

# Revista ~~IN~~SECURITY



[www.coladca.tk](http://www.coladca.tk)

**ÉTICA Y ANTICORRUPCIÓN  
EN LA GESTIÓN DE RIESGOS Y LA  
SEGURIDAD.**

**¡SÍ SE PUEDE!**

**ESTUDIOS DE  
CONFIABILIDAD**

**ESTAMOS LISTOS EN SEGURIDAD  
PARA EL OEA?**

**Comunidad COLADCA  
2 años de Retos y Logros.**

**CUAL ES TU EVEREST ?**

**PROCRASTINAR !  
UN DEFECTO DE LOS CLIENTES..  
O DE LAS ENTIDADES FINANCIERAS**

**PILARES BASICOS  
DE LA SEGURIDAD**



**COLOMBIA. SEGURIDAD  
VS. CONFLICTIVIDAD**

Comunidad  
COLADCA @COLADCA





www.coladca.tk

#COLADCA

@COLADCA

Comunidad coladca



Revista InSecurity COLADCA 01 2017

Linea Editorial COLADCA Q1

Revista InSecurity

Edición 01

Bogotá D.C, Colombia

Mayo de 2017

Publicación gremial de la  
**COMUNIDAD COLADCA**  
para la circulación entre  
Profesionales y Empresas  
vinculadas como un aporte  
a los empleados del sector  
de la Gestión de Riesgos  
y la Seguridad en LATAM

Presidente Ejecutivo

Dr. Aristides B. Contreras F.

Líderes de Equipo Consultor  
Colaboradores y consejo editorial

Orlando Hernandez Angarita

Dr. Omar A. Herran Pinzón

Consultor Nilson Bohórquez R.

Ing. Germán Alexis Cortés

Ing. William Barrera

Consultor Luis Eduardo Serrato

MY (RA) Guillermo Garzón Torres

Consultor Emmanuel Sánchez

Dra. Olga Nieto

Consultor Manuel Camelo

Ing. Miller Romero

Dr. Luis Alfonso Ceballos

Consultor Carlos A. Rojas

TC (RA) Guillermo Riaño

Consultor Daniel Sánchez

CR (RA) Jairo Andrés Cáceres

Ing. Abogado Manuel Puentes

Consultor Rafael E. Bernal C

Dra. Sonia Andrade, CPP

CR (RA) Manuel Gutiérrez Q.

Dra. Liliana González

Dra. Diana Hernandez

Dra. Alejandra Buitrago

MY (RA) Mario Alberto Arenas

Ing. Fernando Correa

Ing. Felix A. Reyes G.

## Sumario

### Mejoramiento de Competencias Profesionales

- El poder de la capacitación **PAG. 4**
- Código de ética, conducta y anticorrupción para el profesional de la Gestión de Riesgos y la Seguridad **PAG. 6**

### Perfil del Sector

- Cuál es tu Everest? **PAG. 8**
- Liderando una cultura antifraude y anticorrupción, "los principios son lo que practicamos, no lo que decimos" **PAG. 9**

### Fuerza Pública

- Albeiro, un símbolo mas de la lucha contra el Terrorismo. **PAG. 12**
- "La tercerización y la logística militar en las FF.MM.; Cerrando la brecha con el sector privado..." **PAG. 13**

### Entorno Latinoamericano

- Colombia, Seguridad vs Conflictividad **PAG. 16**
- Gestión corporativa de la Seguridad de las empresas en el exterior **PAG. 18**

### Tecnología y nuevas tendencias del Crimen

- Procrastinar un defecto de los clientes... O de las entidades financieras? **PAG. 22**
- Confianza y comunicación, seguridad para las diferentes maneras en que los sensores IOT y Smart se conectan a la web **PAG. 24**

### Actualidad y Retos

- Estudios de confiabilidad, base de la prevención y protección **PAG. 28**
- De la Vigilancia a la Gestión de riesgos **PAG. 29**
- Asesoría de Seguridad y prevención: Pilares básicos de la Seguridad **PAG. 31**

### Recomendados para Leer

- SALA - Sumario Analítico Latinoamericano, Perspectivas para el 2017 **PAG. 32**
- Informe Tendencias 2017 ESET - "La Seguridad como Rehén" **PAG. 34**

### Estandarización y Sistemas de Gestión para la Seguridad

- Seguridad en la Cadena de Suministro, Autorización como Operador Económico Autorizado OEA en Colombia. **PAG. 36**

Revista InSecurity es una publicación de la Comunidad COLADCA. Las opiniones expresadas en los artículos reflejan exclusivamente el pensamiento de sus autores y nuestra organización no se hace responsable del contenido de sus artículos. El hecho de que se patrocine difusión no implica conformidad con los trabajos expuestos en estas páginas. El contenido de esta revista es de tipo informativo y de prevención, la información expresada en todo el contenido no pretende ser sustitutivo de las leyes o reglamentos internos establecidos en el orden público o interno de alguna Empresa u Organización. El contenido de los avisos publicitarios es responsabilidad de los anunciantes incluidos en la revista. Ante cualquier duda o aclaración por favor dirigir una comunicación a los emails: coladca@gmail.com - vpcoladca@gmail.com o en la Web: www.coladca.tk

Telefono de contacto  
**+(57) 311 5421737**

Para suscripciones, comercialización  
y contacto, por favor comunicarse  
vía correo electrónico:

**coladca@gmail.com**

Página web:  
**www.coladca.tk**

# Empresas y Profesionales de la Gestión de Riesgos y la Seguridad A LA VANGUARDIA Y EN LA MEJORA CONTINUA.

## *Bienvenidos a Nuestra primera Edición.*

*Apreciado vinculado y lector, en nombre de los 1400 Profesionales que integramos la Comunidad Latinoamericana de Consultores y Asesores en Gestión de Riesgos y Seguridad les saludamos el día hoy. Hemos dispuesto nuestra publicación para seguir logrando las metas trazadas, entre ellas y no menos importante que las demás, el mejoramiento continuo de las competencias personales y profesionales, de los que desde cualquier país y ciudad de Latinoamérica representan el gremio, y mas aun los que por diversas condiciones o circunstancias no cuentan con un medio eficaz y continuo para actualizarse con los temas y las diferentes tecnologías dispuestas para la prestación de un excelente servicio, por supuesto; también para seguir **“Dejando Huella”**.*

*Debemos valorar y dar las gracias a las Empresas que desde el inicio de nuestras actividades hace ya 2 años, nos apoyaron y siguen firmes en el propósito de aportar un grano de arena en la labor de nuestra Comunidad, a Dios y a ellas muchas gracias por su apoyo.*

*Queremos cada día prestarles mejores servicios, ofrecer la mejor capacitación y que con esto puedan certificar sus competencias profesionales acorde a estándares internacionales; Por eso y como lo exprese en el mes de Octubre del año anterior, cuando realizábamos nuestro 1er Congreso **“Avances y Retos en el Profesional integral de la Seguridad”** en la ciudad de Bogotá; seguiremos en la causa y por la necesidad de una organización y un estándar Latinoamericano, con líneas transparentes, constantes, innovadoras y estratégicas, que permita un factor diferenciador y con elocuencia hacia todos los vinculados, que genere una estrategia de carrera y profesionalización, que permita la especialidad y evite la rotación de personal, para que al final poseione a las Empresas que representan el gremio, sin olvidar que todo esto debe dignificar el deseo de aporte a la sociedad.*

*Gracias por ser parte del cambio, que disfruten nuestro trabajo y todas las alianzas estratégicas que lograremos juntos, Éxitos en la labor para ser Profesionales y Empresas Q1.*



ARISTIDES CONTRERAS F.  
Presidente Ejecutivo  
Comunidad COLADCA

Revista  
**INSECURITY**  
OBSERVATORIO DE SEGURIDAD

Somos:

**COLADCA**  
Comunidad Latinoamericana  
de Consultores y Asesores en  
Gestión de Riesgos y Seguridad

**“Dejando Huella”**

**Q1**

**Vincúlate!**

# EL PODER DE LA CAPACITACIÓN



Por. Orlando Hernandez Angarita

Son muchos los factores que en los momentos actuales están a la orden del día a la hora de incidir en el aumento de la competitividad en todos los ámbitos de la vida; a nivel empresarial, aquellas compañías que no se adaptan a los nuevos cambios tienden a desaparecer, como en el caso de las empresas dedicadas a producir rollos para revelar fotografías por citar sólo un ejemplo, o aquellas que no implementan los avances tecnológicos en sus actividades y desaparecen del mercado.

El área de la Gestión de Riesgos y la Seguridad no escapa a la situación descrita y mucho menos en el caso de quienes hemos escogido como profesión esta hermosa actividad que día a día nos plantea nuevos retos. Como en el caso de otras profesiones muy exigentes como el derecho o la medicina por ejemplo, se exige del profesional una capacitación constante que nunca termina; podríamos afirmar del profesional de seguridad que nunca llegará a ser un “producto terminado”, se requiere que tenga una sólida fundamentación profesional, unos excelentes conocimientos básicos de las diferentes actividades profesionales en su área de trabajo, las cuales deberían ser transversales a todos los niveles y cargos existentes en la seguridad.

*La capacitación constante permite el desarrollo de aptitudes, habilidades y competencias, promueve el acceso a nuevos saberes y la adquisición de nuevos conocimientos para un mejor desempeño profesional.*

Cada cargo tiene un perfil de competencias requeridas, existiendo un rasero que nivela los conocimientos y habilidades exigibles desde niveles inferiores hasta los cargos de nivel directivo, no obstante es necesario tener en cuenta que las -exigencias de un mundo cada vez más competitivo y una actividad que en muchos países día a día exige mayor cantidad de profesionales bien formados, idóneos y competentes, sin embargo; podríamos decir que entre la educación.

*El proceso de educación en los profesionales de seguridad, debe responder a un Plan de Mejoramiento Continuo que incentive una insaciable sed de conocimiento, en razón a que continuamente nos enfrentamos a nuevas modalidades delictivas, mutación del crimen, nuevas regulaciones normativas y cambios tecnológicos que traen consigo nuevos riesgos que llevan a que el área de Gestión de Riesgos y Seguridad se constituya en una pieza clave para el negocio.*

básica (aquella dirigida a los niveles inferiores) y la educación profesional en seguridad, existe una brecha bastante grande ya que hay una amplia oferta de educación formal para estos dos niveles, más no para personas que deberían contar con un “Plan de Desarrollo de Carrera” (Supervisores, Coordinadores, Jefes), con su respectivo Plan de Capacitación dirigido al desarrollo metódico y planificado de habilidades y competencias acordes a los requerimientos de cada cargo.

Ahora bien, igual que en la medicina necesitamos fomentar la generación de especialidades profesionales de acuerdo con las áreas de trabajo específicas, ya que lo que normalmente ha venido ocurriendo es que de acuerdo con el área de trabajo o la empresa en la que se desempeña, el profesional de seguridad va adquiriendo la experiencia y los conocimientos propios del cargo, abriendo camino sobre la marcha y por ende ciñéndose a un desarrollo de carrera no planificado de manera estratégica, en tanto que quienes ocupan cargos intermedios que a lo largo de los años venideros están destinados a ocupar cargos directivos por reemplazos en ausencias del titular o por planes de sucesión si es que existieran.

Tampoco cuentan con un plan de fortalecimiento y desarrollo de competencias profesionales que esté dirigido a satisfacer esas necesidades de capacitación con base en un mapa de competencias requeridas para alcanzar cada uno de los cargos existentes dentro de las posibilidades de ascenso, siendo necesario el desarrollo de conocimientos y habilidades específicas que conduzcan a la especialización, a la generación de credibilidad y a la construcción de confianza en el especialista por su demostrada idoneidad.

El proceso de educación en los profesionales de seguridad, debe responder a un Plan de Mejoramiento Continuo que incentive una insaciable sed de conocimiento, en razón a que continuamente nos enfrentamos a nuevas modalidades delictivas, mutación del crimen, nuevas regulaciones normativas y cambios tecnológicos que traen consigo nuevos riesgos que llevan a que el área de Gestión de Riesgos y Seguridad se constituya en una pieza clave para el negocio, toda vez que sobre sus hombros recae la responsabilidad de asegurar los activos, las personas, la reputación y la continuidad del negocio; siendo así, la alta dirección de seguridad se enfrenta al reto de amalgamar bajo su responsabilidad una integralidad de saberes que abarque desde el conocimiento mismo del negocio hasta el universo de medidas necesarias y efectivas para mantener bajo control todos los riesgos que puedan afectar a la organización en su conjunto y minimizar tanto la probabilidad de ocurrencia como los efectos negativos en caso de que estos se materialicen, además, por ser un área tan sensible dentro de la organización, el responsable de Seguridad Corporativa o Patrimonial debe hacer parte del Equipo Directivo o del Comité de Gerencia, en el cual sus conceptos y criterios agreguen valor a los objetivos de la organización y tengan suficiente peso para ser tenidos en cuenta en la toma de decisiones, hecho este que obliga al profesional de seguridad a estar a la altura de otros cargos importantes dentro de la empresa y a participar con solvencia a la hora de sustentar sus aportes para la toma de decisiones, con herramientas como el Análisis Costo Beneficio, Matriz de Riesgos para valorar y priorizar acciones, Conocimiento del Contexto tanto interno como externo, etc.

Tanto si se pretende llegar a esta instancia como si ya ese logro ha sido alcanzado, es necesario mantenernos al tanto de los cambios y las novedades que a diario se presentan en este mundo tan cambiante en aspectos tecnológicos, legales y delictivos, lo que obligatoriamente se traduce en la necesidad de estar permanentemente "afilando la sierra" como lo definiera Stephen Covey en su libro Los 7 Hábitos de la Gente Altamente Efectiva para referirse al séptimo hábito, el cual está constituido por la obligación que tiene todo profesional exitoso de mantenerse al tanto de los avances en su actividad profesional y no alejarse nunca del interés por el conocimiento y la capacitación constante, este es un factor clave de éxito si se le quiere dar a nuestra profesión la altura y la importancia que se merece; la capacitación permanente en

*Liderazgo y Empatía, Habilidades para la Planeación y Organización, Capacidad para discernir, Trabajo en equipo, Habilidad para realizar Presentaciones Efectivas, Capacidad para hablar en público, Determinación*

*Capacidad de persuasión y de negociación, proactividad (Actuar no base en Principios, no ser reactivos), Capacidad de Gestión, Capacidad para la Solución de Problemas, Toma de decisiones bajo presión, Adaptabilidad al Cambio y Creatividad, Capacidad de Resiliencia.*

aspectos inherentes al giro del negocio y las responsabilidades del cargo, se constituye en un factor de competitividad en este mundo cada vez más competitivo, donde las nuevas generaciones vienen empujando dotados de habilidades tecnológicas y el dominio de idiomas extranjeros que les dan ventajas competitivas frente a la experiencia que dan los años de dedicación y entrega con sacrificio a la abnegada profesión de la Gestión de Riesgos y Seguridad, que ha dotado a los profesionales de habilidades que se constituyen en un "Factor Diferencial tan valiosas como:

- Liderazgo y Empatía
- Habilidades para la Planeación y Organización
- Capacidad para discernir
- Trabajo en equipo
- Habilidad para realizar Presentaciones Efectivas
- Capacidad para hablar en público
- Determinación
- Capacidad de persuasión y de negociación
- Proactividad (Actuar no base en Principios, no ser reactivos)
- Capacidad de Gestión
- Capacidad para la Solución de Problemas
- Toma de decisiones bajo presión
- Adaptabilidad al Cambio y Creatividad
- Capacidad de Resiliencia. **Q InSECURITY**

**Autor: Orlando Hernandez Angarita,**

Oficial de la reserva activa de la Policía Nacional de Colombia, estudios en Administración Policial en la Escuela de Cadetes de Policía General Santander, estudios en Negociación y Resolución de Conflictos con la Universidad de Berkeley California y graduado como Instructor en Seguridad del Instituto Professional School of Security en Tel Aviv Israel.

Conferencista en eventos nacionales e internacionales en temas de prevención. Autor del "Manual para la prevención del secuestro y la extorsión" y del libro "Detecte al delincuente y al mentiroso" Leyendo el Lenguaje Corporal, coautor de la V Edición de la "Guía de Seguridad para los Actores de la Cadena de Suministro. Para contactar al autor, hágalo a través del email: ohaorlando@yahoo.com.

# CODIGO DE ÉTICA, CONDUCTA Y ANTICORRUPCIÓN



Por. Aristides Contreras Fernandez

Son varias las razones por las cuales la comunidad latinoamericana de consultores y asesores en gestión de riesgos y seguridad – COLADCA, busca adoptar un código de ética, conducta y anticorrupción, la mas importante es que existen códigos parciales en empresas y en organizaciones no gremiales, allí no se particulariza como debe obrar los profesionales en la sociedad para engrandecer el gremio, solo se tratan temas de carácter interno para la imagen empresarial.

Otra razón no es extraña para la sociedad actual, las diferentes noticias en los medios, nos llaman a reconocer que uno de los graves problemas de las empresas en américa latina es la falta de credibilidad por causa de la corrupción y falta de transparencia institucional, esta nos hace perder millones de pesos, de allí que nuestro gremio se preocupe por la labor de los profesionales en la empresas y mas los de la gestión de riesgos y la seguridad, si bien es cierto; las normas actuales buscan que las empresas mejoren, pero como ya se dijo, ninguna se dirige en particular hacia los profesionales.

Por otro lado, contamos con un creciente grupo de trabajadores que actualmente ingresan al gremio de la Gestión de riesgos y seguridad, un gran numero sin una dirección clara de los principios básicos de actuación sin unos deberes éticos y criterios de profesionalismo, necesarios para ejercer su labor ajenos a las consecuencias de sus actuaciones, un desconocimiento de los deberes y obligaciones que por ende les lleva a traer circunstancias sobre la profesión, que no le permiten crecer acorde a la importancia de la realidad social que tiene actualmente.

Los profesionales de la Gestión de riesgos y seguridad, son parte activa e integral en el futuro de la sociedad.

El profesional de la seguridad “evangelizador de una doctrina cuya filosofía se soporta en la legalidad y el buen actuar” Lider positivo, a los cambios que Colombia requiere en este tiempo coyuntural.

*“El Código debe ser una Herramienta que forje en la sociedad una cultura de legalidad y compromiso de corresponsabilidad empresarial y personal, identificando en el profesional del Riesgo un aliado estratégico que desde su liderazgo y ejemplo individual, puedan fomentar la importancia del buen actuar, sustentado en principios y valores que trascienden incluso en la esfera de lo legalmente exigido a fuerza normativa.” Aporte Frente de Seguridad Empresarial FESEM - DIJIN, Policía Nacional.*

Muy importante mencionar que es el crecimiento del sector y las cifras importantes de contratación en servicios de gestión de riesgos y seguridad, los que preocupan e inquietan para la necesidad de este código a COLADCA, el enfoque multidisciplinario que implica que la seguridad deba trabajar de la mano con especialistas de diferentes profesiones y que se involucren como parte importante para el cumplimiento de los objetivos organizacionales trazados.

Explicaba una noticia en Colombia el día 30 de Marzo de 1993, ya hace mas de 24 años, “LA SEGURIDAD PRIVADA ESTÁ DE MODA” “La seguridad privada está en auge. Las actuales circunstancias del país obligan a la gente a buscar en la seguridad particular la alternativa para la protección de sus bienes muebles, inmuebles, de capital y por supuesto, de sus vidas.” Y no es extraño que al año 2016, cuando se presento el reporte de estados financieros del año 2015 por parte de la Superintendencia de vigilancia y seguridad privada, que el total de ingresos operacionales del sector se había duplicado en apenas 5 años, pues en 2010 se reportaban ingresos por \$ 4.645.892 COP, mientras que para 2015 la cifra alcanza los \$9.830.260 COP, por ello hay que reconocer que el sector esta en auge y que la confianza que se esta depositando en el mismo, es mucho mas grande cada día, por esto mismo debemos establecer para los nuevos empleados del sector un comportamiento basico de conducta acorde a principios eticos y de anticorrupción.

**Gestor iniciativa: Aristides Contreras Fernandez**  
Presidente Ejecutivo Comunidad COLADCA.

Si desea participar, firmar y adherirse como profesional o como compañía al Código de Ética, conducta y anticorrupción de la Comunidad COLADCA, contáctenos a través del email: [coladca@gmail.com](mailto:coladca@gmail.com) o en nuestra web: [www.coladca.tk](http://www.coladca.tk)

**P&P**  
ASOCIADOS  
S.A.S



# ESTUDIOS DE Confianza, EN CONTRATACIÓN DE PERSONAL.



**INVESTIGACIONES  
INTERNAS Y  
PRIVADAS**



**RECOLECCIÓN  
DE PRUEBAS E  
INVESTIGACIONES  
PRIVADAS**



**ANÁLISIS INTEGRAL  
DE RIESGOS**



**CAPACITACIONES  
Y SEMINARIOS**



**OPERACIÓN A NIVEL NACIONAL**

**NO SOMOS PROVEEDORES, SOMOS ALIADOS ESTRATÉGICOS**

**NUESTROS  
CLIENTES**



Contáctenos en:

MOVIL 3203746219

PBX: +57 (1) 3460140

Carrera 9 # 53- 58

Oficina 309

Bogotá D. C

[www.prevencionesproteccion.com](http://www.prevencionesproteccion.com)



DEJANDO  
HUELLA CON  
RESPONSABILIDAD  
SOCIAL.

PERTENECEMOS A



**Prevención y Protección**

# CUAL ES TU EVEREST?



Por. Jose Luis Yepes

**D**urante muchos años de carrera profesional interactuando en varias empresas, he tenido la posibilidad de escuchar diversas charlas motivadoras muy interesantes algunas y otras menos y otras pocas realmente terribles. Las personas de seguridad particularmente venimos de una diversidad de formaciones académicas y profesionales, que pudieran ser diferentes en la forma, pero que en el fondo son las mismas abstracciones que nos tienen donde estamos.

Es fundamental que descubramos que nos motiva?

Que hace movilizar la fuerza más grande del universo...La Voluntad. Sin encontrar que nos moviliza, que nos motiva podríamos caer en el marasmo y el vaivén de las masas y "Quien tiene un porque para vivir, puede encontrar casi cualquier como"

El ser humano tiene 3 abstracciones básicas que lo movilizan y que es muy importante que las conozcas, van a ver porque debemos tenerlas claras cuando comencemos a hablar del Branding o marca personal.

El amor, El Tiempo y la Muerte. Inexorablemente todos deseamos tener Amor por algo por alguien y ser retribuidos, también siempre vamos a creer necesitar más Tiempo y por ultimo todos tenemos a la Muerte.

Si como profesional de seguridad tienes clara esas 3 abstracciones del ser humano podrás entender y valorar sus conductas, sus reacciones y hasta sus miedos.

Siempre he creído que las empresas modernas están cada día buscando nuevos liderazgos movilizadores más que inteligentes, el sistema educativo nuestro premia al inteligente académico y desecha al inteligente emocional, pero este hecho está cambiando y por eso han surgido nuevas tendencias que estudian y entrelazan la neurociencia, la psicología conductual, Programación Neurolingüística y otro ciento de conceptos que hoy tienen ríos de tinta en todas partes.

*Rápidamente tienes que aprender que tener huella personal o recordación de marca va a ser muy justo o injusto por la inmediatez de lo que quieres reflejar y a veces nos auto saboteamos consciente o inconscientemente, por tal motivo es necesario que tengas en cuenta qué buscan las empresas actualmente en sus líderes movilizadores de conciencias y transformación.*





Lo cierto es que la primera impresión cuenta más de lo que uno cree y por eso es importante que siempre estar preparados para dar una primera buena impresión algo que en algún libro que leí decía “Que los 10 primeros segundos cuenten”.

Igual cuando alguien llega a hablar contigo esa primera impresión buena o mala va a ser por lo menos al principio la que vas a tener de esa persona.

### BRANDING

Rápidamente tienes que aprender que tener huella personal o recordación de marca va a ser muy justo o injusto por la inmediatez de lo que quieres reflejar y a veces nos auto sabotamos consciente o inconscientemente, por tal motivo es necesario que tengas en cuenta qué buscan las empresas actualmente en sus líderes movilizadores de conciencias y transformación.

Carisma Complex (Ruben Turienzo) nos da los siguientes principios activos para líderes con carisma y marca personal (Branding).

Seducción (Magnetismo) que la gente quiera permanecer a tu lado.

Influencia (Impacto Social) Grado de importancia en la sociedad objetivo.

Motivación (Potenciar positivamente) Como movilizar las mentes de las personas.

Liderazgo (Tener el Control) Es la proyección nuestra que ven los que nos rodean así no estemos presentes.

Estimulación (Opción memorable) Convertirnos en la mejor tendencia a seguir por nuestro ejemplo.

Si quieres tener mayor información sigue el Link en <https://youtu.be/GZdwkqoXJKM>.



#### Autor: Jose Luis Yepes

Profesional en Ciencias Militares.

Post Grado en Gerencia de seguridad de la Universidad Militar, 30 años de experiencia en Seguridad Física, ha laborado principalmente en el sector Energético y Agroindustrial.

En la actualidad se desempeña como Líder de seguridad física en la Vicepresidencia Regional Central de Ecopetrol S.A. Consultor en temas de Branding y Marca personal, convencido que el mejor talento humano de las organizaciones esta en Seguridad física, solo que no lo sabemos.

Para contactar al autor, hágalo a través de la cuenta de [twitter@totteyepes](https://twitter.com/totteyepes).

## LIDERANDO UNA CULTURA ANTIFRAUDE Y ANTICORRUPCIÓN



Por. Marco Muñoz  
Psicólogo Director CAP



Liderar una cultura resistente al fraude y la corrupción va mas allá de los eventos y las declaraciones. Implica estimular el compromiso personal y de la organización con valores como la integridad, la honradez y el juego limpio pero sobre todo lograr que estos principios se expresen en comportamientos individuales concretos como la no utilización de la información o el poder que confiere un cargo para beneficio personal.

La integridad se manifiesta en las acciones no solo en lo que decimos, no se reduce al eslogan que ponemos en nuestra publicidad, ni a los argumentos, es la coherencia de nuestro comportamiento con nuestros principios a pesar de las tentaciones y necesidades que se nos presenten.

Somos:  **Revista INSECURITY** Vinculate!   
OBSERVATORIO DE SEGURIDAD  
"Dejando Huella"

De nada nos sirve una comunicación, promoviendo los valores, el compromiso, la integridad, si en la organización ocurren casos vergonzosos en donde empleados de confianza defraudan y es conocido por todos el abuso de algunos jefes utilizando su posición de autoridad.

Este tipo de incoherencia entre la promesa que hacemos como personas y como organización y lo que realmente sucede, va desde pequeños actos de corrupción como utilización inadecuada de material de oficina de la compañía para fines personales, hasta comportamientos francamente corruptos como el fraude o la solicitud de coimas para el otorgamiento de contratos.

Como sabemos hay personas y organizaciones en donde la pequeña corrupción es aceptada tácitamente y la gran corrupción se oculta, muchas veces con el argumento de no desprestigiar la compañía ante los clientes y la sociedad. Consideran además, que es aceptable ofrecer sobornos o engañar a los clientes pues lo que importa es el resultado.

Una cultura anticorrupción se expresa en la pulcritud de los comportamientos, en la transparencia de los procesos especialmente en áreas sensibles como compras, selección y contratación, en donde no se tolere la corrupción, así sea grande o pequeña. Todas las actuaciones de los directivos y empleados con clientes, proveedores y autoridades deben demostrar en la práctica el compromiso ético.

Un aforismo antiguo decía “Lo que haces suena tan fuerte que no escucho lo que dices”. Por tanto es contraproducente y ocasiona una doble moral comunicar promesas, sobre las cuales empleados clientes y proveedores están escépticos.

Muchas veces las organizaciones han sobre prometido integridad sin estar preparadas para respaldar esta promesa en la operación diaria del negocio.

### Liderazgo y Corrupción:

Para poder proclamar la promesa de integridad con éxito y respaldarla en la práctica, tenemos que garantizar coherencia entre lo que anunciamos y hacemos y en este punto el liderazgo juega un papel fundamental.

En nuestra cultura, con un fuerte componente patriarcal, hemos aprendido que el jefe es el modelo de comportamiento a seguir para ser aceptado y progresar.

Lo que hace el jefe más que lo que dice, establece los límites entre un comportamiento aceptable y uno inaceptable, Si él utiliza su posición en beneficio propio implícitamente está comunicando que esto es aceptable y digno de ser imitado. Si se piensa que él puede hacer lo que hace porque es el jefe, el subalterno se considera justamente autorizado para hacer lo mismo, utilizando los privilegios e información que le confiere su cargo.

Se cosecha lo que se siembra, por ejemplo si el único mensaje o por lo menos el más frecuente es que lo que importa son los resultados, independiente de cómo se logren, el empleado entenderá que lo que importa es el logro personal independientemente de cómo se obtenga y considerará razonable obtener beneficios por cualquier camino.

Los mensajes sobre integridad determinan cómo la gente va a ir juzgando y decidiendo sus pautas de comportamiento en función de lo que experimenta en la práctica.

“NO ES EL MENSAJE ANTICORRUPCIÓN EL QUE ACTÚA, ES LA EXPERIENCIA DIARIA LA QUE LE DA SIGNIFICADO. SI EL MENSAJE NO ES COHERENTE CON LO QUE PARA NO CON LA CONDUCTA DE LOS LIDERES, NO AFECTARÁ EL COMPORTAMIENTO DE LAS PERSONAS Y LAS DECLARACIONES DE PRINCIPIOS NO PASARÁN DE SER FRASES VACÍAS QUE NO TOCAN EN SU NÚCLEO EL PROBLEMA DE LA CORRUPCIÓN.”

La cultura anticorrupción se construye con base en lo que hacen los jefes, las personas y la compañía, no solamente con lo que proclaman. Un programa anticorrupción que no involucre el comportamiento de los líderes, corre el peligro de convertirse solamente en un puñado de frases vacías.

Somos:  **Revista InSECURITY** Vinculate!   
OBSERVATORIO DE SEGURIDAD  
“Dejando Huella”

COLADCA está en los temas mas coyunturales de la Gestión de Riesgos y la Seguridad

**CIBERSEGURIDAD Y CIBERPREVENCIÓN**



**INVESTIGACIÓN Y PUBLICACIÓN**



**CAPACITACIÓN "DIALOGOS DE SABERES EN SEGURIDAD"**

**CIFRAS y LOGROS**

**1400 PROFESIONALES VINCULADOS A 2017**

**POSTULACIÓN A PREMIO CONTROL SOCIAL 2016 VEEDURIA DISTRITAL**

**300 PROFESIONALES CON MEJORES COMPETENCIAS PROFESIONALES EN 2016**

**OBSERVATORIO DE SEGURIDAD Y CRIMEN**



**GESTIÓN INTEGRAL DE RIESGOS**



**NUEVAS TECNOLOGÍAS**



Profesionales y Lideres Consultores en todas las lineas y Sectores de la Gestión de Riesgos y Seguridad.

**PROTECCION DE INSTALACIONES CRITICAS y DATOS**



**Certificación Q1**

**HONOR Y GLORIA A LA MEMORIA DEL INSIGNE  
PATRULLERO ALBEIRO GARIBELLO ALVARADO,  
QUIEN SE CONSTITUYE EN EL SIMBOLO DE LA  
LUCHA CONTRA EL TERRORISMO.**



Por. General (r) Luis Montenegro R.



El pasado domingo 19 de febrero de 2017, en el sector de la macarena, en la ciudad de Bogotá D.C, exploto un artefacto explosivo ocasionando lesiones graves en 26 policiales y posteriormente la muerte del PT. Albeiro Garibello integrante del ESMAD. (Escuadrón Móvil Antidisturbios) de la Policía Nacional.

El lunes 27 del mismo mes, el ELN, mediante comunicado se adjudico el acto terrorista, señalando que el atentado iba dirigido hacia el personal de la policía del Esmad. Una vez mas este grupo criminal, mostro su cinismo, cobardía, arrogancia, en medio de un proceso que busca el transito hacia la paz. ¿que cerebro tienen los criminales del ELN que colocaron el petardo que le quito la vida al patrullero Albeiro?

Así se deteriora la voluntad de los colombianos, su credibilidad y confianza en el proceso de paz en desarrollo.

De esta manera el gobierno debe pedir explicaciones en la mesa de negociación y si continua las acciones terroristas suspenderla.

La sociedad Colombiana rechazo como un acto cobarde, demencial, con vehemente indignación, el acto terrorista que ejecuto el ELN.

Exhorto a la fuerza pública a continuar enfrentado con contundencia a estos grupos terroristas.

**QUE SIGNIFICO PARA LA POLICIA Y PARA EL PAIS LA MUERTE DE ALBEIRO GARIBELLO? COMO HONRAR SU MEMORIA?**

Albeiro entro a la policía hace varios años y aspiraba superarse y alcanzar en la institución mayores cargos, desafíos y retos a los cuales estaba enseñado a sortear y enfrentar. Albeiro al fallecer a sus 23 años, como Heroe de la Patria, cumpliendo con su deber misional, dejó un legado de cualidades, de valores, de mística, de transparencia, de sacrificio, que todos los colombianos y especialmente los policías activos deben aplicar e imitar.

El sábado 25 de febrero, tuve la oportunidad de rendir el ultimo adiós a nuestro compañero Albeiro; sus compañeros del ESMAD le rindieron tributo de admiración, de honor y gloria, sosteniendo el casco que utilizo en servicio el honorable patrullero. A su lado aparecía su foto portando con orgullo el uniforme policial.

Si queremos honrar la memoria de Albeiro, todos los ciudadanos, debemos convertirnos en informantes, es decir que notifiquen a la autoridades, sin recibir recompensa pecuniaria, la presencia de paquetes, vehículos y personas sospechosas, así podremos ubicar a los responsables de la muerte de Albeiro y de las graves lesiones de los demás compañeros policiales.

El ciudadano debe informar situaciones delictivas, sin esperar recompensa; debe informar por que le nace del corazón, constituye un deber ciudadano.

**“ha muerto un gran héroe de la nación, que se constituye en el símbolo de la lucha contra el terrorismo”**

Soy solidario con los sentimientos de dolor que embarga a la familia policial en cabeza del señor General Jorge Nieto, nuestro director y la familia de Albeiro.

Es necesario desarrollar un frente común, para prevenir y capturar a los autores de estos actos demenciales.

En estos momentos debemos acompañar a nuestra Policía, a las autoridades, convirtiéndonos en informantes como arriba lo indique.

“señalo al terminar, que Albeiro se constituirá para nosotros los policías, en el faro que ilumina, guía y señala el horizonte policial, en medio de las tormentas y dificultades que presenta el quehacer policial”.



**Autor: General (r) Luis Montenegro R.**  
Excomandante de la Policía Nacional Bogotá  
Para contactar al autor, hágalo a través de [coladca@gmail.com](mailto:coladca@gmail.com)

# “LA TERCERIZACIÓN Y LA LOGÍSTICA MILITAR EN LAS FF.MM.; CERRANDO LA BRECHA CON EL SECTOR PRIVADO.”

 Por. Coronel (r) Jairo Andrés Cáceres García

Los Ejércitos modernos de las potencias mundiales, actualmente NO solo miden la potencia de los Ejércitos por el número de Unidades o la capacidad de fuego de los mismos, sino también por su capacidad para sostenerse desde el punto de vista logístico en situación de guerra.

La Logística es vital en la guerra, en la paz, en el sector privado las empresas en la cadena de suministros, la administración absorbe entre un 60% y un 80% de cada dólar que vende una empresa y que puede ser esencial para su estrategia competitiva y la generación de ingresos.

El sector privado y público están siendo presionados por mejorar la calidad de sus productos o servicios, “Solo sobrevivirán y prosperarán, aquellas organizaciones que puedan satisfacer y sobre pasar las crecientes expectativas que sobre ellas se depositan, para así obtener ventajas comparativas por sobre la competencia”.

En muchas ocasiones, es la solución más eficiente, económica y práctica para el negocio es dejar en manos de expertos que se encarguen de una actividad para la cual, su Unidad Militar o empresa no se ha, ni está preparada adecuadamente, o no cuenta con los medios tecnológicos y el talento humano requerido, y que al decidir efectuarlo directamente, implicaría arriesgar el cumplimiento de la misión.

Así mismo sucede en las FFMM, la decisión de tercerizar una operación o función logística, no es nada fácil, pues además de los factores de desconfianza y ceder a terceros el control parcial o total de un requerimiento logístico, le agregamos dos factores adicionales, “Resistencia al Cambio” y la “Seguridad”, por tratarse de temas de Seguridad y Defensa Nacional. Este artículo tiene como objetivo, evidenciar la importancia de la “Tercerización” en la Logística Militar en las FFMM de Colombia, específicamente como, mediante esta buena práctica los Militares Logísticos cierran la brecha con la población civil, la Industria y comercio del Sector Privado, “Outsourcing” palabra que viene del idioma inglés, extranjerismo y objetivo principal del presente trabajo, durante el cual también se empleará dicho término para referirnos al concepto que en español se denomina “tercerización”.



FUENTE: Grafica, Maestría en Informática Academia Politécnica Militar Ejército de Chile y Pontificia Universidad Católica de Chile.

Su aplicación está creciendo en el mundo, se habla en el idioma español y que finalmente son sinónimos, más sin embargo como somos un país hispanoparlante, emplearé el término del idioma español, “tercerización”.

La tercerización es una solución para algunos de los problemas que debe enfrentar una empresa moderna, toda vez que existen una gran cantidad de funciones necesarias, más no básicas, además porque no agregan valor significativo desde el punto de vista del cliente.

La calidad y el costo, son los aspectos básicos que busca optimizar de manera significativa la tercerización, esperando que los expertos seleccionados apoyaran a mejorar el resultado de la empresa que los contrata, a continuación el manual de Logística Militar, ver imagen. Donde se relacionan las tendencias de la Logística Militar, a saber:





SEGURIDAD  TRANQUILIDAD

ESTUDIOS DE SEGURIDAD, CONFIABILIDAD Y POLIGRAFÍA  
Líderes en asesorías, consultoría e investigación, Poligrafía,  
escorta de mercancías, monitoreo de GPS y alarmas,  
sistemas de video vigilancia.

LOCALES COMERCIALES



CONSTRUCCIÓN



ESCOLTA DE MERCANCIAS



SUPERVISORES



RESIDENCIAL



POLIGRAFÍA



GRANDES SUPERFICIES

CENTRAL DE ALARMAS  
24 horas / 7 días

SEGURIDAD HORUS LTDA.



Prestamos servicios de vigilancia, seguridad privada, protección de bienes e inmuebles, personas naturales o jurídicas, escoltas a personas y/o vehículos buscando la satisfacción de las expectativas de nuestros clientes, mediante la aplicación de procesos estandarizados en todas nuestras actividades cuyo referente es la excelencia en el servicio, sobre la base de:

- La administración del riesgo.
- La prevención de actividades ilícitas generadas por terrorismo, riesgo público y otros.
- Cumplimiento del marco legislativo que rige a la organización y otros requisitos, Prevención de accidentes de trabajo y enfermedades laborales.
- Prevención de los daños a la propiedad. Recursos financieros, técnicos y humanos para el cumplimiento de las políticas y objetivos, y la mejora continua de todos nuestros procesos.



**Definición:** La Tercerización Logística en el Medio Militar, se puede definir como la acción de proporcionar algunos servicios previamente determinados o cubrir ciertas necesidades Logísticas de la Fuerza, según unas determinadas condiciones, marcadas claramente en un contrato, bajo la supervisión y con la cooperación de la Fuerza Apoyada.

La Tercerización Logística Militar, comprende desde la alimentación hasta el transporte estratégico, pasando por la Tecnología Informática, el mantenimiento de vehículos, sistemas de armas, servicios de salud, sanidad, suministro de combustibles y lubricantes entre otras funciones logísticas.

En operaciones Militares de larga duración y baja intensidad, la Tercerización Logística da continuidad al Apoyo y Servicios para el Combate Logístico requerido, por su permanencia en la zona por un periodo prolongado de tiempo, incluso contratando personal Local. La tercerización es un hecho, no un proyecto, pues se hace a gran escala desde la guerra del Golfo. La alta rotación del personal militar, va en contra de la eficiencia de los procesos Logísticos.

#### ¿Qué es un Operador Logístico Militar?

Empresa privada que presta servicios logísticos, adaptados a las necesidades específicas del medio Militar.

El Operador Logístico en Colombia ofrece cobertura nacional, soportado en una red de contactos y almacenes de distribución, cuya principal actividad es proporcionar servicios de transporte por vía marítima, terrestre o aérea, de materias primas y mercancías asociadas a operaciones de almacenaje y distribución.

Todo apoyo logístico demanda un adecuado y detallado planeamiento, es necesario estimar el tiempo, la cantidad de hombres y recursos y el modo de satisfacer las necesidades en todo nivel, desde el armamento hasta la alimentación, pasando por supuesto por el tema médico que es literalmente vital. Esto, por supuesto, implica un trabajo conjunto entre las diferentes fuerzas: Ejército, Fuerza Aérea y Armada Nacional.

Esta organización logística ha permitido que sea mucho más eficiente el funcionamiento de nuestro aparato militar, la logística militar bien empleada es un multiplicador de combate. Las líneas de transporte, que les llevan municiones, alimentación, dotaciones, material de reemplazo, entre otros apoyos, también se encargan de recoger heridos, trasladar tropas. Sí, la guerra sin logística estaría perdida y ese ejemplo de gerencia y administración de recursos humanos y materiales está siendo utilizado por las grandes universidades de todo el planeta para recoger el ejemplo de la logística militar aplicándola a la logística empresarial.

**“Finalmente, se trata de una cuestión de estrategia.”**

**¿Por qué Tercerizar en la logística militar?** La tercerización de Servicios Logísticos se debe entre otras a las siguientes razones:

- Buscar una mejor eficiencia, eficacia y efectividad en las operaciones logísticas.
- Amplia y adecuada oferta de recurso humano por parte del Operador Logístico.
- Reducción de presencia Militar, ante los ojos de la población civil
- necesidad de mayor flexibilidad y rapidez de reacción para el reabastecimiento.
- Costos menores, si se incluyen el gasto de instrucción del personal Militar.

- Sitúa a la Fuerza en la vanguardia logística al contratar expertos, acceso a mejores prácticas, lecciones aprendidas, tecnología de punta aplicada a la logística y transferencia del conocimiento. Como Función Social:

Otra importante ventaja que conlleva la Tercerización de Servicios Logísticos y que el Operador Logístico contrate personal civil para ello:

- Crear empleo local, ayudando que la Economía de la región mejore.
- Incremento de la conciencia ciudadana, acerca de la necesidad de la Defensa, su importancia y participación.

#### Algunas CONCLUSIONES:

1. En la actualidad existe una tendencia mundial concreta y evidente en favor de la tercerización de la Logística en operaciones Militares.
2. La Tercerización se considera un modelo estratégico en donde algunos procesos de la Logística Militar y empresarial, se transfieren a otra compañía.
3. Los Ejércitos modernos y las Grandes Potencias Militares, evolucionan hacia la tercerización del Apoyo y Servicios para el Combate (ASPC). ( Mas información del presente Artículo en nuestra web: [www.coladca.tk](http://www.coladca.tk))

**INSECURITY**

**Autor: Coronel (r) Jairo Andrés Cáceres García**

Máster en Informática

Universidad autónoma de Guadalajara, México.

Máster en Ingeniería de Sistemas Logísticos

Pontificia Universidad Católica de Valparaíso y


Academia Politécnica Militar Ejército de Chile. Lider

Comunidad COLADCA

Para contactar al autor del artículo, puede realizarlo

en el correo electrónico: [jacgcolombia@yahoo.es](mailto:jacgcolombia@yahoo.es)

## COLOMBIA, SEGURIDAD VS CONFLICTIVIDAD

 Por. William Orlando Núñez C.

**A**mérica y en especial Colombia en la actualidad se desenvuelven en torno al tema de la seguridad, aspecto éste que mueve multinacionales, empresas de todos los órdenes, partidos políticos, corrientes académicas y filosóficas, de tal forma que el marketing y el consumismo están a la orden del día en los medios de comunicación o en los escenarios más disímiles; en todos ellos se habla de la seguridad como el paradigma a transformar, aparecen entonces sofistas, gurús, tratadistas, analistas, politólogos y expertos que presentan profusos y profundos estudios alrededor de este, el tema en boga.

Lo cierto es que hoy “la gente puede dudar de lo que se dice, pero siempre creerá en lo que se hace”, y es sobre esta frase donde empieza el dilema de la sociedad o mejor del ciudadano del común, quien a través de los medios de comunicación o discursos del más alto nivel, recibe la información que la seguridad está en plena recuperación y que esto conlleva a mejorar los aspectos económicos, porque sectores como el agrícola, el turismo y las exportaciones hacen más dinámico al país; esa crisis que se visualiza en el resto del mundo, no sucede en Colombia gracias a la seguridad, pero será esa la realidad cuando en las calles, parques, vías, buses, colegios y en los hogares se perpetran a diario hechos criminales, que desdican o dejan por el suelo todas la teorías y afirmaciones que sobre el tema se muestran.

Pero que pasa con la seguridad?, los expertos la clasifican en Nacional, Regional o Estratégica, y a la vez la subdividen en Pública y Privada, dándole la responsabilidad de lo público al Estado, quien con sus medios debe procurar brindar la sensación (percepción) que todo marcha bien y que los habitantes del territorio se desenvuelven en la tranquilidad que le provee un cuerpo policial profesional y ético; por otra parte, entrega la seguridad en el aspecto privado a una pujante industria, la Vigilancia Privada, la cual asume roles de protección en aquellos lugares donde el Estado es insuficiente, o no cuenta con los medios tecnológicos para desempeñarse.

### ¿Que pasa con la Seguridad?



Aparecen entonces en ese último aspecto, conceptos de seguridad como el de SEGURIDAD FÍSICA, el cual describe las medidas que previenen o detienen a intrusos antes de acceder a instalaciones, recursos o información; estos pueden ser tan simples como una puerta con candados o tan elaboradas y complejas como múltiples anillos o niveles con guardias armados, la SEGURIDAD EJECUTIVA, dedicada exclusivamente a la protección de personas a través de guardaespaldas; una nueva concepción profesional del tema se presenta con LA INGENIERIA DE LA SEGURIDAD, ciencia encargada del estudio de la temática en comento, la cual luego de diagnósticos termina estableciendo los elementos claves de la seguridad como son:

**1. OBSTACULOS**, diseñados para frustrar a los delinquentes triviales o para retardar a los mas avezados o peligrosos.

**2. ALARMAS**, conjunto de conceptos sobre iluminación, patrullas, y circuitos cerrados, todo diseñado para detectar a los intrusos.

**3. RESPUESTA**, encargada de repeler, capturar o frustrar (función de Policía).

Analizados los párrafos anteriores, se puede entender que:

*“la Seguridad es por regla general una industria dedicada a proteger recursos y en la cual solo se ve al ser humano, al ciudadano, como el objeto final al que se le ofrece, promete y cobra por servicios especiales y muy profesionales de seguridad, se olvidó de plano que es precisamente el pueblo (comunidad) el destinatario de todos los esfuerzos del Estado por brindarle la calidad de vida que se requiere para vivir en armonía.”*



Con respecto a los líderes y al gobierno, afirmaba que sólo el Estado puede cubrir la mejor organización de comunidad humana, y clasificaba en tres las buenas formas de gobierno, una era la Monarquía en la cual el mandatario nunca debería permitir que se degradara a llegar a la tiranía, la segunda, la Aristocracia en la que de la misma forma ese grupo de líderes debía cuidarse de caer en la Oligarquía y por último se refería a la Democracia, la cual posiblemente podría caer en una Demagogia; en la democracia se requiere que el pueblo reciba una buena enseñanza, concepto que viene desde Atenas cuando los sofistas se abrogaron esa responsabilidad por ser sabios o hábiles, Protágoras decía “El hombre es la medida de todas las cosas”, lo que nos invita a retomar sus conceptos para hacer estimativos sobre qué es lo correcto en relación con las necesidades que vive el hombre, como ser social e individual.

Es importante para éste análisis mostrar como el artículo primero de la Constitución de 1991 define a Colombia como “un Estado Social de Derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la supremacía del interés general”; ahora bien, queda claro entonces, que este Estado social de Derecho se funda en la dignidad de la persona humana; lo que significa que el hombre como persona no es un medio, sino el fin último del orden social justo.

Entonces, muy actualizados con el principio donde el hombre es el centro, recordemos como el Humanismo es el movimiento intelectual que se extendió por Europa a partir del siglo XV, viene de la palabra latina homo (hombre), una nueva forma de pensar que confiaba en el ser humano, en su razón y en su capacidad para cultivar todas las ramas de la sabiduría. Lo que se pretendía era una formación integral, claro está, eso era el ideal, por tanto considero conveniente recordar algunos personajes de la época, que de una u otra forma se aproximaron, ellos son:

Maquiavelo, en su obra El príncipe, aconseja cómo ha de actuar el hombre de Estado, el gobernante. Defiende que su conducta debe ser práctica y realista antes que ética, es decir, lo que importa es conseguir los objetivos, aunque lo que se haga no sea justo.

- Tomás Moro, analizó los problemas de la sociedad y propuso un modelo de comunidad perfecta en su obra Utopía.

- Luís Vives, criticó los métodos educativos de la época y esbozó el perfil del humanista perfecto.

Cabe entonces preguntarse ¿Que quiere el hombre de hoy? Pues quiere un mundo humano, donde las personas puedan vivir con seguridad y dignidad, sin pobreza y desesperanza, que aunque es aún un sueño para muchos, debería ser una realidad para todos. En un mundo así, a cada individuo se le garantizaría una vida sin temor y sin necesidades, con igualdad de oportunidades para desarrollar plenamente su potencial humano.

**Construir la Seguridad basado en lo humano es esencial, para lograr por fin el objetivo propuesto de convivir en Paz.**

La expresión “Seguridad humana” fue utilizada por primera vez en 1994 en un informe anual del (PNUD) Programa de las Naciones Unidas para el Desarrollo, se plasmó como una noción amplia y multidimensional de seguridad, donde el centro era esencialmente la persona y la comunidad, y no el Estado. Esencialmente, la seguridad humana significa una vida libre de amenazas profundas a los derechos de las personas, a su seguridad o incluso a sus propias vidas.

A modo de conclusión, se puede apreciar que es este el momento de proponer una investigación social cualitativa y cuantitativa para determinar, como en efecto se realizó con el Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana – CEACSC, que en 19 de las 119 Unidades de Planeación Zonal urbana y rural en que está dividido en territorio distrital de las 20 localidades de Bogotá, se presenta el 52 % de los delitos de acontecen en la Capital de la República Colombiana, propuesta que según el artículo 12 de la ley 062, fue presentado a la alta dirección de la institución encargada de la Seguridad sin que fuera escuchado sólo por provenir de una entidad y no del gobierno central.

**Autor: William Orlando Nuñez Corredor**

Profesional en Derecho, Universidad Gran Colombia. Administrador de Empresas Universidad Cooperativa de Colombia, Especialista en Seguridad Integral, Gobierno y Gerencia Pública. Laboró en la Secretaría de Gobierno de la Ciudad de Bogotá D.C, Ex Director de Seguridad y Convivencia. Consultor docente Universidades Rosario y la Sabana en Derecho de Policía y Planeación Estratégica del Servicio. Actualmente es el director académico de Training de Colombia, CEO de la Red de la Reserva Activa de la República de Colombia. Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [direcciondeseguridadnov2013@gmail.com](mailto:direcciondeseguridadnov2013@gmail.com)

# Gestión Corporativa de la Seguridad de las Empresas en el Exterior



Por. Pedro Sebastián Hidalgo (DSE, MIE y AE).



Una gran mayoría de las empresas delegan las decisiones en materia de seguridad al personal más cercano al terreno de su actividad, la gestión operativa de la seguridad debería estar íntimamente ligada a las políticas y buenas prácticas de la organización y la toma de decisiones. Entre ellas se incluye:

- La elaboración de una Política Corporativa de Seguridad de la empresa u organización — derivada de un acto intencionado como no intencionado (security and safety) — y directrices prácticas sobre la gestión de la seguridad integral.
- Competencia organizativa y responsabilidades para determinados incidentes graves, incluyendo el establecimiento de un equipo que se ocupe de la gestión y respuesta de incidentes críticos en la oficina regional y/o en la sede corporativa para las empresas multinacionales.
- La implementación y gestión de un sistema centralizado de notificación en tiempo real de informes, de manera que todos los incidentes de seguridad, así como los frustrados o fallidos queden registrados, de manera que permita hacer un análisis genérico de los incidentes de seguridad que afectan a la organización.

Las decisiones relativas a si iniciar o no actividades empresariales en ciertos países o zonas de riesgo, y qué tipo de proyectos llevar a cabo, es responsabilidad que normalmente corresponde a la sede corporativa, siempre con el asesoramiento del Departamento Corporativo de Seguridad.

Asimismo, la empresa puede requerir que el personal sénior de la sede tome decisiones sobre ciertos aspectos importantes de la seguridad, como se ha descrito anteriormente. Asuntos relativos a Recursos Humanos, como establecer pólizas de seguro, por ejemplo, son cuestiones que también se gestionan a nivel centralizado en la organización y no a nivel de operaciones individuales o particulares.

Una empresa que desplaza personal a países o zonas de riesgo debería tener implementadas políticas, normas procedimientos y



capacidades suficientes para gestionar sus actividades empresariales en materia de seguridad. Enumeramos aquí una lista de los documentos en los cuales pueden detallarse estas políticas. Estos documentos tienen una dimensión total en la organización, son redactados por el Departamento Corporativo de Seguridad y aprobados por el comité de gerencia o similar, y constituyen recursos de referencia general.

- Mandato de la organización, declaración general de la misión/proyecto o declaración de Valores y Principios Básicos que deben presidir todas las actividades en materia Corporativa de Seguridad Integral.
- Política general de seguridad para toda la empresa u organización y, según corresponda u obligue, comunicados de políticas sobre asuntos específicos relacionados con la seguridad, como el uso de protección armada o no por parte de Fuerzas y Cuerpos de Seguridad, Ejército, proveedores de seguridad privada y protección de la información, sea ésta propia o no.
- Estructura de rendición de cuentas o responsabilidades (matriz de responsabilidades) detallando sobre quienes recaen cada una de las funciones y responsabilidades de la gestión de la seguridad, la gestión y respuesta ante incidentes críticos y la toma de decisiones, (diferenciando entre el personal de sede y en el SITE).
- Guías y manuales de referencia general y específicos, por ejemplo sobre usos y costumbres del país o religión.



## Planificación de la seguridad y preparación

En el terreno, el pilar de la gestión Corporativa de la Seguridad es el Plan de Seguridad. La eficacia e implementación de un Plan de Seguridad Integral para las actividades empresariales dependerá de la calidad del proceso de planificación. Es preferible realizar una planificación en equipo <<conjuntamente entre el personal local, nacional e internacional>> que una planificación individual, aglutinando de esta manera conocimientos y experiencias colectivas que facilita la autoría y el sentido de pertenencia del producto final. Todo proceso de planificación necesita ir seguido de revisiones periódicas — a medida que el entorno varía, es necesario actualizar el plan.

Diferentes empresas redactan e implementan Planes de Seguridad distintos en los cuales deberían plasmar las necesidades de la organización, el contexto y sus Políticas, Normas, Procedimientos e Instrucciones operacionales.

Los componentes más importantes dentro de un Plan de Seguridad Integral podrían incluir los siguientes:

1. Una síntesis del contexto del país, incluyendo conflictos, si corresponde.
2. Los objetivos específicos de las actividades o proyecto en el país.
3. Evaluación de la seguridad
4. El umbral de riesgo aceptable. Ello debe ir acompañado de un comentario que indique cómo se llegó a esa conclusión.
5. Definición de responsabilidades en función de la gestión de la seguridad integral.
6. Medidas preventivas. Algunas de las medidas se abarcarán dentro de los Procedimientos Operacionales Estándar (SOPs), dado que incluirán entre otros asuntos, la seguridad de las instalaciones del SITE o Sede, desplazamientos habituales (de personal, víveres, vehículos, material y equipos) y sistemas de comunicaciones. Algunos de estos Procedimientos Operacionales Estándar pueden traducirse en listas de verificaciones (Check List).
7. Definición clara de los roles y responsabilidades ante la respuesta a incidentes y la gestión de crisis. En algunos casos, será necesaria u obligatoria la participación de una oficina regional o de la sede corporativa.

8. Procedimientos para la notificación de informes sobre los incidentes, así como el análisis de la respuesta a los mismos.
9. Plan de Emergencia y Gestión de Crisis ante incidentes

10. Planes de retorno o cese de las actividades (hibernación, reubicación o evacuación según el nivel de amenaza establecido).
11. Una declaración de principios o una política definida respecto a la colaboración en materia de seguridad con otras empresas que operen en el mismo ambiente, como el reconocimiento de la interdependencia entre las todas las empresas, organismos e instituciones y las responsabilidades mínimas que resulten de ello, incluyendo la comunicación de “alertas” a terceros y la posible colaboración en áreas como análisis y evaluación de riesgos, y poner en común o compartir recursos (en especial vigilancia compartida con el mismo proveedor), información o logística en caso de evacuación.
12. Indicar cuándo se elaboró el plan y revisó por última vez, se implantó, cómo se elaboró (el proceso de planificación y quienes participaron en él), por quién fue aprobado y qué período mínimo será revisado nuevamente.
13. Cartografía e información GIS del entorno de operaciones, incluyendo los emplazamientos de las oficinas y sus vías de acceso y evacuación (mínimo principal y alternativa).

Hay una serie de puntos muy importantes a tener en cuenta cuando se redactan Planes de Seguridad:

# Comunidad COLADCA IMPRESIÓN DE DIFERENTES ACTIVIDADES



**COLADCA**  
Comunidad Latinoamericana de Consultores y Asesores en Gestión de Riesgos y Seguridad

**VINCULATE!**  
Membresía Especial y Autorización de Ejercicio de Profesión  
"Certificación de la idoneidad profesional y reconocimiento a la excelencia vinculada por competencias y conocimientos"  
[www.coladca.tk](http://www.coladca.tk)

**CAPACITACION "DIALOGOS DE SABERES EN SEGURIDAD"**

**NUEVAS TECNOLOGIAS**

**Revista INSECURITY**  
OBSERVATORIO DE SEGURIDAD

**Formadores**  
Operador Económico Autorizado  
CONSULTORIA HABILITACIÓN

**LINEA EDITORIAL Y PUBLICACIONES**  
Comunidad LATAM de Consultores y Asesores en Gestión de Riesgos y Seguridad

**OL COLADCA**

**1400 PROFESIONALES VINCULADOS A 2017**

**800 VINCULADOS CON MEJORES COMPETENCIAS PROFESIONALES AÑO 2016**

**POSTULACIÓN AÑO 2016 PREMIO CONTROL SOCIAL**



[www.coladca.tk](http://www.coladca.tk)  
coladca@gmail.com - info@coladca@gmail.com  
Cel. +51 311 842 1721 - 318 711 4039



Capacitación Empresarial Colviseg Ltda.

I Congreso LATAM de Seguridad aplicada a la Gestión de Riesgos 2016



1er Encuentro de la Seguridad en la Cadena de Suministro y OEA



Frente de Seguridad Empresarial DIJIN - Policía Nacional



Encuentro con Asociaciones de Seguridad Guadalajara - México / AMESP - UNESPA

• Un Plan es un documento de papel. El papel desgraciadamente no reduce los riesgos. Es necesario formar, concienciar, compartir, explicar, ejercitar e implementar los planes.

• Un plan que satisfaga las necesidades actuales no significa que será apropiado en los próximos seis meses. Si la situación evoluciona, hay que volver a examinar el análisis (de riesgos y el contexto de la situación) y por ende actualizar los planes. .

• Las personas que no están familiarizadas con los planes y los procedimientos de seguridad no pueden adherirse a ellos. Es necesario informar/-formar a todos los miembros del personal y a los visitantes/ proveedores en el momento de su llegada y después de realizar cualquier cambio importante.

• La eficaz implementación depende del nivel de competencia e implicación que se tenga. Los mejores planes se derrumban sin los conocimientos y las capacidades para implementarlo. Muchos aspectos de la gestión de la seguridad requieren necesariamente conocimientos, habilidades, actitudes y capacidades específicas.

• La gestión eficaz de la seguridad depende en cierto grado de la práctica. La práctica realizada mediante ejercicios de simulaciones y capacitación periódica - es vital. En todos estos puntos, juega un papel importante la implicación y compromiso de la Dirección de la empresa y resto de Departamentos.

### Tener en cuenta que hay qué:

• **Asegurarse** que todos los miembros del personal están familiarizados con la situación, los riesgos, amenazas y los compromisos de la empresa en función de la reducción de los riesgos y la gestión de la seguridad.

• **Cerciorarse** que todo el personal conoce cuáles son sus responsabilidades individuales con respecto a la seguridad, el trabajo en equipo y la disciplina.

• **Asesorar y prestar** asistencia al personal expatriado, subcontratado o local en los asuntos médicos, financieros y de seguros que les afectan antes desplazarse a países o zonas de medio y alto riesgo.

• **Explicar** claramente cuáles son las expectativas de los responsables del Proyecto y cuáles son los estilos de gestión en circunstancias normales y bajo altos niveles de estrés.

• **Situar** la Seguridad Integral como punto permanente (preferentemente el primer punto) en la agenda de cada reunión de los máximos responsables o gestores del proyecto y en cada reunión regular del personal.



*“Un Plan es un documento de papel, El papel... desgraciadamente NO reduce los riesgos.”*

La transversalidad de la cultura de seguridad integral, tanto a nivel individual entre los miembros del personal como en la empresa, significa considerar las implicaciones de la seguridad en todo lo que la organización innova (o que decide no hacer), desde debates sobre el diseño de los proyectos y mensajes públicos hasta las decisiones sobre la contratación de externos (personas, empresas o instituciones). El empleado “piensa seguridad”, y actúa en consonancia porque entiende su importancia, y se le respeta por ello. La importancia de la Seguridad Corporativa está reforzada continuamente, no sólo por las políticas redactadas sino más bien por los hechos.

El personal sénior tiene la responsabilidad de las decisiones que impactan positiva o negativamente en la seguridad del personal en general. Así mismo, las empresas deberían llevar a cabo auditorías de seguridad anuales de sus oficinas o proyectos sobre el terreno en base a una serie de parámetros de referencia establecidos con anterioridad y actualizables en el tiempo. Generalmente esto se podrá anunciar con anticipación, pero no necesariamente. Las auditorías pueden desarrollarse tras un incidente crítico o no, en tiempos y países o zonas donde el riesgo es alto/extremo, o periódicamente en cualquier entorno de riesgo o amenaza.

**Q1 InSECURITY**

**Autor: Pedro Sebastián Hidalgo (DSE, MIEy AE)**

Consultor Internacional de Seguridad

Vocal de Seguridad Corporativa de ASIS, Capitulo No 143

(España)

Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [coladca@gmail.com](mailto:coladca@gmail.com)

## PROCRASTINAR UN DEFECTO DE LOS CLIENTES ... O DE LAS ENTIDADES FINANCIERAS?

 Por. Luis Alfonso Ceballos G.



**E**n América Latina los productos bancarios han evolucionado a grandes pasos en la últimas décadas, guiados por el desarrollo que demanda la economía global, ciertamente en el proceso el cliente puede estar siendo relegado y bien podría jugar un rol más dinámico en la ecuación de prevención si no se enfocara en otras tareas menos relevantes que la seguridad.

Los clientes al entrar en el mundo de la tecnología de la banca electrónica, la que es dinámica, compleja y cambiante; conlleva a que en el ambiente cibernético puedan sentirse inseguros, ahí es donde aparece un contendor soterrado que siempre está al asecho, es ese delincuente que se ha especializado en analizar, evaluar y permear los sistemas financieros, a sus empleados, clientes e incluso a los círculos cercanos a este.

Pensando como actualizar al cliente y la vez hacerle más exigente su adaptación a los nuevos procesos, se puede llegar a un primer enfoque basado en verter la experiencia de las entidades financieras, las cuales cuentan con la información sobre los el riesgo de la Industria, así contribuye a establecer planes de acción más ajustados a la problemática actual que están basados en la definición de deberes y derechos contractuales, la responsabilidad más importante a mi juicio atañe al cliente el cual debería evaluar el riesgo, definiendo con asertividad los mecanismos de protección a su patrimonio informático y patrimonial, hoy se hace de manera casi intuitiva, al contar con el soporte de las entidades financieras y asesores especializados, sería indudablemente mucho más eficaz.

No es un secreto que la delincuencia busca permanentemente profesionalizarse en el tema del fraude haciéndolo transnacional y multitemático. Vistos los enormes flujos de dinero que genera el delito a este nivel, es claro que tiene la capacidad técnica y financiera de permear desde lo tecnológico hasta lo humano sin el menor reparo.

Solo para hacernos a una idea en Colombia el fraude en el sector financiero genero perdidas por más de 122.000 millones de pesos por concepto del riesgo de su operación para el 2015 de acuerdo a la Superintendencia Financiera; el 2016 no fue diferente, que sumado a la corrupción bien podría llegar a casi un punto del PIB del país, tal como se menciona en el “Conversatorio Fraude Financiero en Contexto de la Seguridad Ciudadana” que se realizo en ESPOL en Octubre del año pasado. Estos flujos de capital perdido bien podrían sacar de la extrema pobreza a un significativo número de conciudadanos o mejorar en un alto porcentaje los servicios asistenciales en todas aquellas zonas complejas del país.

Empecemos por mirar rápidamente la dinámica del delito financiero, hoy un altísimo número de transacciones se mueven a través de la Internet, lo que de alguna manera las ha hecho mucho más expeditas y eficientes para los clientes y la Banca. Indiscutiblemente seguirán evolucionado hasta que el Banco sea una figura virtual en nuestros Smartphone y Portátiles, haciendo inoficioso ir a un Banco físico para solicitar una transacción o crédito, alguien decía que los Bancos necesitan la Internet, la Internet No.

Tiempo atrás el fraude se movía mucho en el mundo de las tarjetas de crédito y el famoso Skimming era el terror de las franquicias, las pérdidas monetarias y las afectaciones a los clientes en dinero y servicio eran enormes, la industria realiza muchos ajustes a sus plataformas de autorización continuamente y además dio un paso enorme en la prevención para la falsificación integral al desarrollar, la tecnología EMV, (acrónimo de "Europay MasterCard VISA), o mejor conocido como “CHIP”, haciendo que el fraude migrara a las tracciones no presenciales, dejando obsoleto el skimming.

La banca en Colombia para el 2014, concentraba el fraude en Tarjetas en un 37% en Crédito y el 24% estaba en la Debito, para el 2016 las TC subieron al 40% y TD bajaron a 14%, lo que claramente indica que el delito no ha menguado, pero si se ha especializado en una zona donde el riesgo para el delincuente es bajo y rentable.

Las proyecciones de la Franquicias indica un crecimiento que en transacciones fraudulentas con tarjeta no presente constante. Un estudio realizado recientemente por LexisNexis y Javelin Research encontró que los emisores de tarjetas están perdiendo \$ 10,9 mil millones de dólares en el último año, el componente de tarjeta no presente se incrementa dramáticamente.

Los Asaltantes de Banco son una modalidad en decadencia dado el alto riesgo y la baja ganancia, el delito ahora donde los delincuentes enfocan su energía son las cuentas corrientes y cuentas de ahorro. En los mismos años (2014 y 2016), vemos un crecimiento que prácticamente duplica los eventos, esto tiene mucho que ver con los Portales Bancarios, la apertura de productos crediticios a partir de la vinculación de “nuevos clientes” en la modalidad denominada suplantación – Robo de identidad, (phishing, falsedad personal, falsedad documental), reflejado por un incremento de los reclamos del mas 30% con respecto al año 2015.

Esto se nota en el número de reclamaciones ante los reguladores las cuales pasan de los 26 mil casos en el último año, por Suplantación presunta de persona 26.656, Vinculación presuntamente fraudulenta 2.448, datos de la Superintendencia Financiera al año 2016; Esta modalidad de fraude antes se veía como víctima principal a los clientes de la banca personal, ahora son clientes empresariales.

La explicación se da en atención a que son mucho más rentables, si descontar que generalmente las empresas tiene más productos a controlar (mayor saldo por supuesto).

Como sabemos que no es posible un 100% de blindaje al fraude pues es quimérico, tenemos que trabajar mucho para reducirlo o mitigarlo basados especialmente en No PROCASTINAR, lo cual significa, “No dejes para mañana lo que debes hacer ya”, perdiendo tiempo en temas no tan relevantes como nuestra seguridad, dando especial atención a todos los puntos en la relación Cliente – Banca.

Los desarrollos tecnológicos, capacitaciones, distribución de información, búsqueda de vulnerabilidades, selección de personal, etc. Todos ellos y muchos más derivados de análisis de riesgos periódicos con un cruce permanente de información y consolidando barreras para hacer más difícil el accionar de los criminales

Asimismo el uso de plataformas confiables, software 100% certificado y actualizado, políticas para seguridad de la información, direcciones IP registradas, planes de confirmación en caso de operaciones de mayor monto, sospechosas o no habituales, manuales de ética entre otros programas;

que comprometan a la empresas y la Banca en el bloqueo sistemático y organizado a los defraudadores, agradando su oportuna denuncia ante las autoridades competentes logrando que el avance sea consistente y continuo permitiendo reducir el fraude.

Para ello se hace necesario que las acciones legales especialmente en materia de Cibercrimen logren acopiar técnicamente en cadena de custodia el mayor número de evidencias, para convertirlas en pruebas contundentes que ayuden a seguir el flujo del dinero y la identificación de los responsables para que estos no continúen ascendiendo en su carrera delictiva, disfrutando de la impunidad y el dinero obtenido ilegalmente que afecta a la economía mundial.

Los clientes deben tener claro que la custodia de sus productos financieros es la garantía numero uno de la seguridad de los mismos, no pueden subestimar la capacidad de los defraudadores para suplantarlos y tomar control de nuestras cuentas y demás activos, recordemos que somos nosotros los que tenemos la llave de la caja de caudales, si la dejamos debajo del tapete de entrada, no podemos abstraernos de nuestra responsabilidad.

Todos los ciudadanos tenemos una dependencia directa de los servicios y productos financieros, lo que nos convierte automáticamente en protagonistas de nuestra seguridad y tranquilidad. No se vale tratar de trasferir el riesgo a la entidad o de no comunicar el evento, para negar la responsabilidad y oportunidad al momento de saber o detectar que esta comprometida o vulnerada nuestra información cuando caemos en trampas como el phishing, ingeniería social o similares.

Una oportuna comunicación es determinante a la hora de contribuir para que otros clientes no caigan en estrategias similares, igual sucede cuando veamos extraños comportamientos en nuestros sistemas o en la portales de nuestro Banco, etc.

La premisa es trabajar en equipo contra un enemigo que no mira quien en ultimas sea la víctima llámese entidad o cliente, al final gana, no importa quién pierda.

**La educación financiera** en el tema **seguridad** debe ser una premisa para el cliente y las entidades y de esta manera puedan: **Prevenir, Detectar y Mitigar** el fraude potencial o real y denunciarlo antes las autoridades competentes.

Instruir al cliente en la forma de realizar un panorama de riesgos personalizado, que interprete la dinámica de los criminales, la evolución del delito, las múltiples formas de proteger el patrimonio económico y la administración de la información.

La primer regla a tener en cuenta es que toda la información que se sube a Internet queda para siempre, en algún sitio y en algún momento esos datos pueden ser utilizados para explotarlos legalmente o ilegalmente; Reitero esto último ya que es la llave maestra para permitir el ingreso a toda nuestra vida comercial y personal, aquí tratare de esbozar algunos puntos de vista sobre las vulnerabilidades desde mi experiencia en el sector.

• **Las contraseñas como fuga de información:** Se dice quién la tiene, posee el poder y esta premisa en el mundo criminal es la que los hace tan exitosos; por lo que custodiaria adecuadamente y compartirla de forma inteligente se convierte en nuestra primera acción de prevención. Hoy en la internet se habla permanentemente de fuga de información, perdida de bases de datos, toma de control de Smartphone, computadores personales, pago de servicios, Ransomware, portales falsos, robo de identidad entre otros. Pero quién de nosotros es consciente de ¿cuanta información hemos vertido en esa Gran Red que es la internet? y lo que conlleva, pero no dimensionamos como pueden los delincuentes construir a partir ella cualquier delito.

Cuántos de nosotros cambiamos periódicamente nuestras contraseñas de acceso a Bancos, correos, redes sociales, etc?

Donde dejamos esta información, será ¿que esta a la vista de los criminales expertos?, por lo cual debemos cuestionarnos y dudar siempre.

• **Los computadores dedicados:** cuando se trate de CPU/Portátiles, se debe limitar el acceso a estas maquinas con contraseñas de usuarios y en lo posible personalice su uso cuando se trate de gestiones financieras o sensibles.

• **Smartphones:** Son parte integral no solo de las comunicaciones entre cliente y Banco, sino también son herramientas transaccionales, que pueden ser anuladas y reemplazadas fraudulentamente para realizar y/o confirmar operaciones. **Nota: especial cuidado cuando viajen y al usar redes Wifi Publicas!**

• **Los software:** se deben actualizar invariablemente en nuestros equipos, verificar que todos los “parches o actualizaciones” estén al 100%, no instalar aplicaciones que no estén certificadas.

• **Las APP's:** En redes sociales, tener claro que muchas aplicaciones solicitan acceso a nuestra información, y con ello pueden controlar hasta nuestra ubicación geográfica.

• **El software malicioso:** este tema es enorme, el mejor preventivo es mantener un software antivirus licenciado de alta calidad, **Nota: las cosas buenas no son gratis.**

**Nota Adicional: Entre menos se exponga al visitar lugares peligrosos y desconocidos en la web, menos se contamina!**

• **El phishing:** es un de las formas más exitosas mediante la cual los criminales capturan información crucial de acceso a los Bancos y otras entidades financieras, lo grave radica en que ni su entidad ni ustedes se enteran hasta cuando es ya es demasiado tarde. No use direcciones que se autocompletan o están en el banner de su navegador, la premisa es verificar las IP address <https://www> , el candado y de cuando en vez verificar toda la dirección.

• Otra modalidad es el uso de links fraudulentos embebidos en la comunicación estos que bajan software malicioso, que captura toda información de la computadora, e incluso lo que se teclea en el momento, como nombre de usuario y contraseñas, el siguiente solo un ejemplo:



Estas son **excusas utilizadas para engañar al usuario:** cambio en la normativa del Banco, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, bloqueo de la cuenta por motivos de seguridad, etc.

Hay mucho material sobre estos temas de prevención, mantengámonos informados y tendremos el poder, mitigando las pérdidas hasta donde sea posible. **Procrastinar..NO!.....**



**Autor: Luis Alfonso Ceballos**

Consultor de Seguridad e Investigaciones Especialista en Seguridad Física e Investigaciones de Fraude Financiero, Líder equipo Consultor Comunidad COLADCA. Ex Vicepresidente A. CSIS por 27 años (Citigroup Investigative & Security Services) - Citibank Colombia.

Profesional en Fraude Interno y su prevención, falsedad, riesgo público y en la cadena de suministros, Evaluación Estratégica de Proveedores, Auditoría Procedimientos y sistemas de Protección Seguridad Física, Evaluación de Riesgo Físico y Reputacional, CIFIN. Aplicación del concepto de Seguridad Inteligente. Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [luisalfonsoceballos@gmail.com](mailto:luisalfonsoceballos@gmail.com)



## Confianza y comunicación, Seguridad para las diferentes maneras en que los sensores IOT y Smart se conectan a la WEB



Por. Dr Chris Mobley Ph.D, M.Phil, B.Eng  
CTO M2M Telecom Ltd.

### Trust and Communication (Versión Original en Inglés)

This article is written to highlight the number of different ways IoT and Smart sensors can connect to the Web.

An embedded IoT device can connect to the Internet over a wide range of communication channels – from Mobile telephony, WiFi, satellite, wired connection and general wireless transmission. For each connection a range of protocols exist to exchange information. For example Mobile telephony has a number of connection methods – SMS, connection switched data circuit (GSM), packet switched data service (GPRS). Industrial and automotive systems have a different set of protocols – Modbus, or CAN Communication Protocol for example.

**Many communication channels for IoT in industrial, automotive and smart sensors have been developed without security in mind - they assume that the channel is a trusted one. Wrong!.**

All forms of communication require four things to enable the secure transmission of information across the channel. These are authentication, impersonation, validation and obfuscation.

### Authentication

Before communication can begin a trusted channel must be established. The sender of the information must be sure that the recipient of the information is the intended recipient. The receiver of the information must be sure that the information is sent from the intended sender.

In the human world this is relatively easy to achieve when the sender and receiver are talking to each other. Either they know each other (and have "history") or they have a mutual trusted friend. For IoT electronic trust is performed by having electronic "history" together, or a trusted 3rd party.



### Confianza y Comunicación (Versión en Español)

Este artículo se escribe para resaltar el número de diferentes maneras en que los sensores IoT y Smart pueden conectarse a la Web. .

Un dispositivo IoT integrado puede conectarse a Internet a través de una amplia gama de canales de comunicación, desde telefonía móvil, WiFi, Satélite, conexión por cable y transmisión inalámbrica general. Para cada conexión existe un rango de protocolos para intercambiar información. Por ejemplo, la telefonía móvil tiene varios métodos de conexión: SMS, Circuito de datos conmutados de conexión (GSM), servicio de datos conmutados por paquetes (GPRS). Los sistemas industriales y automotrices tienen un conjunto diferente de protocolos: Modbus o CAN Protocolo de comunicación, por ejemplo.

**Muchos canales de comunicación para IOT en sensores industriales, automotrices y inteligentes han sido desarrollados sin la Seguridad en mente - Asumen que el canal es de confianza. ¡Incorrecto!.**

Todas las formas de comunicación requieren cuatro cosas para permitir la transmisión segura de información a través del canal. Se trata de autenticación, suplantación, validación y ofuscación. .

### Autenticación

Antes de que la comunicación pueda comenzar, debe establecerse un canal de confianza. El remitente de la información debe estar seguro de que el destinatario de la información es el destinatario. El receptor de la información debe estar seguro de que la información se envía desde el remitente previsto.

En el mundo humano esto es relativamente fácil de lograr cuando el remitente y el receptor están hablando entre sí. O se conocen (y tienen "historia") o tienen un amigo de confianza mutua. Para IoT la confianza electrónica se lleva a cabo por tener "historia" electrónica juntos, o un tercero de confianza.

Electronic "history" is in essence some pre-placed information that the sender and receiver share. Thus it is easy for the sender and receiver to verify each other by exchanging their pre-placed information. A trusted 3rd party can also authenticate that the receiver and sender are who they say they are.

### Impersonation

The problem with authentication is that people and electronic systems can be impersonated (cloned). For example forgery of a signature is impersonation and if successful will allow access to bank funds etc. The MAC address in an IP hardware device is unique (or supposed to be) however in many integrated circuits the MAC address is programmable, allowing for 2 devices to have the same MAC address. Cloning of a mobile phone is easy and has led to many intercepted data and voice calls.

So how do we stop cloning of electronic devices? We need method of providing uniqueness that cannot be cloned – this is often called the Trusted Platform Module (TPM). These work by enshrining a unique feature or numerical value into the electronic device that cannot be read. In Humans anti-clone features are memories that cannot be accessed by force.

### Validation

So now we have built an authenticated system based upon un-cloneable technology, with pre-placed information. We have exchanged the pre-placed information and have established a trusted channel between the sender and receiver of the information. Two problems still exist – how to stop an eavesdropper (man-in-the-middle attack) recording the conversation and how do we stop the alteration of the conversation. When an individual intercepts the message they have the ability to just record the message or to intercept, alter and then re-send it.

So how do we stop a message being altered? We need to validate the message with information that is difficult to alter. A one-way mathematical function – such as the HASH – can be used along with current date and time can be used to validate the message.

It works in the following way – the sender generates a message, they note the current world date and time and then perform a HASH on the message and current date and time. The message is sent to the receiver. The receiver performs the same HASH using current world time and the message. If the HASH's are the same then the message has not been altered. This assumes that world time cannot be altered – and assumes that the message is sent instantaneously from the sender to the receiver.

La "historia" electrónica es en esencia una cierta información previamente colocada que el emisor y el receptor comparten. Por lo tanto, es fácil para el emisor y el receptor para verificar mutuamente mediante el intercambio de su información previamente colocada. Un tercero de confianza también puede autenticar que el receptor y el remitente son quienes dicen que son.

### Suplantación de identidad

El problema con la autenticación es que las personas y los sistemas electrónicos pueden ser suplantados (clonados). Por ejemplo, la falsificación de una firma es suplantación y si tiene éxito permitirá el acceso a fondos bancarios, etc. La dirección MAC en un dispositivo de hardware IP es única (o se supone que sea) sin embargo en muchos circuitos integrados la dirección MAC es programable, permitiendo 2 dispositivos Para tener la misma dirección MAC. La clonación de un teléfono móvil es fácil y ha llevado a muchos datos interceptados y llamadas de voz.

Entonces, ¿cómo detenemos la clonación de dispositivos electrónicos? Necesitamos un método que proporcione unicidad que no pueda ser clonado, a menudo se denomina Trusted Platform Module (TPM). Estos trabajos consagran una característica única o valor numérico en el dispositivo electrónico que no se puede leer. En los seres humanos rasgos anti-clon son recuerdos que no pueden ser accedidos por la fuerza.

### Validación

Así que ahora hemos construido un sistema autenticado basado en la tecnología no-clonable, con información pre-colocada. Hemos intercambiado la información previamente colocada y hemos establecido un canal de confianza entre el remitente y el receptor de la información. Todavía existen dos problemas: cómo detener a un intruso (ataque de hombre en el medio) que graba la conversación y cómo detenemos la alteración de la conversación. Cuando un individuo intercepta el mensaje que tienen la capacidad de simplemente registrar el mensaje o para interceptar, alterar y luego volver a enviarlo.

Entonces, ¿cómo podemos detener un mensaje de ser alterado? Necesitamos validar el mensaje con información que es difícil de alterar. Puede utilizarse una función matemática unidireccional – como el HASH – junto con la fecha y la hora actuales para validar el mensaje.

Esto funciona de la siguiente manera: el remitente genera un mensaje, anotan la fecha y la hora actuales del mundo y luego realizan un HASH en el mensaje y la fecha y hora actuales. El mensaje se envía al receptor. El receptor realiza el mismo HASH usando la hora mundial actual y el mensaje. Si los HASH son los mismos, el mensaje no ha sido alterado. Esto supone que el tiempo del mundo no puede ser alterado - y asume que el mensaje se envía instantáneamente desde el remitente al receptor.

However If the eavesdropper can also perform a HASH instantaneously they can alter the message, perform the HASH with current date and time and re-transmit the data to the receiver. The receiver is none the wiser as the HASH is still valid.

If the sender uses some of the pre-placed information used in the authentication as part of the message HASH then the man-in-the-middle cannot re-do the HASH, as they do not have the pre-placed information.

### Obfuscación

We now have an authenticated, non-cloned, and validated link, but the messages can still be intercepted. We can never stop interception, but we can obfuscate the message in such a way that the message cannot be read (with current technology). The way to achieve this is through the use of encryption. This is a mathematical process that uses a secret key to obfuscate the message in such a manner that only the system with the key can recover the original message.

### Implementación

In a practical system there are a number of hurdles to overcome. In a simple system where the sender only communicates to a single receiver then a simple method of exchanging pre-placed information is sufficient to establish trust and secure the communication channel.

But if the sender can be a receiver and can send and receive from many different sources sequentially, then establishing and maintaining secure channels over numerous periods of time requires a different approach.

Sin embargo, si el intruso también puede realizar un HASH instantáneamente pueden alterar el mensaje, realizar el HASH con fecha y hora actuales y volver a transmitir los datos al receptor. El receptor no es el más sabio pues el HASH es todavía válido.

Si el remitente usa parte de la información previamente colocada utilizada en la autenticación como parte del mensaje HASH, entonces el hombre en el medio no puede volver a hacer el HASH, ya que no tienen la información previamente colocada.

### Ofuscación

Ahora tenemos un enlace autenticado, no clonado y validado, pero los mensajes aún pueden ser interceptados. Nunca podemos detener la interceptación, pero podemos ocultar el mensaje de tal manera que el mensaje no se puede leer (con la tecnología actual). La forma de lograr esto es mediante el uso de cifrado. Este es un proceso matemático que utiliza una clave secreta para ofuscar el mensaje en una mansión tal que sólo el sistema con la clave puede recuperar el mensaje original.

### Implementación

En un sistema práctico hay una serie de obstáculos a superar. En un sistema simple en el que el emisor sólo se comunica con un único receptor, entonces un método simple de intercambio de información previamente colocada es suficiente para establecer confianza y asegurar el canal de comunicación.

Pero si el remitente puede ser un receptor y puede enviar y recibir de muchas fuentes diferentes de forma secuencial, a continuación, establecer y mantener canales seguros en numerosos períodos de tiempo requiere un enfoque diferente.

**Autor:** Dr Chris Mobley Ph.D, M.Phil, B.Eng CTO M2M Telecom Ltd.

Con mas 30 años de experiencia en la investigación y desarrollo de sistemas electrónicos y software de vanguardia para las industrias de defensa, comunicaciones móviles, automoción y energía. Especializado en aplicaciones integradas de alto rendimiento, en tiempo real y de seguridad. Amplio conocimiento de algoritmos de procesamiento de señales digitales e implementaciones en una variedad de plataformas de microprocesador y FPGA. Trabajo para Empresas como Persides, Thales, Motion Media, el Ministerio de Defensa y la Universidad de Bath, obtuvo un MPhil y PhD en Digital Signal Processing.

Para contactar al autor del artículo, puede realizarlo la cuenta de LinkedIn <http://linkedin.com/in/chris-mobley-1537395> o en la **pagina web: <http://blueskytec.com/about/>**



Geepy IoT products designed under strict control of BluGe. They are lightweight, extremely safe and very small. This device is sold in all countries with the Card Global Data, SIM-Free Networks, etc. EU/EEA. Wholesale of 10K+ only.

#### FEATURES

- 4G LTE Cat M1
- 4G LTE Cat N1
- 4G LTE Cat NB1
- 4G LTE Cat NB2
- 4G LTE Cat NB3
- 4G LTE Cat NB4
- 4G LTE Cat NB5
- 4G LTE Cat NB6
- 4G LTE Cat NB7
- 4G LTE Cat NB8
- 4G LTE Cat NB9
- 4G LTE Cat NB10
- 4G LTE Cat NB11
- 4G LTE Cat NB12
- 4G LTE Cat NB13
- 4G LTE Cat NB14
- 4G LTE Cat NB15
- 4G LTE Cat NB16
- 4G LTE Cat NB17
- 4G LTE Cat NB18
- 4G LTE Cat NB19
- 4G LTE Cat NB20



#### JTAG Programming Module



# Estudios de confiabilidad, base de la prevención y protección



Por. Carlos Alberto Rojas Aguirre

Al ser una época de cambios en entornos legales, regulatorios, ambientales, escándalos financieros, fraudes, e incertidumbres, ninguno es inmune a los daños y a impactos potenciales de eventos inesperados o tal vez esperados cuando no hay claridad y planeación de los posibles riesgos que pueden enfrentar las empresas en su entorno. Cada día las juntas directivas de las empresas deben tomar más interés en observar las oportunidades de mitigar y prevenir sus riesgos.

En medio de la competencia y su complejidad toda empresa necesariamente debe conocer y enfrentar los riesgos a que se expone en su nicho de mercado.

Aunque no es un secreto que, para un alto porcentaje de las empresas, todo procedimiento o proceso de confiabilidad adicional que se aplique - **Estudios de seguridad**, que para muchos son considerados un gasto operacional y sin aplicación, se relacionan con los procesos de apoyo.

El protocolo que los estudios de confiabilidad con llevan se puede tomar como perturbadores o dilatadores del proceso de selección o innecesarias, consideran que los incidentes y pérdidas ocasionados por la inseguridad no las justifican, pero esto a futuro se pueden convertir en un riesgo mayor que poco a poco acaba con el buen nombre y patrimonio de las compañías.

Frecuentemente se piensa que el fraude y la corrupción son parte del entorno, que para eso se cuenta con procesos de seguridad, prevención o control pérdidas entre otros, sin tener presente que para cuando estos procesos actúen ya son en calidad de represión y no de prevención. Otro profesar o pensar de la alta gerencia es que al fin y al cabo las personas encontrarán formas inteligentes de evadir normas y controles.

A veces le ayuda a los delincuentes, la falta de una política criminal sería para combatir el delito, muchas empresas optan por ayudar a la propagación del delito sin castigo, antes que incurrir en largos procesos judiciales sin certeza de acción.

A grandes rasgos lo descrito antes hace parte de un conjunto de creencias y actuaciones - que configuran el clima y la cultura de seguridad (prevención) en algunas empresas y organizaciones.

Es necesario entender que la cultura de seguridad (prevención) debe apuntar en el contenido particular del negocio y contribuir a sus resultados, pues está intrínsecamente ligada al compromiso y a valores como la atención al cliente, el control de costos y el trabajo en equipo.

Una cultura positiva de seguridad, promueve prácticas convincentes al mismo tiempo que contribuye con los objetivos económicos, comerciales y de producción, nada de esto es totalmente exitoso si no se realiza desde el principio con una contratación segura y confiable, que lo podríamos definir como un riesgo previsible si es atendido a tiempo y no reactivo cuando ya se tiene el inconveniente.

La alta gerencia debe tener claro la diferencia de conceptos y de resultados, como una **Inversión y "NO UN COSTO"**, se verá reflejado en dinero producto de la reducción de la merma y la alta rotación, la rotación en un enemigo silencioso para la productividad de un negocio, no solo por el gasto operacional también por la fuga de información, siendo esta última la más peligrosa; Las empresas también deben tener en cuenta como su activo más valioso "**La reputación**" de la empresa que en caso de afectación su costo es incalculable.

Una contratación segura, confiable y efectiva promueve prácticas convincentes al mismo tiempo contribuye con los objetivos económicos, comerciales y de producción; cuando se habla de confiabilidad en la contratación se hace referencia a un estudio real, sobre el antes, el ahora, incluyendo una proyección al después de una persona, esto solo se logra uniendo los procesos psicológicos con los estudios de confiabilidad, los cuales minimizan el riesgo y aumentan el buen clima organizacional, la cultura de seguridad (protección).

Los estudios de confiabilidad nos generan una base de partida del colaborador, al ingresar a la compañía y con posteriores sesiones de mantenimiento se puede realizar una comparación de su crecimiento desde que está en ella.

La situación actual del país, y los tiempos que se avecinan deben ser un llamado de alerta a la alta gerencia de todas las empresas, la filtración del personal no idóneo para las compañías y con índices de confiabilidad muy bajos, pueden causar daños sensibles en los diferentes aspectos críticos de las operaciones mismas, el buen nombre y las finanzas de las empresas.

Realizar estudios de confiabilidad, no es una práctica exclusiva de las grandes empresas, se sugiere aun con mayor énfasis que las medianas y pequeñas empresas se blinden desde el principio con este tipo de prácticas que siempre serán reflejadas como beneficios económicos y estructurales para las mismas.

La CONFIABILIDAD, es el sostenimiento de la calidad a través del tiempo respondiendo eficientemente en el momento crítico se puede estimar (evaluar y pronosticar), es importante contar con un aliado estratégico para los estudios de confiabilidad y/o el personal altamente calificado e idóneo toda vez que si la fuente es confiable el resultado es confiable y por ende la información es confiable.

Como lo describe el CR. Luis Enrique La Rota en su libro Consultor Didáctico METIS. SIG "La seguridad integral ha tenido en cuenta para su gestión cuatro aspectos de la confiabilidad operacional: el factor humano, el diseño, el proceso y la prevención. El estudio de seguridad que se inicia con diagnóstico de la realidad actual, para continuar con el pronóstico, donde se elabora el análisis de criticidad, tienen como propósito verificar la confiabilidad, es decir el acierto y la efectividad". La cultura está ligada al compromiso con el éxito y la preservación de la empresa, por esto gestionarla vas más allá de comunicaciones y procesos de sensibilización, es un esfuerzo sistemático que comienza con la medición y termina con la evaluación de los resultados.

La prevención y la seguridad son bases fundamentales para el crecimiento y productividad de las organizaciones, es un reto que la alta gerencia debe asumir como propio, además los profesionales en seguridad, prevención y riesgos debemos escalar y profesionalizar a tal forma que dejen de ser procesos de apoyo y convertirse en procesos misionales transversales en la compañías, en donde los procesos de "seguridad, Prevención Pérdidas, administración del riesgo, entre otros" sean la voz directa y CONFIABLE de la alta gerencia.



**Autor: Carlos Alberto Rojas Aguirre**

Tecnólogo en investigación judicial, Tecnológico de Antioquia, Tecnólogo en Salud Ocupacional, Gerencia de la administración, Administración del recurso humano, Estudiante de Derecho, Oficial de bomberos en rango de teniente (r), Especializado en estudios integrales de riesgo perfeccionándolo desde su visión y obteniendo como resultados, Estudios y análisis aplicables de manera real en prevención y protección representado en cifras reales para las compañías.

Dieciocho años de experiencia en investigación prevención y protección, cuenta con grandes resultados en investigaciones y reducción de mermas empresariales.

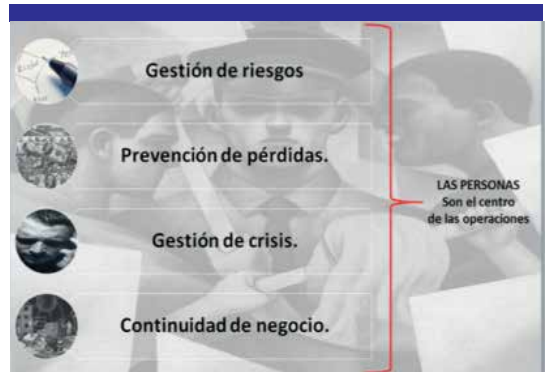
Trabaja constantemente en profesionalizar la seguridad y sus diferentes procesos de prevención y control del riesgo.

Gerente general de la empresa P&P Asociados S.A.S.

Empresa de consultoría y asesoría en confiabilidad, prevención y protección. Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [carlos.rojas@pypasociados.com](mailto:carlos.rojas@pypasociados.com)

# De la Vigilancia a la Gestión de riesgos

 Por. Carlos Moreno



*El modelo de seguridad es cada vez más exigente, pero basado en gestión de riesgos y pérdidas, No en vigilancia.*

Mucho es lo que la seguridad ha evolucionado en Colombia antes y después de la creación de la Superintendencia de Vigilancia y Seguridad Privada.

Para comienzos de los años 90's, el sector estaba en la cuasi informalidad, pero gracias al Estado se pudo entrar a controlar un gremio que hoy factura al año más de 9,8 billones de pesos. No obstante, con la llegada de las multinacionales, el modelo fue madurando hasta lo que hoy los profesionales del sector conocemos. Se han diversificado servicios que nunca se pensaron se pudieran implementar (poligrafía, estudios de seguridad, due diligence, etc) y hoy ya se habla más de gestión de riesgos que de vigilancia, siendo esta última una parte del engranaje mas no define la tranquilidad de una organización.

Esta tranquilidad no está solo dada en tener más guardas, es prevenir las pérdidas a través de la gestión de riesgos de marca, reputación, cumplimiento legal, operaciones y TI.

En mi caso como responsable del programa de gestión de riesgos y pérdidas de una organización dedicada al comercio (modelos de retail y centros comerciales), es mucho lo que se puede hablar en el tema sobre todo cuando estas grandes superficies son facilidades abiertas al público con un tráfico de personas altísimo.

La sabiduría convencional nos ha enseñado que en un modelo de comercio, se debe tener más cámaras y más guardas para prevenir el hurto, no hay algo tan alejado de la realidad como esta teoría.

Las pérdidas de estos negocios son calculadas en el margen de operación pero siempre pensando en el gasto de horas hombre y tecnología vs retorno, pues al final termina siendo más costoso la solución que el problema; Ahora bien, que sucede cuando el problema no es solo variables de pérdidas de mercancía (hurto, daño, consumo, desperdicio, vencimientos, errores administrativos) lo que termina afectando un inventario sino que no se tienen en el radar las posibles acciones de los clientes contra la marca cuando los ambientes de compra o visita no son seguros? Aparecen otras variables de pérdida. Pongamos unos ejemplos que han sido muy conocidos en el comercio Colombiano:

- El cliente que esta de compras y en su recorrido tropieza y cae y como consecuencia tiene lesiones considerables.
- El cliente que al salir de un establecimiento comercial, es agredido por el personal de vigilancia al no estar de acuerdo en los controles.
- El accidente de un menor de edad en un centro comercial sea en una elevación vertical o en la caída al vacío.
- El procedimiento de judicialización donde el sustractor de la mercancía se encerrado o agredido por el personal de vigilancia, desconociendo los mínimos de los derechos humanos del sustractor.

Todos los anteriores casos han pasado en el comercio Colombiano y han tenido resultados catastróficos contra la marca en reputación, demandas, sanciones, señalamientos y escrutinio público, lo que va en contravía del objeto del negocio: la venta y la rentabilidad del negocio.

Hemos visto 4 ejemplos, pero que sucede con riesgos como incendios, accidentes laborales, cese de actividades, ataques informáticos a la red, falsificación de marca o producto, fallecimientos al interior del local, mala selección de contratistas involucrados en lavado de activos, etc. Los riesgos son muchos.

Pensemos en cual fue el papel de la vigilancia en la gestión del riesgo en estos casos? Que matriz de riesgo se utilizó?

Que acciones documentadas se ejecutaron con el objetivo de que se minimizara tanto probabilidad de ocurrencia como severidad?.



Considero que muy pocas empresas en el sector o muy pocos responsables de riesgos podrían dar una respuesta en función de la continuidad del negocio.

**En este nuevo panorama algunos jugadores que no ha madurado, se han visto solo relegados a prestar servicios de vigilancia, dejando el espacio en el mercado a nuevos jugadores que ven más allá de un hombre en un acceso, esto hace la diferencia en las nuevas generaciones de responsables de riesgos, tienen en el radar todos los riesgos desde la concepción de un proyecto y sus costos en seguridad pero gestionan más allá de colocar vigilancia.**

Trabajan sobre legislación colombiana, sobre normas como NFPA, ISO, BASC, etc. y le agregan valor a su gestión: controlan el gasto de seguridad frente a la pérdida en activos y reputación.

Muchas de estas organizaciones no les interesa certificarse, les interesa es tomar las buenas prácticas para ser implementadas hablando siempre un lenguaje de números sobre la premisa de DATOS Y HECHOS.

**Como tip final:** Si usted como responsable de no vio venir alguno de los cuatro ejemplos, usted es un Jefe de seguridad, no un Director de riesgos y su actividad solo se está limitando a administrar un contrato de vigilancia y una central de cámaras.

**INSECURITY**

**Es el momento de que tome la iniciativa!**

**Autor: Carlos Hernando Moreno.**

Gerente de prevención de pérdidas en Falabella de Colombia.

Master en gestión de riesgos.

Ingeniero en salud y seguridad en el trabajo.

Tecnólogo en higiene y seguridad industrial.

28 años en el sector de la seguridad.

Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [coladca@gmail.com](mailto:coladca@gmail.com)

# Asesoría de Seguridad y prevención: Pilares básicos de la Seguridad



Por. Pedro Valdivia Castillo

Según Abraham Maslow, la seguridad es una necesidad primaria del hombre como consecuencia de la percepción de las amenazas y peligros potenciales que afectan a su integridad física y bienes. Hoy en Chile y en gran parte de América Latina, esta seguridad tiene dos ámbitos, la Pública, entendida como el derecho individual y comunitario a ser protegidos por el Estado, y la Privada, donde los recursos dependen exclusivamente de los que decidan invertir las distintas entidades de origen privado.

Dicha inversión, se traduce en proteger la seguridad interna de las instalaciones, por cuanto la externa es tarea de la fuerza pública a través de sus Policías. Entendiendo este concepto, se puede generar una política de seguridad preventiva para el normal funcionamiento de las actividades sin poner en riesgo la integridad física de sus integrantes, sus bienes y además el prestigio, todo lo que finalmente repercute directamente en el desarrollo comercial.

Es lamentable observar como aun hoy se desestima invertir en seguridad, por considerarlo un gasto más, no obstante tener presente que un evento de naturaleza crítica, finalmente en forma irremediable derivará en una grave situación, donde más allá de la pérdida del Bien, afectará directamente la imagen corporativa de las empresas.

De allí la importancia de evaluar el costo beneficio que significa para las Compañías invertir en sistemas de seguridad adecuados, los que en todos los casos debieran tener como objetivo un sistema de prevención eficiente que permita detectar, controlar o reaccionar ante todo evento por ínfimo que este sea, dado que cualquiera sea su origen, potencialmente puede transformarse en una emergencia de alto riesgo.

El problema de la delincuencia hoy en Chile y en gran parte de los países latinoamericanos es un problema contingente, real, transversal y que no siempre se logra controlar en forma eficiente ya que generalmente se reacciona con los sentimientos antes de prevenir con el razonamiento, afectando por tanto al desarrollo integral de nuestra sociedad, donde el delincuente en el ejercicio de su actividad ilícita, no hace ningún tipo de distinción;



Atacando transversalmente por el logro de sus objetivos sin importar si sus víctimas son personas, Empresas o Instituciones. El fin justifica los medios pareciera ser su afán, sin conciencia de que ese fin está lleno de perversidad. Y lo más grave que no solo aumentan los hechos delictuales, sino progresivamente la violencia en los medios empleados para con las víctimas.

Hoy debemos enfrentar esta problemática social con sabiduría e inteligencia y evitar así cometer el primer error cuando somos víctimas de un delito implementando medidas de seguridad como reacción a la situación vivida, sin ponderar lo ocurrido, analizar por qué ha sucedido y corregir lo que en su momento no pudimos, o no supimos hacer.

Ello nos obliga a tener un compromiso con nuestra seguridad, más allá de las políticas de los gobiernos y de lo que hacen las Policías. Eso se llama prevención y no reacción, inversión y no gasto, conciencia ciudadana y no reproche social.

Entendiéndolo así, podemos valorar lo que es la prevención y darle forma real y tangible materializándolo en Políticas que se puedan desarrollar con medidas preventivas acordes a lo que realizamos o esperamos.

La prevención no debe obedecer a una conducta reactiva, sino a un conjunto de medidas que nacen de análisis técnico denominado Diagnóstico de Seguridad, desarrollado a través de una asesoría que sea capaz de determinar las debilidades y fortalezas de cada instalación con el objetivo de que los recursos financieros que se invertirán se adecuen a la inversión que disponga y que sean proporcionales a lo que se quiere o necesita proteger.

Desarrollar una política de seguridad en una Empresa, sobre la base de un Diagnóstico de Seguridad, significa rentabilizar la Inversión implementando medidas de seguridad equilibradas respecto del bien protegido y demostrando que una instalación segura, no necesariamente es la que tiene más elementos tecnológicos o humanos incorporados, sino que aquella donde los recursos invertidos, responden al que, como, cuando, donde y porque pueden generarse situaciones de riesgo que puedan terminar en delitos.



Un diagnóstico de seguridad debe determinar las debilidades y o amenazas que puedan afectar a la Empresas mediante un estudio acabado para concluir en una solución de seguridad que considere equilibradamente cuáles serán los recursos tecnológicos más adecuadas a cada circunstancia, y el perfil de los recursos humanos competentes.

## Q InSECURITY

**Autor: Pedro Valdivia Castillo**

Coronel (r) de Carabineros de Chile

Asesor de Seguridad.

Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [coladca@gmail.com](mailto:coladca@gmail.com)

Somos:  **Revista InSECURITY**   
Comunidad Latinoamericana de Consultores de Seguridad  
OBSERVATORIO DE SEGURIDAD  
"Dejando Huella"

# SUMARIO ANALITICO LATINOAMERICANO



Por. ESR GLOBAL CORP,  
Expert Security Resources

En la mayor parte de América Latina, de Argentina a México, Chile a Brasil, Centroamérica y el Triángulo Norte, existe una sensación incómoda, casi un temor sobre las perspectivas para 2017. Las causas tienen raíces diferentes dependiendo del aspecto individual. Para algunos la preocupación tiene que ver con la lenta muerte del neoliberalismo que causa tanta pobreza en todo el continente. Para otros, el continuo efecto del narcotráfico y la inevitable guerra contra los estupefacientes, que ha provocado tanta violencia y corrupción en la región. Las desapariciones de decenas de miles de personas, muchos de las mismas mujeres e infantes es también la causa de ansiedad y dolor individual.

Como si eso no fuera suficiente, la inesperada elección del Sr. Trump en Estados Unidos, es otro factor que genera una considerable inestabilidad cuyas consecuencias en América Latina aún no se han visto. No cabe duda de que su presidencia podría tener algunos efectos positivos en la economía de la región, pero éstos irán acompañados de cierto dolor y trastorno de las viejas formas de hacer negocios.

Solamente un tonto hace predicciones sobre el futuro ya que normalmente son erróneas. Pero el consultor y sociólogo Austriaco/Americano Peter Drucker astutamente observó: (1) la mejor manera de predecir el futuro es crearlo; (2) observar lo que está pasando y hacer una proyección razonable para un futuro a corto plazo.

Tomando en cuenta estas observaciones, el propósito del "Sumario Analítico Latinoamericano" es intercambiar información con nuestros lectores sobre los cambios y retos sociales que Latinoamérica enfrenta por hoy, incluso los de seguridad pública y nacional. Para eso fin invitamos a nuestro estimados leyentes que se comuniquen con nosotros para expresar los temas que más les interesa al mismo de sus preocupaciones y retos profesionales.

Hay ciertas condiciones que son estructurales en todo el mundo, hasta en los países desarrollados. Pero son particularmente dañinos en América Latina por la gran disparidad social y la vulnerabilidad de los ciudadanos de las regiones. Poblaciones particularmente vulnerables como las mujeres, los niños, los discapacitados y los ancianos.



Estas condiciones son:

- Corrupción oficial.
- Impunidad de los social, políticamente y económicamente poderosos.
- Ineficiencia de agencias oficiales.
- Tolerancia social del crimen, inmoralidad, y violencia.

Paulatinamente la tecnología está cambiando este estatus quo. Aunque sistemas de cómputo automatizados son vulnerables a la manipulación indebida, estos sistemas registran todas las transacciones y pueden ser auditados si es que hubiese evidencia de hacking o manipulación inapropiada. La capacidad de un solo individuo para cometer un delito es cada vez más limitada.

#### ¿Qué podemos anticipar para el futuro cercano?

Así como la tecnología ofrece una solución, lleva en si un reto. Las amenazas futuras son lo que llamamos el Quinteto de la Victoria.

#### 1. Volumen.

A medida que las empresas se dependen más y más en la información el volumen de la información va a crecer exponencialmente. El reto futuro no es solo es el volumen, ni la infraestructura o la tecnología, si no la falta de profesionales de tecnología con habilidades que pueden organizar, analizar y utilizar esos datos. Estos profesionales, son cada vez más difíciles de encontrar. Inevitablemente tendremos que gastar más en entrenamiento, educación y capacitación tecnológica.

#### 2. Velocidad.

La velocidad con la cual el mundo moderno se comunica, es un factor en la inestabilidad presente. Un terremoto en Japón, un ataque terrorista en París, detalles trágicos del último ataque terrorista, son comunicados instantáneamente alrededor del mundo.

#### 3. Veracidad

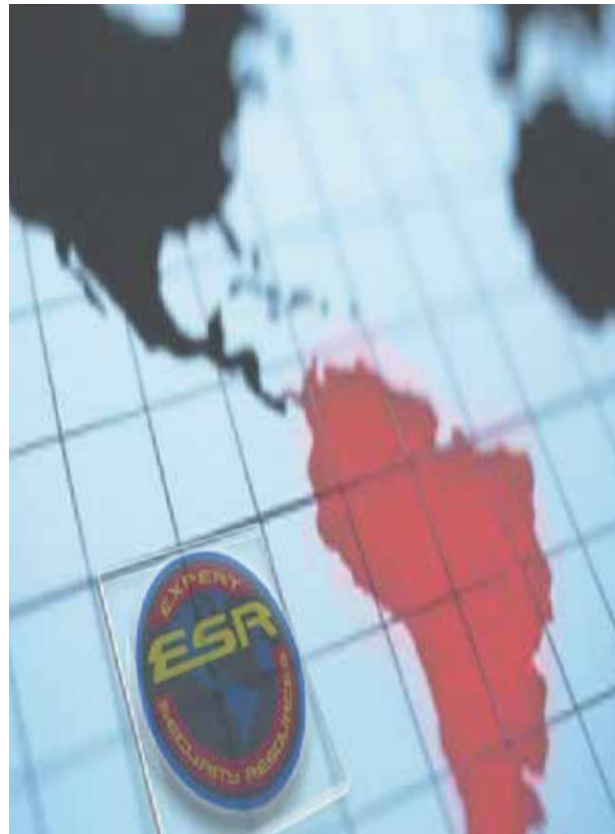
Activistas enmascarados como candidatos políticos, delincuentes cibernéticos disfrazados de ejecutivos, hombres/mujeres pretendiendo ser otras personas.

#### 4. Validación (Por cliente / usuario final)

La validación de la inteligencia/información solamente proviene del usuario final, sea este/esta oficial de gobierno o ejecutivo corporativo. La valides es establecida por el resultado de la decisiones tomadas a base de la información y análisis ofrecido.

#### 5. Amenaza interna / sabotaje

En cualquier actividad humana nadie conoce nuestras debilidades e vulnerabilidades también como nuestros compañeros íntimos o familiares. No es accidental que los seres humanos en todo el planeta reservan su más fuerte odio y resentimiento para los que han traicionado esa confianza.



Como se ha establecido ampliamente alrededor del mundo, las más grande vulnerabilidad del mundo moderno es la del sabotaje de sistemas complejos o el individuo motivado internamente – por razones desconocidas dispuesto a dañar a sus compañeros/compañeras o la institución para la cual laboran.



Autor: ESR GLOBAL CORP, Expert Security Resources  
Representante para Colombia - Emmanuel Sanchez

Para contactar al autor del artículo y obtener mas información, puede realizarlo en el correo electronico:  
[coladca@gmail.com](mailto:coladca@gmail.com)

## RoT: el Ransomware de las Cosas

De todas las tendencias de 2016, lo que más me preocupa es la disposición de algunas personas a participar de las siguientes tres actividades a escala: secuestrar sistemas informáticos y archivos de datos (mediante ataques de ransomware); denegar el acceso a datos y sistemas (con ataques de Denegación de Servicio Distribuido o DDoS); e infectar dispositivos que forman parte de la Internet de las Cosas (IoT, del inglés).

Lamentablemente, creo que estas tendencias continuarán en 2017 y es posible que incluso se vayan combinando a medida que evolucionen. Algunos ejemplos podrían ser utilizar los dispositivos IoT infectados para extorsionar sitios web comerciales con la amenaza de lanzar un ataque de DDoS, o bloquear los dispositivos IoT para pedir el pago de un rescate, a lo que yo llamo "jackware".

### Amenazas pasadas y futuras

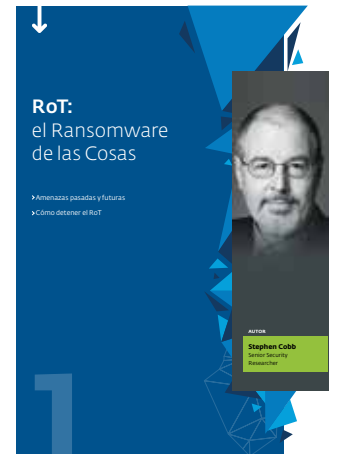
El uso indebido de los sistemas informáticos para extorsionar a los usuarios y sacarles dinero es casi tan antiguo como la computación misma. En 1985, un empleado de TI de una empresa de seguros de los Estados Unidos programó una bomba lógica para borrar registros vitales si alguna vez lo despedían. Dos años más tarde efectivamente lo despidieron y borró los registros, lo que condujo a la primera condena por este tipo de delitos informáticos. En 1989, se observó un tipo de malware que usaba el cifrado para secuestrar archivos y pedir rescate, como [cuenta David Harley](#). Para el año 2011, la actividad de bloquear las computadoras para pedir rescate ya había comenzado a tomar nuevas formas cada vez más despreciables, tal como explica mi colega [Cameron Camp](#).

Entonces, ¿de qué forma estos elementos evolucionarán o se fusionarán en el transcurso de 2017? Algunas personas se

han estado refiriendo al año 2016 como "El año del Ransomware", pero me preocupa que dentro de poco los titulares pasen a ser: "El año del Jackware". **El jackware es el software malicioso que intenta tomar el control de un dispositivo, cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital.**

Un buen ejemplo son los "automóviles conectados", como vienen muchos de los modelos más recientes en la actualidad. Estos vehículos realizan una gran cantidad de procesamiento de datos y de comunicaciones; sin embargo, esa no es su función principal: su objetivo primordial es llevarte desde el punto A hasta el punto B. Entonces, **piensa en el jackware como una forma especializada de ransomware.** Con el ransomware tradicional, como Locky y Cryptolocker, el código malicioso cifra los documentos del equipo y exige el pago de un rescate para desbloquearlos. En cambio, **el objetivo del jackware es mantener bloqueado un automóvil u otro dispositivo hasta que pagues el rescate.**

El escenario de una víctima de jackware puede ser el siguiente: en una helada mañana de invierno abro la aplicación de mi automóvil instalada en el teléfono para arrancarlo y calentar el motor desde la comodidad de mi cocina, pero el coche no enciende. En cambio, aparece un mensaje en mi teléfono diciéndome que tengo que entregar X cantidad de moneda digital para



Autor: ESET LATINOAMÉRICA



Algunos se refieren a 2016 como "El año del Ransomware". Me preocupa que dentro de poco los titulares sean "El año del Jackware".



Para contactar al autor del artículo y obtener el informe completo puede solicitarlo en el correo electrónico: [coladca@gmail.com](mailto:coladca@gmail.com) o puede descargarlo en el Link:

<https://www.welivesecurity.com/wp-content/uploads/2016/12/>

[Tendencias-2017-eset.pdf](#)

RoT: el Ransomware de las Cosas 7

# La educación en seguridad, una responsabilidad a nivel social

Hay una amenaza que lleva muchos años entre nosotros y que durante 2016 cumplió 25 años de haberse masificado a través de correos electrónicos.

Millones de usuarios en la red se habrán encontrado con ella pero a pesar de que muchos la puedan identificar, la realidad es que todavía hay personas que pueden verse envueltas por su engaño, unas por inocentes y desconocedoras, otras porque por simple curiosidad contestan para ver qué va a pasar y al final quedan atrapadas.

Si aún no saben de qué hablo, vamos a develar el misterio: **se trata de la famosa "Estafa Nigeriana" o "Estafa 419"**. El origen de [este tipo de engaño se remonta al siglo XIX y probablemente desde antes](#), con cartas ofreciendo repartir un jugoso tesoro. Pero esta estafa centenaria, lejos de desaparecer, **tomó fuerza con la evolución de la tecnología** y con el tiempo aparecieron múltiples variantes que migraron al correo electrónico.

Después de tanto tiempo, aún se siguen viendo mensajes en redes sociales y páginas web con el mismo tipo de engaños: que eres el visitante número 1.000.000, que te ganaste una lotería, que fuiste elegido para un viaje soñado son solo algunas de las excusas. Pero si las amenazas informáticas han venido evolucionando en los últimos años y ya hasta hablamos de ataques dirigidos, ciberguerra y APT, **¿cuál es la razón de que se siga viendo este tipo de engaños?**

## Cambian las amenazas, pero la propagación se mantiene

Hace apenas cinco años, en nuestro informe de [Tendencias 2012](#), hablamos de la

**Para contactar al autor del artículo y obtener el informe completo puede solicitarlo en el correo electrónico: [coladca@gmail.com](mailto:coladca@gmail.com) o puede descargarlo en el Link:**

**<https://www.welivesecurity.com/wp-content/uploads/2016/12/>**

**[Tendencias-2017-eset.pdf](#)**

La educación en seguridad, una responsabilidad a nivel social

Comunidad COLADCA - Revista InSecurity - [www.coladca.tk](http://www.coladca.tk)

**La educación en seguridad, una responsabilidad a nivel social**

- » Cambian las amenazas, pero la propagación se mantiene
- » Características: una actividad desatendida y eficiente
- » La educación no es solo cuestión de edad
- » La paradoja actual: más información, menos conciencia de seguridad
- » Pequeños cambios hacen grandes diferencias
- » La educación hace la diferencia

**AUTOR**  
Camilo Gutiérrez  
Instituto de Análisis de Seguridad

**Mobile: el malware y su realidad... ¿aumentada?**

- » Traspasando los límites de la percepción
- » Apps maliciosas con API no tan seguras
- » Virtualidad... ¿un sistema integrado?
- » Apps maliciosas en dispositivos oficiales
- » Facilidad de actualización
- » Plataformas móviles bajo ataque

**AUTOR**  
Denise Gustavo Bilic  
Security Researcher

Autor: ESET LATINOAMÉRICA



**¿Por qué un ladrón se tomaría el esfuerzo de cavar un túnel para entrar a una casa si solo tiene que llamar a la puerta?**





Operador  
Económico  
Autorizado  
COLOMBIA

## Seguridad en la Cadena de Suministro Autorización como Operador Económico Autorizado OEA en Colombia.

 Por. Manuel Camelo

El pasado 28 de Enero de 2017, la Comunidad COLADCA organizó el 1er Encuentro de la Seguridad en la cadena de suministro y Operador económico autorizado OEA, iniciativa propia y requerida por el sentir de todos los profesionales y empresas vinculadas a la labor de Gestión de Riesgos y Seguridad en Colombia.

Fue un escenario muy dinámico e importante con la asistencia de más de 100 invitados de diferentes empresas y con el apoyo especial de Aliados Colombia Internacional y los representantes del Consejo de Seguridad de la cadena de suministros de México, los asistentes conocieron el tema principal dirigido al Operador Económico Autorizado (OEA), el cual es la autorización que otorga la autoridad aduanera (DIAN) de Colombia, atendiendo los lineamientos propuestos por la Organización Mundial de Aduanas, a empresas exportadoras e importadoras y diferentes eslabones de la cadena de suministro que cuenten con la calidad de usuarios aduaneros, que demuestren estar comprometidas con la seguridad, mediante el cumplimiento de requisitos mínimos y de condiciones de seguridad e historial satisfactorio de obligaciones aduaneras y fiscales.

OEA garantiza operaciones de comercio exterior seguras y confiables; por lo tanto, la Empresa solicitante es autorizada como tal por la DIAN, con base en condiciones establecidas en el Artículo 6° Decreto 3568 de 2011 y resoluciones 015 (Sector exportador) y Resolución 067 (Sector importador).



Desde la Comunidad COLADCA, reconocemos la necesidad de generar las competencias básicas para realizar auditorías internas en la seguridad de las cadenas de suministros, especialmente bajo los estándares del OPERADOR ECONOMICO AUTORIZADO OEA, el pasado mes de Abril se dio inicio al primer curso de técnicos de auditoría para profesionales interesados y seguiremos desde COLADCA abriendo espacios, asesorías y consultorías sobre el tema; Es importante mencionar que debemos cumplir algunos requisitos bajo estándares mínimos de:

**-Análisis y administración del riesgo, -Asociados de negocios, -Controles de acceso físico, -Seguridad de personal, -Seguridad de procesos, -Seguridad física, -Seguridad en tecnologías de la información, -Entrenamiento de seguridad a todos los involucrados en la cadena de suministro.**

¿Cuál es el alcance de los programas de OEA en el mundo?

**“Garantizar unos niveles mínimos de seguridad y facilitar el flujo del comercio internacional, forjando alianzas sólidas entre el sector público y privado que permitan garantizar la seguridad de toda la cadena de suministro y construir relaciones de confianza, teniendo como último estadio el reconocimiento mutuo, resultado de las alianzas entre las aduanas.**

En caso de requerir más información, dejemos saberlo y le ayudaremos, contamos con un equipo de trabajo a su servicio.



**Autor: Manuel Camelo**

Administrador de empresas, Capitán (RA) Policía Nacional de Colombia, Auditor Internacional BASC, Formador de Formadores BASC, Auditor Líder en ISO 28000-Seguridad de la Cadena de Suministro, Gerente de riesgos certificado por PECB bajo la norma ISO31000, Auditor y Especialista OEA - Líder Consultor OEA en la Comunidad COLADCA, Docente universitario  
Para contactar al autor del artículo, puede realizarlo en el correo electrónico: [manuelcamelot62@gmail.com](mailto:manuelcamelot62@gmail.com)

# MAESTRÍA EN DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL

ESCUELA DE POSTGRADOS FUERZA AÉREA COLOMBIANA  
SNIES 105360



## Contáctenos

Carrera 11 No. 102-50 Edificio Escuela Superior de Guerra - Bogotá Colombia.  
Horario de atención: De Lunes a Viernes de 7:30 am a 4:30 pm  
Departamento de Educación Superior - Programa MADGSI - Of. 410  
Teléfono 6206518 EXT 1960/1719  
Email: admisiones.madgsi@epfac.edu.co

[www.epfac.edu.co](http://www.epfac.edu.co)



Somos:



“Dejando Huella”

**I Revista**  
**INSECURITY**  
OBSERVATORIO DE SEGURIDAD

Vinculate!



[www.coladca.tk](http://www.coladca.tk)

#### - Claustro de Maestros.

Los maestros que impartirán cada materia, son profesionales en el área de su competencia y cuentan con la experiencia teórica y práctica, que los acredita como expertos en el área de la seguridad.



- Inicio del Programa: 1º de Julio de 2017

- Tiempo de Duración: 12 meses.

- Curso Online: 300 horas (25 horas por módulo, por mes).

- Costos, Inscripciones y Contacto:

El costo del diplomado será de \$24,000 pesos mva + IVA (12 pagos mensuales de \$2,000 pesos mexicanos).

• La Institución que registre a 5 o más alumnos, obtendrá el 10% de descuento.

Lic. Ricardo Miguel Salas Martínez.

Av. La Paz #2757-2, Col. Arcos Sur.

C.P. 44500, Guadalajara, Jal, México

#### Teléfonos:

+53 (81) 2109 - 59 32

+52 (33) 3630 - 43 20

+52 (33) 3831 - 58 65

+52 (33) 1943 - 32 51

+52 (33) 1116 - 88 40

#### Correo Electrónico:

ricardosalas60@gmail.com

rsalas@gpojim.com

ajimenez@gpojim.com

sjimenez@gpojim.com

profesionalizacion@gpojim.com

## DIPLOMADO EN DESARROLLO DE HABILIDADES Y COMPETENCIAS PARA LA SEGURIDAD DE LAS INSTITUCIONES PRIORITARIAS.

CURSO ONLINE



Dirigido a:

- Comisarios y Directores de Seguridad Pública de los Gobiernos Municipales, Estatales y Federales de los países de América Latina.
- Directivos de Empresas de Seguridad Privada de América Latina.
- Consejeros y Asesores en Materia de Seguridad.
- Egresados de las Carreras Profesionales de la Seguridad.
- Personal Directivo de Seguridad de las Instituciones Prioritarias.
- Consejeros Ciudadanos de Seguridad.
- Directivos de Organismos de la Sociedad Civil en Materia de Seguridad.

DIPLOMA EXPEDIDO POR LA UNIVERSIDAD DEL VALLE DE ATEMAJAC (UNIVA)

#### OBJETIVO.

El Alumno de este curso desarrollará las habilidades, destreza y competencias para dirigir equipos de seguridad para instalaciones de alta prioridad. Conocerá de tecnologías de vanguardia y podrá desarrollar e implementar programas que prevengan riesgos y garanticen la seguridad de estas instituciones.

Los Alumnos del curso obtendrán habilidades, destrezas y conocimientos para:

- Entender la problemática de la seguridad de manera sistémica, integral y multinacional.
- Diseñar e implementar las metodologías de manera sistémica y que le permitan prever y anticipar las amenazas y riesgos en su entorno.
- Elaborar e implementar programas de seguridad en donde colaboren las corporaciones de seguridad e instituciones prioritarias.
- Desarrollar planes y programas de seguridad para estas instituciones y empresas de alta prioridad.
- Diseñar programas, métodos, procesos, modelos, sistemas y tecnologías para controlar y reducir los riesgos.
- Conocer de las tecnologías de vanguardia en la seguridad y poder implementarla.
- Desarrollar y aplicar sistemas de Inteligencia y contra-inteligencia, de obtención de información y su procesamiento, clasificación y análisis para la seguridad.

Más información para vinculados a la Comunidad COLADCA obtenga % de Descuento y Precio especial en el email: [coladca@gmail.com](mailto:coladca@gmail.com)

#### CONTENIDO TEMÁTICO (Módulos).

- 1.- Seguridad Cibernética y Seguridad de la Información.
- 2.- Seguridad Exterior y Controles de Acceso.
- 3.- Sistemas de la Información para la Seguridad.
- 4.- Programas de Comunicación, Contacto e Imagen Pública y Colaboración de la Comunidad.
- 5.- Sistemas de Control en Instalaciones de Alta Seguridad.
- 6.- Protocolos de Actuación y Sistemas de Operación.
- 7.- Sistemas de Identificación Biométrica, Minerías de Datos, Video Vigilancia y Diseño de Sistemas, UAV y USV para la Seguridad, Utilización de Sistemas de Posicionamiento Global y Seguridad en el Transporte.
- 8.- Crimen Organizado y Delincuencia Transnacional.
- 9.- Programas de Formación de Personal para Instalaciones Prioritarias.
- 10.- Alta Seguridad en Instalaciones Prioritarias I. (Centros Penitenciarios, Instalaciones Petroleras, Nucleares y de Energía).
- 11.- Alta Seguridad en Instalaciones Prioritarias II. (Puertos Marítimos, Aeropuertos, Centrales de Transporte).
- 12.- Alta Seguridad en Instalaciones Prioritarias III. (En Eventos Masivos Deportivos, Cívicos, Manifestaciones, Desastres y Emergencias Naturales).

#### TEMAS COMPLEMENTARIOS DE VALOR HUMANO.

- 13.- Sentido Trascendente del Desarrollo Humano en el Trabajo y la Seguridad.
- 14.- Nuevo Modelo de Justicia Penal, Acusatorio Adversarial.
- 15.- Prevención y Tratamiento de Uso de Drogas en el Trabajo y en el Hogar.
- 16.- Prevención de Suelos y su Negociación.



Somos:



Revista  
**INSECURITY**  
OBSERVATORIO DE SEGURIDAD

Vinculate!



[www.coladca.tk](http://www.coladca.tk)

"Dejando Huella"