2 CONGRESO INTERNACIONAL EN TECNOLOGÍAS DE LA INFORMACIÓN Y CIBERSEGURIDAD

EMAVITIC

"Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia"

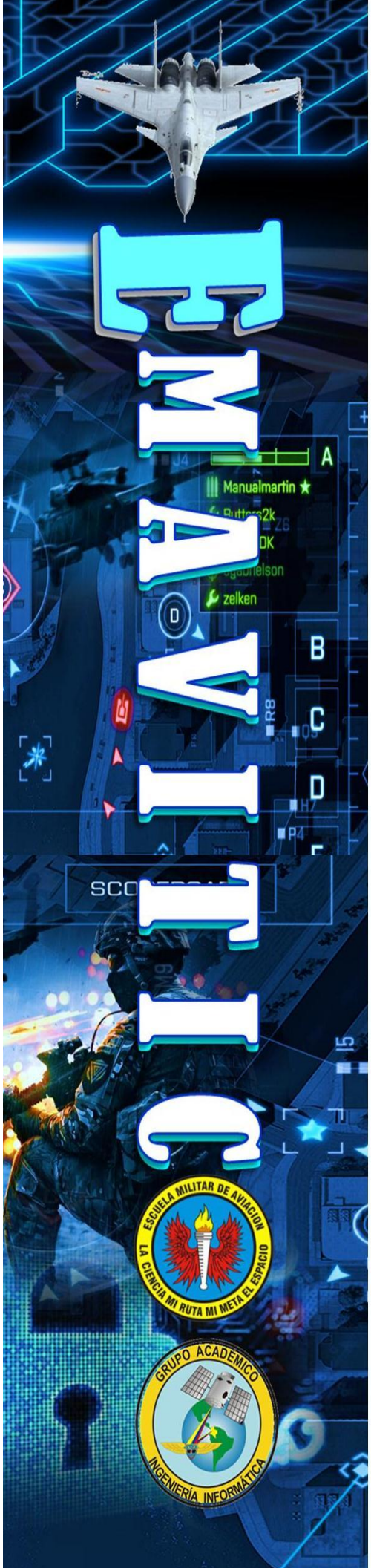
Octubre 25 2016

http://emavitic.wixsite.com/emavitic

ESCUELA MILITAR DE AVIACIÓN MARCO FIDEL SUÁREZ
PROGRAMA DE INGENIERÍA INFORMÁTICA

Lugar: Cra 8 No. 58-67 Barrio La Base, Cali, Valle del Cauca
Info: emavitic@emavirtual.edu.co
http://www.facebook.com/piinfemavitic

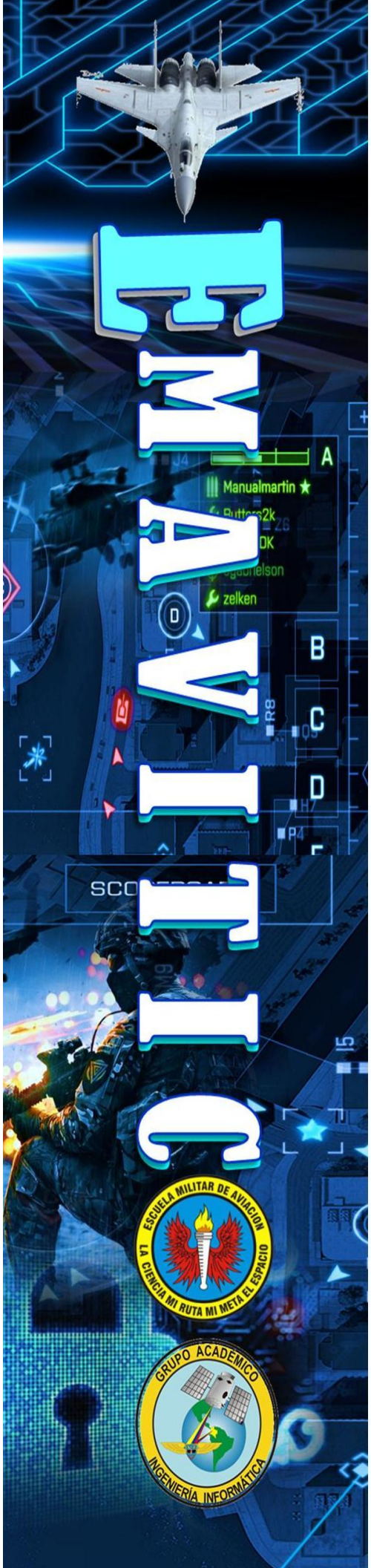

2 CONGRESO INTERNACIONAL EN TECNOLOGÍAS DE LA INFORMACIÓN Y CIBERSEGURIDAD
"Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia"
Octubre 25-2016
http://emavitic.wixsite.com/emavitic
EMAVITIC
CON FUERZA Y DISCIPLINA
ASÍ SE VA A LAS ALTURAS



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Colaboradores y Autor(es):
Capitán Zarate Luna, Paola Andrea Colombia Directora del Libro, Autor
Gutiérrez Rancruel Liliana Colombia Coordinadora, Autor
Donoso Meisel, Yezid Colombia Autor
Sánchez Rubio, Manuel España Autor
Guzmán Caballero, Andrés Colombia Autor
Huertas Calle, Leonardo Colombia Autor
Sánchez Lozano, Martha Liliana Colombia Autor
Berrio Lopez, Juan David Colombia Autor
Gaitán Rodríguez, Andrés Colombia Autor
Castillo Peña, Fabián Colombia Autor

ESCUELA MILITAR DE AVIACIÓN
"MARCO FIDEL SUÁREZ"
PROGRAMA DE INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

ISBN Obra Independiente
978-958-57589-5-7

Sello Editorial
Escuela Militar de Aviación Marco Fidel Suárez
(958-57589)

Responsable ISBN
Jefe Sección Investigación
Capitán Luis Carlos Villamil Rico

Jefe del Programa de Ingeniería Informática
Capitán Paola Andrea Zarate Luna

ESCUELA MILITAR DE AVIACIÓN
"MARCO FIDEL SUÁREZ"
PROGRAMA DE INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI

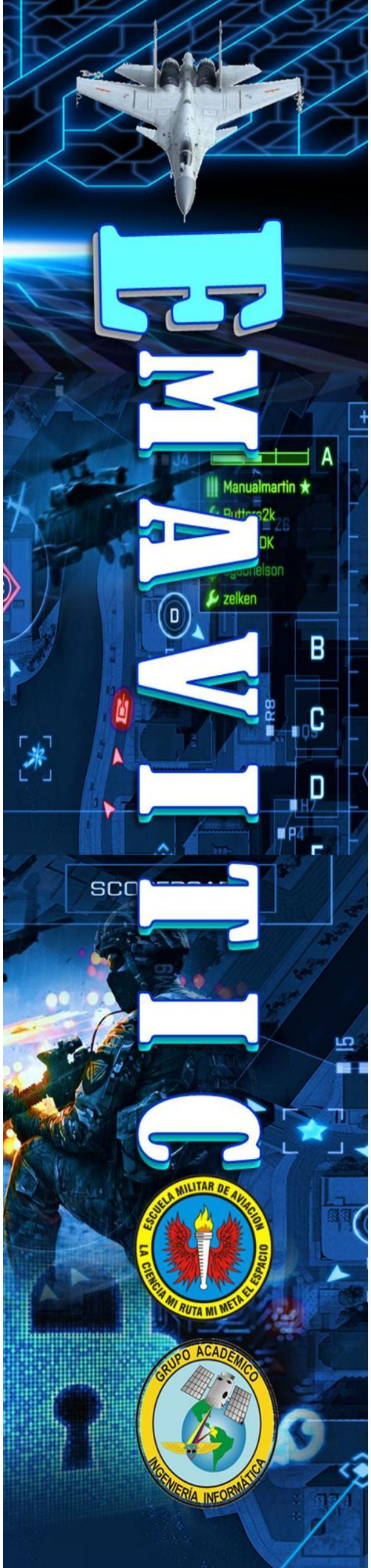


TABLA DE CONTENIDO

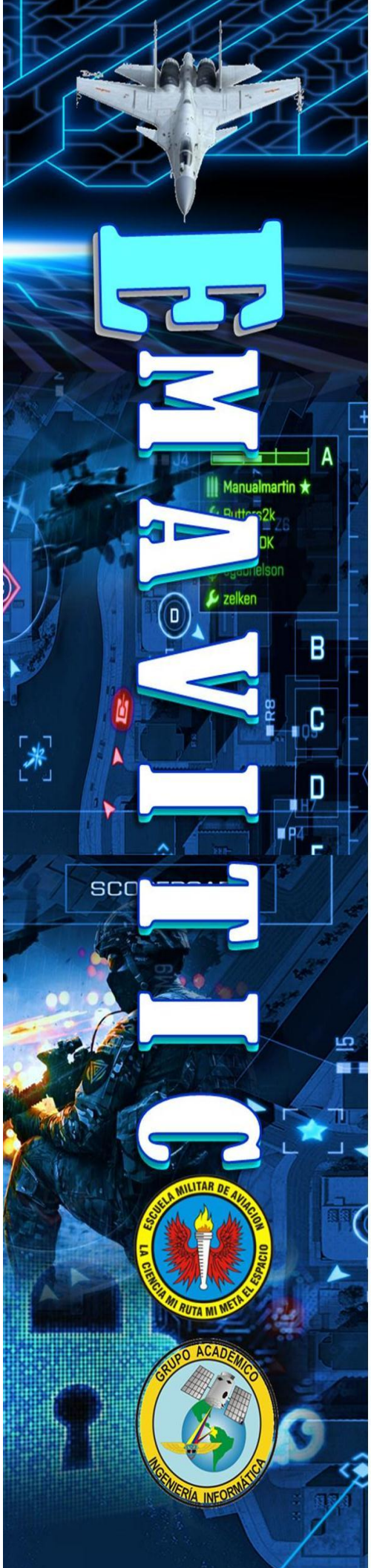
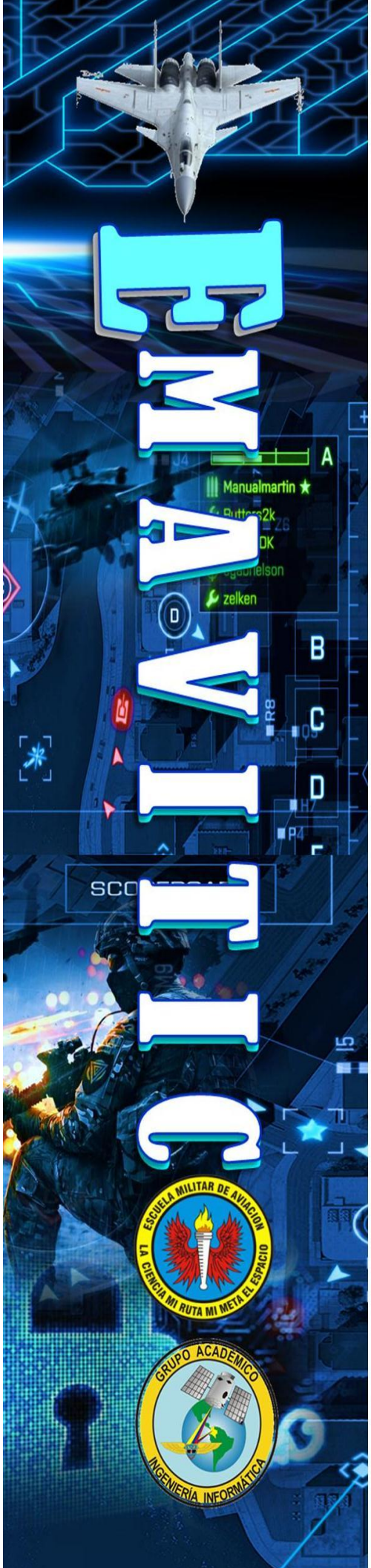


TABLA DE ILUSTRACIONES



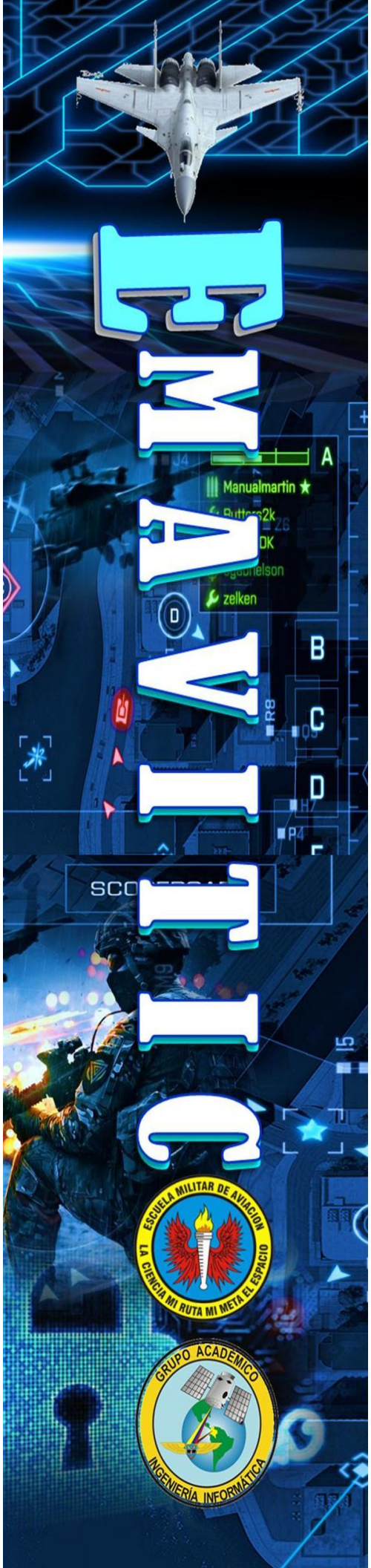
INTRODUCCIÓN

El Programa de Ingeniería Informática de la Escuela Militar de Aviación Marco Fidel Suarez, organizo el 25 de Octubre de 2016 el Congreso Internacional En Tecnologías de la Información y Ciberseguridad EMAVITIC Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC.

Este congreso fue un espacio donde la Academia, la Empresa y el Estado compartierón experiencias significativas con respecto a la ciberseguridad en ciudades inteligentes, los riesgos de la datavigilancia y los retos que presupone la preservación del ciberespacio, dado el carácter transnacional de la ciberseguridad.

Adicionalmente, este congreso conto con las muestras de los proyectos de aula realizado por los estudiantes del Programa de Ingeniería Informática, evidenciando trabajo interdisciplinario y fomento de la investigación.

El propósito de este documento es entregar la recopilación de las presentaciones de los diferentes conferencistas, su hoja de vida, justificación e información de los aliados estratégicos que hicieron parte de EMAVITIC en su segunda versión.

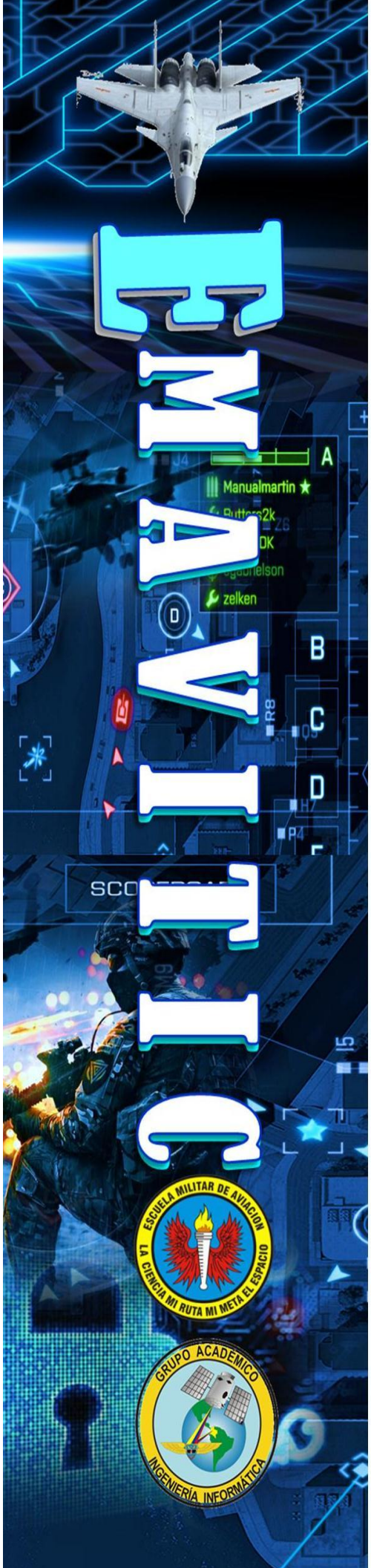


2 PRESENTACIÓN

En una sociedad hiperconectada, donde las tecnologías móviles, la computación en la nube, big data y el internet de las cosas, generan para 2020 más de 50.000 millones de dispositivos conectados y múltiples puntos susceptibles a ingreso de los ciberdelincuentes en infraestructuras del estado, empresa, academia y personal, los cuales deben preocuparse por proteger diversos dispositivos con variedad de versiones, aplicaciones, software y sistemas operativos, para salvaguardar la información, el cual es un activo de valor incalculable.

Es en este punto donde se debe establecer una estrategia 360 grados que incluya un plan de contingencia y continuidad de negocio, con soluciones tecnológicas avanzadas de ciberinteligencia capaces de defender a los sistemas frente a los ataques siendo resilientes y actualizables.

También se debe implicar en esta estrategia a todo el equipo humano de la organización, dado que el eslabón más débil en materia de seguridad son las personas y su desconocimiento de la política y sus responsabilidades frente a los dispositivos y la información que manejan, ya que los ciberataques tienen consecuencias operacionales, económicas y reputacionales, es por ello que están importante el fomento de capacidades para mitigar estas situaciones con proactividad antes de que se conviertan en amenazas.



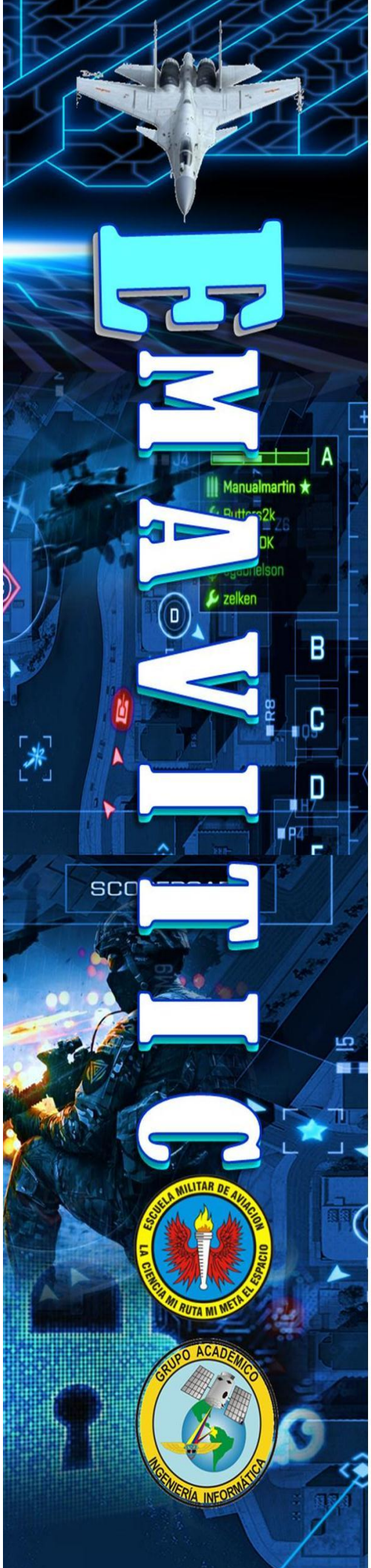
Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

El Programa de Ingeniería Informática de la Escuela Militar de Aviación Marco Fidel Suarez, se encuentra comprometido con el fomento de la seguridad de la información-ciberseguridad, es por esto que como estrategia de apropiación social del conocimiento, organizó por segunda vez EMAVITIC "Retos de la Ciberseguridad y Ciberdefensa en Ciudades e Infraestructuras Inteligentes: De Los Hackers a la Datavigilancia", congreso que tuvo como objetivo fortalecer las capacidades de prevención, defensa, detección, análisis, resiliencia y respuesta a los ciberataques, aplicando la investigación, el desarrollo tecnológico y la innovación.

Debido a que genera consciencia sobre la seguridad de la información-ciberseguridad, amplia la percepción de riesgos y vulnerabilidades a que esta expuesto día a día una institución o persona, desmitifica conceptos, promueve buenas prácticas de seguridad en un ambiente corporativo y/o público externo, previniendo pérdidas materiales e intangibles de la institución.

EMAVITIC, es el producto de conocimiento, experiencias, y trabajo en conjunto de representantes de la Academia, Empresa y Estado, esfuerzo que lo que lleva a posicionarse a nivel nacional e internacional, logrando ser parte de los eventos realizados en el mes de la Ciberseguridad de Europa promovido por ENISA-Agencia Europea de las Redes y de la Información y del mes de la Seguridad de Brasil y América Latina fomentados por la Red Nacional de Enseñanza e Investigación RNP, por medio de su Centro de Atención a Incidentes de Seguridad -CAIS.



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

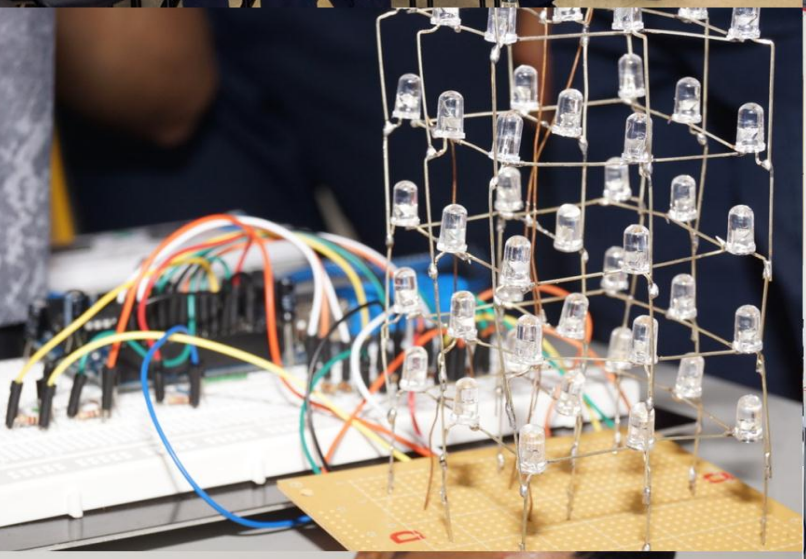
En el marco de este importante evento se llevó acabo la muestra de proyectos de aula de los estudiantes del curso 92D del Programa de Ingeniería Informática, la cual tenía como objetivo mostrar el trabajo interdisciplinario e investigativo que realizan estudiantes y docentes del Programa, así como enriquecer la experiencia de los asistentes.

EMAVITIC fue organizado por el Programa de Ingeniería Informática y su Semillero de Investigación SIGINTEL a cargo de la Capitán Paola Andrea Zarate Luna.

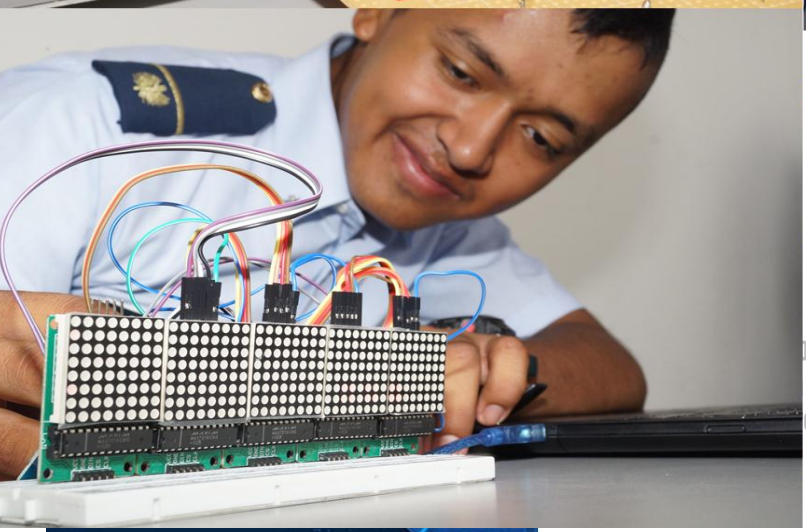
Para esta segunda versión de EMAVITIC se contó con los siguientes aliados estratégicos:

- ENISA-Agencia Europea de las Redes y de la Información
- Red Nacional de Enseñanza e Investigación RNP de Brasil
- Red Nacional Académica de Tecnología Avanzada, RENATA
- Asociación Red Universitaria de Alta Velocidad del Valle del Cauca, RUAV
- Universidad de los Andes
- Universidad Libre Seccional Cali -Programas de Ingeniería,
- CISCO Networking Academy
- ElevenPaths Innovación Radical y Disruptiva en Seguridad –Telefónica
- DSTEAM Seguridad Informática

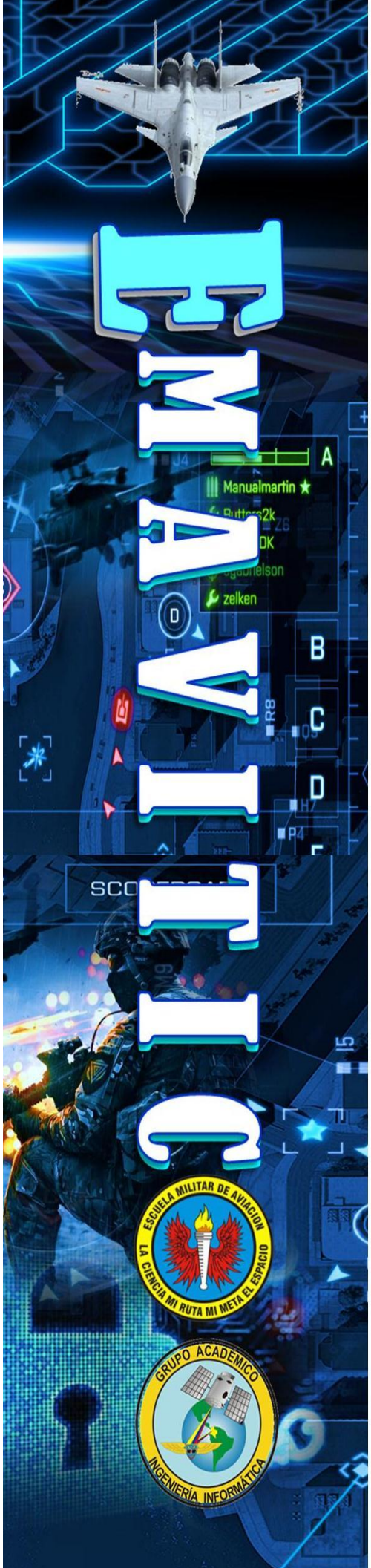

2 CONGRESO INTERNACIONAL EN
INFORMACION Y CIBERSEGURIDAD
ASI SE VA A LAS
ALTURAS




OBJETIVO
Integrantes del proyecto:
UN CUBO LED
Fuerza Aérea Colombiana
Escuela Militar de Aviación
"Marco Fidel Suárez"
Fuerza Aérea Colombiana
Escuela Militar de Aviación
"Marco Fidel Suárez"




Fuerza Aérea Colombiana
Escuela Militar de Aviación
"Marco Fidel Suárez"
Programa de Ingeniería Informática
INVESTIGACIÓN
Desarrolla competencias de análisis, solución de problemas, innovación y capacidad de implementar tecnologías apropiadas a las necesidades de la FAC.
La educación y la investigación están íntimamente relacionadas.
El Semillero de Investigación en Ingeniería Informática "SIINFA" y el Grupo de Investigación SIIANTEL surgen como una propuesta para fomentar la investigación en los primeros semestres de la formación profesional que conduzcan al fortalecimiento de las líneas de investigación del programa de Ingeniería Informática.
El avance tecnológico en la Fuerza Aérea Colombiana cobra gran valor por las necesidades de currículo con la Misión Institucional con el desarrollo permanente de proyectos que permitan dar solución a problemáticas en las áreas de Seguridad Informática, Redes, Ingeniería de Software, Simulación y Domótica.
SIINFA

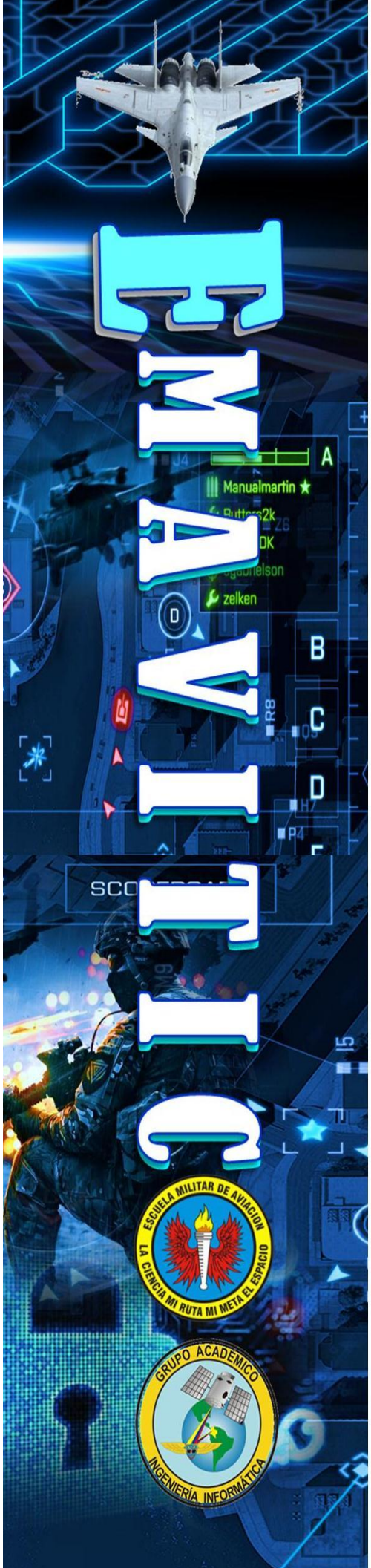


3 PANORAMA CIUDADES INTELIGENTES

Desde hace varios años, las ciudades han integrado las nuevas tecnologías a su gestión, pero últimamente la adopción tecnológica se ha acelerado y ciudades de todo el mundo están haciéndose más 'inteligentes', lo que lo hace un fenómeno global, creciente e imparable, que busca optimizar recursos, ahorrar dinero y proporcionar mejores servicios a los ciudadanos.

Es por ello que podemos definir las ciudades inteligentes como aquellas ciudades que se caracterizan por el uso intensivo de las TIC aplicando gobernanza, innovación, movilidad, inclusión social para conectar a los ciudadanos y empresas con la ciudad entre sí, mejorando la toma de decisiones, así como la eficiencia de las operaciones y de los sectores económicos, sociales y medioambientales, reduciendo la brecha de vacíos de información y de impactos negativos mediante la distribución inteligente de los recursos.

Es aquí, donde la securización adquiere un rol vital para el sostenimiento de estas infraestructuras, donde la conectividad es una cuestión crítica y el panorama del riesgo cibernético evoluciona exponencialmente; lo que con lleva a generar estrategias defensivas resilientes y proactivas que



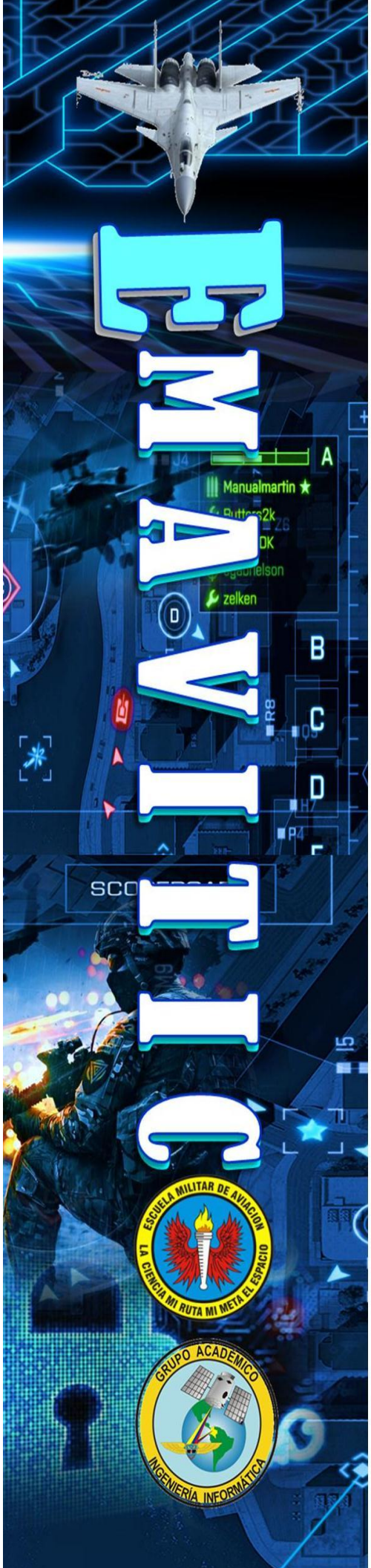
mitiguen las amenazas y restablecezcan las operaciones habituales tras un ataque o accidente, garantizando la continuidad de los servicios de la institución, salvaguardando sus activos, la propiedad intelectual y protegiendo la información que posee con el fin de proporcionar productos o servicios a su base de grupos constitutivos y clientes.

Un modelo simple de la arquitectura de ciudades inteligentes consta de sensores y dispositivos conectados; infraestructura de red y comunicaciones urbanas inteligentes; plataformas para la gestión de M2M (Machine-to-Machine), computación en la nube, y aplicaciones verticales[1]

Entre las herramientas que componen la estructura de las Ciudades Inteligentes, la más significativa es la Smart Grid, las cuales son redes que proporcionan la inteligencia necesaria para optimizar la administración de recursos y migrar de una gestión de la oferta eléctrica a una gestión de la demanda a través de la señalización en tiempo real de tarifas a los consumidores finales, que se da por la interconexión entre las infraestructuras TIC del productor, la empresa distribuidora, la comercializadora y el cliente final.

Uno de sus beneficios es la oportunidad de verificar los datos de consumo por medio de dispositivos inteligentes que tengan capacidad de telemedida, permitiéndole conocer cifras de consumo de cualquier servicio que se pueda dar a un grupo de ciudadanos (electricidad, agua, gas) de forma remota, lo que posibilita la eficiencia energética, la reducción de emisiones de gases de efecto invernadero, el consumo de energía primaria, eleva la utilización de las energías renovables.

[1] (Bergenti, Chiappone y Gotta, 2015, pp. 227-228)



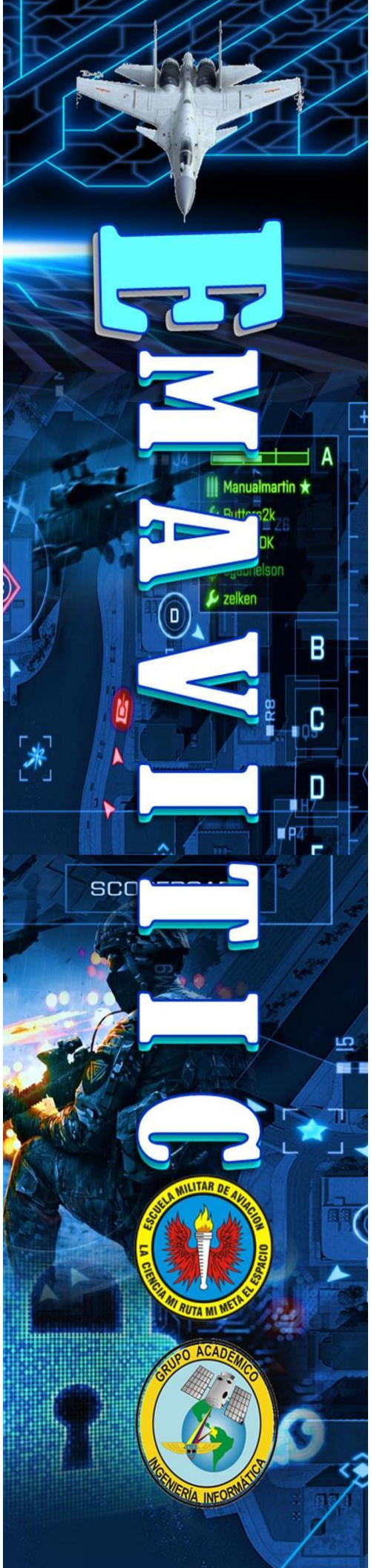
Sin embargo, los Sistemas de Control Industrial fueron diseñados sin tener en cuenta ningún mecanismo de seguridad, lo que facilita que un atacante pueda interceptar la información transmitida y obtenga los consumos instantáneos de los clientes, descubriendo rutinas y patrones de conducta, por lo que la seguridad inteligente debe ser tenida en cuenta como producto básico. Dicha seguridad inteligente debe incluir componentes de seguridad urbana y de infraestructuras críticas (redes eléctricas, transporte público, sistemas de distribución de aguas o servicios de emergencias) para salvaguardar la economía y el desarrollo de las ciudades inteligentes.

Saber los planos del ciberespacio en la ciudad facilita la comprensión de cómo está organizada la infraestructura de TIC del municipio. Es posible distinguir cinco planos: geográfico, físico, lógico, de las ciberpersonas y supervisor.

Ilustración 1 Planos del Ciberespacio en las ciudades.

Tabla 1. Planos del ciberespacio en las ciudades	
Plano supervisor	Puede ser muy complejo, debido a potenciales desavenencias políticas. Además suele ser proclive a la compartimentación, lo que lastra todavía más la cooperación en asuntos de seguridad.
Plano de las ciberpersonas	Engloba a las identidades de los líderes y empleados municipales. Estas pueden estar abiertas a la interacción con los votantes para conseguir ganancias electorales, pero también facilitar ataques de *spear-phishing* y otros fraudes.
Plano lógico	Las incompatibilidades entre el *software* de los sistemas son frecuentes. Muchos sistemas pueden estar funcionando en *hardware* y *software* heredados, debido a requerimientos normativos o a elevados costes de actualización.
Plano físico	Puede ser muy importante en supuestos de desastres naturales o causados por el hombre. Su rendimiento puede verse mermado por conexiones de bajo ancho de banda y por la falta de redundancia en la capa física de la conectividad.
Plano geográfico	Es de gran relevancia, porque la infraestructura de TIC de una ciudad generalmente está ligada al área geográfica del municipio. Cualquier desastre puede acabar causando pérdidas de energía o de conectividad en red.

Fuente: https://telos.fundaciontelefonica.com

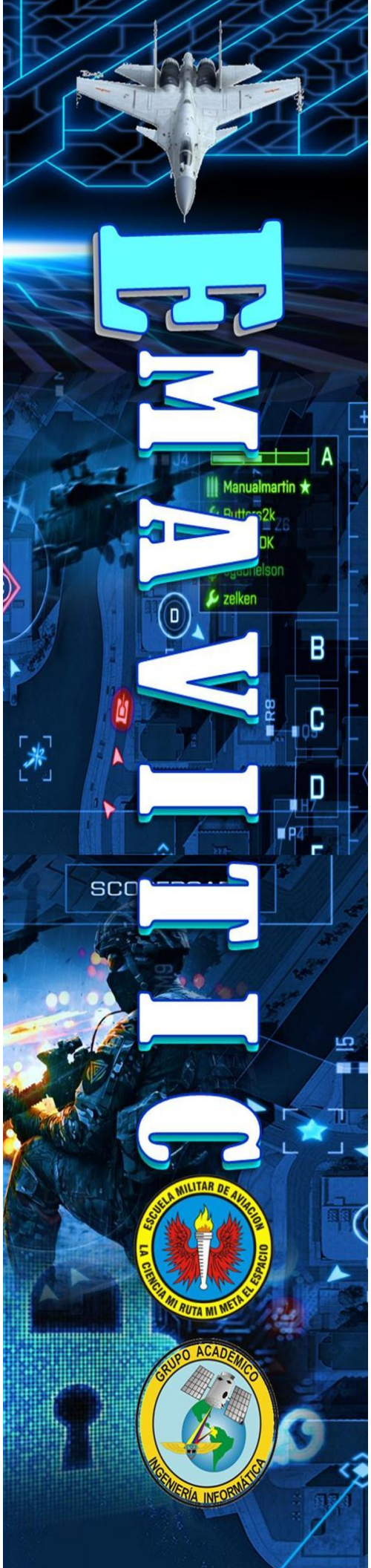


Por otro lado se debe conocer las posibles categorías de ciberataques que incluyen virus, malware, troyanos, bombas lógicas, phishing, APT (Amenazas Persistentes Avanzadas), ataques de denegación de servicio, accesos no autorizados (normalmente para el robo de propiedad intelectual o información confidencial), ransomware y ataques a sistemas de control (tipo SCADA).

Los espacios en los cuales se pueden recibir estos ciberataques son los siguientes:
Capa física: Hace referencia a las infraestructuras y equipamientos informáticos que sustentan los sistemas de información. Sin esta capa, el resto de niveles que conforman el ciberespacio desaparecerían, lo que le convierte en un objetivo de acciones armadas convencionales (operaciones cinéticas) para imposibilitar las capacidades informáticas de un determinado actor.

Capa sintáctica: Contempla las instrucciones y configuraciones introducidas por los administradores y usuarios de los equipos informáticos, junto a los protocolos que permiten a los dispositivos comunicarse. Este es la capa sobre el cual actúan los hackers con el fin de suplantar la autoridad de los responsables legítimos y controlar el comportamiento de los equipos informáticos o provocar un funcionamiento anómalo

Capa semántica: Aborda la información que el dispositivo informático contiene, incluyendo tanto los datos almacenados por el usuario, como el software y los códigos que permiten al ordenador desarrollar determinadas funciones. Este nivel no siempre es fácilmente distinguible del sintáctico.



Capa de usuario: Está sujeto a ataques de ingeniería social, profusa que se pueden generar por errores humanos.

Las ciudades son vulnerables incluso cuando no hay nadie intentado alterar las infraestructuras críticas u otros sistemas importantes, es por ello que uno de los ciber-riesgos está relacionado con problemas de gestión de las tecnologías o ciber-gestión lo que conduce a fallos en cascada causados por mal funcionamiento, falta de privacidad y confidencialidad, problemas de trazabilidad digital/responsabilidades, censura, saturación de información y/o desinformación de los ciudadanos cuyo resultado es la afectación no solo a los ciudadanos, sino también a organizaciones/organismos o todo un país generando caos e incertidumbre.

En cuanto a posibles modelos o marcos de referencia para la gestión de la ciberseguridad, conviene tener en cuenta que se está considerando, cada vez más, como un riesgo empresarial[2].

En consecuencia, se están buscando modelos de mitigación y gestión así como métricas de cuantificación de riesgos. Los niveles de madurez varían entre organizaciones, y en consecuencia también entre naciones y ciudades inteligentes.
De igual forma se ve la necesidad de valorar el riesgo/amenaza en función del impacto en la organización teniendo en cuenta los bienes de negocio, la percepción de la amenaza, detección de ataques, la defensa proactiva e Integral, la resiliencia y la gestión de respuestas a ataques.

[2] Wipro Insights, World Economic Forum Annual Meeting 2014: Cyber Risk Resilience http://www.wipro.com/microsite/WEF-2014/insights.html

4 CONFERENCISTAS Y CONFERENCIAS

El Congreso Internacional en Tecnologías de la Información y Ciberseguridad EMAVITIC contó con expertos nacionales e internacionales en ciberseguridad del sector defensa, empresarial y académico, quienes compartieron sus conocimientos y experiencia con los presentes.

Ilustración 2 EMAVITIC

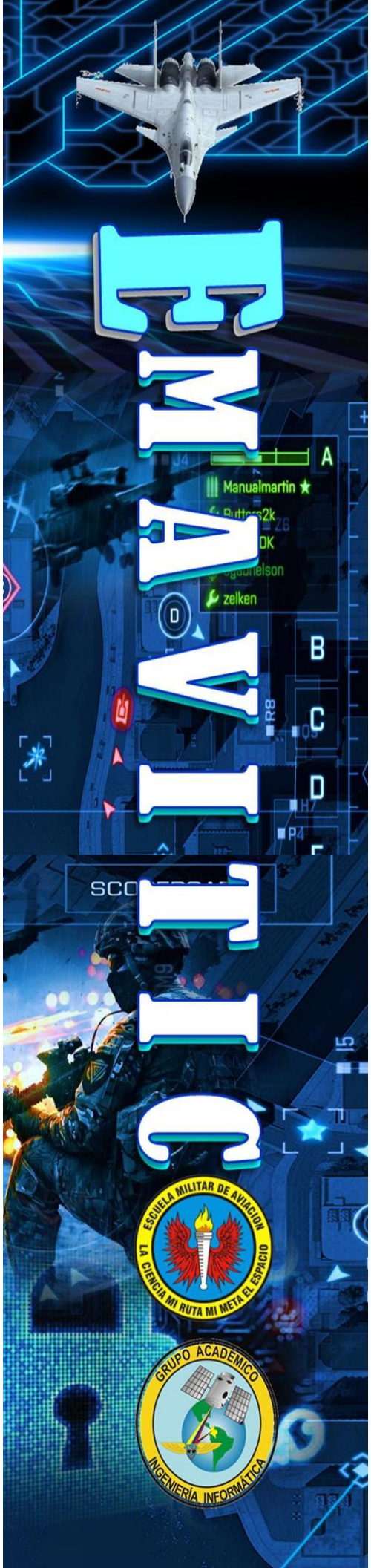
Fuente: El Autor.

4.1 YEZID ENRIQUE DONOSO MEISEL

Ilustración 3 Conferencista YEZID ENRIQUE DONOSO MEISEL

Fuente: El Autor.

Profesor Asociado Departamento de Ing. De Sistemas y Computación, Subdirector Académico Dpto. Ing. De Sistemas



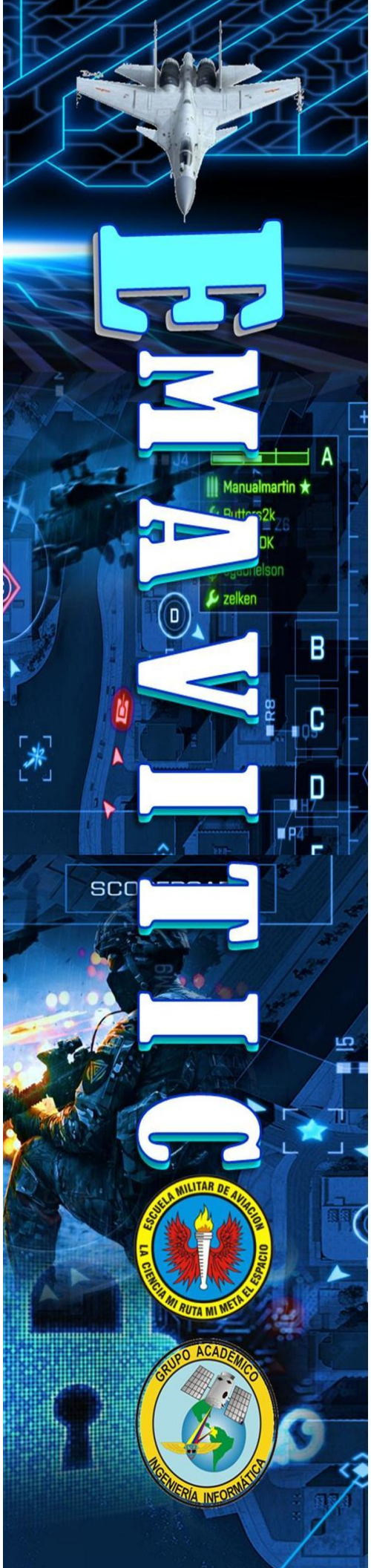
Coordinador Maestría en Seguridad de la Información, Coordinador Especialización en Seguridad de la Información Universidad de los Andes, Investigador Senior. Colciencia. Colombia, Senior Member IEEE, Past-Chair IEEE Colombia Evaluador Experto de la Comisión Europea.

Estudios

Ph.D. (Cum Laude) en Tecnologías de la Información, Universidad de Girona,Girona, España.
PostPhD en Tecnologías de la Información. Universidad de Girona.
D.E.A. en Tecnologías de la Información. Universidad de Girona, Girona,España.
Master (MSc) en Ingeniería de Sistemas Computación, Universidad de los Andes, Bogota, Colombia.
Ingeniero de Sistemas, Universidad de Norte, Barranquilla, Colombia.

Algunos Premios y Reconocimientos

• Medalla al Mérito Tecnológico. Otorgado por la Policía Nacional – Oficina de Telemática. 2016.
• Senior Member IEEE (Instituto de Ingenieros Electrónicos y Eléctricos) desde 2005.
• DVP (Distinguished Visitor Professor) para IEEE Computer Society. 2005 – 2009.
• Premio Nacional de Investigación de Operaciones dado por la Sociedad Colombiana de Investigación de Operaciones. 2004.
• Premio “Mejor Trabajo de Investigación” en el congreso IEEE ICN (Internacional Conference on Networking). 2004.
• Reconocimiento como “Profesor Distinguido”. Universidad del Norte. Octubre 2004.



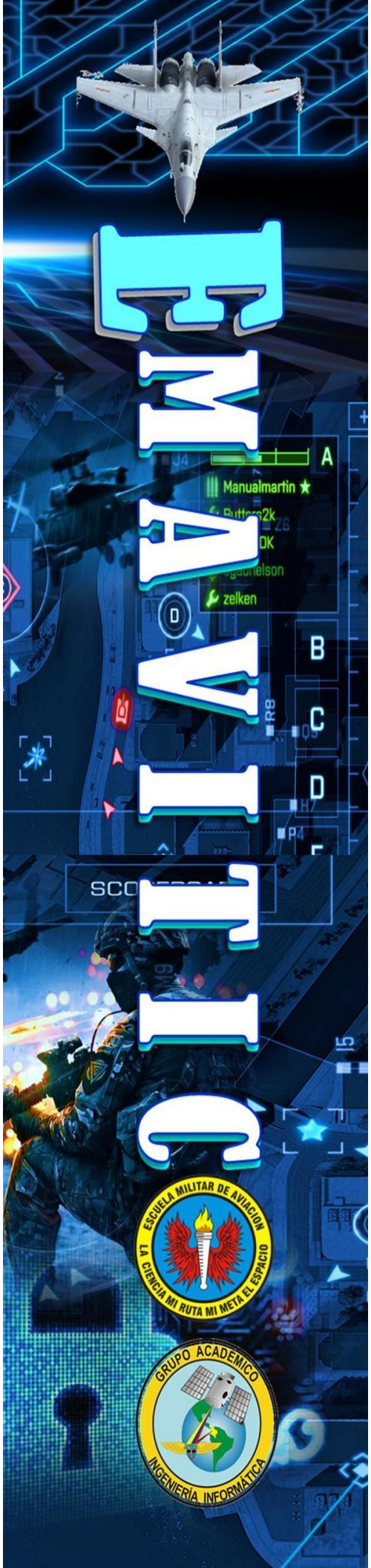
Tiene varios reconocimientos como profesor invitado en universidades nacionales e internacionales.

Professional Certifications

Certificate in Information Security. Software Engineering Institute. Carnegie Mellon University. USA.
Certificate in Incident Response Process. Software Engineering Institute, Carnegie Mellon University, USA.
Information Security Management Systems Auditor/Lead Auditor BS ISO/IEC 27001:2013 BSI - British Standards Institution
Certified Business Continuity Management Systems Auditor/Lead Auditor. BSI (British Standard Institute). United Kingdom.
Certified Functional Continuity Professional (CFCP). DRII (Disaster Recovery Institute International). USA.

Libros

Network Design for IP Convergence. DONOSO MEISEL, YEZID. 1 ed. Boca Raton. CRC Press, USA. 2009.
Multi-Objective Optimization in Computer Networks using Metaheuristics. Y. Donoso, R. Fabregat. CRC Press. 2007.
Donoso, Yezid, Fabregat, Ramon. Multi-Objective Optimization in Multicast Flows.
Multi-Objective Optimization Scheme for Static and Dynamic Multicast Flows. VDM Verlag Dr. Muller. Germany. 2009. V.1. p.157.
Javier Sierra, Yezid Donoso. Optimización de Redes de Transporte ÓpticasWDM. 1 ed. Editorial UPB, Colombia. 2011.



Tiene más de 140 artículos publicados en revistas internacionales indexadas, IEEE, ACM, IFIP y Conferencias Internacionales

CONFERENCIA: CIBERSEGURIDAD Y EL RETO CON LAS NUEVAS TENDENCIAS TECNOLÓGICAS.

La charla se enfocó a 3 temas:
1-Nuevos servicios y plataformas
2-Defensa estratégica
3-y Si el ataque es efectivo que?
Se hizo énfasis en la importancia de seguridad teniendo en cuenta las nuevas tendencias como IoT, SDN y NFV.

Se destacó un modelo sugerido de plataforma de 6 niveles: Comunicaciones (ITE), EPC, openMTC, IMS,OTT (MtoM) y Aplicaciones.

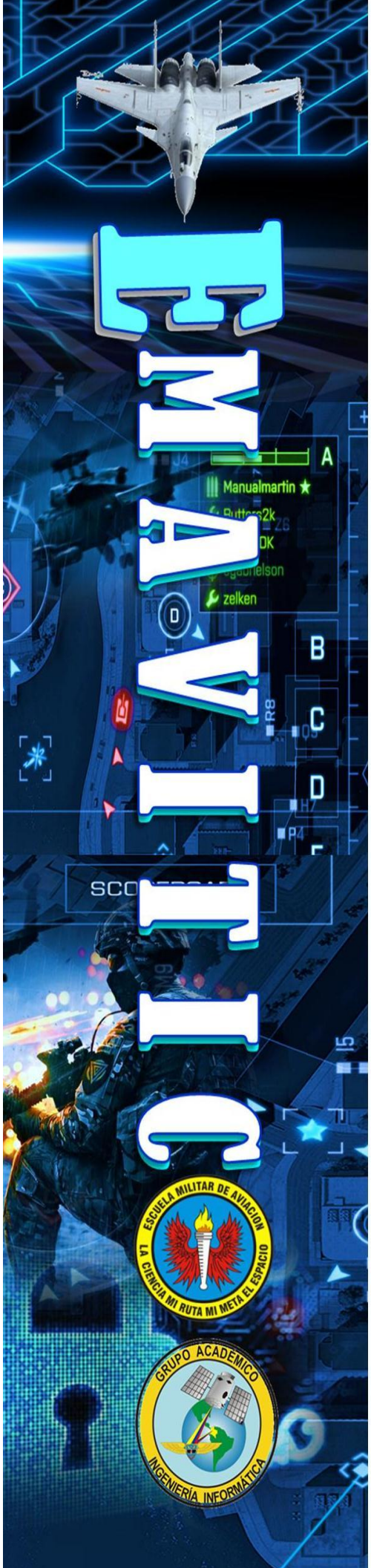
Se hizo énfasis en la necesidad de definir estrategias de seguridad, todo está conectado y cómo actuar ante situaciones de ataques efectivos. Resilencia.

4.2 ANDRÉS GUZMÁN CABALLERO C.E.O Adalid Corp Colombia

Ilustración 4 Conferencista Andrés Guzmán Caballero

Fuente: El Autor.

Abogado especializado en Derecho y Tecnología, Magister Excutive en Administración de Empresas y Liderazgo Estratégico, Cybercrime and Electronic Evidence, Perito ad honorem en evidencias digitales, Perito en casos de evidencia y crimen informático, Especialización en Derecho



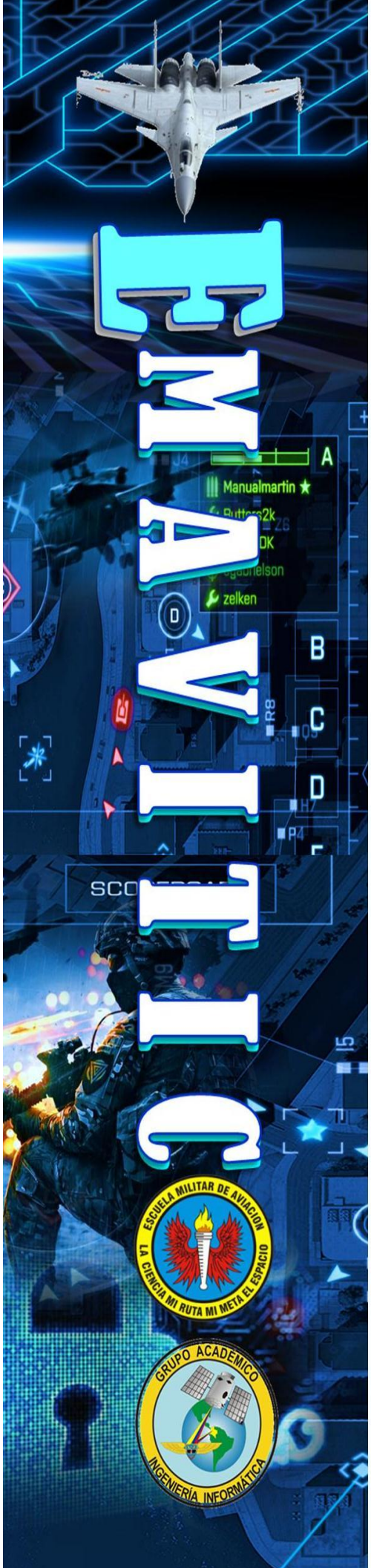
Administrativo, Diplomado en Internet, Comercio electrónico y su regulación, Docente de Postgrados, Director de la Maestría de Protección de Datos de la Universidad Sergio Arboleda.

Especialidades:
Pruebas técnicas, seguridad de la información, derecho informático, derecho de autor, derecho de la competencia, CIBERCRIMEN.

Con más de 20 años de experiencia vinculados a la promoción y gestión proyectos tecnológicos de alta especialización, abordando tanto actividades de investigación y desarrollo experimental, hasta integración y etapas de pre-industrialización.

Actualmente se desempeña como CEO (Chief Executive Officer) de la compañía Adalid Corp Colombia, empresa líder en Colombia y Latinoamérica para la gestión de Pruebas Electrónicas y Evidencias Digitales y la prevención del fraude relacionado con nuevas tecnologías, ofrece asesoría y apoyo técnico-legal para la implementación de mecanismos y controles que aseguren la disponibilidad, confidencialidad e integridad de la información dentro de los sistemas y activos de información de sus clientes.

Andrés Guzmán Caballero, es el único colombiano certificado por la Unión Europea en la defensa de personas saboteadas por internet, ha asumido casos de congresistas y personalidades, entre otros

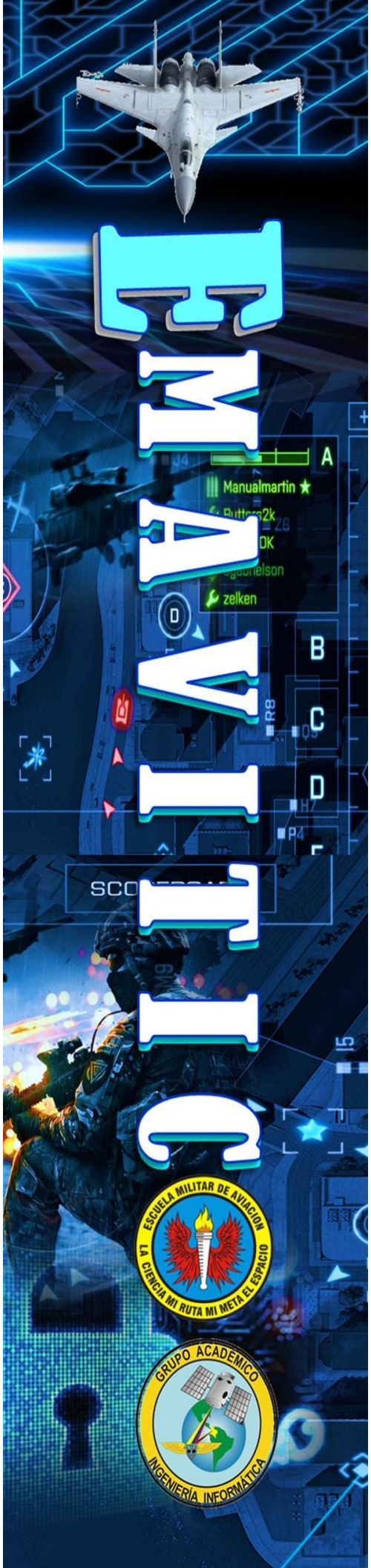


Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

El doctor Andrés, busca que la información de sus clientes esté protegida y que cumpla con los requisitos legales y contractuales, estableciendo o implementando las mejores prácticas y perímetros de seguridad para lograr que todos los procesos o servicios informáticos en la red, sean confiables, con una estrategia que se basa en el cambio y la cultura de las personas de su organización, en seguridad de la información.

Así mismo, se ha destacado por su exitosa participación en campañas de seguridad de la información como la “Campaña Computador Seguro en compañía” en instituciones como la Procuraduría General de la Nación, la Secretaria de Movilidad y el Consejo Profesional Nacional de Ingeniería -COPNIA-, entre otras.

Por otra parte, su carrera se ha visto impactada positivamente con fallos a favor ante el Tribunal Superior de Bogotá por las tutelas interpuestas por ADALID Corp, en las cuales se pretende proteger los derechos al buen nombre y otros vulnerados a través de medios sociales tecnológicos como el Internet.



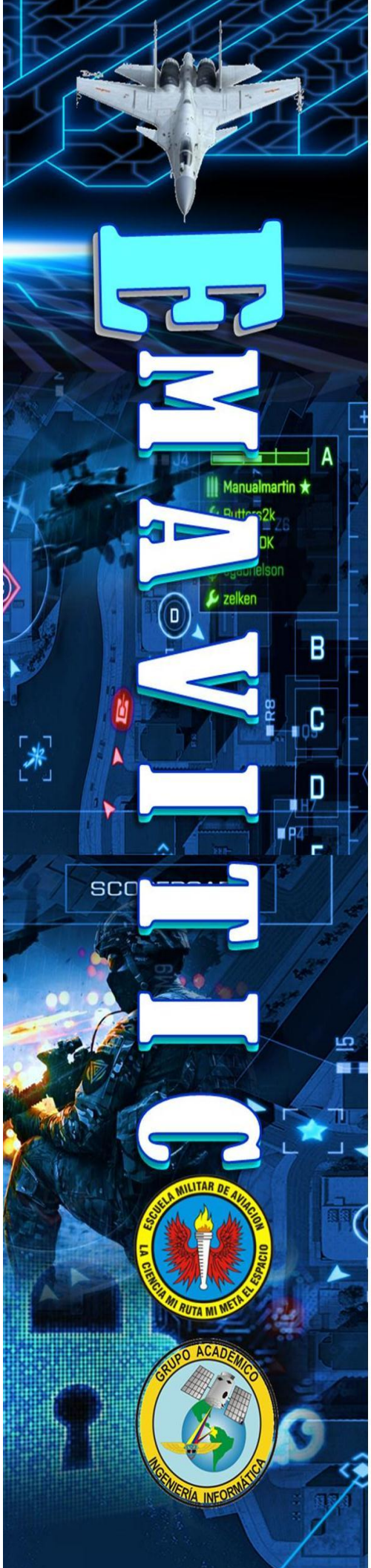
CONFERENCIA: PROBANDO EN LA RED. EVIDENCIAS DIGITALES DEL FUTURO

Contexto General:

Posiblemente el contexto legal de las actividades del ciberespacio tomó un nuevo rumbo con la aplicación de normatividad y penalización de delitos informáticos en Colombia.

En derecho de familia aproximadamente el 65% de los casos de divorcio cuentan con pruebas con mensajes de texto, correos, Facebook o whatsapp, en el ámbito comercial más de 1’000.000.000 de dólares en negocios se hacen usando internet; en derecho penal, aproximadamente 3.000 delitos diarios se cometen usando internet, entre los cuales, se encuentran: el robo, la suplantación, la pedofilia, el fraude bancario, robos financieros, piratería, el narcotráfico, la estafa, injurias, calumnia, plagio.

En derecho administrativo todos los contratos estatales se publican en internet.



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

El ciberespacio ha contribuido con pruebas documentales nuevas: chat, grabaciones de voz, fotografías, páginas web, archivos, ayudando al derecho procesal con la cadena de custodia, el análisis de archivos, búsqueda de información, rastreo, borrado de información, verificación de emails, en fin un sin número de pruebas que pueden presentarse en juicios, y gracias a esto en los procesos judiciales, la ayuda de la tecnología se ha convertido en una herramienta poderosa al servicio del Derecho.

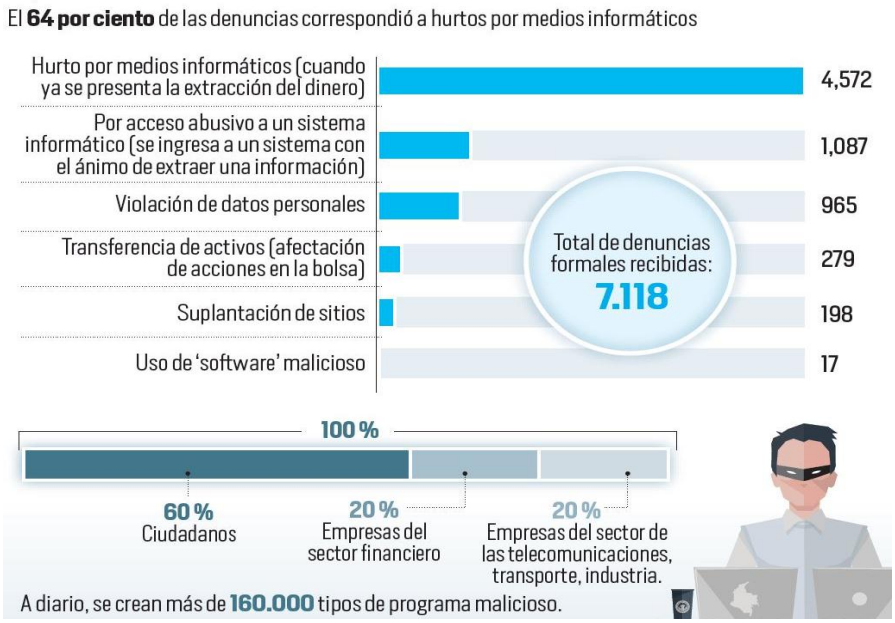
El Dr. Caballero inicio su conferencia motivando a los presentes, mostrando un ejemplo de cómo alguien podía enviar un correo electrónico falso de renuncia, y solo se podía probar su autenticidad mediante una traza del correo electrónico.

LEY 527 DE 1999 (18 de agosto)

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se implementó para definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

En esta ley se definen términos como: Mensaje de Datos, firma Digital, entidad de Certificación, EDI, Sistema de Información.

Ilustración 5 Radiografía de los delitos informáticos en Colombia 2015

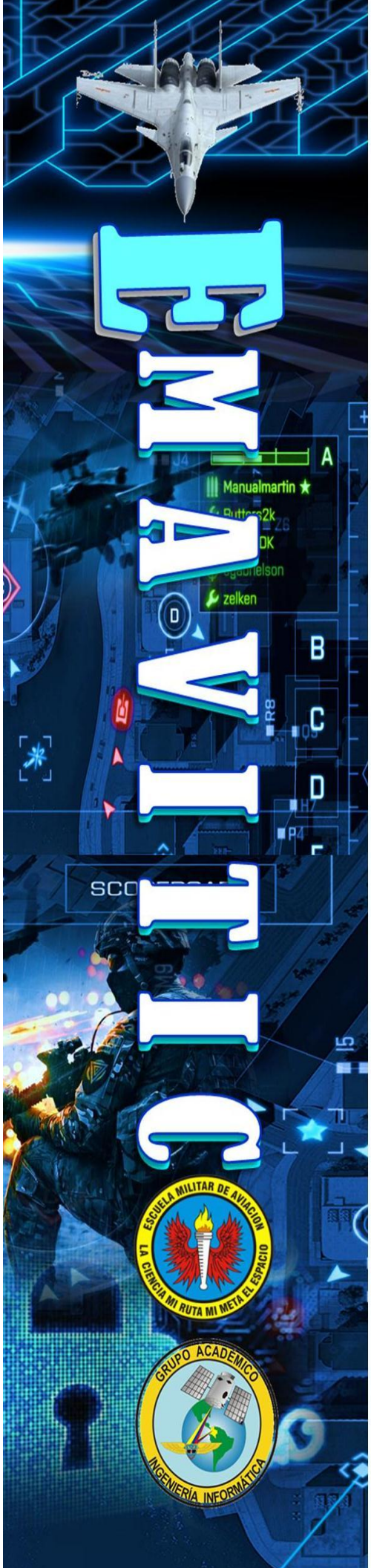


Fuente: Unidad de delitos informáticos de la Dijin

Herramienta HASH ON LINE

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varios cometidos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.



En definitiva las funciones hash se encargan de representar de forma compacta un archivo o conjunto de datos que normalmente es de mayor tamaño que el hash independientemente del propósito de su uso.

Herramientas Para Montajes de Laboratorios

En el mercado ya se logra contar con herramientas digitales que facilitan el trabajo de un perito forense:

- EVLAB, es una plataforma (App y Web), que permite certificar diferentes evidencias digitales de forma sencilla y segura.

  Es el primer laboratorio de evidencias digitales en la nube en Latinoamérica.

  Para certificación de documentos digitales de forma sencilla y segura, certificación de mensajes de correo electrónico, páginas web y fotografías tomadas con el celular sin necesidad de ningún conocimiento técnico.

  Con EVLAB se puede probar la certificación de un correo electrónico, el Contenido del correo electrónico, constancia de envío y recepción, confirmación de recepción y lectura, Informes de hora y fecha.

Ilustración 6 EVLAB

Fuente: https://evlab.co/

- DOCUSIGN, proporciona una manera sencilla y segura de firmar documentos y recopilar firmas de terceros de forma electrónica. La aplicación acaba con las molestias, los costes y la falta de seguridad derivados de la impresión, el envío por fax o el escaneo de los documentos que requieren una firma, o del hecho de que deban esperar al día siguiente para firmarse, tiene la posibilidad de redactar y enviar incluso contratos que se requieran firmar en la misma interfaz.

  A continuación se describen los siguientes pasos:

  1. Una vez redactado el contrato, se envía mediante correo electrónico un link a la otra parte con el contrato o documento que se vaya a suscribir.

2. La parte (en este caso en firmante) abrirá el documento, que está almacenado en la nube, para poder revisarlo y aprobarlo.

3. Ya aprobado se procede a realizar la firma de ambas partes. El sistema presenta una serie de filtros y preguntas para poder realizar la firma.

4. Por último se hace una revisión de ambas partes y se genera una aprobación final.

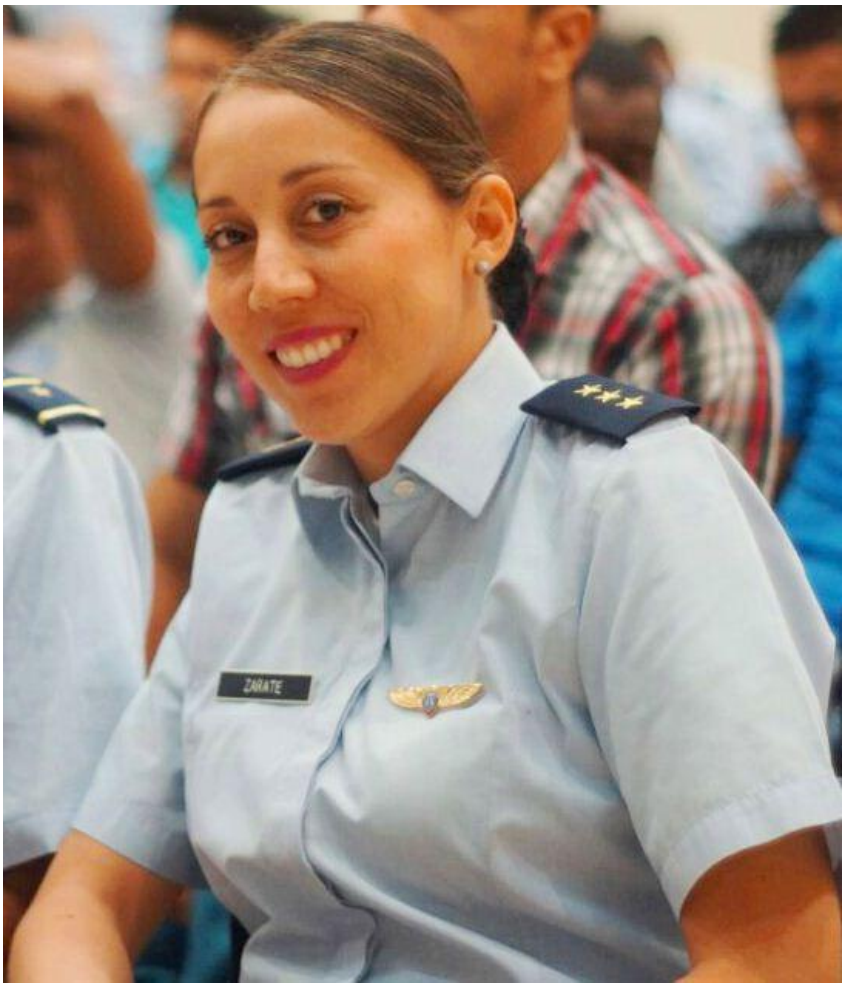
Lo importante de esta alternativa es que las entidades que tienen que verificar la validez del contrato deben aceptar este tipo de firmas, ya que así lo ordena la ley que fue decretada el año anterior.

Ilustración 7 DOCUSIGN

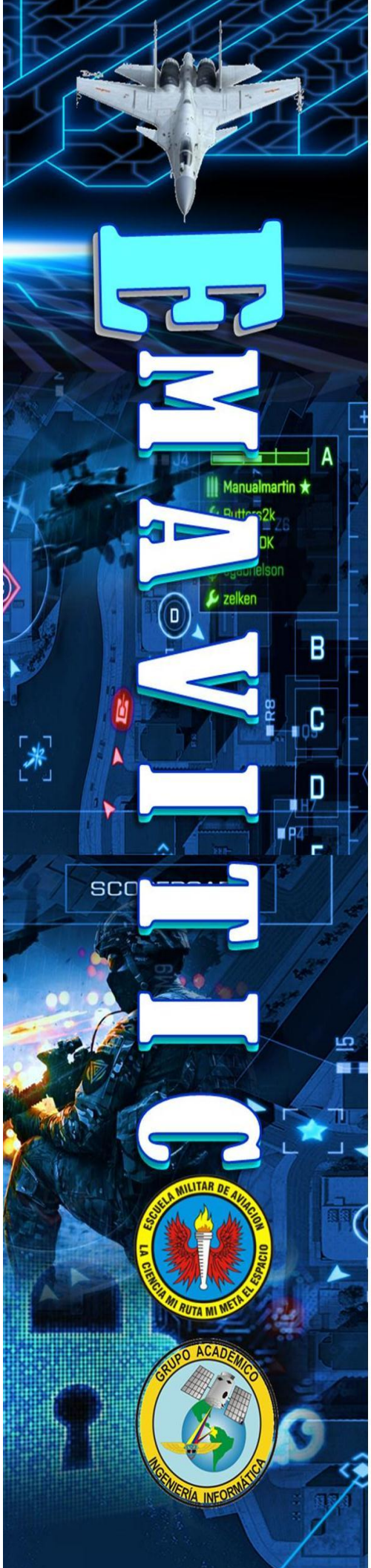
Fuente: Autor

4.3 CAPITÁN PAOLA ANDREA ZARATE LUNA

Ilustración 8 Conferencista Capitán PAOLA ANDREA ZARATE LUNA



Fuente: Autor



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

Capitán Paola Andrea Zarate Ingeniería de Sistemas con Especialización en Seguridad Informática.
Auditora SGSI, Evidencia digital y forense. Suite Ethical Hacking ETEK.

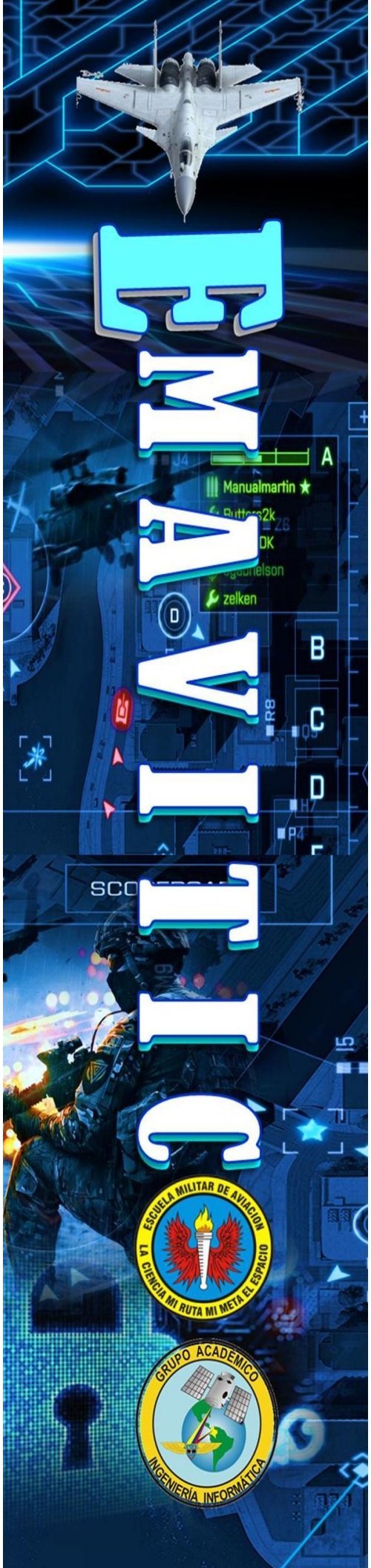
Se desempeñó como Asesora de Proyectos de APP de MINDEFENSA, JAL-DITIN Subdirectora de Sistemas de Información, Comandante del Escuadrón de Telemática de CACOM-4 y CACOM-1.

Actualmente se desempaña como Jefe del Programa de Ingeniería Informática de la Escuela Militar de Aviación y la Sección Sistemas del Grupo Académico.

CONFERENCIA: DE LOS HACKERS A LA DATAVIGILANCIA

Ilustración 9 Datavigilancia

Programa de Ingeniería Informática
Escuela Militar de Aviación Marco Fidel Suárez
"El Ciberespacio, El Quinto Dominio de la Guerra



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

El avance de la tecnología ha demostrado hoy en día que se están entregando proyectos con gran potencial que marcan una ruta de cambios en las organizaciones, cuyo objetivo está enfocado a mejorar la calidad de vida de los ciudadanos y estimular la nueva economía utilizando las nuevas tecnologías de la información y de la comunicación (TIC), de forma transversal para transformar la ciudad, a través de por ejemplo los sensores distribuidos por toda la ciudad q capten información esencial para los proyectos de gestión de agua inteligente, iluminación inteligente y energía inteligente trayendo consigo resultados como ahorro de servicios, sostenibilidad para las ciudades, generación de empleos entre otros.

Protección y seguridad: este aspecto es extremadamente sensible en la conciencia pública. La incorporación de servicios como redes de videocámaras, iluminación adecuada de zonas comunes, vigilancia y patrullaje intensivo, mecanismos adecuados de verificación de la identidad de los ciudadanos y la respuesta rápida a las llamadas de emergencia están en la lista de las expectativas que deben cumplir las ciudades inteligentes

Programa de Ingeniería Informática
Escuela Militar de Aviación Marco Fidel Suárez
"El Ciberespacio, El Quinto Dominio de la Guerra

CARACTERÍSTICAS DE UNA CIUDAD DIGITAL

La integración de estos servicios impulsa el desarrollo de una cultura digital.

CENTRAL DIGITAL

Todo el sistema es dirigido por los municipios desde una central digital.

ADMINISTRACIÓN PÚBLICA

Reducir la burocracia, incrementando la transparencia administrativa y agilizando la atención ciudadana.

SITUACIONES CRÍTICAS

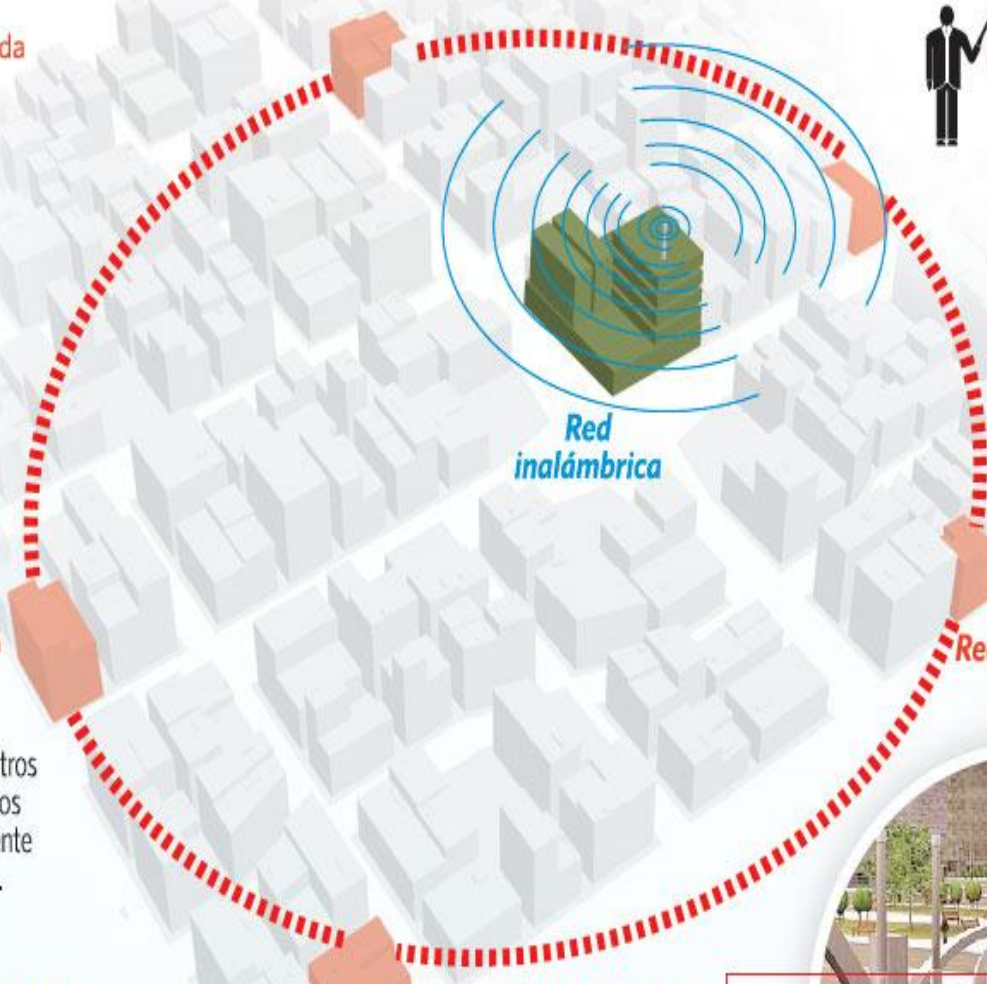
Ante situaciones críticas todas la fuerzas públicas estarán intercomunicadas al instante en cualquier lugar de la ciudad.

CIUDAD DIGITAL

Prototipo de ciudad conectada a través de redes cableadas e inalámbricas de banda ancha, combinando tecnologías MECH, WIMAX yWIFI.

SISTEMA EDUCATIVO

La conectividad entre instituciones educativas favorecerá la integración de los alumnos y hará posibles los programas de educación a distancia y acceso a la información global.



EMERGENCIAS

Bomberos, policía y ambulancias estarán conectados con los centros de salud, optimizando los tiempos de reacción frente a cualquier emergencia.

SALUD

Los centros de salud interconectados permitirán compartir información , bases de datos, historias clínicas de los pacientes, interconsultas entre profesionales y diagnósticos a distancia.

SEGURIDAD

Los sistemas de video vigilancia y comunicaciones inalámbricas de las fuerzas de seguridad ayudarán a prevenir y resolver hechos delictivos de diversos tipos.

Fuente: **Motorola.**

LA REPÚBLICA

A continuación se presentan ejemplos de ciudades inteligentes del mundo:

Tokio:

Considerada la Smart City por antonomasia con proyectos de mejora de la gestión energética, urbanización inteligente, movilidad… Llama la atención el despliegue de tecnología NFC (Near Field Communication) en medios de transporte público como el metro, o en superficies comerciales, para realizar el pago de productos o servicios con el teléfono móvil.

Ilustración 10 Tokio - Smart City

Ámsterdam:

Entre las muchas iniciativas smart que ha puesto en marcha esta capital europea, destacan el proyecto de "luz inteligente". Consiste en un alumbrado público que permite ajustar la iluminación en función de la situación o necesidad del lugar donde se despliegan. Las autoridades pueden adaptar la intensidad de la luz según el clima o cambiar su color. Las farolas consumen menos energía que las convencionales.

Ilustración 11 Ámsterdam - Smart City

Fuente: VI Edición del Evento Smart City

Singapur:

La ciudad tiene desplegada una inmensa red de sensores conectados a Internet que recopila datos en tiempo real del funcionamiento de la ciudad.

El objetivo es utilizar la información para llevar a cabo iniciativas que mejoren la vida de los ciudadanos.

En la práctica, estos sensores permiten, por ejemplo, detectar el riesgo de inundación de los desagües, evitar atascos, ofrecer información sobre el transporte público, detectar la calidad del aire, encontrar un parking libre.

Ilustración 12 Singapur - Smart City

Barcelona:
La ciudad cuenta con conexión gratuita a Internet gracias al servicio Barcelona Wifi que ofrece su ayuntamiento. Con sus 590 puntos de acceso es una de las redes inalámbricas de conexión a la Red más grandes de Europa. Centros de barrio, Centros de la tercera edad, Centros cívicos, Centros culturales y museos, Centros deportivos, Oficinas administrativas y de atención ciudadana, Bibliotecas, Mercados municipales, Interiores de manzana y parques cerrados con horario establecido, Salas de estudio nocturna.

Ilustración 13 Barcelona - Smart City

Barcelona:

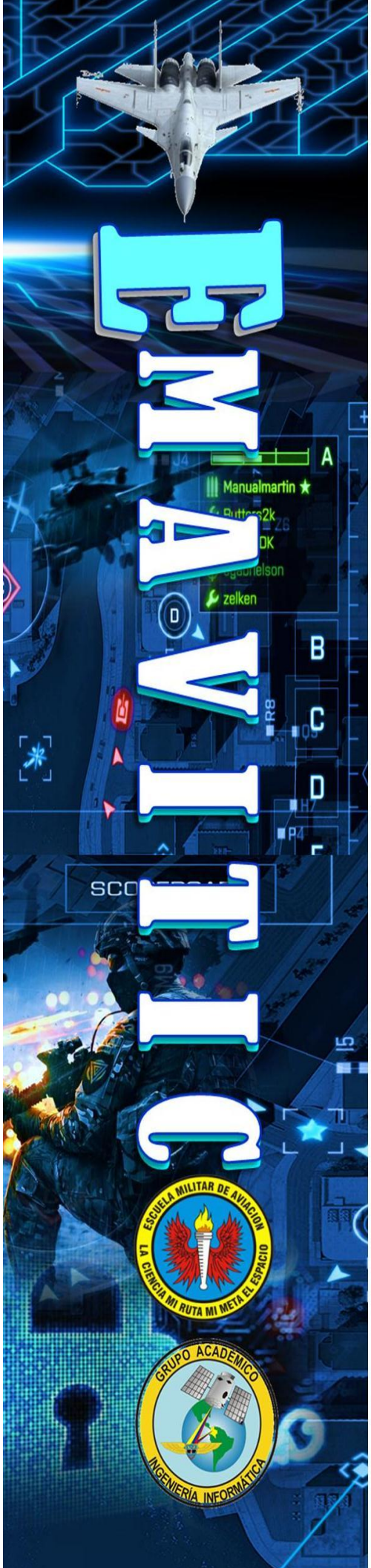
La ciudad cuenta con conexión gratuita a Internet gracias al servicio Barcelona Wifi que ofrece su ayuntamiento. Con sus 590 puntos de acceso es una de las redes inalámbricas de conexión a la Red más grandes de Europa. Centros de barrio, Centros de la tercera edad, Centros cívicos, Centros culturales y museos, Centros deportivos, Oficinas administrativas y de atención ciudadana, Bibliotecas, Mercados municipales, Interiores de manzana y parques cerrados con horario establecido, Salas de estudio nocturna.

Ilustración 14 Barcelona - Smart City

Santiago de Chile:

La capital chilena ha puesto en marcha el primer prototipo de ciudad inteligente en el Parque de Negocios Ciudad Empresarial. Entre las virtudes de Smartcity Santiago está "la gestión inteligente de la red eléctrica, aumentando la eficiencia energética del sistema y el cuidado del medio ambiente", según indica la web del proyecto. Pero esta iniciativa va mucho más allá al integrar en el centro de negocios múltiples innovaciones tecnológicas como pantallas informativas, vehículos electrónicos, wifi público, controles de iluminación o edificios domótico

Ilustración 15 Santiago de Chile - Smart City



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

ERA DE LA DATAVIGILANCIA

Busca:

- Gestión eficiente en todas las áreas de la ciudad (urbanismo, infraestructuras, transporte, servicios, educación, sanidad, seguridad pública, energía).
- Satisfacer las necesidades de los ciudadanos
- Encontrar el equilibrio entre el bienestar de los ciudadanos y la preservación del entorno.

Y si todo está conectado…como garantizamos la seguridad?

Entre los ataques cibernéticos presentados en el mundo, se encuentra el que golpeó a algunos de los gigantes de internet y afectó las operaciones de varios sitios como Twitter, Netflix, Spotify, The New York Times y The Guardian.

Funcionarios dijeron a Reuters que el Departamento de Seguridad Nacional y la Oficina Federal de Investigaciones (FBI) están investigando "todas las posibles causas" del ataque. Pero no sólo las redes sociales y los sitios de comercio electrónico vivieron la conmoción: diarios como Infobae, Boston Globe o The New York Times, y cadenas de noticias como CNN, figuran entre las víctimas del hackeo.


MAPA DE INTERRUPCIÓN DE LA CONEXIÓN 13:52 HRS
EL PRIMER ATAQUE A LOS SERVIDORES DE DYN COMENZÓ A LAS 7 DE LA MAÑANA Y FUE RESUELTO DOS HORAS DESPUÉS
EL SEGUNDO ATAQUE COMENZÓ POCO DESPUÉS DE LAS 12 DEL DÍA Y UN TERCER ATAQUE COMENZÓ A LAS 1:37 DE LA TARDE
ESTE ATAQUE DDOS HA AFECTADO A MÁS DE 70 DE LOS MÁS IMPORTANTES SITIOS DE TODA LA WEB, COMO NETFLIX, PAYPAL, REDDIT, SPOTIFY, THE NEW YORK TIMES.
EL ATAQUE COMENZÓ EN LA COSTA ESTE DE ESTADOS UNIDOS Y SE EXTENDIÓ HACIA LA COSTA OESTE, EUROPA, LATINOAMÉRICA Y ASIA.
DYN, LA COMPAÑÍA QUE SUFRIÓ EL ATAQUE DDOS, PUBLICÓ EN SU SITIO WEB QUE HABÍA RESUELTO EL PROBLEMA. A LA 1:53 DE LA TARDE HORA DE MÉXICO, AÚN NO SE PUEDE ACCEDER A MUCHOS DE LOS SITIOS AFECTADOS

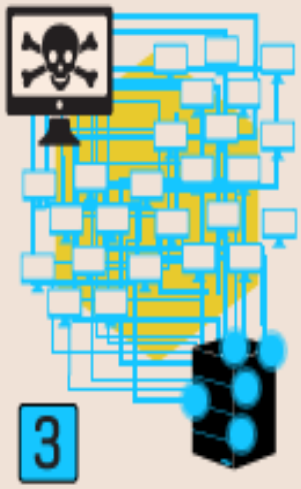
¿QUÉ ES UN DDOS?

1

Los **Servidores de Nombres de Dominio** *(Domain Name Servers)* actúan como guías y facilitan las solicitudes a páginas web específicas, para que una solicitud termine en la página que buscan.

2

Un **ataque de denegación de servicio** o **DDoS,** es un ciber ataque de un grupo de computadoras a una red que causa que un servicio sea inaccesible a otros usuarios legítimos.

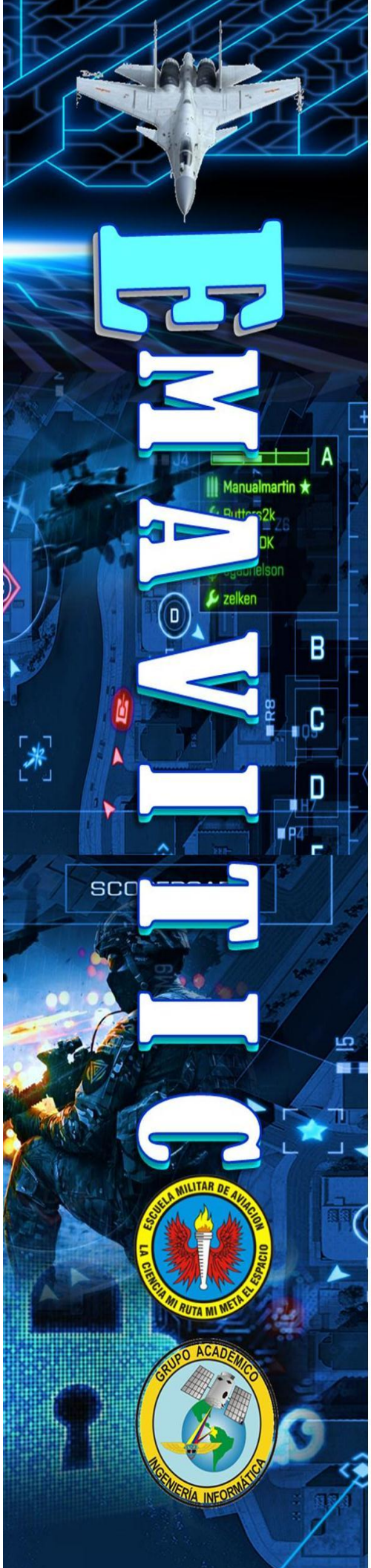


3

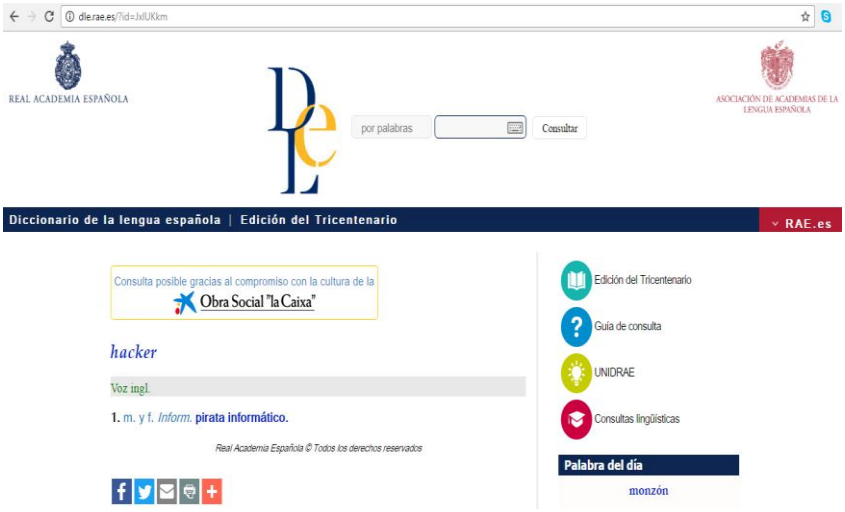
Los *hackers* **utilizan computadoras infectadas** para crear un flujo de tráfico que se origina a partir de muchas fuentes diferentes logrando la ayuda de cientos de miles de computadoras.

4

Cuando se atacan los servidores **los navegadores no pueden encontrar la información** para cargar en las pantallas de los usuarios. Defenderse de los servidores contra ataques DDoS puede ser difícil, pero hay maneras de prevenir interrupciones.



QUE SIGNIFICA SER UN HACKER REALMENTE…



Usualmente la palabra "hacker" suele tener una connotación despectiva o negativa, pues se relaciona a acciones ilícitas o a un ciber delito. Por ello, actualmente existen otras denominaciones para mencionar a quienes utilizan sus conocimientos con fines maliciosos, tales como “piratas informáticos” o “hackers de sombrero negro”.

En tanto, quienes ejercen lo que saben con objeto de desarrollar sistemas de seguridad más avanzados son conocidos como “hackers de sombrero blanco” (white hat hackers).

Lo cierto es que el mundo de hoy, donde las tecnologías de la información avanzan a grandes velocidades, es cada vez más vulnerable al ataque de estos individuos.

Como un modo de llevar este tema al debate público, el diario británico Telegraph publicó una lista con los hackers más famosos del mundo, describiendo, por supuesto, las hazañas" que lanzaron a estos genios informáticos a la popularidad.

La palabra utilizada en determinados ámbitos de las nuevas tecnologías para denominar las pequeñas modificaciones que se le pueden hacer a un programa.

Su derivado, 'hacker', parece provenir del prestigioso Instituto Tecnológico de Massachussets (MIT), donde los investigadores encargados de hacer 'hacks' (alteraciones) de programas se convirtieron en los 'hackers' del equipo.

Desde entonces, ha habido dos cosas que han contribuido a alterar el significado inicial de la palabra: la prensa y Kevin Mitnick.

TOP 5

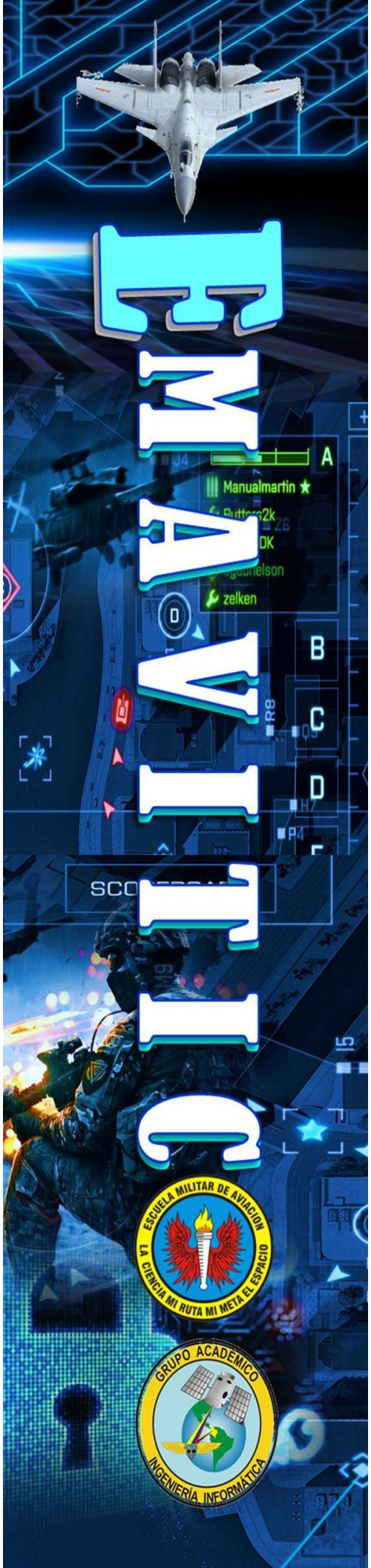
POSICION No.5 ADRIAN LAMO
"El Hacker Vagabundo"

Conocido así por que viajaba continuamente y realizaba todos sus ataques desde cibercafés y bibliotecas.

Su trabajo más famoso fue la inclusión de su nombre en la lista de expertos de New York Times y penetrar la red de Microsoft.

En 2002 fue condenado a 6 meses de arresto domiciliario y 2 de libertad condicional por robar los datos de más de 2.000 suscriptores del diario The New York Times.

Este hacker también se ha hecho conocido porque delató al soldado Bradley Manning cuando este filtró a Wikileaks información del ejército y la secretaría de Estado de EEUU. Irónicamente Ahora trabaja como periodista.



POSICION No. 4. VLADIMIR LEVIN

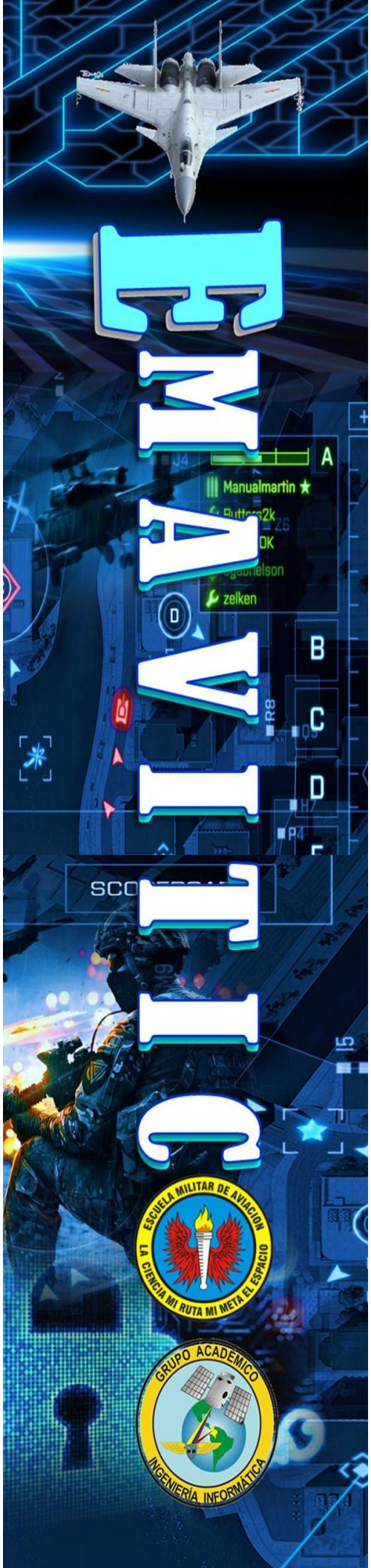
"Robó 10 millones de dólares a clientes de la red de Citibank"

Es un bioquímico graduado en matemáticas por la Universidad Tecnológica de San Petersburgo, Rusia.

Abandonó la ciencia para dedicarse al asalto de sistemas informáticos de entidades financieras, lo que le proporcionaría mayor rentabilidad que sus estudios por si solos. Accedió a la red del Citibank (conocida entidad financiera) y obtuvo una lista de los códigos de cuenta y contraseñas de cientos de usuarios.

Durante las primeras semanas que Levin estuvo accediendo a la red de Citibank, pudo transferir alrededor de 3.7 millones de dólares que trasladaba a cuentas corrientes de su grupo en Argentina, Estados Unidos, Finlandia, Holanda, Alemania e Israel. Para tal hazaña contó con el apoyo inicial de un conductor de autobús (quien también era hombre de negocios) y que Levin había conocido en julio de 1994, al cual informó de lo que había podido hacer y del que se hizo amigo y socio, formando un grupo internacional de hackers.

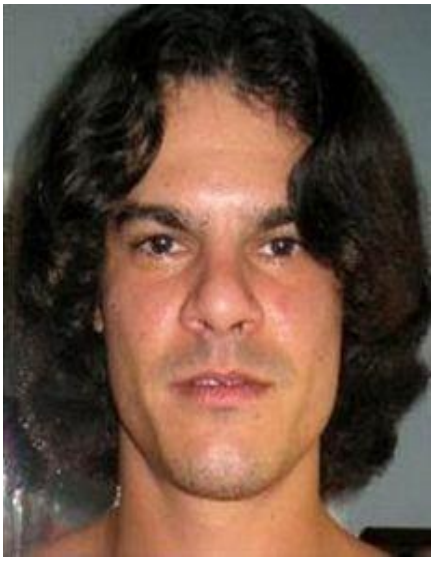
En semanas posteriores a este encuentro se hicieron otras muchas transferencias a cuentas corrientes mantenidas por



Shore Corp. gracias a un amigo de Vladímir, Yevguenij Korolkov. Al menos 40 transferencias más fueron realizadas a Argentina, Suiza, Israel, California, Alemania y Holanda.

Cuando el banco notó las transferencias contactaron con las autoridades, quienes siguieron la pista durante meses hasta Levin, quien finalmente sería arrestado por laINTERPOL en 1995 en el aeropuerto de Heathrow, en Inglaterra y más tarde extraditado a los Estados Unidos.

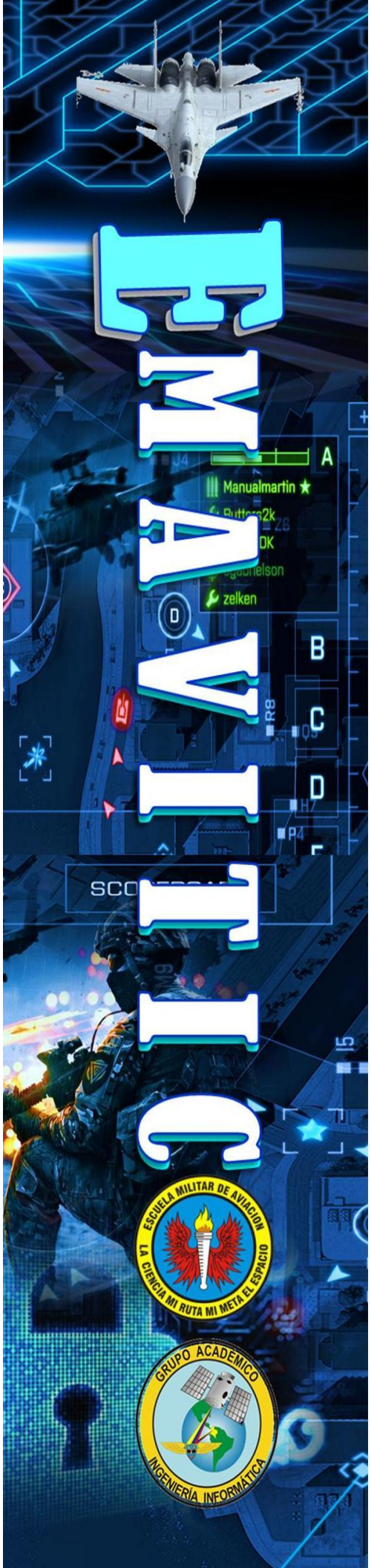
POSICION No.3. ALBERT GONZALEZ "Soupnazi"
170 millones de tarjetas de crédito hackeadas desde Miami Beach



Cubano: es la persona que se escondía detrás del sobrenombre de "soupnazi", el responsable de uno de los mayores robos de identidad de la Historia de Internet.

Consiguió acceder y robar a las cuentas de más de 170 millones de tarjetas de crédito de usuarios de todo el mundo.

Este hacker fue detenido en 2008 en un hotel de Miami Beach y en 2010 fue condenado a 20 años de prisión por un tribunal federal en Nueva Jersey. Se cree que González trabaja con otros hackers que nunca pudieron ser detenidos por ocultarse en diferentes países.



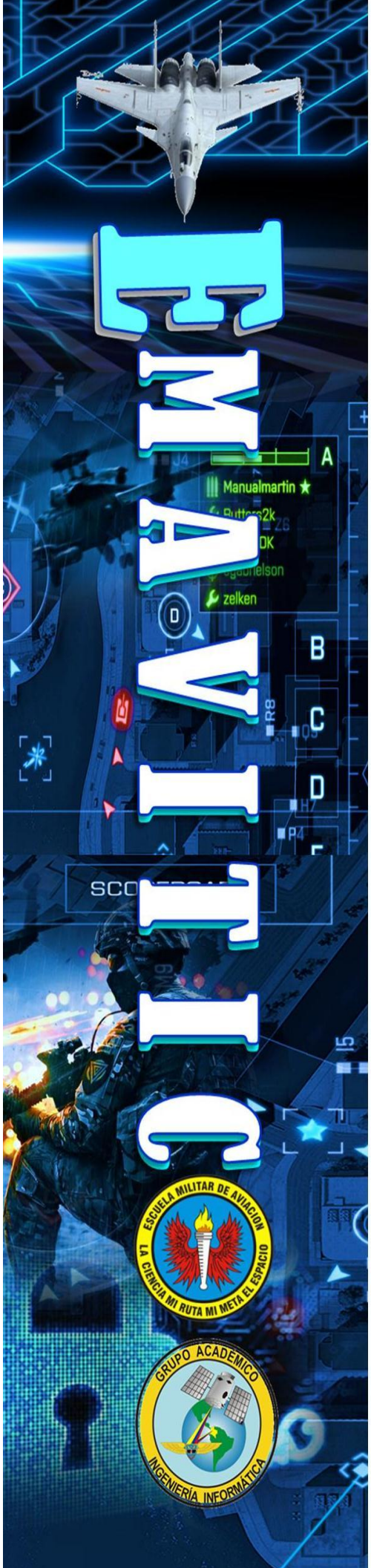
POSICION No.2. KEVIN MITNICK (El Condor)
"El criminal informático más buscado de la historia"

Sin duda uno de los hackers más famosos y recordados por diferentes generaciones, ya que este estadounidense, conocido como "El Cóndor", fue calificado como "el criminal informático más buscado de la historia" por el Departamento de Justicia de EU.

¿Qué hizo? Si bien su ilegal actividad cibernética comenzó en los 70 –cuando utilizaba el sistema de acceso para los autobuses en Los Ángeles y así poder viajar gratis–, fue a partir de los 80 cuando ganó fama, luego de que penetró sistemas ultra protegidos, como los de Nokia y Motorola, para robar secretos corporativos, incluso se sabe que hasta "hackeaba" a otros hackers.

Fue apresado en 1995 y su encarcelamiento alcanzó gran popularidad entre los medios por la lentitud del proceso y las estrictas condiciones a las que estaba sometido; recibió una condena de más de 5 años tras las rejas.

Se le liberó en 2002 y ahora se dedica a la consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security. Además es autor y conferencista. Del cibercriminal más buscado de Estados Unidos al reconocido emprendedor en ciberseguridad.



POSICION No.1. "CRACKA"
El misterioso adolescente británico que hackeó al director de la CIA.

El último ciberdelincuente en llamar la atención de la prensa internacional es un joven británico que a sus 16 años consiguió hackear los correos personales del Director de la CIA, el director del FBI y el Director de Inteligencia Nacional. Además, hackeó las cuentas de teléfono de este último y reveló la identidad de 31.000 agentes del gobierno de Estados Unidos: CIA, Seguridad Nacional, FBI. La verdadera identidad de este joven no se ha desvelado pero sabemos que se hace llamar "Cracka" y asegura ser miembro de un grupo de hackers llamado "Crackas with Attitude" que actúa en defensa del Movimiento Palestino. "Cracka" fue detenido el mes pasado en el sureste de Inglaterra.

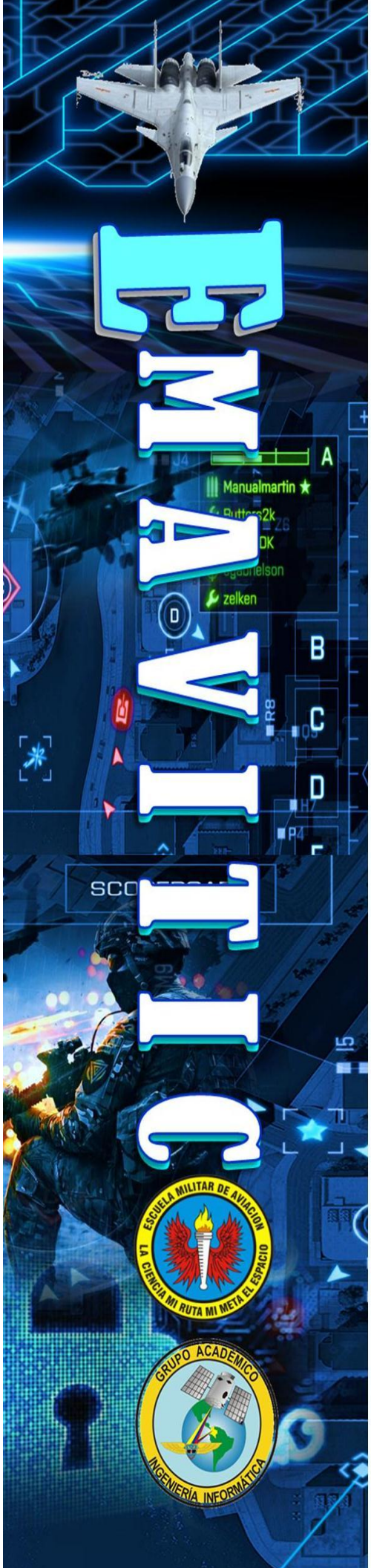
Los episodios de la historia demuestran la facilidad con la que los servicios de Internet pueden ser vulnerados en una escala nunca antes vista. ES O NO NECESARIA LA DATAVIGILANCIA EN LAS CIUDADES INTELIGENTES…**CIUDADANO DIGITAL EMPIEZA POR TU CULTURA**…

4.4 LEONARDO HUERTAS CALLE

Ilustración 16 Conferencista Leonardo Huertas Calle

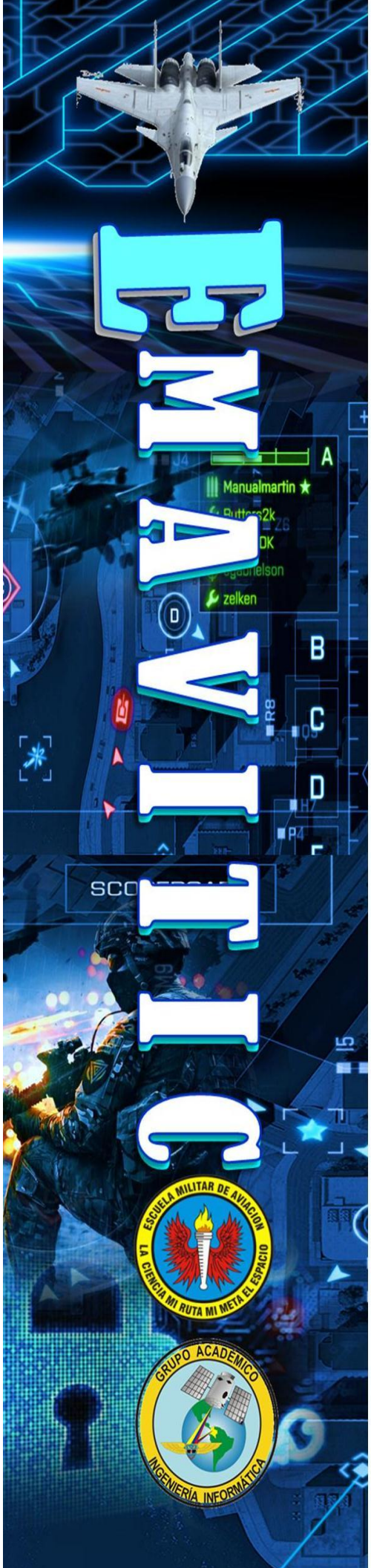
Fuente: Autor

Ha sido speaker internacional en temáticas de Seguridad y entre otros estudios, realizó con la Universidad de Carnegie Mellon el curso de “Advanced Incident Handling”, capacitado por el Gobierno americano y por la misma Organización de



los Estados Americanos – OEA, en diferentes temáticas de ciberseguridad, cuenta con la certificación como hacker ético expedida por la ECCouncil.

Es Ingeniero de Sistemas de la Universidad EAN de Bogotá y de igual forma, cuenta con las especializaciones de Gerencia de Proyectos de Ingeniería y Gerencia Informática de la misma universidad, es especialista en Seguridad de Redes y Especialista en Seguridad de Sistemas Operativos de la Universidad Ouberta de Catalunya. Dedicó 20 años de su vida a trabajar para el Ministerio de Defensa de Colombia donde se desempeñó como Asesor de Ciberseguridad y Ciberdefensa. Durante este periodo de tiempo formó parte de mesas bilaterales de cooperación en temas de seguridad cibernética entre Colombia y los gobiernos de Israel y Corea del Sur. Fue el responsable técnico en la generación de la "Política Nacional de Ciberseguridad y Ciberdefensa - CONPES 3701" de Colombia, y posteriormente se encargó de diseñar e implementar el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, donde finalizó su carrera en el Gobierno como coordinador del grupo.



CONFERENCIA: BUCEANDO EN LAS PROFUNDIDADES DE LA DEEP WEB

El mundo de internet parece no acabar. Una página conduce a otra, un enlace se conecta con otro y así, de manera casi infinita.

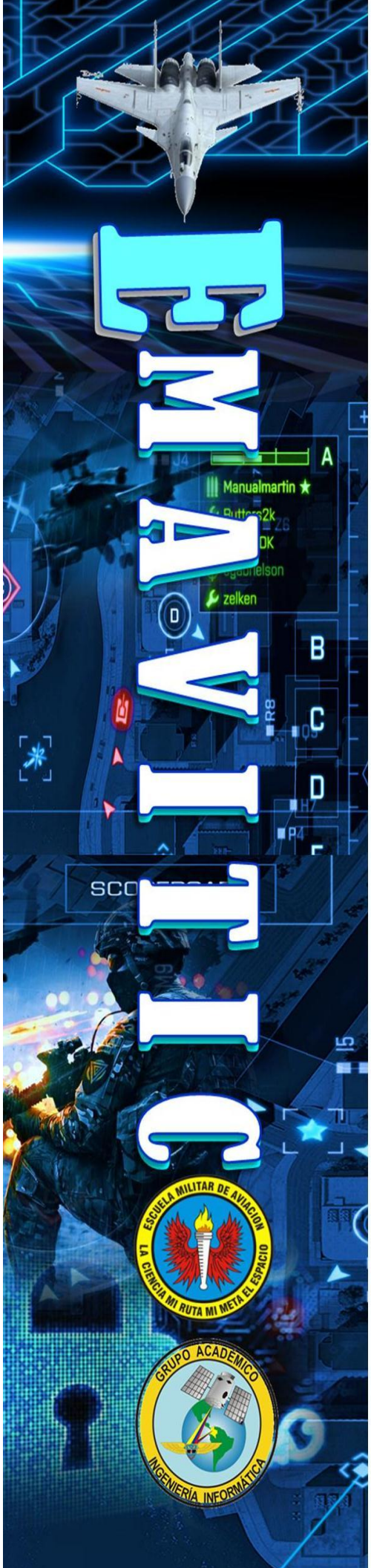
Sin embargo, el internet que todos creemos conocer es solo el 15 por ciento; el 85 por ciento restante está debajo de la punta del iceberg en lo que se denomina la Deep Web (‘web profunda’).

Google, el gigante de los buscadores, puede indexar 45.000 millones de páginas web, pero la Deep Web se calcula en más de 500 veces esa cantidad. Contraseñas de correos, transacciones bancarias, intranets y todo lo que se considere confidencial pasa por la Deep Web.

Por eso, esta es la parte de internet que más gusta a hackers, ciberdelincuentes y activistas proderechos humanos que viven en regímenes totalitarios.

De igual forma, las Darknets (redes oscuras) permiten acceder a los lugares más profundos de la DeepWeb.

Para qué se utilizan las Darknets (redes oscuras)? Anonimato: Ocultar quien soy yo



Privacidad: Ocultar lo que se transmite Cibercrimen.

La Deep Web carga miles de datos a los que solo se puede acceder con navegadores especializados, tanto para actividades legales como para cometer delitos. Y para sumergirse en esta red de una manera un poco más segura, se usa el software The Onion Router, más conocido como TOR.

El Proyecto TOR (www.torproject.org) surgió en los laboratorios de la Armada estadounidense para proteger las comunicaciones navales. Hoy es un software de código abierto en el que participan el Departamento de Estado de Estados Unidos, Google o la Fundación Ford, entre muchos otros donantes.

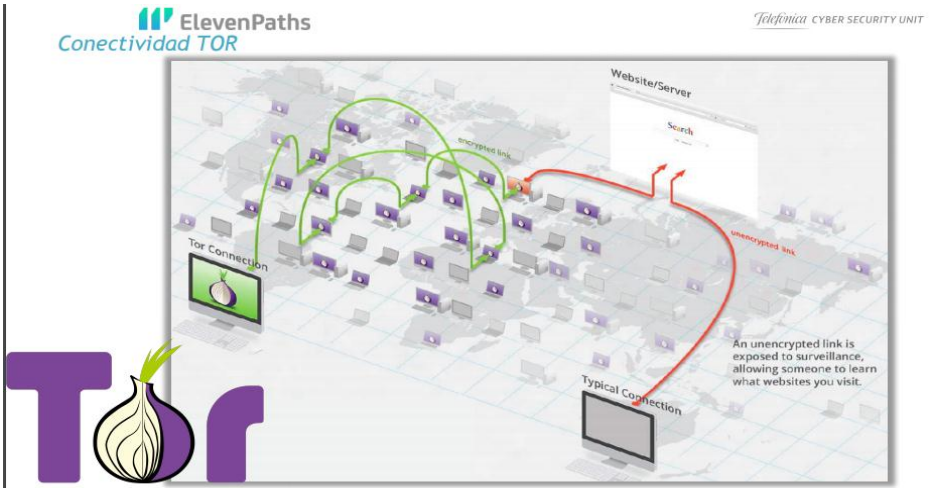
TOR siempre está desarrollando nuevas formas de garantizar la privacidad de los navegantes para que no quede ningún rastro de su paso por internet. Civiles preocupados por la libertad de expresión, periodistas, disidentes y ONG se valen de TOR para denunciar y comunicarse.

Las autoridades también lo utilizan para hacer labores de inteligencia sin ser descubiertas o para capturar ciberdelincuentes. Por supuesto, hay quienes le dan un uso indebido para lucrarse.

Los gobiernos hacen circular por aquí sus informes top secret, pero gracias a los Wikileaks de Julian Assange o a las revelaciones de Edward Snowden sobre las prácticas de la Agencia de Seguridad Nacional de Estados Unidos, hoy sabemos que no hay nada oculto bajo el sol.[3]

[3] http://www.eltiempo.com/archivo/documento/CMS-14462675

Dos desventajas de TOR:
• Por una parte, es un sistema lento.
• Por otra, ya ha sufrido diversos ataques y/o vulneraciones de la privacidad por parte de las autoridades

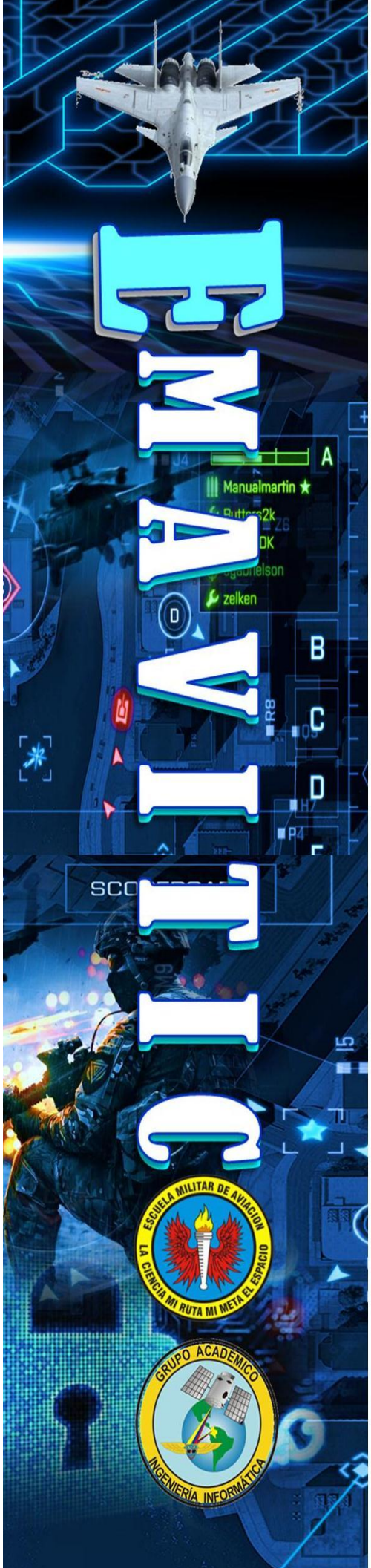


Otras de las herramientas empleadas es I2P y FREENET

I2P (sigla para Invisible Internet Project, que significa Proyecto de Internet invisible) es un software que ofrece una capa de abstracción para comunicaciones entre ordenadores, permitiendo así la creación de herramientas y aplicaciones de red con un fuerte anonimato.

Sus usos incluyen páginas webs anónimas, servidores y clientes de chat, blogging, transferencia de archivos, además es una red que se adapta muy bien a las redes P2P. I2P es software libre y utiliza varias licencias libres.

La red I2P está basada en el concepto de túneles entrantes y salientes, lo cual ofrece facilidad para la adaptación de programas preexistentes a la red I2P. Cada túnel está



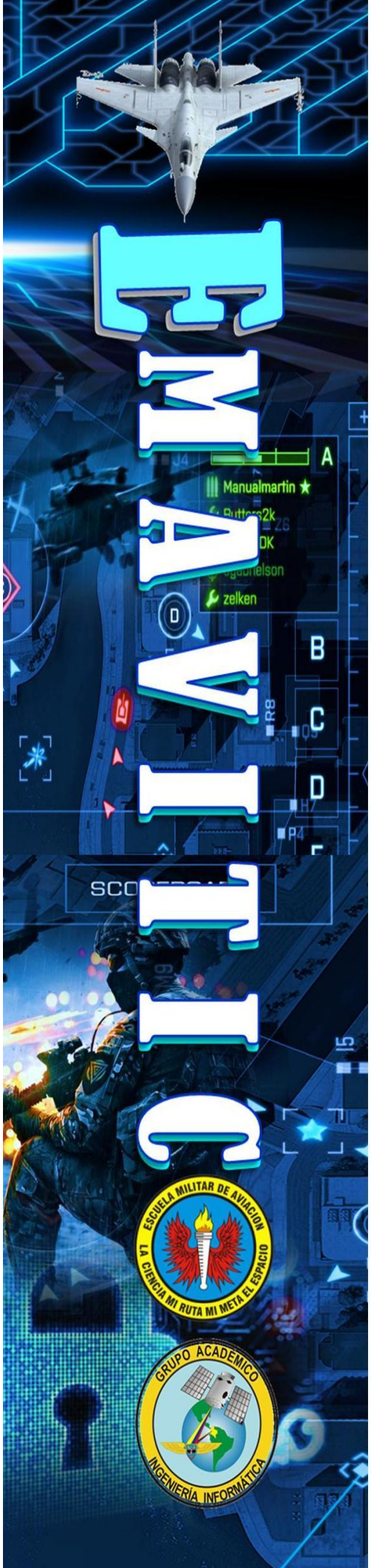
compuesto por una secuencia de nodos padres, los cuales transportan la información en un sentido unidireccional.

I2P soporta la mayoría de los protocolos de red TCP y UDP, tanto sobre IPv4 como sobre IPv6.

I2P es una red que se fortalece contra diversos tipos de ataques contra la privacidad y el anonimato con el número de usuarios, cuantos más usuarios tiene la red más difícil es usar efectivamente la mayoría de estos ataques.

El software más usado y probado de I2p está escrito en Java,[cita requerida] pero existen dos versiones más del núcleo de la aplicación en C y C++. La versión java incluye además la consola del router donde se permite configurar la mayoría de las opciones de la red.

ElevenPaths
Telefónica CYBER SECURITY UNIT
Consola I2P

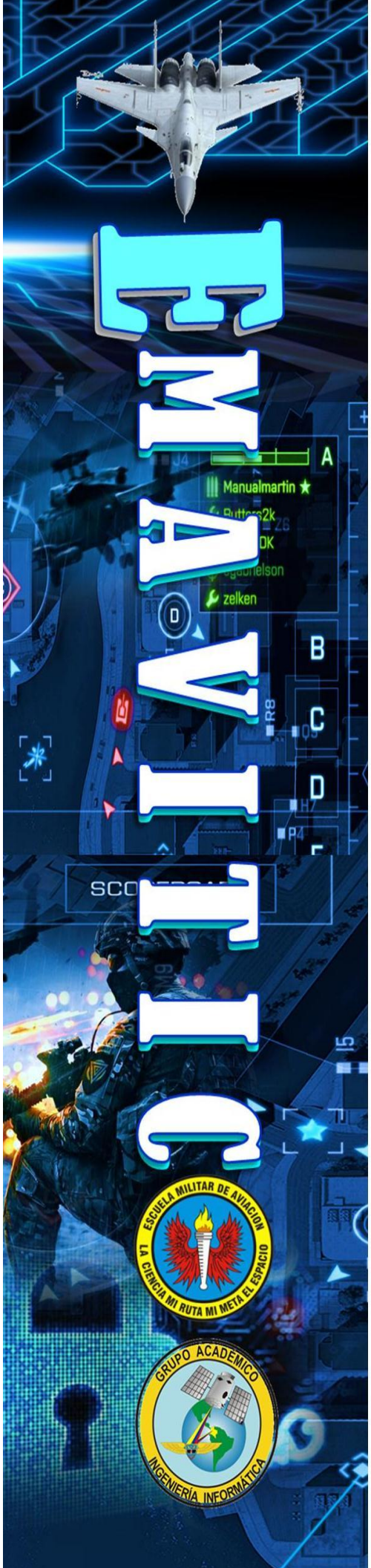


Por otro lado, Freenet es una red de distribución de información descentralizada y resistente a la censura diseñada originalmente por Ian Clarke. Freenet tiene por objeto proporcionar libertad de expresión a través de las redes de pares mediante una fuerte protección del anonimato; como parte del apoyo a la libertad de sus usuarios, Freenet es software libre. Freenet trabaja por medio de la puesta en común del ancho de banda y el espacio de almacenamiento de los ordenadores que componen la red, permitiendo a sus usuarios publicar o recuperar distintos tipos de información anónimamente. Freenet ha estado bajo continuo desarrollo desde el año 2000

Freenet es una red inproxy, Osea que solo permite la conexion a esa red y no a una externa (Es una VPN en el sentido mas puro) y dentro de esta red se pueden crear grupos mas pequeños de "Friends" y solamente se pueden comunicar entre ellos. Basicamente es poder conectarse a con tus amigos a una red privada dentro de una red privada.

Ejemplos de uso ilegítimo:

• “Servicios Financieros”: lavado de bitcoins, cuentas de PayPal robadas, tarjetas de crédito clonadas, falsificación de billetes...
• “Hackers” por encargo (es mejor llamarlos delincuentes cibernéticos)
• “Servicios comerciales”: explotación sexual y mercado negro de gadgets robados, armas y munición, documentación falsa, en un alto porcentaje venta de drogas.
• Secretos de Estado y soplones: hay un mirror de WikiLeaks en la deep web.



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

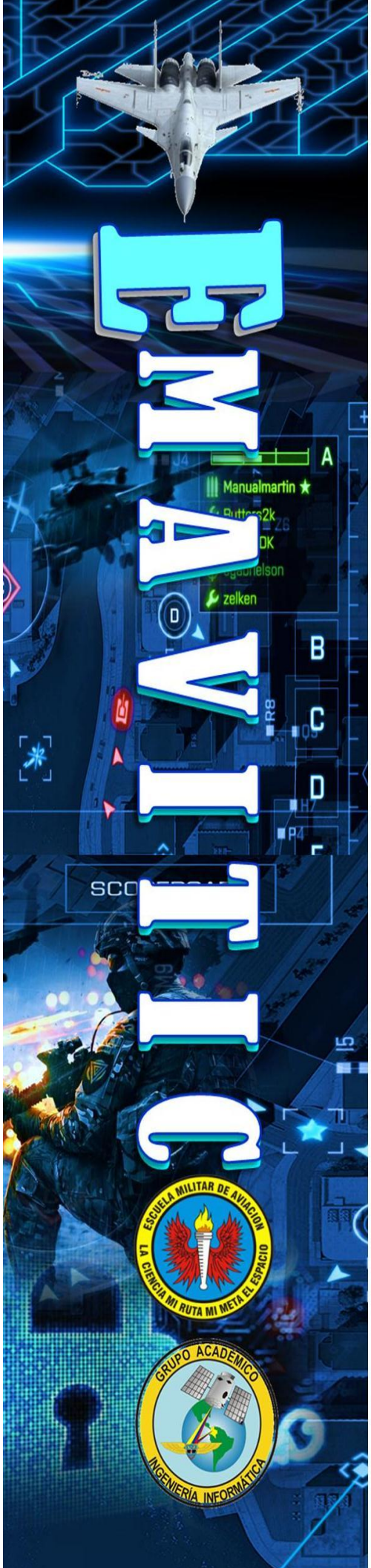
El coste del cibercrimen ya representa un 0,8% de la economía mundial, superando al tráfico de drogas y armas.

Algunos precios de hacking por servicio:

- Hackear un servidor web (VPS o hosting): 120 US
- Hackear un ordenador personal: 80US
- Hackear un perfil de Facebook, Twitter, etc: 50US
- Desarrollar spyware: 180 US
- Localizar a alguien: 140 US
- Investigar a alguien: 120 U

ElevenPaths
Uso de la darkweb por los terroristas

Telefónica CYBER SECURI



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

ElevenPaths

Telefónica

Peligros de navegar en la DeepWeb

ElevenPaths

Telefónica CYBI

Recomendaciones para navegar en la DeepWeb

Programa de Ingeniería Informática
Escuela Militar de Aviación Marco Fidel Suárez
"El Ciberespacio, El Quinto Dominio de la Guerra

DEEP DARK INTERNET

WEB

LO QUE ENTENDEMOS POR INTERNET: REDES SOCIALES, MEMES, FOTOS DE GATITOS Y LO QUE SEA QUE ENCUENTRES CON GOOGLE.

DEEP WEB

CUALQUIER COSA A LA QUE **PUEDES ACCEDER** EN INTERNET PERO QUE NO ESTÁ INDEXADO EN LOS BUSCADORES (MUCHAS VECES PORQUE A NADIE LE IMPORTA).

CONTRARIO A LA LEYENDA POPULAR, LA DEEP WEB ES UN LUGAR MUUUUY ABURRIDO.

DARK WEB

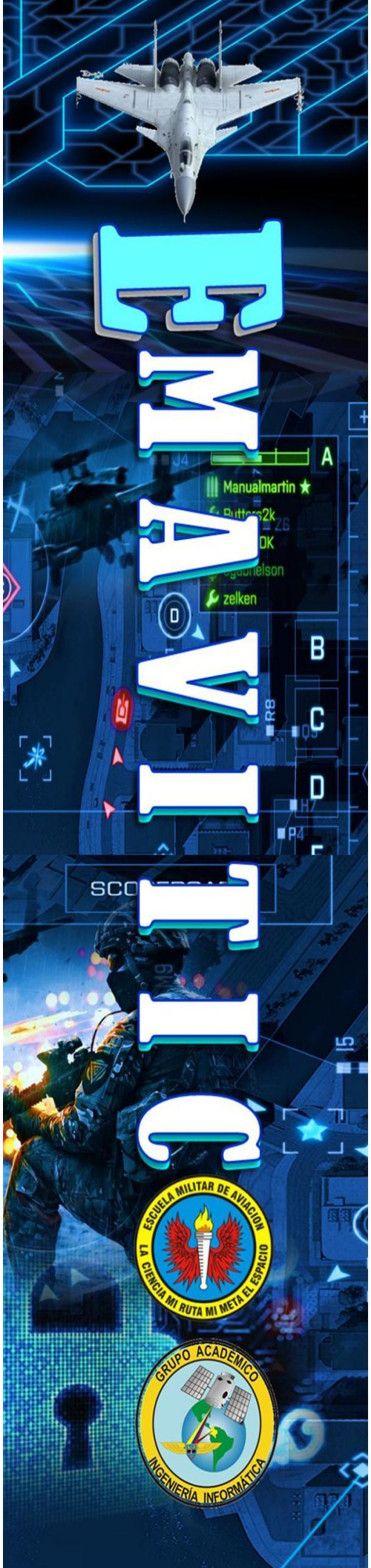
ES TECNOLOGÍA Y SITIOS ENCRIPTADOS QUE **NI SON VISIBLES NI QUIEREN SER RASTREADOS.**

PICTOLINE.COM

4.5 CORONEL (R) MARTHA LILIANA SANCHEZ

Ilustración 17 Conferencista Coronel (R) Martha Liliana Sánchez

Fuente: Autor



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

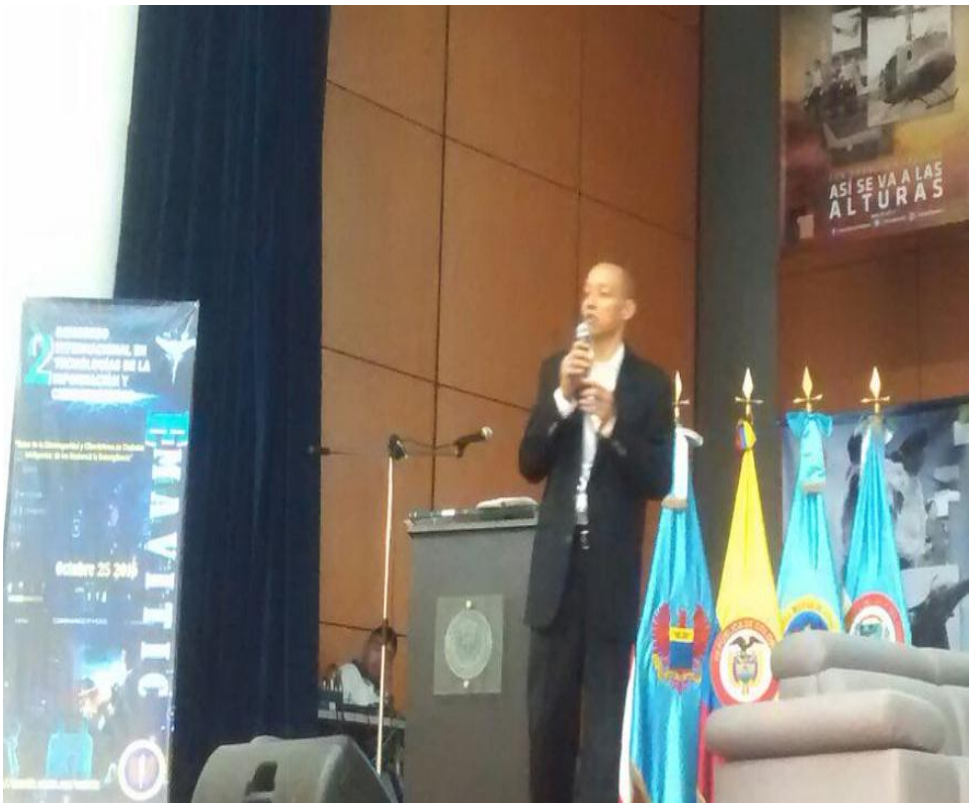
Congreso Internacional

Oficial de la Fuerza Aérea Colombiana (R), Profesional en Ingeniería de Sistemas, Magister en Administración de Empresas, especialista en sistemas de información, con estudios de maestría en Seguridad y Defensa Nacional, diplomado en Ciberseguridad y ciberdefensa y actualmente Doctorante de la Universidad Alfonso X el Sabio de Madrid-España.

Posee conocimiento y experiencia en seguridad de la información y líneas de ciberseguridad y ciberdefensa, procesos de gobierno, seguridad y defensa nacional, coyuntura pública, innovación social y comportamiento organizacional.

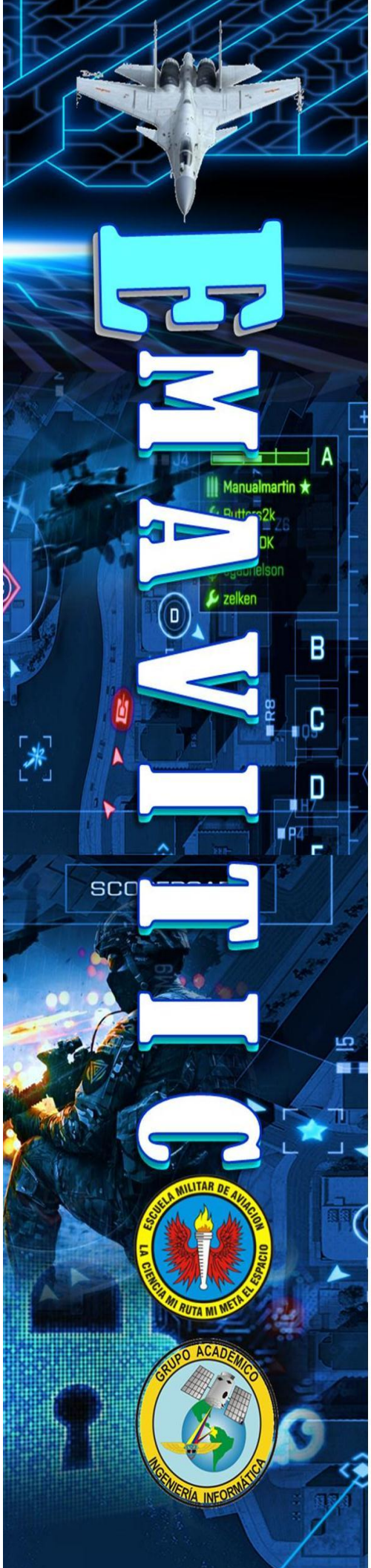
4.6 FABIAN CASTILLO PEÑA

Ilustración 18 Conferencista FABIAN CASTILLO PEÑA



Fuente: Autor

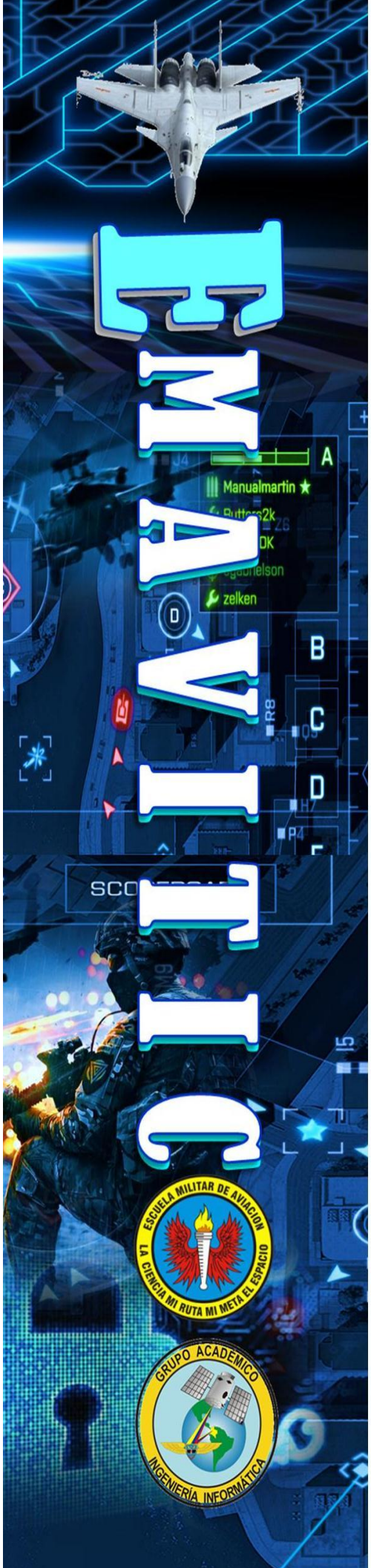
Ingeniero de Sistemas, Especialista en Auditoría de Sistemas, Magister en Educación y con Estudios de Doctorado en Educación. Director del Programa de Ingeniería de Sistemas de la Universidad Libre. Líder de los grupos de Investigación SINERGIA UNO y GITEL Auditoría y Telemática).



Auditor Líder (ISO 27001:2013), Auditor Interno en Sistemas de Gestión Integral QHSE (ISO 9001: 2008, ISO 14001: 2004, OHSAS 18001: 2007 e ISO 19011:2012), Auditor Interno (ISO 9001:2008). Presidente REDIS Nodo Valle del Cauca y RUAV. Coordinador académico ASUOC- RUA, Miembro académico RENATA – RIBIE.

CONFERENCIA CIBERSEGURIDAD Y CIUDADES INTELIGENTES OPORTUNIDADES DE INVESTIGACIÓN – RUAV

Una Ciudad Inteligente “Smart Citie” es una ciudad innovadora que utiliza las Tecnologías de la Información y Comunicación (TIC) y otros medios para mejorar la toma de decisiones, la eficiencia de las operaciones, la prestación de los servicios urbanos y su competitividad, este modelo de ciudad obliga a que elementos como el urbanismo, infraestructura, transporte, servicios, etc., evolucionen hacia

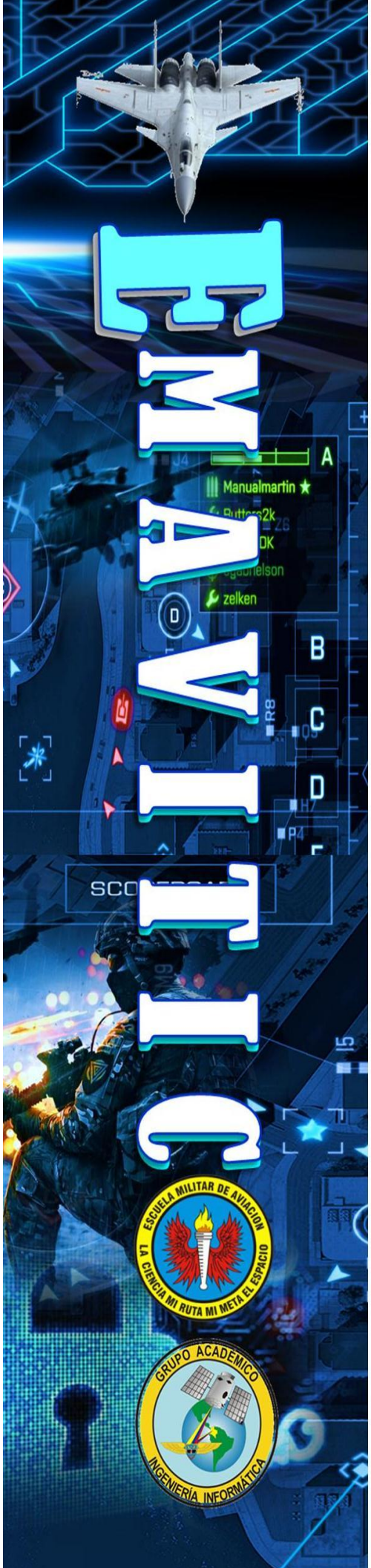


plataformas inteligentes que interactúen entre sí para lograr una gestión eficiente. Al mismo tiempo, procura satisfacer las necesidades de las generaciones actuales y futuras en relación con los aspectos económicos, sociales y del medio ambiente. Ciudades en las que existirá una red compleja de sensores accesibles a través de los cuales se obtendrá información para el funcionamiento y la toma de decisiones.

Para esta tarea de recolección es necesario que todas las áreas se encuentren interconectadas a través de una red de comunicaciones que permita el análisis y control permanente en tiempo real mediante servicios, aplicaciones y herramientas basados en software como servicio.

El desarrollo de una ciudad inteligente resulta interesante para los ciudadanos, empleados y empresarios, pues genera un espacio con mejores servicios y con un ambiente de innovación que incentiva soluciones creativas y amigables que permite la generación de empleo y la inclusión social. De esa manera, las Ciudades Inteligentes promueven un ciclo que produce bienestar económico y social. La implementación de una Ciudad Inteligente es una tarea compleja que requiere de gran liderazgo y visión, y que supone múltiples beneficios para los gobernantes y la ciudad, estimula la cooperación público privada y promueve la competitividad local.

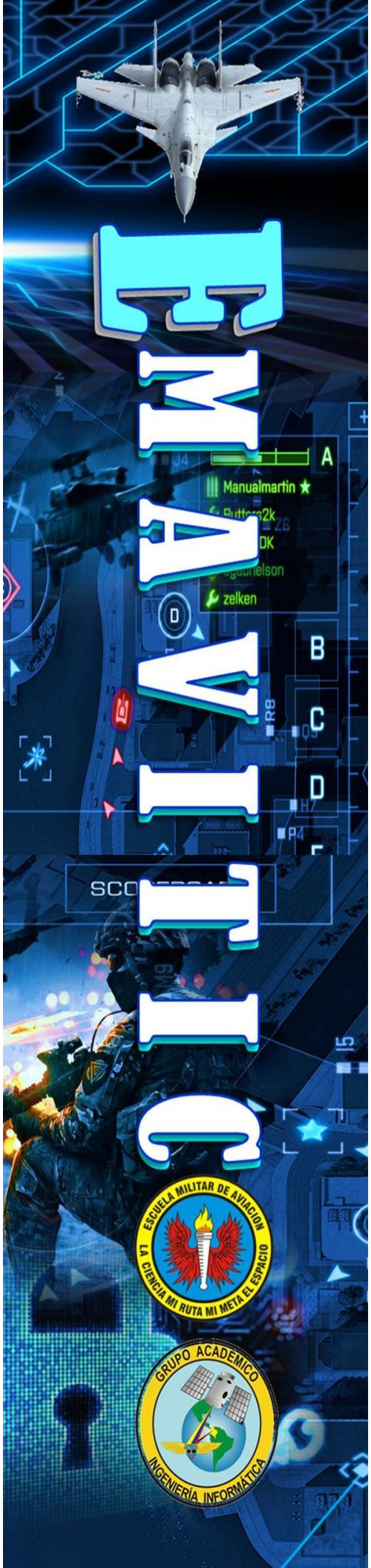
Las Tecnologías de la Información y Comunicación (TIC) se han convertido en un aliado fundamental para la gestión de ciudades inteligentes, en la actualidad las ciudades de América Latina y el Caribe se han convertido en protagonistas de uno de los procesos de crecimiento demográfico más significativos que ha vivido el planeta, con grandes consecuencias para la sostenibilidad, la calidad de



vida y la competitividad de la región. Para poder hacer frente a estos retos es necesario un cambio en el ámbito de la gobernanza y la toma de decisiones, así como el uso cada vez más eficiente de los recursos de nuestras ciudades, con miras a emprender una gestión inteligente, aunado con esfuerzos del sector educativo, aportes en investigación, desarrollo e implementación de herramientas y conocimientos desde la academia para la construcción de una mejor sociedad, que aporte mayor progreso y competitividad para todos sus ciudadanos; en aras de lograr estos cambios es necesario determinar un marco de normatividad que defina las leyes, decretos, acuerdos y normas de seguridad y confidencialidad con el fin de preservar la privacidad e integridad de la información de todos los usuarios, por medio de la seguridad física, la gestión y el desarrollo de software.

Estas ciudades inteligentes apoyadas con el uso de la tecnología deben garantizar la gestión eficiente integración y análisis de la gran cantidad de datos generados y capturados en diferentes fuentes que sirvan para anticipar, mitigar e inclusive prevenir situaciones de crisis, mecanismos que permitan ofrecer mejores servicios, alertas e información a los ciudadanos. Sin embargo, a pesar de su importancia, la tecnología es solo una herramienta que debe vincularse al proceso de planificación y de gestión.

El uso de las TIC debe generar modificaciones en los procesos, retroalimentar la planificación, modificar dinámicas en la oferta de servicios públicos, transformar problemas en soluciones creativas, agregar valor a la infraestructura instalada y mejorar los indicadores de desempeño. Es decir, hacer una ciudad más inteligente supone contar con resultados efectivos y cuantificables, que pueden ser verificados por los habitantes y por quienes visitan la ciudad.



Sin embargo, el uso de estas tecnologías debe ser entendido como un medio y no como un fin, es necesario un cambio en los ciudadanos, es decir cada día tener más ciudadanos inteligentes, personas con rol de beneficiarios pero también de partícipes de la transformación a partir del uso activo de dispositivos y aplicaciones móviles que facilitan cada vez más el seguimiento y la colaboración con las políticas del gobierno.

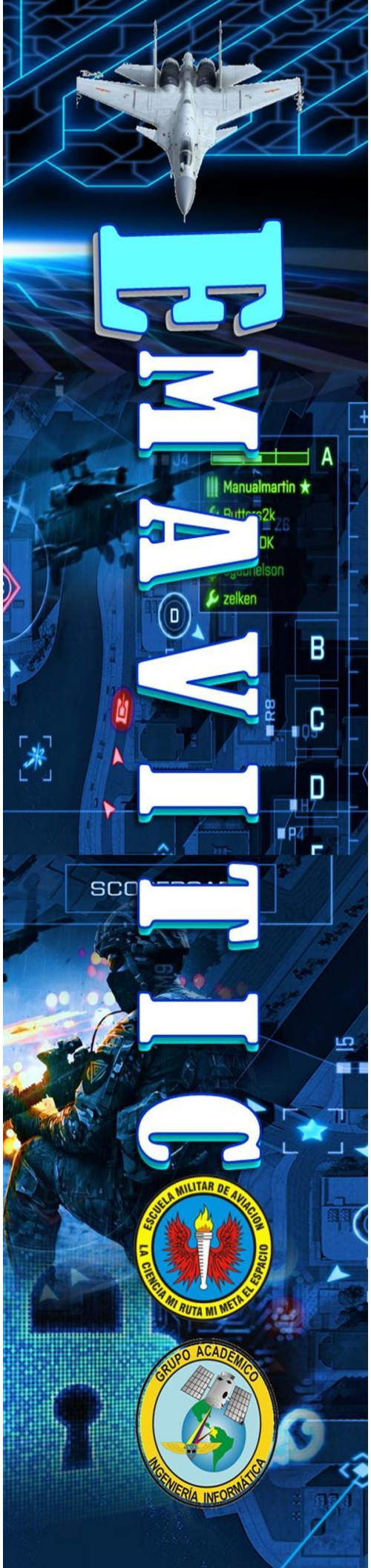
4.7. JUAN DAVID BERRIO LOPEZ

Ilustración 19 Conferencista Juan David Berrio López

Fuente: Autor

Profesional en Ingeniería Informática con Maestría en Seguridad Informática, Posgrado en Seguridad en redes y en Administración: Énfasis Redes Corporativas Nuevas Tecnologías e Integración de Tecnologías, Coordinador de Auditorias de Tecnologías de la información.

CEO Certified Offensive and Defensive Security Expert-Specialist.
CEO curso de Entrenamiento Certified Offensive and Defensive Security Forensic.

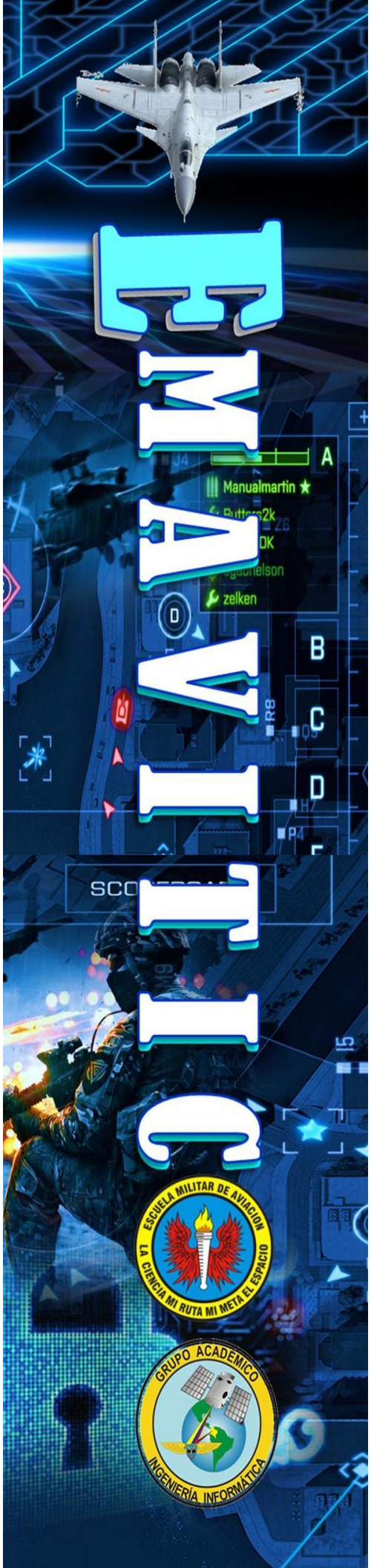


CONFERENCIA HACKING ÉTICO - ATACANTE INFORMÁTICO VS INVESTIGADOR FORENSE

Una batalla de fortalezas y destrezas se genera entre estas dos personalidades del ámbito digital, cuando se produce un incidente de seguridad informático o un ciberdelito.

Cada uno aspirara a que su contrincante sea menos suspicaz, ágil y conozca menos de su materia. Estos, tienen como plataforma de combate la evidencia digital y sus fuentes.

Si revisamos un poco de bibliografía sobre procesos de hacking, nos encontraremos con las fases que se recomiendan a seguir para dicho fin, así tenemos al footprinting, la enumeración, la obtención Acceso, la escalada de Privilegios, entre otros, pero destacaremos un paso muy importante que es el BORRADO DE HUELLAS,



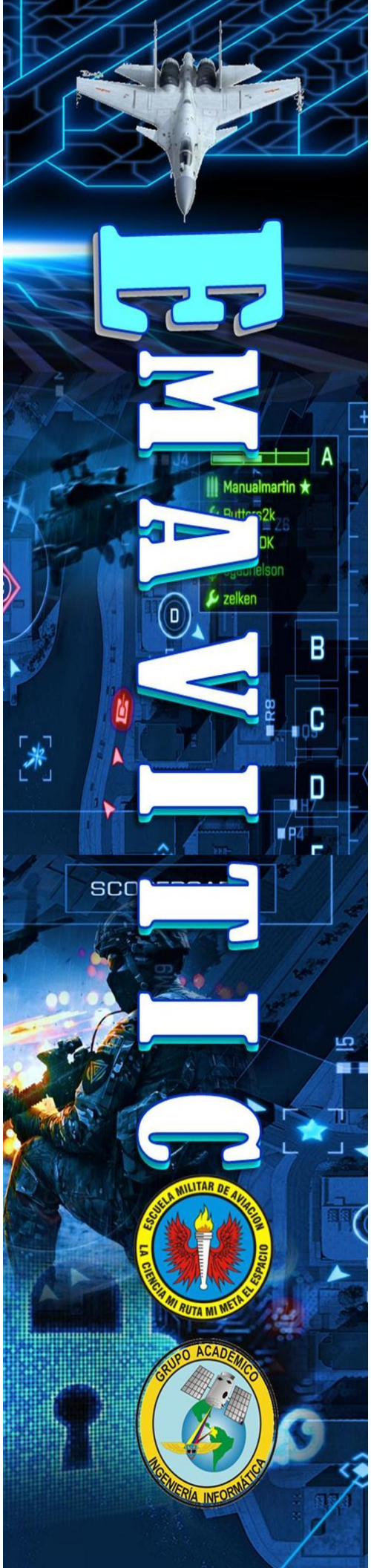
que pocos los realizan y nos permite determinar la capacidad del atacante.

¿Que requiere un "hacker" para realizar un borrado de huellas? – Saber dónde se generan.
¿Es una destreza?, Así es.

Es una destreza que debe tener un atacante, saber que datos genera cada acción que realiza sobre un sistema ajeno, para luego realizar el borrado de huellas que ocultara su acción y porque no su identidad.

Aquí entra en la batalla un informático forense, que así como el "hacker" deberá conocer donde se generan las evidencias y de cada una de sus fuentes, extraerlas correctamente, para ser analizadas y esclarecer lo sucedido.

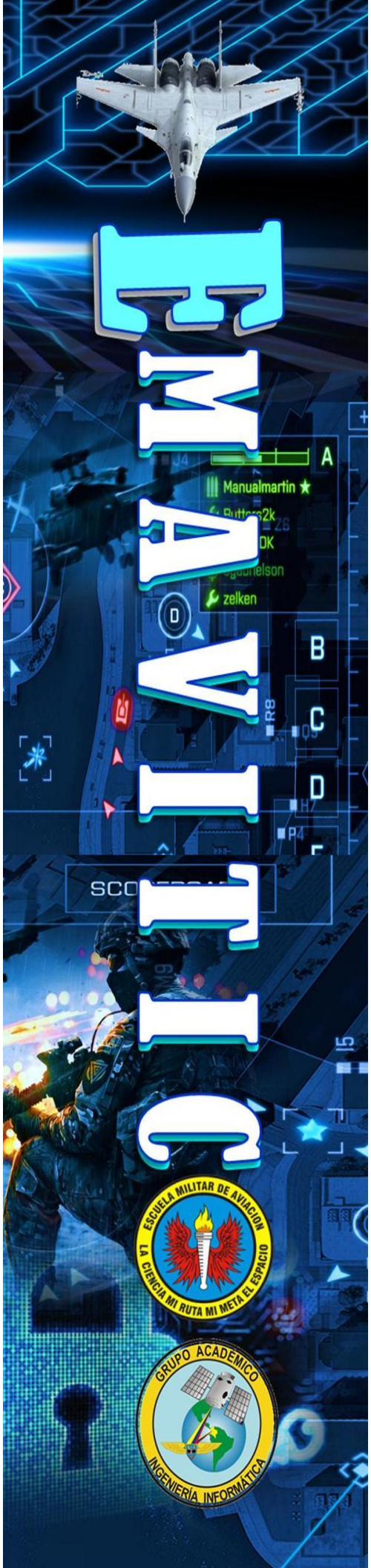
El forense informático encontrara lo que el atacante dejo o por desconocimiento nunca lo borro, siendo los peores errores de los atacantes novatos, que realizan una mala acción dentro de un sistema sin conocerlo apropiadamente.



4.8. MANUEL SÁNCHEZ RUBIO

Co- Director de la Cátedra DARS de Ciberinteligencia- Escuela Politécnica Superior - Universidad de Alcalá – España , Doctor por la Universidad de Alcalá, Ingeniero en Informática, Diplomado en Informática de Sistemas.

Científico titular de la OPI en el Instituto Nacional de Técnica Aeroespacial del Ministerio de Defensa. Profesor Asociado del Departamento de Ciencias de la Computación de la Universidad de Alcalá. Investigador Principal del Grupo de Investigación Cybersecuritics. Subdirector de la Cátedra amaranto de Seguridad digital.



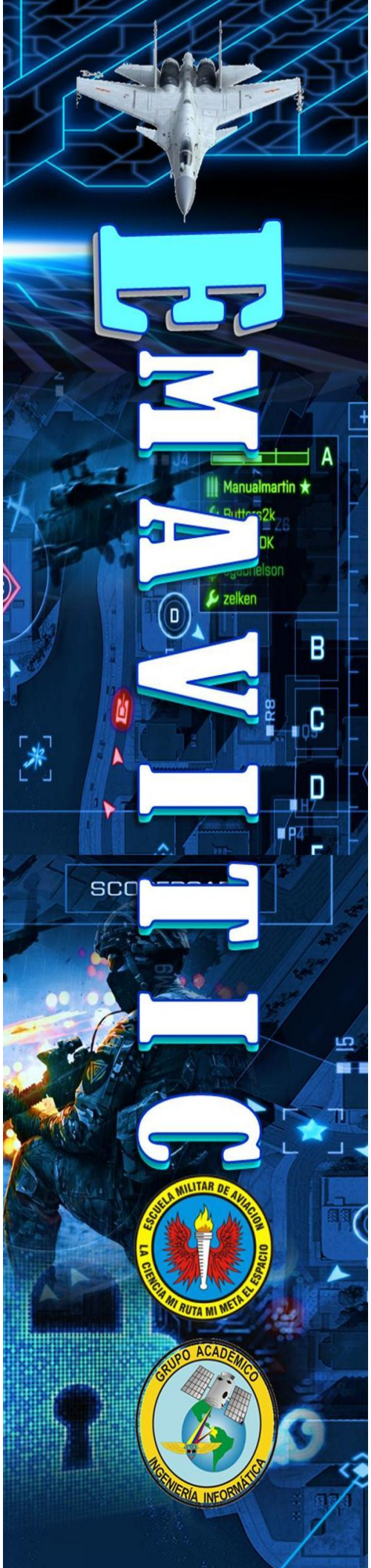
5. WORKSHOP CURSO 92D

Como parte de EMAVITIC se tiene el Workshop que realizarán los Cadetes del Curso 92D del Programa de Ingeniería Informática de la Escuela Militar de Aviación, donde presentaran sus conocimientos y proyectos de aula que evidencian el uso de la electrónica y la programación de sistemas embebidos en proyectos multidisciplinarios que nacen del trabajo interdisciplinario de los Cursos de Fisica I, Arquitectura Computacional e Informática II que dictan los Orientadores de Defensa Sandra Milena Ramos, Jair Abadia y Tulio Nel Benavides.

A continuación, se listan los proyectos presentados en el workshop

TABLERO LED:
CD2 Méndez Becerrra José David
CD2 Muñoz Prada Juan Camilo
CD2 Olaya Sierra Juan Sebastian
CD2 Mayorga Mendieta Miguel Angel
CD2 Portillo Cruz Carlos Arturo
CD2 Loaiza Ortega Cesar Camilo

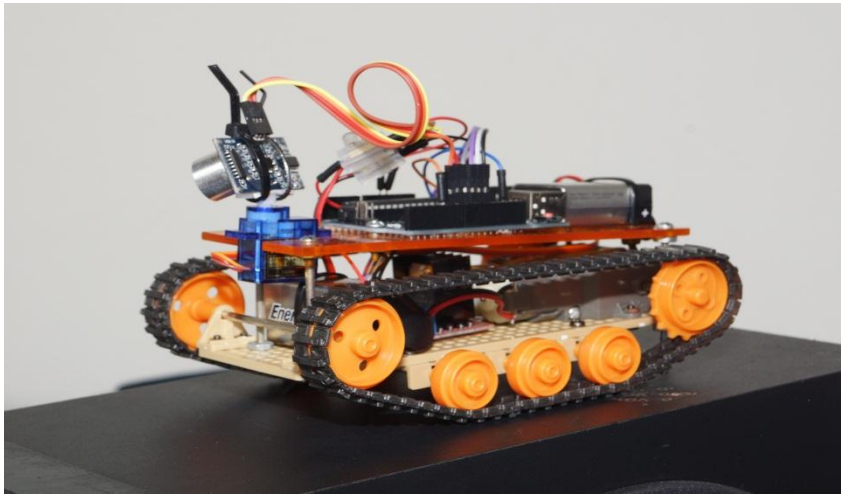
CERRADURA ELECTRONICA:
CD2 Ramirez Castro Cristhian David
CD2 Rios Bustamante José Dayron
CD2 Rodriguez Velasquez Sebastián
CD2 Solano Pardo Fernando Enrique
CD2 Yepes Fernandez Cristian Ivan



CUBO LED:
CD2 Giraldo Marulanda Diego Alejandro
CD2 Jaramillo Galvis David Felipe
CD2 Gonzalez Galeano Gustavo Alejandro
CD2 Antolines Leon Santiago Arturo
CD2 Sanchez Sanchez Oscar Sebastian

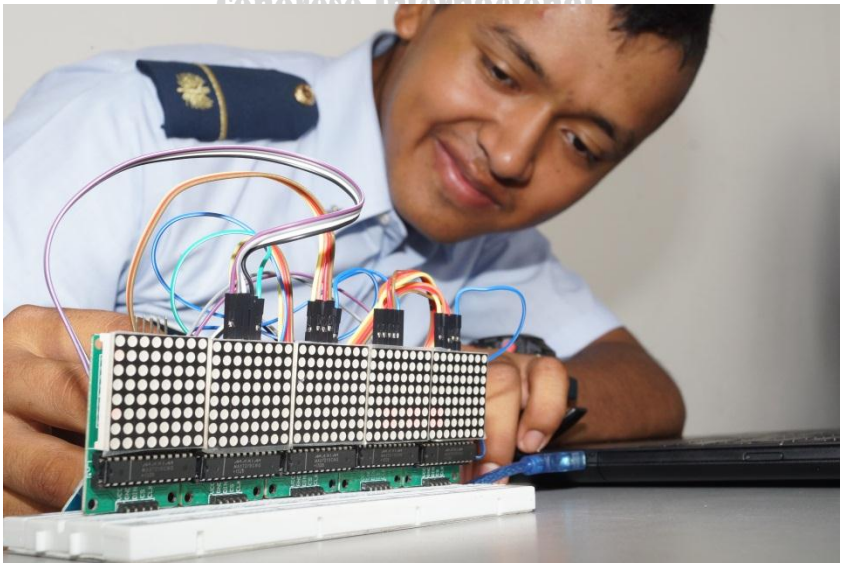
CARDUINO:
CD2 Hernandez Bohorquez Fabian Andres
CD2 Buitrago Ruiz Julian Felipe.

Registro Fotográfico del Workshop



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

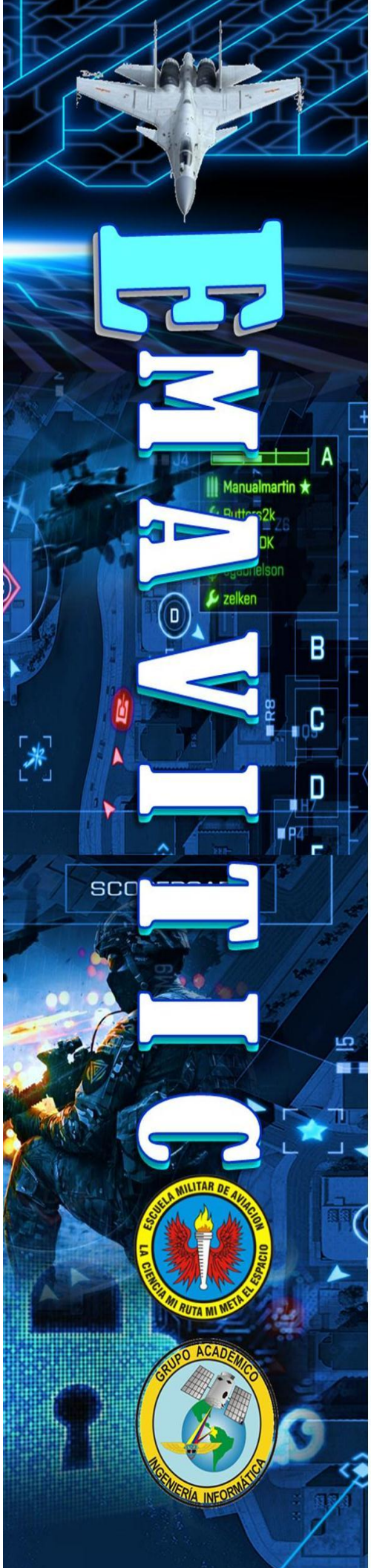


Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC
Congreso Internacional

6. AGENDA

HORA	ACTIVIDAD AGENDA
7:30 - 9:00 am	Registro
8:05 – 8:20am	**Apertura**
8:25 - 8:55 am	**Ciberdefensa: De Los Hackers a la Datavigilancia** Conferencista: Ct Paola Andrea Zarate L. Jefe Programa de Ingeniería Informática Escuela Militar de Aviación
8:55 - 9:40 am	**Buceando en las Profundidades de la DEPP WEB** Conferencista: Leonardo Huertas Calle - CSA – Chief Security Ambassador de Eleven Paths
9:40 - 10:00 am	**Asesoría de Paz-Trabajando para que la Paz deje de Ser un Sueño y se Vuelva una Realidad** Conferencistas: Nos Navi Romero y Alexandra Díaz
10:00 - 10:45 am	Refrigerio – **Recorrido Workshop**
10:45 - 11:30 am	**Ciberseguridad y el Reto con las Nuevas Tendencias Tecnológicas** Conferencista: Post Ph.D. Yezid Enrique Donoso Meisel Subdirector Académico - Coordinador Maestría y Especialización en Seguridad de la Información - Dpto. Ingeniería de Sistemas y Computación Universidad de los Andes
11:30 - 12:20 pm	**Probando En La Red. Evidencias Digitales Del Futuro.** Conferencista: MSc. Andrés Guzmán Caballero CEO e Adalid Corp. y docente en postrados de pruebas técnicas e inspección Judicial.
12:20pm – 1:00 pm	**De la Era de la Disuasión a la Era del Control: la Transformación de la Guerra a partir de la Cibernética** Conferencista: MSc. Andrés Gaitán Rodríguez
1:10pm - 2:20 pm	ALMUERZO LIBRE
2:30 - 3:30 pm	**Hacking Ético - Atacante Informático vs Investigador Forense** Conferencista: MSc. Juan David Berrio López Consultor Certified Offensive and Defensive Security Professional/Security Expert/ Security Specialist/ Security Forensic
3:30 - 4:20 pm	**Foro "Retos de la Ciberseguridad y Ciberdefensa en Ciudades e Infraestructuras Inteligentes: De Los Hackers a la Datavigilancia"** (Ph.D Manuel Sánchez Rubio, Post Ph.D. Yezid Enrique Donoso Meisel, MSc. Andrés Guzmán Caballero, Leonardo Huertas Calle, Coronel ® Martha Liliana Sánchez, Capitán Paola Andrea Zarate L, Juan David Berrio.)
4:20 pm - 4:40 pm	Refrigerio– **Recorrido Workshop**
4:40pm - 5:20 pm	Ciberseguridad desde la Academia Conferencia Coronel ® Martha Liliana Sánchez
5:20pm - 5:50 pm	Ciberseguridad y Ciudades Inteligentes Oportunidades de Investigación - RUAV
5:50pm - 06:20 pm	Actividad Cultural – Palabras de Cierre

Programa de Ingeniería Informática
Escuela Militar de Aviación Marco Fidel Suárez
"El Ciberespacio, El Quinto Dominio de la Guerra



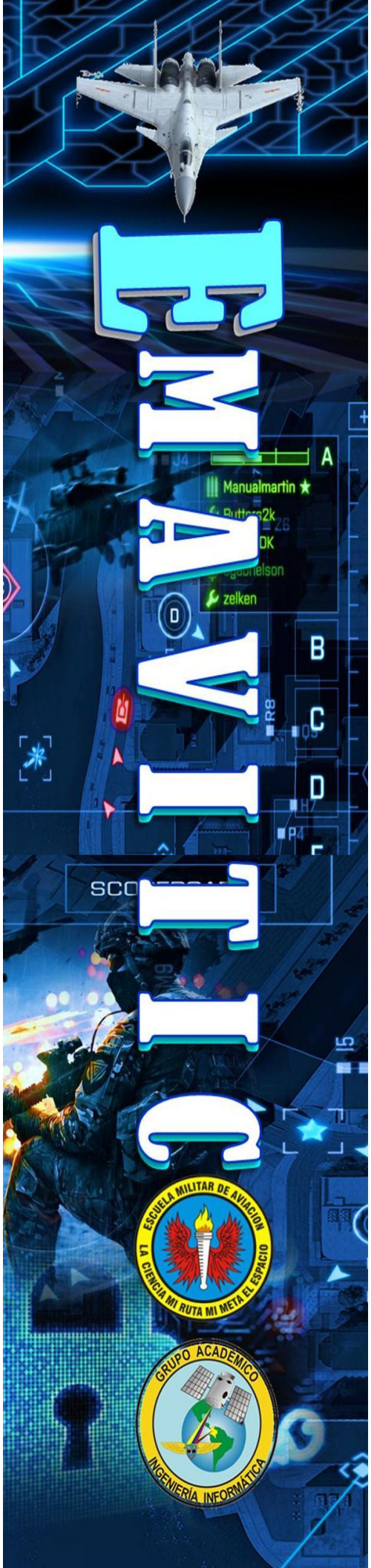
7. CONCLUSIONES

Las ciudades inteligentes pueden aumentar la productividad y la eficacia, pero también tienen un serio problema cuando su seguridad se infravalora. Alcanzar el máximo potencial de todas las iniciativas impulsadas hoy por los gobiernos locales empieza necesariamente con poner en práctica las mejores prácticas de ciberseguridad desde el primer minuto.

Las ciudades, como cualquier entorno TIC, pueden experimentar distintos tipos de ciberataques. Conforme los sistemas se hacen más complejos, están más interconectados y gestionan más información, aumenta su exposición a vulnerabilidades, ya sean debidas a actividades maliciosas o a errores humanos. El gobierno de la ciudad necesita identificar las áreas más críticas que proteger y los tipos de amenazas, incluyendo las categorías de atacantes y sus posibles motivaciones (económicas, criminales o financieras).

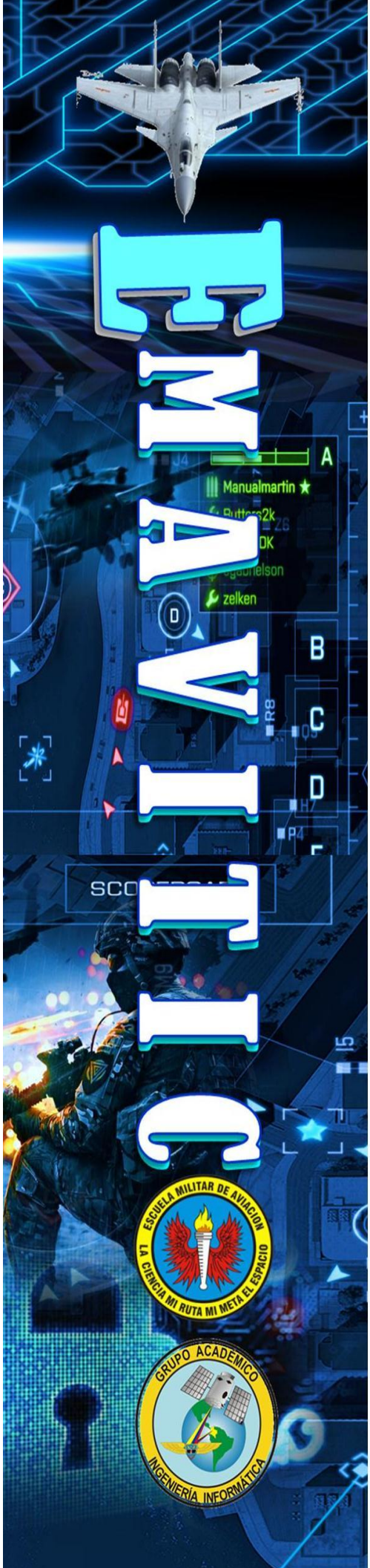
Las operaciones de ciberguerra pueden tener como objetivo los servicios y las infraestructuras de las ciudades.

Las metas de una ciudad inteligente no se lograrán si la información no está correctamente asegurada.



8. FUENTES

- http://www.slideshare.net/ansanz/capacidades-de-china-para-la-ciberguerra
- http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-identifica-la-operaci%C3%B3n-%E2%80%9Coctubr
- http://intelreport.mandiant.com/
- http://investigadordigital.com/un-hacker-vs-un-forense-informatico/
- http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/133.pdf
- http://espionageware.blogspot.com.co/2011/10/advanced-persistent-threat-model.html
- http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat/
- http://lamiradadelreplicante.com/2014/03/19/operacion-windigo-comprometida-la-seguridad-de-miles-de-servidores-linux/
- https://blog.kaspersky.com.mx/regin-apt-una-campana-altamente-sofisticada/4617/
- http://www.viruslist.com/sp/analysis?pubid=207271277
- http://www.ismgcorp.com/global-apt-defense-summit/los-angeles-12
- https://www.linkedin.com/pulse/advanced-persistent-threat-tansel-akyuz-cissp-pmp?trk=seokp_posts_primary_cluster_res_title
- http://unsecuritynow.blogspot.com.co/
- http://espionageware.blogspot.com.co/2014/02/profiling-apt-attackers.html?view=timeslide



Retos de la Ciberseguridad y Ciberdefensa en Ciudades Inteligentes: de los Hackers a la Datavigilancia EMAVITIC

Congreso Internacional

Programa de Ingeniería Informática
Escuela Militar de Aviación Marco Fidel Suárez
"El Ciberespacio, El Quinto Dominio de la Guerra