓN

TEL: 6 06 06 06- CR 15 No 72-73

Cursos vigentes

¡Inscríbase ya!

Curso: Moviltrónica Android y Arduino usando Bluetooth
Marzo 4 de 2014

Curso: Especificación de Requerimientos con Casos de Uso
Marzo 4 al 11 de 2014

Curso: Fundamentos ISO/IEC 20000:2011
Marzo 12 al 21 de 2014

Curso Virtual: Desarrollo de Aplicaciones Móviles esenciales con Android
Marzo 12 al 29 de 2014

Seminario-taller Actualización a la Quinta Edición del PMBOK® versión 2013
Este seminario otorga 12 PDU´s a Project Management Professionals- PMP®s
Marzo 18 al 20 de 2014

Curso: Arquitectura Empresarial y TOGAF: Conceptos y metodología de definición
Marzo 25 a Abril 4 de 2014

Curso Virtual: Metodologías de desarrollo de software (para gerenciar proyectos)
Marzo 28 al 8 de Abril de 2014

Curso: Seminario Taller de Recuperación de Proyectos en Problemas
Este curso otorga 8 PDUs en categoría B.
Abril 3 de 2014

Curso: Introducción a la Mineria de Datos
Abril 21 al 29 de 2014

Curso: Introducción a PERL y su aplicación en el desarrollo de soluciones Web
Abril 21 al 30 de 2014

ACIS

Asociación Colombiana de Ingenieros de Sistemas
Calle 93 No. 13 - 32 of. 102
Tels: 616 1407 - 616 1409 - 610 4842
Bogotá, D.C.
www.acis.org.co

Mayor información en:
www.acis.org.co

Fuerzas Militares y las TIC

En esta edición, como en otras, la revista incursiona en diferentes ambientes con el propósito de mostrar a los lectores el uso y alcance de las Tecnologías de Información y Comunicaciones –TIC-. De ahí, haberlas escogido como tema central en este número.

Manuel Dávila Sguerra

La Asociación Colombiana de Ingenieros de Sistemas –ACIS- enfatiza su trabajo en torno a las Tecnologías de Información y las Comunicaciones –TIC-, no sólo en las diferentes áreas de la Ingeniería de Sistemas y los aspectos que contempla esta profesión, sino que va más allá.

Nos referimos a las tecnologías de punta implementadas a nivel mundial de las que incentivamos el debate sobre sus conveniencias, sus aplicaciones en la industria, sus ventajas y desventajas, como se puede observar en la sección *Cara y Sello*, producto de un foro al que son convocados expertos para responder las inquietudes más relevantes alrededor del tema central de la publicación.

En ese contexto, el interés de Acis no es promover una u otra tecnología, sino permitir las intervenciones de manera abierta y objetiva para conocer los diferentes aspectos que puedan preocupar sobre lo que está sucediendo en el sector.

En su permanente diálogo sobre las posibles mejoras y adecuaciones a las necesidades del momento, el Consejo de Redacción ha venido pensando en otras alternativas para tratar otros

asuntos, motivados por la amplísima penetración de la tecnología informática en la sociedad misma. No podemos desconocer que la vida de los seres humanos está impactada por las TIC, a tal grado, que ya es un tema de política pública.

Hoy en día las TIC están presentes en los automóviles, los aviones, los barcos, las instituciones, la medicina, la política y no hay casi seres humanos que no tengan en su haber un dispositivo móvil. Las ciudades inteligentes ya son un hecho; la georeferenciación de los territorios es de uso público y cotidiano; y el software es considerado un producto de seguridad nacional.

El Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos –IEEE-, con relación al futuro de Internet de las cosas estipula que en el 2020 habrá más de 50 billones de dispositivos conectados a Internet, lo que convierte a la nube en un problema ecológico y considera necesario trabajar sobre tales tecnologías, no sólo desde el punto de vista técnico, sino humano y social. Si una consulta de Google consume 0.2 gramos de CO_2, ¿podemos imaginar lo que sucede con las realizadas a nivel mundial?

Por esa razón, algunos de los últimos números de la revista se han ocupado de temas como la Medicina, las Políticas de Gobierno, las Redes sociales, el TLC, la Seguridad y la privacidad y se ha invitado a ministros, médicos y hasta psiquiatras, como sucedió en la edición dedicada a las redes sociales. Sin duda alguna, se trata de temas que están influyendo en la cotidianidad de las personas y cambiando el mecanismo como se relacionan los seres humanos en esta nueva visión del mundo.

Por todo lo expuesto, en esta ocasión hemos decidido acercarnos a las instituciones militares del país, por tratarse de un sector de máxima importancia, toda vez que su actividad se centra en la protección de los individuos y de la sociedad, para lo cual el uso de la tecnología es fundamental.

Cabe anotar cómo las fuerzas militares de muchos países han influenciado el desarrollo de las TIC. Tal vez, debido a lo esencial de su quehacer en la protección de la vida, es que los procesos de investigación en ciencia y tecnología tienen en sus manos un aceleramiento tan considerable.

Basta citar algunos ejemplos. La creación del protocolo TCP/IP, que dio lugar a la aparición de Internet, la red mundial, producto de la investigación de la agencia para los proyectos de investigación avanzada, DARPA, del sector defensa de los Estados Unidos, en un proyecto denominado Arpanet, dirigido por Vinton Cerf en el año 1972, desde la Universidad de Stanford. Dicho sea de paso, Vinton Cerf asistió a un encuentro de Acis con la Red de Decanos y Directores de Ingeniería de Sistemas –REDIS-, como se puede ver en http://www.youtube.com/watch?v=0DSW9rtPZkQ. Así mismo, son notables los avances en la educación virtual, debido en gran parte a la necesidad de capacitar a

los soldados como lo muestra la historia de esta modalidad de educación. Uno de los desarrollos, de gran importancia en esta modalidad de educación fue el modelo Sharable Content Object Reference Model - SCORM-, un estándar para crear cursos virtuales. Muy famosa fue la máquina de Turing que permitió desencriptar los códigos de los alemanes en la segunda guerra mundial y que dio lugar a la creación de la ciencia de la computación.

El otro elemento que nos motiva a trabajar con esta institución es seguir contribuyendo, desde ACIS, en la consolidación de las relaciones entre universidad, empresa, Estado y sociedad, un reto tanto para la academia como para el gremio de los Ingenieros de Sistemas.

Encontraremos en esta edición un debate en la sección *Cara y Sello* con la participación de las unidades más relevantes del sector defensa. Entre ellas, el Control de Comunicaciones y Sistemas del Comando General de las Fuerzas Armadas; los directores de Ciencia y Tecnología del Comando General de las Fuerzas Militares, del Ejército Nacional y de la Fuerza Aérea; la dirección de Investigación Desarrollo e Innovación de la Armada Nacional y la unidad de Telemática y Electrónica de la Policía Nacional.

Por su parte, los colaboradores invitados nos han enriquecido con los aspectos centrales de la revista que resumimos en este editorial.

Nidia Patricia Herrera García presenta un contexto de lo adelantado sobre política educativa en el Ministerio de Defensa Nacional, cuyo fin es unificar los procesos de formación, capacitación y entrenamiento dentro de las escuelas y centros de formación de las Fuerzas Armadas y la Policía Nacional. Trata el artículo sobre la búsqueda de la profesionalización del servicio y la excelencia académica de los hombres y mujeres que las conforman.

Juanita Rodríguez Kattah nuestra columnista invitada, se refiere al desarrollo tecnológico como un desafío hacia la independencia estratégica. Como representante del Ministerio de Defensa escribe sobre la importancia de la innovación, en aras de revolucionar los procesos que antes se adelantaban de manera tradicional para generar mejoras sustanciales en los niveles estratégicos, operacionales y tácticos. Describe el compromiso para crear un modelo tecnológico que con posteridad, pueda tener aplicación dual y que repercuta en la consolidación del país, como un referente en ciencia y tecnología.

El coronel Alberto González Guerrero, del Ejército Nacional, nos muestra el proceso de creación del Sistema de Ciencia y Tecnología desde el año 2009 y sus opiniones sobre la necesidad de conceptualizar el objetivo de la investigación y el desarrollo tecnológico en el contexto del sector defensa, implementando estrategias de corto y mediano plazo. Señala el uniformado que se trata de fortalecer e instituir los esfuerzos innovadores, producto de las especiales necesidades de la

fuerza. Y, resalta la importancia de la investigación, el desarrollo y la innovación en estos procesos.

El Capitán de Fragata (Reserva Activa) Carlos Enrique Ortiz Rangel, explica en su artículo la conformación de los grados y jerarquías de las Fuerzas Armadas de Colombia, a través de un recuento contextual y gráfico.

Esperamos con esta edición resaltar los esfuerzos en investigación y desarrollo de nuestras instituciones de defensa, además de aportar a favor de la Ingeniería de Sistemas.

Manuel Dávila Sguerra. *Ingeniero de Sistemas de la Universidad de los Andes. Decano Facultad de Ingeniería Uniminuto. Creador de la Unidad de Educación Virtual: Uniminuto Virtual. Coordinador Académico de la Asociación Colombiana de Ingenieros de Sistemas y director del Salón de Informática año 2001 y 2004 sobre Software Libre. Columnista de Computer World, eltiempo.com sobre Linux y el software libre: 120 artículos publicados. Autor de e-Genesis- El Generador de sistemas. Mención especial en el Premio Colombiano de Informática 2006. Autor de los textos en el curso virtual sobre Software libre desarrollado para el Distrito de Bogotá 2006. Escogido entre los 25 IT Manager del año 2008 por la revista IT-Manager. Conferencista en la presentación de la ley del Software Libre en el Congreso de la República de Colombia. Exprofesor e investigador de la Universidad de los Andes. Miembro Fundador de varias asociaciones: Asociación de industriales del software Indusoft, hoy llamada Fedesoft; Asociación Colombiana de Ingenieros de sistemas –Acis-; gestor y Expresidente de la red de Decanos y Directores de Ingeniería de sistemas, REDIS. Autor de los libros "GNU/Linux y el software libre" y "Software libre una visión".*

Más allá de las TIC en Mindefensa*

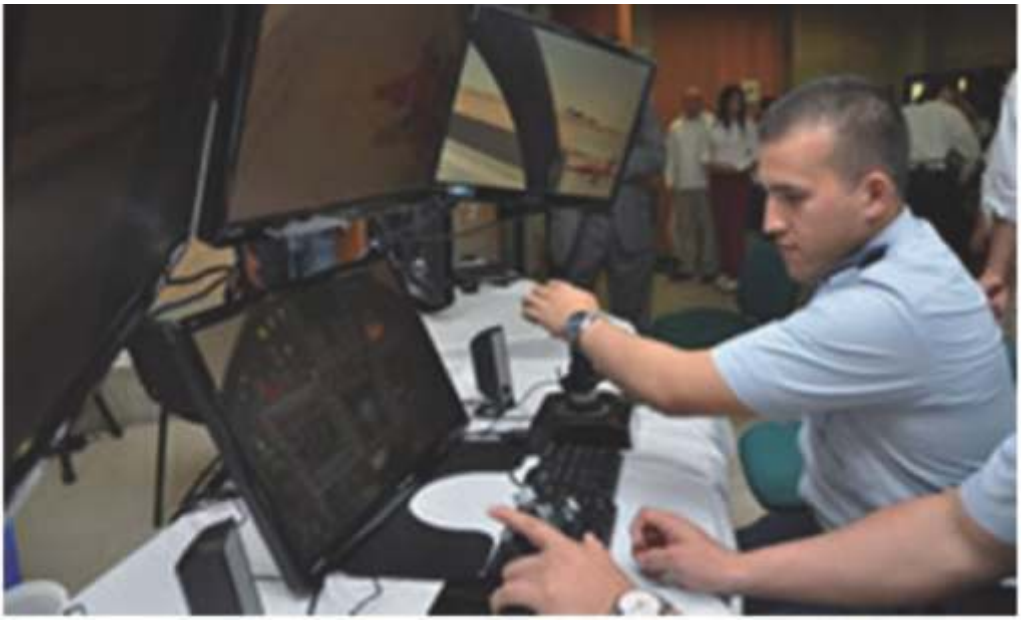
El Grupo de Respuesta a Emergencias Cibernéticas de Colombia –colCERT- y la Dirección de Ciencia, Tecnología e Innovación –Ctel-, se pronunciaron en torno a varias inquietudes.

Estas dos áreas del Ministerio de Defensa dieron respuesta a las inquietudes formuladas por la revista. La primera –colCERT- "tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional". Mientras la Dirección de Ciencia, Tecnología e Innovación –Ctel- contempla como función principal "la definición de la línea estratégica –en tales aspectos- del Sector Defensa, en el marco del programa de modernización de la Política Integral de Defensa y Seguridad para la Prosperidad".

Revista Sistemas. ¿Cómo define el Ministerio la seguridad informática, en el marco de la seguridad nacional?

En Colombia se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones, elevando su nivel de exposición a amenazas cibernéticas; por tanto, la seguridad informática es una prioridad.

RS: El presidente Juan Manuel Santos ha destacado los desarrollos en ciencia, tecnología e innovación, como herramienta estratégica, en procura de mejorar la seguridad aérea, terrestre y marítima en todo el territorio nacional. En ese contex-



to, ¿qué significado tiene para el Ministerio el ciberespacio? ¿Está contemplado como un escenario de operaciones similares a las adelantadas en tierra, mar y aire?

El Ciberespacio es definido según Resolución CRC 2258 de 2009, como el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información, que es utilizado para la interacción entre usuarios. Teniendo en cuenta esto, es para nosotros primordial dar lineamientos de seguridad de la información para el ciberespacio, que minimicen el nivel de riesgo al que las entidades están expuestas.

RS: ¿Cómo está conformada el área responsable del ciberespacio –si existe- dentro del Ministerio?

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia, colCERT, es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa; y, presta su apoyo y colaboración a las demás instancias nacionales, tales como el Centro Cibernético Policial –CCP- y el Comando Conjunto Cibernético –CCOC-.

RS: ¿Cuáles son los planes a mediano y largo plazo en torno a la ciberseguridad? ¿Habrá un comando dedicado a ello? ¿Estará conformado sólo por militares o habrá espacio para personal civil?

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia, tiene como responsabilidad central la coordinación de la ciberseguridad y ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano, frente a

emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. El colCERT es un grupo del Ministerio de Defensa Nacional, integrado por funcionarios civiles, personal militar y en comisión de otras entidades.

El Comando Conjunto Cibernético de las Fuerzas Militares tiene la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio y el Centro Cibernético Policial, está a cargo de la prevención, la investigación y apoyará la judicialización de los delitos informáticos.

RS: ¿La ciudadanía tendrá un reporte público de los ataques informáticos detectados e identificados sobre la plataforma tecnológica del Ejército, Armada, Fac, Policía Nacional?

La información de ataques informáticos detectados e identificados sobre las plataformas tecnológicas de las Fuerzas Militares y el Ministerio de Defensa es de carácter reservado y secreto, porque existen ciertos tipos de ataques que no sólo afectan la imagen de las organizaciones, sino que también pueden contemplar información sensible y confidencial que pueden afectar las operaciones de las Fuerzas. Por lo tanto, esta información no es publicada.

RS: La nube es usada por los ciudadanos en el mundo entero, ¿qué opinión les merecen los peligros de la apertura de tales plataformas frente a la seguridad nacional?

La computación en la nube representa un nuevo modelo de prestación de servicios de negocio y tecnología, en el cual están infraestructuras, plataformas y software, entre otros. Sin embargo, dejando a un lado las ventajas que ofrece, es necesario establecer medidas de seguridad de la información para la protección de los datos que reposan en la nube y proteger las comunicaciones hacia y desde ella.

RS: ¿Existe dentro del Ministerio algún grupo especialista y dedicado a la investigación y desarrollo en el contexto de las TIC? ¿Cuáles son las políticas al respecto?

El Ministerio de Defensa Nacional cuenta con un grupo de TIC que define la política en la materia, para todo el sector defensa. Es un grupo que –en conjunto con la Fuerzas- determina estándares sectoriales etc.

El Ministerio de Defensa Nacional ha hecho una apuesta por el desarrollo tecnológico que le permita autosuficiencia e independencia estratégica. Varias de las apuestas (modelación y simulación y sensores), por ejemplo, involucran el desarrollo propio de TIC. En este sentido, la Corporación de Alta Tecnología para la Defensa –entidad del Grupo Social Empresarial para la Defensa- está comprometida con el desarrollo de software, sistemas de comunicaciones y visualización. Se han constituido dos grupos de investigación en la materia, debidamente registrados ante Colciencias, por lo cual se puede afirmar que el sector está desarrollando TIC para la defensa, pero siempre con la vocación de aplicación hacia el ámbito civil.

RS: ¿Cuenta el Ministerio con apoyo de otros países en esas tareas? ¿En qué términos? ¿Con-

tratan talento extranjero? ¿Supera éste el talento nacional?

El Ministerio de Defensa al interior de cada uno de sus grupos, cuenta con cooperación de otras entidades, que pueden ser del sector público, privado o internacional. En el colCERT somos partners de la OEA y trabajamos en conjunto con ellos para cooperaciones internacionales entre los CERT de países de Latinoamérica y convenios con empresas del sector privado internacional. El apoyo de otros países no supera el talento nacional.

RS: ¿Cómo funciona la relación con la Corporación de Alta Tecnología? Sabemos de varios de sus desarrollos, entre ellos el primer simulador de vehículos blindados 4X4 o los relacionados con aeronaves o con buques, ¿existen desarrollos específicos relacionados con TIC? ¿Cuáles?

La relación con la Corporación es muy estrecha, en la medida en que es una de las empresas del grupo social empresarial para la defensa y es la llamada a ejecutar las Apuestas Sectoriales en materia de Ciencia, Tecnología e Innovación, que ha diseñado el Ministerio de Defensa Nacional. Las dos apuestas que se están ejecutando –modelación y simulación y sensores- tienen un alto contenido de TIC, toda vez que son en gran medida desarrollo de software y protocolos de comunicaciones y electrónica. Adicionalmente, la Corporación se ha especializado en desarrollo de software para la educación y entrenamiento de las Fuerzas, a través de Objetos Virtuales de Aprendizaje y CBT's (Computer Based Training).

RS: Finalizado el CONPES 3701, ¿está segura la continuidad de los entes creados para soportar la estrategia de ciberseguridad nacional?

El CONPES 3701 de 2011 busca generar lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país, la estratega nacional continúa en desarrollo, así como los entes creados.

Objetivos de colCERT

- Coordinar y asesorar a CSIRT's y entidades tanto del nivel público, como privado y de la sociedad civil, para responder ante incidentes informáticos.
- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.
- Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta técnica.
- Promover el desarrollo de capacidades locales/sectoriales, así como la creación de CSIRT's sectoriales para la gestión operativa

de los incidentes de ciberseguridad en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.

- Desarrollar y promover procedimientos, protocolos y guías de buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad para las infraestructuras críticas de la Nación, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.

- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad.

- Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.

- Fomentar un sistema de gestión de conocimiento relativo a la ciberdefensa y ciberseguridad, orientado a la mejora de los servicios prestados por el colCERT.

Servicios que ofrece

- Análisis de aplicaciones web
- Análisis infraestructura tecnológica
- Coordinación y gestión de incidentes
- Sensibilización en materia de seguridad informática

Dirección de Ciencia, Tecnología e Innovación

La Dirección de Ciencia, Tecnología e Innovación, tiene como función principal la definición de la línea estratégica en ciencia, tecnología e innovación (CTeI) del Sector Defensa, en el marco del programa de modernización de la Política Integral de Defensa y Seguridad para la Prosperidad. Para ello, esta Dirección articula la interacción entre el Sector y los demás actores, en aras de promover una estrecha relación Universidad-Empresa-Estado.

Para lograr que la CTeI apoye el cumplimiento de la misión constitucional de la Fuerza Pública, buscando alcanzar la autosuficiencia e independencia estratégica del Sector y el país, el Ministerio de Defensa Nacional (MDN) ha decidido concentrar sus esfuerzos en unas áreas tecnológicas que deben cumplir con las siguientes características: representar necesidades del sector y apoyar

el plan de guerra; constituirse en áreas tecnológicas transversales a todas las Fuerzas; tener una potencial aplicación dual (es decir en la sociedad, fuera del ámbito militar); y, ser sostenibles al largo plazo. Estas áreas tecnológicas han sido denominadas Apuestas o Programas Estratégicos y su desarrollo asegurará una independencia tecnológica nacional, lo cual llevará a convertirlas en un polo de desarrollo de la Nación, una vez estas hayan sido apropiadas por la sociedad. Los primeros programas en los que se concentrará el Ministerio de Defensa Nacional son modelación y simulación, radares, y salud operacional y contarán con el apoyo de entes territoriales, la academia y Colciencias, a través del Programa de Ciencia y Tecnología para Defensa y Seguridad.

**Respuestas obtenidas en coordinación con la Dirección de Comunicación Sectorial (Oficina de Prensa) del Ministerio de Defensa Nacional.*

Columnista Invitado

Desarrollo tecnológico:

un desafío hacia la independencia estratégica

Juanita Rodríguez Kattah

La innovación revoluciona los procesos que antes se adelantaban de manera tradicional, y genera mejoras sustanciales en los niveles estratégico, operacional y táctico. Nuestro compromiso es asentar un modelo tecnológico, que con posteridad, pueda tener aplicación dual y que repercuta en la consolidación del país como un referente en ciencia y tecnología.

La innovación y el desarrollo tecnológico han sido de gran importancia para los planes estratégicos de las Fuerzas Militares y de Policía en Colombia. La implementación de sistemas de información, comando y control, el gran avance en el campo de las comunicaciones y el perfeccionamiento de los sistemas de defensa empleados en combate pueden evaluarse a partir de los supuestos teóricos-estratégicos de Andrew Marshall, ex-director de la Oficina de Asesoramiento de la Oficina del Secretario de Defensa de los Estados Unidos, cuyo aporte se basa en analizar el impacto de los adelantos tecnológicos y científicos en el éxito de las operaciones militares en tiempos de paz y guerra.

De tal forma surgió la aproximación al tema de la Revolución en los Asuntos Militares, (RMA, por sus siglas en inglés) que determina que existe "[…] un cambio mayor en la naturaleza de la guerra, que es a su vez provocado por la innovadora aplicación de nuevas tecnologías que al combinarse con profundos cambios en la doctrina militar y en los conceptos operacionales y organizacionales, alteran de modo fundamental el carácter y la conducción de las operaciones militares"[1] demostrando que en la actualidad, la efectividad de cada una de las Fuerzas se encuentra ligada a estos condicionamientos.

Este soporte permite evaluar de qué manera el incremento del potencial y de las capacidades de las Fuerzas Militares tiene sus bases en el desarrollo de nuevas tecnologías para la defensa, razón por la que la Ciencia, la Tecnología y la Innovación (CTeI) se constituye en un objetivo de primer orden en la agenda del Ministerio de Defensa Nacional.

En esta medida, se ha incrementado en forma progresiva la tendencia en la que los desarrollos militares son fuertemente aprovechados para usos civiles, posibilitando para ambos sectores tanto el desarrollo y adquisición de equipos de uso compartido, como la asimilación de tecnologías críticas a menores costos.

Siguiendo esta pauta, la investigación con fines militares ha ido adquiriendo un papel estratégico para mejorar la capacidad de proyección y el sostenimiento del pie de fuerza, por lo que el Sector Defensa (SD) juega un rol relevante, al integrar todos los procesos que fortalezcan las capacidades operacionales del Estado en el camino hacia la independencia estratégica y tecnológica.

En este escenario, la CTeI juega un papel fundamental, pues es la llamada a permitir que cada vez se vaya “más alto, más rápido, más lejos y con más potencia y que, además, nos permite disponer de los elementos de mando y control adecuados, adquirir la información necesaria para operar eficazmente, no causar daños innecesarios”[2], razón por la cual el proceso de modernización de las Fuerzas trae consigo

1 Watts, Barry D. *The Maturing Revolution in Military Affairs.* Washington D.C.: 2011.

2 Reino de España. Centro Superior de Estudios de la Defensa Nacional. CESEDEN. Monografías del CESEDEN, XII Jornadas Universidad Complutense de Madrid. “Investigación, Desarrollo e Innovación en la Seguridad y la Defensa”.

una apuesta por la innovación y el desarrollo tecnológico.

Ciencia, Tecnología e Innovación en el Ministerio de Defensa

En los últimos años la Dirección de Ciencia, Tecnología e Innovación del Ministerio de Defensa Nacional le ha apuntado a objetivos visibles que demuestren el ingenio de las Fuerzas, su capacidad de desarrollo tecnológico y la proyección tecnológica del sector.

Esto sustenta cómo "la autosuficiencia como principio rector de esta política busca generar procesos que permitirán al SD y al país acumular una base de conocimiento científico y tecnológico. Esta base llevará como consecuencia, a reducir la dependencia del sector de actores extranjeros en áreas estratégicas"[3].

Planes Estratégicos de Ciencia, Tecnología e Innovación

La gestión y administración de la CTeI, el fomento de la innovación, la generación de conocimiento mediante la investigación y el desarrollo tecnológico, y la utilización de dicho conocimiento en procesos de innovación y de producción permite alcanzar los objetivos misionales y sociales de la Fuerza Pública y del sector en su conjunto, en la medida en que se generen nuevos prototipos funcionales que cuenten con la propiedad de ser fácilmente escalables por la industria nacional y que permitan, a su vez, la sostenibilidad e independencia estratégica del sector y la posibilidad de aplicarla al ámbito civil.

Cada plan estratégico se concentra en una necesidad específica dentro de los roles y misiones de las Fuerzas, las cuales han venido desarrollando proyectos ambiciosos y de suma importancia para llevar a cabo sus operaciones. Así, la Armada Nacional, de la mano de Cotecmar, se propuso desarrollar una fragata 100% colombiana para el año 2025 aprovechando las capacidades adquiridas con el desarrollo de la Patrullera de Apoyo Fluvial, el sistema de armas barracuda, la fabricación de las OPV y el apoyo del clúster de empresas metalmecánicas.

Por su parte, la Fuerza Aérea Colombiana se encuentra trabajando en el desarrollo de un sistema de visualización, mando y control de radares, que ya se implementó y que tiene varias empresas internacionales interesadas en su licenciamiento.

El Ejército y la Policía Nacional hacen parte de un piloto que está desarrollando la Dirección de Ciencia, Tecnología e Innovación del Ministerio de Defensa para licenciar y transferir la tecnología incorporada a una camilla para la rápida atención de los heridos en combate (EJC), una barra de luces para las patrullas que permite la filmación de los operativos y un cono lumínico que procesa y reserva energía solar para operaciones nocturnas (PONAL) y cuya intención es que sea fabricada en el sector privado.

3 Dirección de Gestión de la Información y Tecnología, *Política de Ciencia, Tecnología e Innovación del Sector Defensa y Seguridad*, pág. 3 – 4, octubre de 2011.

Ambas instituciones ya cuentan con sus respectivas patentes de modelo de utilidad, por lo que en alianza con INN-pulsa[4] estamos llevando estos desarrollos hacia la aplicación civil.

Apuestas sectoriales o programas estratégicos

Los programas de desarrollo tecnológico que propenden por la autosuficiencia e independencia del sector en tecnologías críticas son denominados Apuestas Sectoriales o Programas Estratégicos. Así, la Dirección de Ciencia, Tecnología e Innovación del Ministerio de Defensa Nacional gerencia los programas cuya tecnología atienda a una necesidad operacional de alguna de las Fuerzas, tenga aplicación transversal en todas ellas (que les reporte beneficios a todas), que los proyectos que se deriven de la apuesta identificada sean financiera y técnicamente auto-sostenibles, y, que las tecnologías a desarrollar tengan un uso dual hacia el campo civil.

Una vez que en todo sentido se comprueba la viabilidad de la Apuesta, en compañía de expertos de las Fuerzas se elabora la Hoja de Ruta Tecnológica realizando una identificación de tecnologías que se priorizan para su apropiación y desarrollo. Esto implica conocer la situación actual de las capacidades del sector, el futuro deseado, las barreras tecnológicas que puedan presentarse y las soluciones ante las mismas.

4 INN-pulsa Colombia es la unidad del Gobierno Nacional creada para promover la innovación empresarial y el emprendimiento dinámico como motores para la competitividad y el desarrollo regional.

Las primeras hojas de ruta que se elaboraron se describen a continuación, en el orden seguido.

Modelación y simulación

Busca generar capacidades de escenarios virtuales para el entrenamiento táctico operacional de las Fuerzas Militares y la Policía Nacional. Para el 2018, Colombia será autosuficiente en el desarrollo de simuladores de talla mundial de cualquier aeronave, equipo militar o maquinaria de cualquier sector.

Esta Apuesta cuenta con financiación del Ministerio de Defensa Nacional y del Municipio de Villavicencio, ciudad que busca generar una nueva vocación tecnológica e industrial.

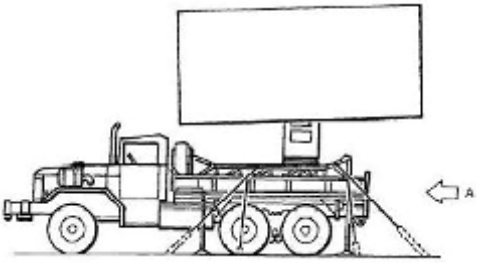
Esta Apuesta empezó con el desarrollo de simuladores tácticos operacionales, utilizando modelación y simulación estática y, hoy por hoy, la Corporación de Alta Tecnología para la Defensa -CODALTEC- está en el proceso de investigación para desarrollar simuladores con movimiento, próxima tecnología definida en la hoja de ruta (Imagen 1).

Bajo esta Apuesta se entregó el primer simulador de una aeronave remotamente tripulada- SIMART® y un simulador del vehículo blindado de transporte de tropa ligero con torreta de tiro diseñado y construido según las necesidades tácticas del Ejército Nacional. En marzo de 2014, se entregará a la Fuerza Aérea Colombiana, un simulador para avión monomotor tipo regional/utilitario turbohélice de corto alcance.

Imagen 1

Sensores

Busca que en Colombia se desarrolle el conocimiento y las capacidades para construir sistemas que permitan el desarrollo de tecnologías orientadas a cubrir las necesidades transversales de las Fuerzas, en las áreas de vigilancia y control del territorio nacional. De igual forma, se busca generar la aplicación dual de la tecnología apropiada por el Sector Defensa para apoyar el sector civil en temas como meteorología, atención de desastres, sector petrolero, entre otros.



Dentro de esta Apuesta se busca apoyar a las Fuerzas Armadas en la simulación de diferentes tipos de vehículos terrestres y aéreos, tripulados y no tripulados, por lo que estamos desarrollando Objetos Virtuales de Aprendizaje (OVA) y *Computer Based Training* (CBT) en nuestro proceso de incorporar Tecnologías de la Información y la Comunicación (TIC) para la Defensa.

Actualmente, está en implementación el “Proyecto Radar”, que permitirá adquirir capacidades en diseño, desarrollo y producción de un prototipo de radar de corto alcance que cubra las necesidades de las Fuerzas, en el área de vigilancia y detección temprana. Para su desarrollo se contará con la transferencia tecnológica de un gobierno extranjero.

Este proyecto será desarrollado por un equipo de 20 ingenieros colombianos

entre uniformados y civiles, con el apoyo del Ministerio de Defensa Nacional, la Gobernación del Meta, la Alcaldía de Villavicencio y Ecopetrol, bajo el proyecto "Fortalecimiento a la capacidad de las Fuerzas Militares".

Corporación de Alta Tecnología para la Defensa

Tanto la Apuesta de Modelación y Simulación como la de Sensores, están siendo desarrolladas por la Corporación de Alta Tecnología para la Defensa, entidad sin ánimo de lucro creada por el Ministerio de Defensa Nacional, cuyo objetivo es el desarrollo de las apuestas en áreas de electrónica y desarrollo de software, así como el apoyo de la gestión tecnológica de los proyectos de las Fuerzas que así lo requieran.

De este modo, CODALTEC busca gestionar la disminución de la brecha tecnológica del Sector Defensa en el país, proveyendo soluciones de tecnología para la industria. Esto ha motivado un gran ejercicio para integrar los sectores productivos público y privado con el fin de fortalecer la producción tecnológica nacional y territorial.

Adicionalmente, la Corporación de Alta Tecnología para la Defensa trabaja de la mano de las empresas privadas que conforman la base industrial de defensa, aprovechando sus capacidades e integrándolas. Un ejemplo de ello, es la Apuesta de Simulación que, para el desarrollo de sus simuladores, realizó alianzas estratégicas con empresas nacionales reconocidas en este medio como Kirvit, Antares y Palcort, para el desarrollo de las cabinas y demás piezas necesarias para los simuladores antes mencionados.

Con la creación de CODALTEC, se realizó la mayor apuesta humana en el departamento del Meta para el desarrollo de tecnología de Defensa, con la generación de 38 empleos calificados para profesionales metenses de las más altas calidades, de los cuáles 33 hacen parte del Programa de Modelación y Simulación y cinco del programa de Sensores.

Conclusiones

La Ciencia, la Tecnología y la Innovación en el Sector Defensa tienen como función apoyar los Planes Espada de Honor de las Fuerzas Militares y la Estrategia Corazón Verde de la Policía Nacional; es decir, la misión constitucional de las Fuerza Pública.

En ese sentido, se han diseñado las Apuestas Sectoriales o Programas Estratégicos y de la misma manera los Planes Estratégicos de las Fuerzas en la materia.

Este es el lineamiento de los proyectos que desarrollan las empresas del GSED. Pero más allá, el sector está dando un paso, hasta ahora no recorrido. Se trata de licenciar tecnología desarrollada dentro de las Fuerzas para que sea escalada a nivel industrial a través de la base industrial de defensa nacional.

Este primer paso permitirá, no sólo que las Fuerzas puedan aprovechar las soluciones generadas, sino atraer rega-

lías que permitan seguir desarrollando proyectos de Ciencia, Tecnología e Innovación dentro del sector. Este ejercicio permitirá, a su vez, que la tecnología militar se derive en soluciones para el ámbito civil y con ello se apoyará el desarrollo nacional de manera general.

Juanita Rodríguez Kattah. *Directora de Ciencia, Tecnología e Innovación del Ministerio de Defensa Nacional desde agosto de 2010. Es abogada de la Universidad de los Andes, con estudios en derecho de los negocios internacionales y en derecho aplicable a la conducción de las hostilidades. Anteriormente, estuvo a cargo del diseño, redacción y desarrollo de la política sectorial de Offset y tiene experiencia de más de 7 años en reconocidas firmas de abogados nacionales y en la Oficina del Alto Comisionado para la Paz de la Presidencia de la República.*

XIV Jornada Internacional de Seguridad Informática

HACKING RECARGADO

Junio 16 y 17 de 2014

Cámara de Comercio de Bogotá, Sede Chapinero.

Llamada a trabajos XIV Jornada Internacional de Seguridad Informática

Fechas importantes:

* Abril 6 de 2014 - Fecha límite de recepción de artículos

* Mayo 6 al 11 de 2014 - Notificación de Aceptación o Rechazo de artículos y comentarios de los evaluadores

* Junio 1 de 2014 - Envío de artículos corregidos para publicación final y el PPT con máximo 10 transparencias.

Llamado a conferencistas - Charlas para la XIV Jornada Nacional de Seguridad Informática ACIS 2014

Fechas importantes:

* Marzo 22 de 2014 - Fecha límite de recepción de propuestas

* Mayo 6 al 11 de 2014 - Notificación para los autores aceptados.

* Junio 1 de 2014 - Envío de la presentación final.

* Junio 16 y 17 de 2014 - Realización XIV Jornadas Internacionales de Seguridad Informática

ACIS

Asociación Colombiana de Ingenieros de Sistemas
Calle 93 No. 13 - 32 of. 102
Tels: 616 1407
616 1409 - 610 4842
Bogotá, D.C.
www.acis.org.co

Cualquier inquietud adicional sobre esta iniciativa favor comunicarse al correo administrador@acis.org.co

Sector Defensa y TI. Sistemas de investigación

Comando General, Ejército, Fuerza Aérea Colombiana (FAC) y Policía Nacional acudieron a la cita para debatir en torno a las Tecnologías de Información y Comunicaciones TIC.

Sara Gallardo M.

El ciberespacio como teatro de operaciones similar al de tierra, mar, aire y espacio. El marco legal que regula las estrategias de ciberseguridad nacional. Las vidas humanas y los referentes contemplados en la aplicación segura de las Tecnologías de Información y las Comunicaciones, TIC. La relación entre Ingeniería Electrónica y la Ingeniería de Sistemas en el diseño de dispositivos de seguridad. La nube y la seguridad de la nación. Y, el uso de software, fueron los temas planteados en la reunión.

A la mesa de debate acudieron representantes de las distintas Fuerzas Militares del país, grupo encabezado por el brigadier general Oscar Alberto Quintero G., jefe de Control Comunicaciones y Sistemas del Comando General de las Fuerzas Armadas, acompañado por el coronel Alberto González, director de Ciencia y Tecnología del Ejército; el coronel Mauricio Zuleta L., director de Ciencia y Tecnología de la Fuerza Aérea Colombiana (FAC); la capitán Samira Andrea Ramos R., oficial de Seguridad Infor-

Manuel Dávila Sguerra, moderador del foro, abrió el debate preguntando sobre el ciberespacio.

mática del Ejército; y, el subteniente Alejandro Garzón U. de Telemática y Electrónica de la Policía Nacional. Como invitado también asistió Jeimy J. Cano, profesor de la universidad de Los Andes.

Francisco Rueda, director de la revista y Manuel Dávila, decano de Ingeniería de Uniminuto y moderador del foro dieron la bienvenida a los asistentes y agradecieron su presencia.

"Sería muy interesante poder sacar en claro cuáles son los grandes desafíos que tienen ustedes en los asuntos relacionados con la Informática, para estudiar de qué manera podemos unir esfuerzos", señaló Francisco Rueda.

Por su parte, el brigadier general Oscar Alberto Quintero tomó la vocería del grupo: "para nosotros es muy interesante entrar en contacto con entidades privadas como esta para trabajar en conjunto sobre asuntos relacionados con las tecnologías y el futuro. La ciberguerra, la ciberdefensa son temas de especial importancia, teniendo en cuenta lo que ha sucedido en otros países. La amenaza del fusil, del misil o del cañón está siendo reemplazada por la amenaza a través de los sistemas informáticos que pueden destruir y desestabilizar completamente un país", indicó el uniformado.

Después de la presentación protocolaria de los participantes, comenzó el debate.

Manuel Dávila
Moderador del foro
Decano Facultad de Ingeniería
Uniminuto

¿Debe ser el ciberespacio otro teatro de operaciones similar al de tierra, mar, aire y espacio? Si la respuesta es afirmativa, ¿qué deben hacer las Fuerzas Militares y qué están haciendo en este sentido?

Brigadier General Oscar Alberto Quintero González
Jefatura Control Comunicaciones y Sistemas
Comando General Ministerio de Defensa

Nosotros miramos el entorno internacional de los ataques cibernéticos donde no hay fronteras; nos referenciamos, por ejemplo, en hechos tales como la destrucción de los generadores de energía, en la que no hubo confrontación directa entre el Estado y las Fuerzas, sino en el ciberespacio. Eso nos lleva a hablar de ejércitos cibernéticos con una connotación de escuadrones de reconocimiento, de inteligencia, de ataque y destrucción. Es necesario establecer unos límites para el empleo del ciberespacio, disponer de unas leyes similares a las que rigen el espacio físico, que contemplen el nuevo tipo de vida que se genera.

Jeimy J. Cano
Profesor
Universidad de Los Andes

Siguiendo la evolución del Estado en estos temas de ciberseguridad, una de las acciones claves que se deben adelantar es declarar el ciberespacio como otro teatro de operaciones equivalente a tierra, mar, aire y espacio. Es decir, modificar la Ley de Defensa Nacional para incluirlo como un nuevo escenario para control de la soberanía, con lo cual quedaría incluido de inmediato dentro del presupuesto nacional. El CONPES 3701 establece los lineamientos de la estrategia de ciberseguridad de la nación, creando el Centro Cibernético Policial, el Comando Conjunto Cibernético y el ColCERT, tres nuevos entes que articulan el tema en el país. En este contexto, ¿cómo van a soportar de aquí en adelante el presupuesto de estas ins-

El brigadier general Oscar Quintero se refirió a los ejércitos cibernéticos.

Para el coronel Alberto González, el ciberespacio es clave en las operaciones militares.

tancias, teniendo en cuenta, que la vigencia del CONPES termina en diciembre de 2014 y que aún no está contemplado en la Ley de Defensa Nacional?

Brigadier General Oscar Alberto Quintero

En este momento se está desarrollando la ley y por ello para nosotros es muy importante que la Asociación Colombiana de Ingenieros de Sistemas (Acis), nos acompañe en ese proceso. Los países deben conformar una ley que les permita actuar sin tanto recelo, toda vez que en el ciberespacio no existen las fronteras, el enemigo ataca silencioso y se va. Es inminente una ley de cara al futuro, que se acoja al ordenamiento nacional, de manera que no se dé lugar a la incertidumbre. Las películas de ficción, orientan en términos de las tecnologías de información y las comunicaciones, TIC.

Coronel Alberto González
Director de Ciencia y Tecnología
Ejército Nacional

El ciberespacio ya es considerado un teatro de operaciones, no sólo por los acontecimientos de índole local, sino mundial. Tenemos muchos referentes como la situación en Irán con el reactor nuclear, objeto de una manipulación a través de las redes informáticas, lo cual obstaculizó la reacción de dicho equipo y lo dejó paralizado por más de una década. En ese orden de ideas, para el Ejército de Colombia el ciberespacio juega un papel muy importante dentro del desarrollo de las operaciones militares. Quien maneje el ciberespacio y tenga el dominio de la información y de ese escenario lleva la delantera respecto a las intenciones de los enemigos del Estado. Coincido en la importancia de la creación del Comando Conjunto Cibernético orientado a la defensa, a proteger la infraes-

tructura crítica de las Fuerzas Militares de la nación. Eso nos va a garantizar nuestra propia protección y un paso hacia adelante para frenar las pretensiones de los enemigos del Estado en el ciberespacio.

Coronel Mauricio Zuleta L.
Director Ciencia y Tecnología
Fuerza Aérea Colombiana (FAC)

El concepto que nosotros manejamos se orienta al manejo de un sistema en el que todo está interconectado. La libreta de ahorros se acabó y es la analogía perfecta para indicar la evolución tecnológica. Todo está completamente sistematizado y lo realizamos a través de la red. Cuando hablamos de las áreas críticas de una nación, todo está basado en sistemas electrónicos, virtuales. En otras palabras, todo los conceptos antecedidos con la letra "e", ejemplo e-commerce, entre otras, representan un escenario supremamente complejo, al que debemos garantizar un ambiente seguro; de lo contrario, tendríamos efectos nefastos, por ejemplo, sobre la economía del país. En otras palabras, perderíamos la guerra. Tenemos referentes en el mundo como la Fuerza Aérea de Estados Unidos, cuya misión es muy sencilla: "ganar la guerra en el aire, el espacio y en el ciberespacio". En algún momento todo girará en torno a lo electrónico, basta citar los drones y el debate generado al respecto. Todo eso se mueve a través de TIC, cualquier cosa que lo afecte paraliza una Fuerza Aérea. No sé si recuerdan la película en la que un hacker muy joven penetró los sistemas de defensa rusos y norteamericanos e inició juegos de guerra que sucedieron en la realidad. Ese es el escenario al que nos estamos enfrentando. El radiograma, el télex ya no existen y forman parte del pasado. Hoy en día las órdenes nos pueden

Según el coronel Mauricio Zuleta, el ambiente de las TIC es muy complejo y se debe garantizar su protección.

A los riesgos de la información transportada en medios electrónicos, se refirió el subteniente Alejandro Garzón.

llegar de manera instantánea, por medios que no son seguros como el correo electrónico con nuevas coordenadas para el cambio de rumbo. Las posibilidades de ser vulnerados se aumentan exponencialmente cada vez que surge un nuevo desarrollo tecnológico. De ahí que sea necesario considerar el ciberespacio como un teatro de operaciones mucho más defensivo, estamos muy expuestos. La mejor defensa va a ser el ataque para no exponer la vida de los hombres y bloquear todo un sistema de defensa de una nación.

Subteniente Alejandro Garzón Urbina

Escuela de Telemática y Electrónica
Policía Nacional

Durante los últimos años la evolución de la tecnología es un escenario complejo de vital importancia en cualquier organización e incluso de manera personal. Basta citar el sistema de almacenamiento, a través del cual es posible guardar gran cantidad de información en medios electrónicos, utilizados para cometer una infinidad de actividades ilícitas. Resulta difícil demostrar quién se encuentra al otro lado del ciberespacio. Sin embargo, deja huellas digitales, que a la luz del conocimiento de las TIC permiten demostrar que el análisis de la información digital coadyuva a la Administración de Justicia en las diferentes conductas punibles. La Escuela de Telemática y Electrónica ha venido innovando en una serie de tecnologías que van a la vanguardia en el servicio de policía, como eje fundamental en la política de gobierno sobre la lucha para la convivencia pacífica, Hemos tratado de unir esfuerzos entre el Ejército, la Fuerza Aérea, la Armada y la Policía.

Capitán Samira Andrea Ramos R.
Oficial de Seguridad Informática
Dirección Telemática del Ejército Nacional

Para la defensa de los sistemas informáticos de las FF.MM en el ciberespacio contamos con infinitas herramientas, la tecnología siempre ha estado a la mano y el Ejército Nacional las ha implementado para la defensa de su infraestructura. Sin embargo, tenemos que revisar a fondo el tema de normatividad, políticas y sistemas de defensa jurídicos dentro de la Fuerza con las cuales podamos actuar en estos temas. Aunque se han creado ciertas leyes como la de protección de datos y algunos delitos tipificados en el Código Penal, existen carencias para actuar en un marco de legalidad institucional en materia de seguridad. Debemos pensar en la creación de una constitución para el ciberespacio, que norme nuestro proceder en el mismo.

Manuel Dávila

Las plataformas de la nube en las que ponemos nuestros datos, yo las denomino la "caja fuerte del vecino", Googledocs, gmail, entre otras. Allí ponemos nuestra información, que es casi lo mismo que poner dinero, sin pensar que son plataformas localizadas en otros países. En Utah, por ejemplo, acabaron de crear un centro de datos muy grande y Estados Unidos advirtió: "-Voy a leer todo lo que me llegue por razones de seguridad y si está encriptado lo voy a desencriptar, en la medida de lo posible". Cito esto como contexto de la siguiente pregunta: Teniendo en cuenta que el uso de la nube es ya un estándar en el mundo, ¿cómo ven ustedes los peligros de la apertura de las plataformas versus la seguridad nacional?

Para la capitán Samira Andrea Ramos es necesario revisar el marco jurídico que regula las acciones relacionadas con las TIC.

La protección de la información confidencial y privada es el gran reto de las Fuerzas Militares, de acuerdo con Jeimy J. Cano.

Coronel Mauricio Zuleta L.

Ese concepto es bastante crítico, porque dentro de lo que yo conozco de la Fuerza Aérea, manejamos cierta cantidad de servidores y los volúmenes de información requieren una infraestructura muy robusta que, en términos presupuestales, no estamos en capacidad de afrontar. De ahí que muchos de estos sistemas los utilicemos para poner información no crítica, pero se trata de diversificarla para redistribuir la infraestructura con la que contamos y aprovechar esos espacios, ante las carencias. Obviamente, contamos con sistemas cerrados, una Intranet con servidores para manejar exclusivamente la información operativa. Pero, por la movilidad y la dinámica de la FAC, toda vez que en muchas oportunidades necesitamos movernos en diferentes direcciones, existe el riesgo. Es un asunto complejo para considerar con el área de Telemática de la Fuerza Aérea, encargada de tales asuntos. La idea es que siempre existan sistemas cerrados, autocontenidos, que no permitan salidas de información. En algunas de las operaciones realizadas, se encontraron en los computadores los nombres de los pilotos, con todos sus datos. En tal sentido, es necesario ser muy estrictos y cuidadosos. Aunque en la Fuerza Aérea se ha tratado de mantener espacios muy cerrados, ha existido fuga de información.

Jeimy J. Cano

El gran reto de las Fuerzas Militares y los encargados de la seguridad de la información, en general, es la protección de la información confidencial y privada, en un ambiente abierto y público. Ese es el gran reto. Si seguimos pensando en el concepto de sistemas cerrados, basados en el concepto de seguridad y control en entornos

conocidos como el de los años 70, soportados en equipos como el 3270 de IBM y similares, no es viable asegurar un nivel de protección adecuado, toda vez que hoy tenemos un mundo abierto, móvil e instantáneo. Ese es el foco de quienes trabajamos en seguridad. De hecho, los modelos recientes planteados en informes como el de Gartner [1] para 2020, señalan que la prevención será inefectiva. Es decir, el tema ahora es identificar y clasificar la información, monitoreo activo y respuesta a incidentes. "Tarde o temprano tu radio será un Phillips". La brecha de seguridad se va a producir. El problema es ¿qué hacer cuando la brecha se presente?, ¿cómo se va a actuar?

Coronel Mauricio Zuleta L.

¿Cuál es la brecha en Colombia sobre temas de seguridad, vs. el resto del mundo?

Jeimy J. Cano

La seguridad de la información la podemos ver, entre otras aproximaciones, como una función donde intervienen personas, procesos y tecnología. En el primer caso, la información no se percibe como un activo y a las personas les parece fácil manejarla sin la protección adecuada. La transportan en una USB y si este dispositivo se pierde, no hay preocupación ni consecuencias. El segundo punto se refiere a procesos. Es decir, la información viaja y tiene valor sólo en el contexto de los procesos de las compañías. Sin embargo, no se conoce ni se tiene claridad sobre la clasificación (nivel de sensibilidad) de la misma y menos su estrategia de tratamiento. En este sentido, muy pocas compañías en el país tienen clasificada la información. Si le agregamos el componente tecnológico, sin una adecuada clasificación, la

Según el coronel Alberto González, el Ejército Nacional es consciente de las vulnerabilidades en el manejo de la información.

seguridad se ve nuevamente afectada. La tecnología es un medio para lograr el nivel de aseguramiento deseado e igualmente susceptible a fallas conocidas o vectores de ataque desconocidos. De manera que todos estos componentes puestos sobre la mesa, lo que generan es un "caldo de cultivo" para que la inseguridad de la información nos sorprenda. El problema no es llegar al 100% de seguridad, situación que no es viable, toda vez que la ausencia de riesgo no es posible. El tema es declarar un umbral de exposición que estamos dispuestos a asumir, para saber cómo actuar cuando los incidentes se materialicen.

Coronel Mauricio Zuleta L.
Nosotros iniciamos un proyecto financiado por Colciencias que debe empezar este año, sobre el mejor modelo a utilizar para mover grandes volúmenes de información de manera segura, a través de redes públicas. En estos asuntos habrá cientos de ofertas, de conceptos. ¿No sería mejor tener un solo modelo interno? o ¿generar varios modelos independientes? Sobre todo asociándolos a las cadenas logísticas. Nosotros tenemos 42 tipos diferentes de aviones, es decir, 42 proveedores, 42 aspectos diferentes qué atender. ¿Sería un esfuerzo nacional para adelantar o más bien un esfuerzo institucional para que las cosas funcionen?

Jeimy J. Cano
Un esfuerzo institucional.

Coronel Alberto González
Quiero hacer un aporte relacionado con la “caja fuerte del vecino”. El Ejército de Colombia es consciente de las vulnerabilidades en el manejo de la información. La dirección de Informática hace varios años se fusionó con la

dirección de Telemática y, en este momento, las comunicaciones están liderando todo lo relacionado con el manejo de la información. Los expertos en han tomado las medidas necesarias para minimizar esos riesgos que a diario se presentan. Algunas muy sencillas, como el uso de memorias USB. Los computadores nuestros no tienen habilitados esos puertos para que la información pueda salir de los equipos. Son medidas sencillas que han funcionado. Por supuesto, no ha sido fácil que los operadores de estos equipos entiendan el porqué, pero poco a poco, lo estamos logrando en todos los niveles de la institución. Los asuntos de carácter estratégico son ultrasecretos, se tiene un manejo confiable dentro de la entidad, para minimizar al máximo que la información vaya a esa "caja fuerte del vecino".

Manuel Dávila
¿Eso quiere decir que no utilizan la nube?

Capitán Samira A. Ramos R.
Actualmente, no estamos utilizando servicios en la nube pública de proveedores externos. Sin embargo una de las metas que persigue la Dirección de Telemática es precisamente permitir la movilidad de nuestros usuarios, y que ellos puedan disponer de la tecnología. De tal manera, el Ejército ha publicado en Internet muchos de sus servicios de información y de comunicación. Las acciones del área de seguridad informática y otras dependencias, tanto del Ejército como de Unidades superiores, son las de monitorear, detectar, controlar y ver qué está sucediendo con la información y el comportamiento de nuestros usuarios, basada en la identificación de las amena-

La capitán Samira Ramos explicó el alcance en el uso de la nube.

Jeimy J. Cano describió el marco jurídico que regula a los servidores públicos.

zas, riesgo y el impacto que esto genere. Así mismo, estamos evaluando llevar otros servicios como el correo electrónico y archivos compartidos a la nube privada, bajo una infraestructura segura, para permitir flexibilidad en el quehacer laboral. Sobre el tema de fuga de información se ha trabajado con sistemas que no impiden el uso de dispositivos como las USB, sino que encriptan la información que se transporta, y a la que puede acceder sólo quien está autorizado para ello. Lo que hemos visto sobre seguridad es la fuga de información a nivel interno, lo que requiere de un trabajo importante en la educación del manejo responsable de la información, por parte de nuestros funcionarios. Es así como en el Ejército se realizan campañas de sensibilización y se enseña a los funcionarios en el manejo adecuado de la información y los sistemas que los pueden apoyar en la consecución de dicho objetivo.

Jeimy J. Cano

Dado que ustedes son servidores públicos, el Código Único Disciplinario, la Ley 734 de 2002, en el Artículo 34, trae los deberes de los servidores públicos. En el numeral quinto se declara que es un deber de todo servidor público proteger la información a la cual tiene acceso por ocasión de su cargo. De manera explícita dice:"*5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos".* Esto no es un favor del funcionario hacia la institución, sino un deber funcional. Ese es un tema relevante para el ejercicio de la función

pública. Además, la Ley 734 en el artículo 48, donde se detallan las faltas gravísimas, en el numeral 43 establece aquella conducta catalogada como gravísima frente a inadecuados tratamientos de la información:"*43. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas".* Tales elementos dentro del contexto de la Fuerza Pública, deben ser también interiorizados, en la medida en que todo ellos son servidores públicos.

Coronel Mauricio Zuleta L.

Pero también se trata de un problema cultural. Estamos en el cambio de dos generaciones. Una que se formó con el lápiz y el papel y otra que está creciendo a punta de iPAD. La tecnología va mucho más rápido que la cultura sobre el manejo de la información dentro de las organizaciones. En poco tiempo la caligrafía será un asunto romántico. Hay que mirar ese entorno con el propósito de plantear estrategias no represivas, sino estimulantes hacia el buen manejo de la información. Por ejemplo, si un funcionario está fuera de la oficina lo ideal sería que pudiera avanzar y ganar tiempo trabajando en un equipo móvil. Sin embargo, lo que prevalece es el medio en el que nos estamos moviendo, en el sentido de la velocidad de los desarrollos tecnológicos y el cambio cultural. Desde nuestra perspectiva, la tecnología móvil hace el desempeño mucho más eficiente, pero todavía no manejamos la suficiente cultura dentro de un marco de seguridad y buen manejo de

El coronel Mauricio Zuleta enfatizó en la necesidad de fomentar una cultura hacia las nuevas tecnologías.

la información. Así que dentro de la cultura de seguridad es necesario ir introduciendo los conceptos en forma paulatina, para que no genere rechazo y pueda llegar a que los equipos no se utilicen y los funcionarios recurran a sus equipos personales. A veces los sistemas de la Fuerza Aérea, tienen tantas cosas, que prender el computador se demora 25 minutos, tiempo que significa pérdida para cualquier compañía. ¿Cuánto puede representar en dinero la demora de encendido? Ahí es donde el esfuerzo debe ser conjunto desde todas las perspectivas, no solo represiva, sino hay que mirar cómo se va migrando. En la medida en que las exigencias del entorno actual se orientan a que las personas se adapten para cumplir con su misión. De ahí que sea necesario poner en marcha una cultura que oriente las acciones de las personas dentro de la institución.

Jeimy J. Cano

En los tres componentes que rodean la seguridad de la información hoy en día: personas, procesos y tecnología, la cultura es un elemento fundamental. Dada la constitución de las organizaciones actuales, y particularmente la de las Fuerzas Militares, la seguridad de la información se basa en el concepto de comando y control. Es decir, "o las órdenes se cumplen o la milicia se acaba", como versa el adagio popular. En este contexto, ¿cómo se aprende en esta cultura? Los elementos disciplinarios son inherentes a ese tipo cultura. Por tanto, existe un conflicto entre dos culturas (una orientada a compartir y otra dirigida a proteger), y cuando anoto el tema disciplinario es porque es inherente al oficio mismo del tema militar y la manera como se moviliza el asunto. Por tanto, la pregunta es: "-Y si yo no cumplo con esto ¿qué me pasa?". La cultura latinoamericana generalmente requiere de un requisito normativo obligatorio para implementar cosas, mientras no exista, sencillamente no hacemos nada.

Coronel Mauricio Zuleta L.

La dinámica varía y existen acciones que demandan inmediatez, en medio de decisiones muy graves. A veces, se exigen respuestas rápidas.

Jeimy J. Cano

Es una declaración que ustedes deben hacer. Lo importante es tener visible cuál es el riesgo al tomar esas decisiones. Esa claridad debe ser generalizada. Cuando pensamos en seguridad pensamos en el 100% y eso no va a ocurrir, porque vivimos en un entorno natural de inseguridad. Lo importante es establecer cuál es el umbral de riesgo que estamos dispuestos a afrontar frente a un incidente.

Coronel Mauricio Zuleta L.

Hago la analogía con el diseño de un avión, con cientos de sistemas diferentes y de componentes. Los de aerodinámica quieren que sea perfecto, el de carga útil lo quiere lleno de bombas; el de propulsión un avión de 18 motores con tanques de gasolina; el de fabricación lo que quiere son dos palos pegados con una puntilla, para que sea lo más fácil. Llegar al punto medio de todo es lo difícil, ese balance es complicado. A veces, se imponen ciertos criterios que tienden a minar la importancia de los demás sistemas. La idea es interoperar como sistemas, dentro de un engranaje muy balanceado y eficiente.

Francisco Rueda, director de la revista, indicó cómo las redes sociales han influenciado, entre los jóvenes, el concepto de privacidad de la información.

Subteniente Alejandro Garzón

El uso de la información en una empresa pública o privada es cada día más vulnerable. El simple hecho de acceder a un sistema informático lo deja expuesto a que la información sea alterada o sustraída. Esta problemática se presenta de cierta manera por no cumplir los protocolos de seguridad y los estándares establecidos con responsabilidad. En otras palabras, la manipulación y administración de la información depende de nosotros, aplicando las normas disciplinarias de confidencialidad y reserva con un minucioso seguimiento de la protección de la información.

Francisco Rueda

El concepto que se manejaba antes de privacidad de la información ya no es tan importante. Es un tema cultural. Para los jóvenes el tema no es relevante. Ese es un gran desafío. Los jóvenes que van llegando a las instituciones traen la cultura de compartir su información privada (fotos, familia, etc.) y ahí está el riesgo.

Coronel Alberto González

Con relación al tema de las normas jurídicas, el desconocimiento de las mismas no nos exime de su cumplimiento. Eso nos lo enseñan desde el primer día de ingreso a las Fuerzas Militares. Estamos en la obligación de cumplirlas, porque son la esencia del militar. Se presentan situaciones de pérdida de información, no por desconocimiento de la norma, sino por los tentáculos de los enemigos o de quienes tienen pretensiones en contra nuestra, influyen a través de nosotros mismos, comprando conciencias, penetrando nuestras propias filas.

Infortunadamente, dentro de nuestras filas existen personas con una doble moral, capaces de vender su propio Ejército. A quienes han sido detectados se les ha aplicado las normas disciplinarias y penales. Esas acciones las hemos tomado, se que en todas las Fuerzas ha sido así. A veces el dinero compra conciencias, somos conscientes de eso, situación que se presenta en muchos niveles del mando. La obligación es hacer entender a nuestros hombres el camino correcto.

Manuel Dávila

Teniendo en cuenta que las instituciones orientadas a la seguridad y la defensa ciudadana están relacionadas con la vida de las personas, ¿qué referentes o formalismos estudian ustedes para la aplicación segura de las tecnologías?

Coronel Alberto González

Dentro de nuestras líneas de investigación enfatizamos en los proyectos orientados a minimizar el efecto de los artefactos explosivos. También trabajamos en lo relacionado con las enfermedades tropicales, degenerativas, apoyados en los lineamientos del Ministerio de Protección Social y el área de Sanidad Militar. Tales proyectos se desarrollan en el marco de la ética, porque estamos utilizando hombres para determinar su viabilidad para la implantación en las Fuerzas Militares y en la población. Así mismo trabajamos en la detección de explosivos para bloquear las minas y frenar su activación. Desarrollamos inhibidores de señales en todas las gamas de frecuencia utilizados por los terroristas. También contemplamos una etapa de concientización de los hombres para que en las salas de operaciones tomen

Manuel Dávila y el coronel Mauricio Zuleta hablan sobre los referentes en la aplicación segura de las tecnologías.

El foro generó el interés de las Fuerzas Militares en trabajar de manera conjunta sobre diferentes proyectos.

las medidas respectivas. Involucramos tecnología y electrónica, dentro de un plan educativo.

Coronel Mauricio Zuleta

Nosotros trabajamos en dos grandes áreas. Una tiene que ver con doctrina aérea y espacial, basada en el análisis de las acciones adelantadas por la FAC en toda su historia, en procura de que las siguientes sean mucho menos letales. Estamos creando un sistema de información alrededor de las operaciones aéreas para la mejor toma de decisiones, por parte de los pilotos. Estudiamos la doctrina para minimizar los efectos colaterales y aumentar la protección de la población civil. El último eje es el de medicina aeroespacial, en el que se han hecho grandes avances, en términos de la fisiología del aviador, que han sido transferidos a varias aerolíneas. Así mismo, tenemos un centro de investigación en este campo con un grupo amplio de médicos dedicados a la experimentación. De igual manera, sobre apropiación social, para que todos los desarrollos logrados sean incorporados a la vida cotidiana. Hace unos años desarrollamos un casco para los aviadores que fue ofrecido a la sociedad civil. El GPS es un ejemplo de los desarrollos provenientes del sector defensa y seguridad de los desarrollos, se generalizó por completo. Y eso es lo que buscamos, además de promover una dinámica industrial con la empresa privada y la universidad para el desarrollo tecnológico, en una participación 70% externa y 30% interna.

Jeimy J. Cano

Observando lo que ocurre en otras latitudes, hay eventos internacionales diseñados para mostrar los desarro-

llos e investigaciones realizadas por las Fuerzas Militares. Buscar esa apertura a través de ese tipo de encuentros, permite aunar esfuerzos y compartir conocimiento y experiencias.

Coronel Mauricio Zuleta L.

En los Estados Unidos la defensa genera desarrollos. Allá tienen prohibido comprar tecnología, no pueden importar, deben fabricarlo allá, como una condición de seguro prevalente. Desde 1902 ellos crearon la Ley de Tecnología Crítica, en la que se hablaba de simuladores y automatización. Uno de los grandes retos que encontré cuando empecé a trabajar en tecnología fue llegar a la universidad privada y a la pública. Esta última continúa siendo tabú, aunque se han hecho grandes avances. El mismo Colciencias se abstenía de financiar algún proyecto relacionado con Defensa, porque involucraba según ellos la guerra. Pero, la Defensa es un tema muy amplio, menos del .5% tiene que ver con tecnología que le quita la vida a otras personas.

Coronel Alberto González

No solamente las universidades o las instituciones educativas públicas, sino también las privadas. Uno llega con un proyecto de Defensa, y lo rechazan. Se intenta acceder a una Gobernación o una Alcaldía y tampoco. En ese sentido, nos falta y le falta a la Academia avanzar para lograr la integración con la Fuerza Pública. Hemos logrado integración en temas científicos en áreas como las enfermedades tropicales, en los que trabajamos con universidades, ministerios y otras instituciones. En el tema de minas estamos trabajando, creando conciencia de que se trata de un asunto que compete a todos.

Hubo consenso en la necesidad de ampliar la participación en encuentros internacionales.

La Defensa es un asunto que el Estado debe trabajar con la población, indicó Jeimy J. Cano.

Jeimy J. Cano

La Defensa es un asunto que el Estado debe trabajar entre la población para comprenderlo en profundidad; fomentar su sensibilización y alcance es muy importante. Estas deben ser iniciativas de doble vía: de las Fuerzas Militares hacia la población y de la población a las Fuerzas.

Coronel Mauricio Zuleta L.

La historia colombiana se ha desarrollado en medio del conflicto que le ha costado al país muchísimo dinero. Hace unos años se creó el programa de Tecnologías para el Desarrollo de la Defensa, con el patrocinio de Colciencias y muy poca financiación, pero el espacio está dado. Un ejemplo puede ser un tanque de guerra, cuyas partes en su mayoría nada tienen que ver con el tema bélico y se parecen más a un tractor, por su sistema hidráulico. En tal sentido, si se pensara en un desarrollo local con ese tipo de proyectos, significaría abrir la puerta de avances muy importantes, para minimizar la dependencia tecnológica. En esos asuntos hay un tema cultural de por medio, al considerar que todo lo importado es lo bueno. El 95% de los desarrollos en defensa son aplicables a la vida cotidiana del ser humano.

Coronel Alberto González

Y esos asuntos cobran mucha vigencia en la actualidad del país. La situación política, los diálogos para el proceso de paz que algún día se cristalizará. Y como dicen los jefes y lo repetimos nosotros los soldados, quienes más rezan por la paz son los soldados, porque somos los que sufrimos las más hondas heridas de la guerra. Con las universidades venimos trabajando para promover la imagen del Ejército del futuro, que busca atender las regiones más apartadas del país, afectadas

por el flagelo del terrorismo. Hoy en día tenemos conocimiento para exportar, producto de nuestro avance. Somos potencia mundial en operaciones de selva con visores nocturnos. La inteligencia es preponderante en cualquier escenario. Las misiones internacionales van a cobrar mayor vigencia. Y también en la protección del medio ambiente. El año pasado estuvimos presentando nuestros proyectos en el evento que realiza la Asociación para el Avance de la Ciencia. Tenemos planes con varias universidades, entre ellas Uniminuto, Los Andes, Eafit y otras de similar importancia.

Subteniente Alejandro Garzón
La Policía Nacional ha conservado el acercamiento a la comunidad en ciudades, barrios y comunidades enteras, a lo largo y ancho del país, como un principio de apoyo en la protección y el bienestar del ciudadano, con actividades de avances tecnológicos tendientes a la protección del territorio nacional de mar, tierra, aire y el ciberespacio, en donde prima la perseverancia en la investigaciones tecnológicas para el beneficio de la sociedad en general.

Manuel Dávila
Otra inquietud está relacionada sobre automatización y robótica. La ingeniería Electrónica está cambiando, se está volviendo un comodity. ¿Qué piensan ustedes al respecto, sobre el estado del arte en ese sentido?

Subteniente Alejandro Garzón
La Escuela de Telemática y Electrónica de la Policía Nacional ha venido cumpliendo unos de los objetivos primordiales en el seguimiento, orienta-

Llegar a las comunidades del país con los avances tecnológicos, es una prioridad, según el subteniente Alejandro Garzón.

Las vidas humanas, una prioridad frente al uso de las nuevas tecnologías. Asunto que ocupó a los asistentes.

ción, creación y aporte de herramientas tecnológicas enmarcadas en las políticas del desarrollo científico y tecnológico policial, trabajando de manera correlacionada con entes públicos y privados. El estudio realizado dentro del campo de la robótica se establece como una herramienta móvil de observación de áreas y la desactivación de artefactos explosivos, diseñado de manera autónoma con sistemas electrónicos, hidráulicos, software y hardware que permiten una mejor seguridad en al campo de la seguridad ciudadana rural y urbana.

Coronel Alberto González

Nosotros partimos de la experiencia de los demás y lo que queremos es diseñar nuestros propios proyectos en robótica y automatización, algunos ya en marcha. Trabajamos también la Escuela de Comunicaciones para depender cada vez en menor proporción de la tecnología foránea.

Coronel Mauricio Zuleta L.

Las tareas que nosotros adelantamos están orientadas a la protección de las vidas humanas. Los drones, por ejemplo, son una muestra para minimizar las pérdidas de vidas. El gran motor en el mundo se dirige a reemplazar al ser humano por robots en escenarios hostiles, con máquinas que puedan desarrollar la actividad. Es más fácil ver una máquina destruida que un soldado sangrando.

Capitán Samira A. Ramos

En el Ejército Nacional se han desarrollado e implementado muchos servicios y sistemas tecnológicos para el cumplimiento de la misión. Me refiero

al desarrollo de sistemas de información relacionados con la logística, el componente operacional, información de personal, sistemas de georeferenciación, etc. En temas de comunicaciones, no sólo utilizamos los medios analógicos, sino otros sistemas de telefonía IP e imagen digital para apoyar la toma de decisiones y garantizar el mando y control. Todos estos sistemas y cualquier proyecto tecnológico de la Fuerza son tratados con la rigurosidad de seguridad como con la innovación tecnológica. Conocemos de la importancia que tienen los servicios tecnológicos en el marco institucional y sabemos aún más que, dentro de ellos, se almacena o transmiten datos que no sólo ayudan en el cumplimiento misional del Ejército, sino que por su contenido podrían incluso exponer la vida de nuestros hombres o la seguridad de la Nación. Por ello es un deber proteger nuestros sistemas y la información institucional.

Manuel Dávila
¿Trabajan con software libre?

Capitán Samira A. Ramos
No desarrollamos bajo software libre, aunque hemos probado algunos sistemas no críticos bajo esa plataforma, como los de gestión documental. Pero, en general, trabajamos con software de marca, licenciado, para cumplir con los requerimientos de ley.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Autora del libro "Lo que cuesta el abuso del poder". Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res, empresa de 1800 empleados; corresponsal de la revista IN de Lanchile. Es editora de esta publicación.*

Educación, promotora del crecimiento y calidad académica de la Fuerza Pública Colombiana

El presente artículo pretende ofrecer un contexto de lo adelantado en materia de política educativa en el Ministerio de Defensa Nacional, a fin de unificar los procesos educativos de formación, capacitación y entrenamiento. Actividades realizadas dentro de las escuelas y centros de formación de las Fuerzas Armadas y la Policía Nacional, en búsqueda de la profesionalización del servicio y la excelencia académica de los hombres y mujeres que las conforman.

Nidia Patricia Herrera G.

Desde el año 2007 el Ministerio de Defensa de Colombia dentro del proyecto de "Reestructuración de la Educación de la Fuerza Pública", en el Marco de la Política de Consolidación de la Seguridad Democrática, definió los lineamientos ideológicos y estructurales para la "Educación y Formación", a través de la consolidación de un sistema educativo integral, moderno y flexible, que le entregue al país hombres y mujeres de indeclinable espíritu militar o policial, ejemplo de virtudes y valores éticos, con excelen-

te preparación profesional, fundamentada en el desarrollo humano, conocido como el Sistema Educativo de la Fuerzas Armadas –SEFA-.

Su función primordial es la de dinamizar los procesos de formación, actualización, capacitación, instrucción y entrenamiento de la Fuerza Pública (Fuerzas Militares y Policía Nacional), articulándolos con la misión institucional y políticas del Ministerio de Defensa y Ministerio de Educación Nacional.

Para ello se soporta en cuatro subsistemas[1]:

- **Subsistema de Doctrina:** Este subsistema reúne la doctrina Conjunta (entre las Fuerzas Militares), Coordinada (entre Fuerzas Militares y Policía Nacional), combinada (con Fuerzas Militares de otros países) y de Fuerza. Le permite a la Fuerzas Armadas afianzar el proceso de investigación, análisis, priorización, socialización, producción, difusión y evaluación de la doctrina de cada una de las fuerzas dentro del marco legal.

- **Subsistema de Aseguramiento de la Calidad.** Es una organización que no sólo evalúa estándares y características de calidad, sino que asegura su presencia y sostenibilidad en el proceso educativo. Fomenta la cultura de la autoevaluación y autorregulación.

- **Subsistema de Certificación Militar y Policial.** Este es un Subsistema que certifica y asegura la calidad de los procesos de formación, actualización, capacitación, instrucción y entrenamiento, desarrollados a través de acciones orientadas a promover, gestionar y mejorar en forma permanente las competencias individuales, colectivas y de los líderes, así como la eficacia de los proceso inherentes, los programas y las instituciones, de acuerdo con las especialidades y la misión de cada fuerza.

- **Subsistema de Investigación, Desarrollo e Innovación.** A través de este subsistema las Fuerzas Armadas proponen soluciones o recomendaciones innovadoras, basadas en investigación de alto rigor técnico, tecnológico y científico, que involucran la transferencia de conocimiento, problemas, necesidades o desafíos al interior de cada fuerza. Su ejercicio está estrechamente relacionado con los ejes temáticos prioritarios institucionales, así como las líneas de acción estratégica del SEFA.

Así mismo, los elementos que conforman el Sistema Educativo de las Fuerzas Armadas son:

- Escuelas, Centros e Institutos de Formación, Capacitación, Instrucción y Entrenamiento.

- Principios del Sistema Educativo.

- Cultura Institucional.

- Marco Normativo.

- Procesos Educativos.

[1] PESE – Plan Estratégico del Sistema Educativo de la Fuerzas Armadas.

- Políticas Educativas.
- Modelo Pedagógico.
- Organización Educativa.
- Niveles Educativos.

A través de su organización y estructura, desarrolla los currículos que respetan los niveles y particularidades de cada Fuerza, en coherencia con la misión institucional, como se muestra en la figura 1.

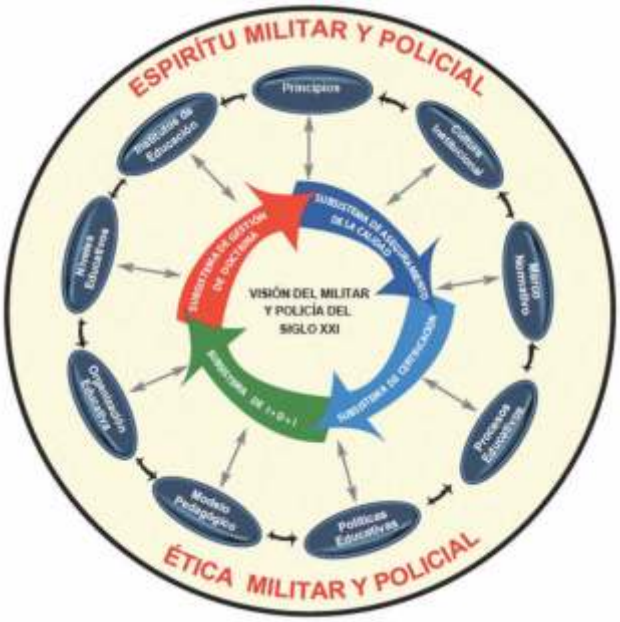
Es importante recordar que las Fuerzas Militares y la Policía Nacional han sido instituidas legítimamente en la Constitución Política, en donde se determina su misionalidad. Y es aquí, donde se destaca el papel preponderante de los procesos educativos, para la formación profesional militar y policial, que garanticen, con efectividad, la responsabilidad impuesta por nuestra carta magna.

Esta acción educativa se encuentra inserta en un amplio sistema de valores, núcleo básico que da sentido a lo militar y policial[2]. Los principios y valores son de tal importancia en los procesos formativos, porque actúan como el conjunto de creencias construidas colectivamente para otorgar estabilidad a los procesos de transformación y cambio.

El Proyecto Educativo de las Fuerzas Armadas, determina los siguientes valores como elementos sustantivos en la organización y actividades que adelantan las Fuerzas Armadas:

[2] PEFA. Proyecto Educativo de la Fuerzas Armadas.

Figura 1: Subsistema y elementos constitutivos SEFA



- Honor: Es la consistencia de la esencia moral del ser con los principios que ha prometido defender y acatar.

- Justicia: Es dar a cada quien lo que le corresponde por sus méritos y actos.

- Honestidad: Es actuar con rectitud, sinceridad, transparencia y legalidad.

- Lealtad: Es la plena manifestación de fidelidad hacia la verdad, proyectada a uno mismo, la familia, la institución y la patria.

- Valor: Es actuar con coraje, arrojo, intrepidez y prudencia para defender el bienestar de la Nación.

- Responsabilidad: Es cumplir una obligación, así como asumir y aceptar las consecuencias de nuestros actos libres y conscientes.

- Disciplina: Es reconocer y cumplir las normas y disposiciones sociales e institucionales.

- Respeto: Es la atención digna con que se considera a los demás, trátese de personas, ideas, creencias, tradiciones, cosas o de la naturaleza de su totalidad.

- Compromiso: Es la obligación moral del cumplimiento de los deberes, obligaciones y servicios, con el Estado, la sociedad, la familia y la institución.

- Solidaridad: Es el sentimiento que lleva a las personas a apoyarse y a ayudarse mutuamente.

- Servicio: Es hacer algo a favor de otra persona, institución o a la sociedad en general.

- Transparencia: Es actuar en el marco de los principios y valores institucionales que garantizan la legitimidad.

Igualmente, el SEFA cuenta con políticas que constituyen un conjunto de directrices para proyectar el quehacer educativo hacia metas de calidad y sirven de respuesta a la necesidad de tener continuidad en el tiempo y en los procesos educativos de las Fuerzas Armadas.

Las metas

- Reforzar la formación en las “Competencias del Ser”.

- Potenciar la Educación Profesional Militar y Policial.

- Transformar a la Institución Armada en una organización de aprendizaje.

- Educar de manera ininterrumpida y ascendente.

- Redimensionar los currículos para fundamentarlos en competencias.

- Establecer un modelo educativo institucional de alta calidad.

- Implementar la formación por ciclos propedéuticos.

- Aprender una o más lenguas extranjeras.

- Privilegiar el autoaprendizaje significativo.

- Incorporar las tecnologías de la información y la comunicación TIC a los procesos educativos.

- Fortalecer la formación para el liderazgo militar y policial.

Incorporación de mediaciones pedagógicas y tecnológicas

El apoyo de las mediaciones pedagógicas y tecnológicas adelantadas en las Fuerzas Militares y la Policía Nacional en sus procesos educativos, se constituye en un ecosistema integrado a la naturaleza de la organización de forma planificada, cuya ventaja significa un nivel de interacción que supera las barreras espacio temporales, permitiendo adelantar un proceso estratégico de gestión.

Se ha logrado incorporar a través de la adquisición de portales educativos, plataformas de administración del aprendizaje LMS, bases de datos digitales, correos electrónicos institucionales, y otro número de tecnologías, además del diseño académico y curricular de programas educativos en diferentes modalidades, tales como las reflejadas en la figura 2.

Para el diseño de estos programas de formación, capacitación, instrucción y entrenamiento, se toman como bases estándares internacionales de calidad y de diseño instruccional, como lo muestra la Figura 3.

Fase 1. Análisis

Se enmarca dentro de un estudio académico, administrativo, financiero y de perfectibilidad que permita sustentar la necesidad y pertinencia de incorporación de mediaciones pedagógicas y tecnológicas, en los programas académicos que desarrolla la institución.

Figura. 2: Modalidades programas académicos

Figura 3: Diseño Instruccional de Programas Académicos

Fase 2. El diseño académico y producción de mediaciones pedagógicas

Esta fase involucra las actividades de concepción y diseño curricular, así como las adecuaciones metodológicas y de autoría de contenidos que deben adelantarse para la producción de materiales educativos, actividades de aprendizaje, guionización y adecuaciones pedagógicas de materiales complementarios.

Fase 3. El diseño y producción de mediaciones tecnológicas

Esta fase involucra las actividades de diseño instruccional y gráfico para la incorporación de tecnologías y estrategias e-learning de los programas nuevos y/o los ya existentes que deseen desarrollarse, bajo la metodología de educación virtual o con apoyo tecnológico.

Fase 4. Evaluación

La evaluación como último elemento del diseño instruccional sirve de base para tomar decisiones, tales como el enfoque teórico de los cursos; ajustes para lograr mayor pertinencia y pertenencia de las actividades de aprendizaje y de los contenidos; coherencia con el modelo educativo institucional para la modalidad seleccionada; actualización de textos y otros materiales de apoyo; calidad y pertinencia del diseño gráfico; claridad en las indicaciones, calidad y funcionalidad de la estructura de navegación; además de la claridad y pertinencia de los objetivos propuestos.

Como resultado de este trabajo, que a la fecha completa siete años en su implementación, representa un gran avance en el desarrollo curricular, incorporación tecnológica, cobertura y estructuración de lineamientos de calidad. Características que han permitido a las diferentes instancias que las componen, fundamentarse y convertirse poco a poco en organizaciones de aprendizaje, de investigación científica y tecnológica, generadoras de conocimiento.

Referencias

[1] PESE – Plan Estratégico del Sistema Educativo de la Fuerzas Armadas. 2007 – 2019. Ministerio de Defensa Nacional. República de Colombia. 2008.

[2] PEFA- Proyecto Educativo de las Fuerzas Armadas. Ministerio de Defensa Nacional. República de Colombia. 2008.

***Nidia Patricia Herrera García**. Coordinadora de Educación Virtual en la Escuela Superior de Guerra. Miembro del Comité TIC del Ministerio de Defensa Nacional. Asesora Pedagógica y consultora en Educación virtual y estándares de calidad en e-learning. Docente universitaria e investigadora en diferentes Instituciones de Educación Superior. Magister en Tecnología Educativa del Tecnológico de Monterrey. Especialista en Docencia Universitaria de la Universidad Militar Nueva Granada. Administradora de Empresas de la Universidad EAN.*

Dos

Ciencia y Tecnología en el Ejército Nacional de Colombia

El presente artículo muestra el contexto en el que se desarrollan las actividades de investigación y desarrollo tecnológico (I+D+i) en el sector defensa, con el propósito de dar a conocer las prácticas y resultados obtenidos de estas actividades.

Coronel Alberto González G.

El Sistema de Ciencia y Tecnología del Ejército Nacional fue creado en el año 2009 a partir de la activación de la Dirección de Ciencia y Tecnología. Sin embargo, la brecha existente entre éste y sus pares alrededor del mundo aún es grande. Es necesario conceptualizar el objetivo de la investigación y el desarrollo tecnológico en el contexto del sector defensa e implementar estrategias al corto y mediano plazo que fortalezcan e instituyan los esfuerzos innovadores, producto de las especiales necesidades de la fuerza.

La directiva permanente 0120 del 28 de Mayo de 2013 materializa los objetivos concebidos para el Sistema de Ciencia y Tecnología del Ejército (SICTE. No obstante, para que se puedan desarrollar, es necesario que la acción de los componentes del SICTE esté alineada con estos objetivos.

1. La investigación, el desarrollo tecnológico e innovación

Para ambientar el desarrollo de este documento es relevante remitirse a la definición básica de I+D+i, desde la cual este aborda el trabajo creativo llevado a cabo de forma sistemática para incrementar el volumen de conocimientos del hombre y la sociedad, así como el uso de estos conocimientos en aplicaciones reales (OECD, 2003). A pesar de la claridad existente sobre el componente de innovación que rodea la definición de I+D+i, su interpretación es bastante subjetiva y está sujeta a diferentes interpretaciones (Harley, 2011).

Otro aspecto que vale la pena considerar es el concepto de innovación definido como la introducción de un nuevo o significativamente mejorado producto, proceso o método en las prácticas internas de la organización (OECD, 2005). Este documento hace énfasis en que las actividades innovadoras de una organización están constituidas por las operaciones científicas, tecnológicas, organizativas, financieras y comerciales que conllevan a la introducción de innovaciones, dentro de las cuales aparecen las de I+D+i, como un componente fundamental.

De esta manera, las actividades de I+D+i son la fuente formal de la que se desprenden las innovaciones por medio del ejercicio científico (Mark, Katz, Rahman, & Warren, 2008). Aunque existen discusiones alrededor del tema y en la literatura no es fácil encontrar un punto de consenso, la definición propuesta por (Jadad & Lorca Gómez, 2007) en la que se considera la investigación como "invertir dinero para obtener conocimiento" y la innovación "como invertir conocimiento para obtener dinero", parece ser un punto de partida válido.

Cabe decir que el consenso sí ha encontrado convergencia en los beneficios de la innovación, los cuales se asocian a la eficiencia, calidad de vida y crecimiento productivo convirtiéndose en un factor clave para cualquier economía. Esta situación que se analiza en detalle en la sección 3, ha permitido que los Gobiernos promuevan y promocionen a las organizaciones en términos de innovación.

Una vez conceptualizado el entorno de la I+D+i es necesario evaluar su coherencia con el sector defensa. Éste contribuye directamente en los resultados en seguridad y defensa del país, facilitando su autosostenibilidad. También le permite a las industrias de defensa nacionales responder mejor a los requerimientos especializados de las operaciones armadas (Harley, 2011). Así mismo, contribuye para que la sociedad en la que se encuentra inmersa disfrute de posibles *spin-off*[1] tecnológicos (Ruttan, 2006).

2. Relevancia del I+D en el sector defensa

Esta reflexión encuentra su punto inicial en evidenciar los beneficios de

[1] Un spin-off tecnológico son compañías que pertenecen a las siguientes categorías: (i) compañías que tienen inversión patrimonial de una universidad, (ii) compañías que licencian tecnología de un centro de tecnología o universidad, (iii) compañías fundadas por universidades o empresas del sector público, (iv) compañías que se establecen directamente por un centro de desarrollo tecnológico (Callan, 2001).

contar con un sector defensa sustentado en un direccionamiento hacia la innovación, como lo recomienda el documento CONPES 3582 (DNP, 2009).

Aunque los casos de éxito de las actividades de I+D+i son numerosos y se han presentado en diferentes contextos y países, como se aprecia en la sección 4, la supremacía de los Estados Unidos en estos temas hace que se considere un referente por excelencia.

En esta sección se analizarán algunos de los resultados de mayor relevancia logrados por las actividades de I+D+i en el sector defensa.

La **industria aeroespacial,** fue en gran medida concebida desde la División de Comunicaciones del Ejército de los Estados Unidos al adquirir el primer aeroplano de ese ejército directamente de los hermanos Wright. Posteriormente durante la primera guerra mundial se creó la NACA considerada la madre de la NASA, encargada de la investigación aeronáutica, además Boeing participó activamente en el desarrollo de aeronaves para la guerra, incluso el Boeing 747 fue concebido primero para uso militar.

En junio de 1942 el Ejército de los Estados Unidos inició las investigaciones en **energía nuclear,** por medio de la construcción de una red de laboratorios y ciudades como Oak Ridge, Hanford y Los Alamos. Una vez la bomba atómica fue utilizada, también se empezó a integrar la tecnología nuclear en los reactores de los submarinos.

El Laboratorio de Balística del Ejército de Estados Unidos diseño el primer **computador**, llamado ENIAC para agilizar los cálculos matemáticos, incluso las necesidades de la investigación sobre radares de la Fuerza Aérea permitió que IBM desarrollará el primer computador personal.

Las investigaciones en Bell correspondientes a la **industria de semiconductores** se financiaron en gran parte por la División de Comunicaciones del Ejército de Estados Unidos. En 1960, al menos el 80% de las ventas de semiconductores, se dirigían al sector defensa.

A finales de los años 60 la Agencia para Proyectos de Investigación Avanzada del Departamento de Defensa desarrolló la red ARPANET, cuya arquitectura consideraba el acceso de terminales individuales por medio de una conexión telefónica. Sin embargo, sólo hasta 1990 el computador personal permitió que el **internet** comenzara a ser utilizado con las mismas características de ARPANET.

Finalmente, la **industria espacial** nació por medio de las necesidades de inteligencia de los ejércitos, sobre todo cuando la USSR colocó en órbita el satélite Sputnik en 1957. En 1959 la Fuerza Aérea de los Estados Unidos lanzó el satélite de reconocimiento CORONA, cuyas misiones de I+D son de reconocimiento para los sistemas de información geográfica y pronóstico del clima.

3. El entorno de I+D

En el contexto internacional de I+D+i en el sector defensa, es necesario

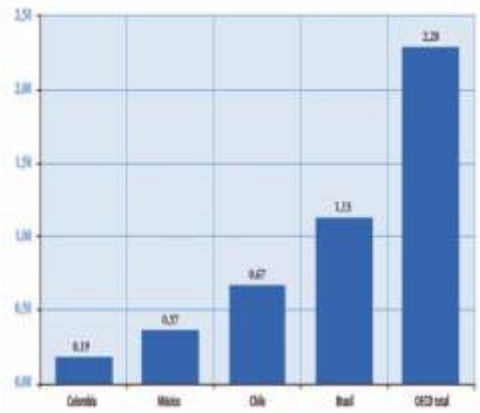
considerar las cifras agregadas disponibles en la Organización para la Cooperación y el Desarrollo Económico (OCDE. Los datos de carácter nacional están consignados principalmente en el Departamento Administrativo de Ciencia, Tecnología e Innovación de Colombia (Colciencias), teniendo en cuenta que Colombia hasta el año anterior es parte de la OCDE.

Es necesario considerar las tendencias que rigen actualmente los procesos de I+D+i en el sector defensa en las diferentes naciones. Cabe resaltar que de acuerdo con (Harley, 2011) la noción de I+D+i y las cuentas nacionales pueden verse afectadas por un sinnúmero de variables. Para llevar a cabo este análisis se analizaron países con estadísticas disponibles en las bases de datos de la OECD (Organización para la Cooperación y el Desarrollo Económico) (OECD, 2010) y que por su PIB son comparables en su capacidad económica con Colombia, basándose en las estadísticas del Banco Mundial (World Bank, 2011).

En la Gráfica 1 se observan los resultados del análisis realizado.

Infortunadamente, a nivel nacional no hay información desagregada de la inversión realizada en I+D+i por el sector defensa[2]; sin embargo, de acuerdo con las estadísticas disponibles (Colciencias, 2012), hasta la fecha se han invertido 18,95 millones de dólares; contra 357,89 millones de dólares invertidos por el sector gubernamental.

Con el ánimo de complementar los datos recopilados es importante mencionar que la inversión de los Estados Unidos en I+D+i alcanza los 72 mil millones dólares, una proporción 1:4000 con nuestro país. Otros referentes son Corea del Sur y el Reino Unido, con una inversión aproximada de 2 mil millones de dólares, e Israel, cuya información es de carácter confidencial.



Gráfica 1. Inversión en el Sector Defensa de I+D en millones de dólares
Fuente: (OECD, 2010)

En el caso de Estados Unidos sus capacidades científicas son tales, que la tercera parte de los científicos del país están vinculados al sector defensa, otro dato relevante es que de acuerdo con el informe presentado por (Congressional Research Service, 2013), el sector defensa absorbe el 50,6% de la inversión en I+D+i del sector público. Así mismo las líneas que recibieron mayor financiación fueron el Desarrollo de Sistemas Operativos y el

[2] Esta situación obedece a que el Programa de Ciencia, Tecnología e Innovación en Seguridad y Defensa aún no aparece en las estadísticas de Colciencias (Colciencias, 2012).

Desarrollo de Componentes, evidenciando que tan sólo se invirtió el 9,5% en investigación mientras que el desarrollo tecnológico involucró el 85% de la inversión.

En el caso español, la existencia de la Dirección General de Armamento y Material involucra la coordinación de más de 379 empresas dedicadas a proveer productos al sector defensa o incluso a exportarlos a otras naciones. Las ventas de estas empresas se dirigen principalmente a los sectores aeronáutico y naval. De forma paralela la Estrategia de Tecnología e Innovación para la Defensa (ETID) se enmarca en las áreas de actuación de Armamento, Plataformas, TIC e ISTAR (Intelligence, Surveillance, Target Acquisition & Reconanaissance).

Corea del Sur cuenta con la Agencia para el Desarrollo de la Defensa (ADD) cuyo objetivo es desarrollar proyectos de desarrollo para el sector defensa, como actores principales se identifican: Ministerio de Defensa, Fuerzas Armadas, el Programa de Administración de Adquisiciones para la Defensa (DAPA) y la Agencia para la Tecnología y la Calidad. Esta alianza se complementa también con las universidades e institutos encargados de la investigación básica y aplicada, además de la industria con el desarrollo tecnológico, prototipado y producción en masa.

El Maf´at se encarga de la administración para el desarrollo de las armas y la infraestructura tecnológica de Israel. Sus funciones contemplan la promoción, direccionamiento y coordinación de la ciencia y tecnología, establece alianzas estratégicas y opera el programa TALPIOT para la formación de recursos humanos. Su campo de acción logra integrar las necesidades operativas de las fuerzas con las industrias militares, aeroespaciales, de investigación biológica y universidades.

En Suramérica, Brasil por medio del Ministerio de Defensa ha configurado la administración de ciencia y tecnología a través de la Comisión Asesora de CyT para la Defensa Nacional (COMASSE) y la Comisión Militar de la Industria de la Defensa (CMID), desde donde se coordinan las actividades para tal fin. En la actualidad, tan sólo por medio de la convocatoria Innova Aerodefensa, invierte 1.428 millones de dólares, apoyando proyectos en las temáticas aeroespacial, defensa, seguridad pública y materiales especiales.

Por su parte, México enfoca sus avances tecnológicos principalmente desde la Dirección General de la Industria Militar DGIM y una red de institutos dedicados a la investigación y desarrollo en defensa,. Argentina opera fondos para la ciencia y tecnología por medio del Programa de investigación y desarrollo de la defensa (PIDDEF) y actualmente vincula más de 400 investigadores y 60 becarios.

4. El sistema de ciencia y tecnología del Ejército Nacional de Colombia

En Colombia el Ministerio de Defensa ha organizado sus esfuerzos en innovación por medio de la Dirección de Ciencia y Tecnología del Ministerio de Defensa, en la que se circunscribe el SICTE y en su cabeza la Dirección de

Ciencia y Tecnología (DITEC. Estos esfuerzos se encuentran soportados principalmente por la Política de Ciencia y Tecnología (DNP, 2009) y el apoyo del Departamento Administrativo de Ciencia, tecnología e Innovación (COLCIENCIAS).

Por medio de la Directiva 0120 se han definido de manera clara los actores que conforman el SICTE conformados por: (i) el comité directivo de Ciencia y Tecnología del Ejército Nacional; (ii) el comité de Ciencia y Tecnología de la Jefatura de Educación y Doctrina del Ejército; (iii) DITEC; (iv) unidades coordinadoras Centro Nacional de Entrenamiento CENAE, Centro de Educación Militar CEMIL, Escuela Militar de Cadetes ESMIC y Escuela de Suboficiales ESSUB y Unidades Operativas Mayores; y, (iv) los comités locales de ciencia y tecnología de las escuelas de formación y capacitación.

Esta estructura permite que en las escuelas se generen mayores puntos de convergencia del conocimiento, establecidos en torno a los grupos de investigación, generando los procesos que brindan al Ejército la posibilidad de mejorar sus capacidades como resultado del desarrollo de la ciencia y la tecnología, tal y como lo establece el objetivo 21 del mapa estratégico del Ejercito Nacional.

Así mismo, la directiva ha considerado establecer diez (10) líneas institucionales como lineamientos para establecer el interés y las necesidades de investigación en la fuerza:

- Detección y neutralización de artefactos explosivos y desminado.
- Aplicación de explosivos.
- Procesos, materiales e insumos para la ingeniería civil y militar.
- Actualización y mejoramiento de las tecnologías civiles y militares.
- Simulación y generación de entornos virtuales y digitales.
- Logística civil y militar.
- Medicina, biomedicina, sanidad y bienestar.
- Sistemas y procesos de seguridad y defensa.
- Investigación de operaciones y teoría de la decisión y doctrina.
- Pedagogía, desarrollo humano y social.

Finalmente, se ha logrado establecer una serie de incentivos para reconocer el trabajo investigativo, dándole el estatus que contribuye a la fuerza y al país. Entre estos incentivos aparecen dos tipos de acuerdo con su beneficiario.

Las distinciones son otorgadas a los miembros que logren resultados de investigación con impacto en la institución. Entre otros están (i) Distintivo de Investigación Científica; (ii) Becas de Estudios Superiores; (iii) Planes de Bienestar y comisiones en el exterior; (iv) Apoyo de traslados.

Los trabajos obtenidos también serán susceptibles de reconocimiento por medio de los siguientes mecanismos: (i) Apoyo en la participación de eventos; (ii) Apoyo en la elaboración de prototipos.

Este panorama busca fortalecer los procesos investigativos para lograr, no sólo cerrar la brecha existente entre el I+D+i en Colombia frente al mundo, sino que a largo plazo, nuestro país

sea un referente en el contexto internacional, gracias a su desarrollo y tecnología.

Conclusiones

Por medio del presente trabajo se realiza una recopilación sobre la importancia de la investigación y desarrollo en el sector defensa, como del panorama en el que se desarrollan estos procesos, tomando como punto de referencia otros sistemas de ciencia y tecnología del sector defensa alrededor del mundo.

También se enuncian los principales componentes de la Directiva 0120, pretendiendo darle un vistazo a la actualidad de la investigación, focalizada en el Ejército Nacional de Colombia.

Es claro que en términos de recursos, la brecha que separa nuestro país de otros países aún es significativa. Sin embargo, el fortalecimiento que ha logrado en los últimos cuatro años el SICTE, gracias a los esfuerzos realizados desde la DITEC, comienzan a dar frutos obedeciendo a las dinámicas de la investigación, cuyo curso de acción implica procesos que se estructuran lentamente.

Para finalizar, la DITEC considera oportuno seguir fortaleciendo el SICTE. Esta vez con miras a garantizar la visibilidad de sus procesos de investigación, facilitando los vínculos entre la sociedad y la comunidad científica, de tal manera que estos actores sean partícipes y beneficiarios de los adelantos tecnológicos generados.

Entre los mecanismos previstos se encuentran herramientas de difusión, firma de convenios de cooperación bilateral, participación en eventos y la divulgación en publicaciones especializadas.

Se prevé una participación cada vez más protagónica en Colciencias, de los grupos de investigación del Ejército Nacional, apoyándose también en el Programa Nacional de Seguridad y Defensa.

Referencias

[1] Colciencias. (2012). Capacidades en CT e I del Programa Nacional de CT e I en Seguridad y Defensa. Recuperado el 28 de 3 de 2012, de Colciencias: http://www.colciencias.gov.co/sites/default/files/ckeditor_files/files/Capacidades%20en%20CT%20e%20I%20del%20Programa%20de%20Defensa.pdf

[2] Colciencias. (2012). Indicadores de Ciencia y Tecnología 2012. Bogotá.- Congressional Research Service. (2013). Federal Research and Development Funding: FY2013. Washington D.C.

[3] DNP. (2009). Política Nacional de Ciencia, Tecnología e Innovación, Documento CONPES 3582. Bogotá.

[4] Harley, K. (2011). Defence R&D Spending A critical review of the economic data. World Economics, 12(1), 103-114.

[5] Jadad, A., & Lorca Gómez, J. (2007). Innovación no es lo mismo que “novedad”: El papel de las viejas Tecnologías en la promoción del Bienestar. Revistaesalud, 3(9).

[6] Mark, M., Katz, B., Rahman, S., & Warren, D. (2008). MetroPolicy: Shaping A New Federal Partnership for a Metropolitan Nation. Brookings Institution: Metropolitan Policy Program Report.

[7] OECD. (2003). The Measurement of Scientific and Technological Activities. Frascati Manual 2002: Proposed Standard Practice for Surveys on Research and Experimental Development. Paris: OECD.

[8] OECD. (2005). Oslo Manual: Guidelines for collecting and interpreting innovation data. Paris.

[9] OECD. (2010). Main Science and Technology Indicators. Paris.

[10] Ruttan, V. W. (2006). Is War Necessary for Economic Growth? Military Procurement and Technology Development. Staff Paper Series, 1-21.

[11] World Bank. (2011). World Development Indicators 2012. New York.

Coronel Alberto González Guerrero. *Director de Ciencia y Tecnología del Ejército Nacional*

Tres

Fuerzas Armadas de Colombia, grados y jerarquías

Recuento contextual y gráfico de las insignias y grados en las Fuerzas Armadas.

Capitán de Fragata Carlos Enrique Ortíz R.

Las Fuerzas Armadas de Colombia se encuentran conformadas por oficiales, suboficiales, soldados y personal no uniformado que integran el Ejército, la Armada Nacional, la Fuerza Aérea y la Policía.

La misión constitucional para cada una de ellas varía, de acuerdo con la formación, especialización y teatro de operaciones donde les corresponde asumir responsabilidades a sus integrantes.

Existen dos grandes formas de agrupar dichas Fuerzas por su organización y fines misionales. Las Fuerzas Militares integradas por el Ejército, la Armada y la Fuerza Aérea, también denominados Ejércitos de tierra, mar y aire. Sus integrantes son militares de carrera, regidos por un reglamento y fuero especial que les permite el cumplimiento de sus misiones, asignadas siempre en función de salvaguardar las fronteras del país de amenazas externas, estableciendo disuasión creíble para mantener un equilibrio estratégico y geopolítico en la región; asegurando en ese propósito, la vida, honra y bienes de los connacionales a lo largo y ancho del territorio patrio donde les corresponde operar.

Por su parte las Fuerzas Armadas, además de incluir a las tres Fuerzas Militares antes mencionadas, incluyen a la Policía Nacional, que es un cuerpo armado de naturaleza civil, con funciones centradas en el mantenimiento del orden interno y la seguridad social de los colombianos y contempla sus propios reglamentos para el cumplimiento de su misión, asignada en el desarrollo de la carrera profesional.

Ha sido nuestro conflicto interno de tantas décadas el que ha obligado a las Fuerzas de seguridad del Estado a realizar operaciones de tipo conjunto, que han ajustado la misión de todas las Fuerzas Armadas, para atender varias hipótesis de forma simultánea.

En tal sentido, el orden interno cobra relevancia por cuenta de la desestabilización que históricamente ha tenido Colombia, por el fenómeno de la subversión, las bandas criminales y la delincuencia común, grupos que han creado un escenario operacional complejo de atender por parte de las Fuerzas Armadas, en el mantenimiento del orden público y la democracia.

Hechas estas precisiones, defino entonces algunos de los términos relacionados con los grados, insignias y responsabilidades asignados por formación para la carrera de los oficiales y suboficiales de las Fuerzas Armadas de Colombia.

Los oficiales

Son los profesionales de las armas que integran las Fuerzas Armadas de Colombia, formados y capacitados para ejercer labores de comando especialmente, y cuya carrera en las escuelas de formación les permite ejercer el mando de sus hombres y mujeres bajo la misión asignada por la constitución misma.

Los estudios que los oficiales adelantan son de tipo superior. Se gradúan como profesionales en Ciencias Militares, Navales o Aeronáuticas.

Algunas escuelas ofrecen otras carreras universitarias dentro de su formación, entre ellas el derecho, la ingeniería Naval u oceanografía, entre otras.

Existen tres tipos de oficiales por rango en las Fuerzas Armadas.

Los oficiales subalternos, que son los tres primeros grados de la profesión, donde el personal se capacita y especializa desde cargos que lo van formando para ejercer labores de comando.

Los oficiales Superiores o los tres siguientes grados en el escalafón de la carrera y son aquellos que ya están formados para ejercer mando a nivel táctico y operativo.

Y los oficiales generales o de insignia, que son los últimos grados de la carrera del oficial que los lleva a ocupar cargos con responsabilidades estratégicas en el desarrollo de las diferentes responsabilidades asignadas para cada Fuerza.

Los suboficiales

Son los hombres y mujeres formados para ejercer el mando desde cargos técnicos y tácticos, cuya formación normalmente está centrada en carreras intermedias que les permiten la conducción de hombres y material de guerra en apoyo de las operaciones para cada Fuerza en particular.

Su formación en las escuelas los habilita para conocer diferentes áreas, dependiendo de la Fuerza y especialidad.

No obstante lo anterior, existen muchos suboficiales con carreras de pregrado, especialización y hasta maestría, que les permiten oficiar como asesores del mando en sus diferentes cargos, razón por la cual recientemente se creó una instancia donde se pueden desempeñar en cargos de asesor de comando en el pináculo de su carrera militar.

Por norma, en los suboficiales se basa el desarrollo de todo tipo de operaciones, toda vez que son quienes articulan y ejecutan las órdenes de los oficiales en los diferentes teatros de operación donde les corresponde actuar. Además de tener bajo su directa supervisión y control los soldados, infantes de marina, de aviación y policías que integran la base de las operaciones de la Fuerza pública en Colombia.

Grados y equivalencias, oficiales Fuerzas Armadas

En el Ejército y la Fuerza Aérea se usan los mismos grados y distintivos del mando.

En la Armada y la Policía Nacional tienen las siguientes equivalencias Figura 1.

Grados y equivalencias, suboficiales Fuerzas Armadas

Los grados de los Suboficiales en las Fuerzas Armadas son muy disímiles por la forma de sus insignias, pero guardan proporción en lo que a tiempo de servicio, antigüedad y requisitos existe entre ellos.

Las equivalencias para los Suboficiales del Ejército, la Armada, la Fuerza Aérea y Policía Nacional son en su orden, Figura 2.

La Policía Nacional cuenta con un nivel adicional denominado "Ejecutivo", conformado por Patrulleros, Subintendentes, Intendente, Intendente Jefe, Subcomisario y Comisaria, los cuales reemplazarán en el tiempo el escalafón de los Suboficiales.

Igualmente, la Infantería de Marina cuenta con oficiales y suboficiales con

Figura 1

General	Teniente General	Mayor General	Brigadier General	Coronel
Almirante	Almirante Escuadra	Vice - almirante	Contra - almirante	Capitán Navío
General	Teniente General	Mayor General	Brigadier General	Coronel

Figura 2

Sargento Mayor Comando Conjunto	Sargento Mayor de Comando	Sargento Mayor	Sargento Primero	Sargento Viceprimero
Suboficial Jefe de Comando Conjunto	Suboficial Jefe de Comando	Suboficial Jefe Técnico	Suboficial Jefe	Suboficial Primero
Jefe Técnico de Comando Conjunto	Jefe Técnico de Comando	Técnico Jefe	Técnico Subjefe	Técnico Primero
		Sargento Mayor	Sargento Primero	Sargento Viceprimero

Teniente Coronel	Mayor	Capitán	Teniente	Subteniente
Capitán Fragata	Capitán Corbeta	Teniente Navío	Teniente Fragata	Teniente Corbeta
Teniente Coronel	Mayor	Capitán	Teniente	Subteniente

Sargento Segundo	Cabo Primero	Cabo segundo	Cabo tercero
Suboficial Segundo	Suboficial Tercero	Marinero Primero	Marinero segundo
Técnico Segundo	Técnico Tercero	Técnico Cuarto	Aerotécnico
Sargento Segundo	Cabo Primero	Cabo segundo	

grados proporcionales en denominación a los del Ejército Nacional.

Sus insignias son de color Rojo sobre fondo negro.

Nuestras Fuerzas Armadas rinden culto y homenaje a muchas tradiciones que vienen desde la época de la independencia, y son salvaguardas en todas las instituciones del Estado y la República.

La historia de nuestro país se ha escrito sobre la sangre de muchos héroes de la patria que siguen ofrendando su vida por todos y cada uno de los colombianos, tal y como reza la oración que soldados, marinos y pilotos recordamos todas las noches antes de pasar a descansar y que dice:

"Colombia Patria mía, te llevo con amor en mi corazón, creo en tu destino, y espero verte siempre grande respetada y libre.

En ti amo todo lo que me es querido, tus glorias, tu hermosura, mi hogar, las tumbas de mis mayores, mis creencias, el fruto de mis esfuerzos, y la realización de mis sueños.

Ser Soldado tuyo, es la mayor de mis glorias, y mi ambición más grande, es la de llevar con honor el título de Colombiano, y llegado el caso morir por defenderte".

Capitán de Fragata Carlos Enrique Ortíz R., *(Reserva Activa. Ingeniero Naval Electrónico.*

ENTER.CO

LA REVISTA DE TECNOLOGÍA NÚMERO UNO DEL PAÍS

Conozca los últimos lanzamientos del mundo tecnológico y acceda a consejos, noticias y guías prácticas para aprender a comprar y usar la tecnología.

Esta publicación, dirigida a todo aquel que le guste o quiera entender del tema, incluye secciones como movilidad, fotografía y video, sitios recomendados y pymes, que le permitirán sacarle provecho a los avances que la tecnología le brinda.

Para mayor información comuníquese al 7560200 en Bogotá y a nivel nacional al 018000180044

@eContent_ /eContentSAS www.econtent.net.co/enterco

daptiv PPM

Solución integral
para la administración
del portafolio
de proyectos

www.daptiv.com
www.cass.com.co

¿Que es Daptiv PPM?

Daptiv PPM es la herramienta líder en su tipo para la administración y colaboración de proyectos, permitiendo administrar eficientemente documentos, tareas, riesgos, cambios, costos y demás elementos propios de un proyecto.

Todo en un poderoso ambiente fácil y sencillo de operar. Puedes encontrar más información en Daptiv PPM **(www.daptiv.com)** o en CasS **(www.-cass.com.co)**, incluso se puede observar un video demostrativo para conocer las funcionalidades de la herramienta.

Los beneficios de operar sus proyectos con Daptiv PPM:

- Mayor visibilidad de todo lo que ocurre con el portafolio de proyectos.
- Automatización de reporte de estatus.
- Administración de recursos, horas por proyecto, costos, etc.
- Automatice todo el ciclo de vida del portafolio de proyectos.
- Integre las solicitudes de proyecto de los usuarios directamente desde su Intranet.
- Realice una calificación de solicitudes integrando criterios de negocio.
- Identifique facilmente el estatus del portafolio.
- Comparta y colabore con su equipo de manera más eficiente.
- Ofrece toda una solución para gestionar el portafolio desde un punto de vista de rentabilidad, riesgo y esfuerzo.

Avalado por analista

Gartner FORRESTER IDC *Analyze the Future*

Contáctenos

CasS

Carrera 13 No. 63 - 39 Oficina 602.
PBX: 571- 742 90 02.
Móvil: 311 279 86 81.
daptiv@cass.com.co.
Twitter: @cassriesgos.
Bogotá - Colombia