MACRO Seguridad

MASEC

La Seguridad es el centro del desarrollo en un mundo global

Decima Primera Edición | Junio 2019
ISSN 2520-9132

La Video Vigilancia en la Seguridad Ciudadana en República Dominicana

La presencia Rusa en América Latina:

"El sistema Operativo Aurora OS (Avrora OS) que podría utilizar Huawei, desarrollado por la empresa rusa Jolla Ltd"

EQUIPO EDITORIAL

Director General
Melvin Pérez

Administración y Comercialización
Gregoria Wooter

Asesores de Contenido
Richard Pérez
Félix Quintín Ferreras Méndez

Corrección de Estilo
Oscar Quezada
Flavio Ernesto Peña

Fotografía
Macroseguridad
Depositphotos

Diagramación y Diseño
Ramón Abreu

Impresión
RA Design

COLABORADORES EN ESTE NÚMERO

Alfonso De Los Santos
Máximo Patiño
Joel Delgado
ISACA Capítulo Santo Domingo

info@macroseguridadrd.com
MacroSeguridad
www.revistamacroseguridad.com
809-373-1729

NOTA RELATIVA A LOS ARTÍCULOS:

Los artículos son responsabilidad de sus autores, por lo que no expresan necesariamente la opinión de nuestra revista. En tal sentido, la Revista Macro Seguridad MASEG, no se hace responsable de las opiniones expresadas por los colaboradores en sus artículos. Se prohíbe la reproducción total o parcial de esta publicación sin la autorización de la Dirección.

Mensaje del Director

La seguridad ciudadana ha sido una de las principales preocupaciones de la población por más de una década. En el mes de mayo del 2019, la encuesta Gallup-Hoy reflejó que "para el 68% de los ciudadanos los robos y los asaltos son los principales problemas del país".

Si se analizan otros datos de esa misma encuesta, los mismos guardan relación con el problema "delincuencia", como son: el desempleo, que obtuvo un 34.7% y al alto costo de la vida con un 32.3%. Sin embargo, aunque no reflejó un porcentaje relevante, el narcotráfico es otro factor generador de actos delictivos y violencia, así como la corrupción en el aparato judicial y del orden público que ha imperado de manera incremental.

Precisamente ese último aspecto es un motivador o promotor de la delincuencia. Existe una idea generalizada de que con "dinero en mano nadie es condenado, apresado o procesado", y que solo el delincuente de los más bajos estratos sociales, es decir, aquel que no tiene recursos económicos, es el que tiende a ser condenado. Pero ¿cómo se puede enfrentar esta situación? La repuesta a esta pregunta se puede resumir en una breve oración que generaría un gran plan y un conjunto de medidas a corto, mediano y largo plazo, y esta es "erradicando la cultura de la impunidad y promoviendo la transparencia e integridad".

La encuesta citada más arriba y otras en la misma línea, llenan el vacío que tiene la población de no tener acceso a las estadísticas reales de los índices de violencia y delincuencia. Especialmente el indicador de delincuencia ayuda a tomar las decisiones correctas, pues tener la información sobre las zonas que generan mayor cantidad de denuncias de actos delictivos y/o los tipos de delitos más denunciados, es una herramienta que facilita la manera de abordar el problema.

Si bien se han implementado planes de seguridad ciudadana, unos más efectivos que otros, desde mi punto de vista el más exitoso, el "Plan de Seguridad Democrática", nos queda un largo camino por recorrer, ya que la falta de solidez institucional hace que planes exitosos se degraden en el tiempo, generando posteriormente un mayor esfuerzo para recuperar el orden.

Melvin Pérez
Director

Contenido

EN PORTADA

La Video Vigilancia en la Seguridad Ciudadana en República Dominicana 10

¿Es aconsejable integrar a la Policía Municipal a la Seguridad Ciudadana? 4

Certificaciones para profesionales de Auditoría, Seguridad, Gobierno y Control de Riesgos de TI. 6

Una nueva certificación ante las nuevas amenazas cibernéticas 16

"El sistema Operativo Aurora OS (Avrora OS) que podría utilizar Huawei, desarrollado por la empresa rusa Jolla Ltd" 18

Para publicitarse contáctenos:
Tel. 809-373-1729
Email: info@macroseguridadrd.com
www.revistamacroseguridad.com

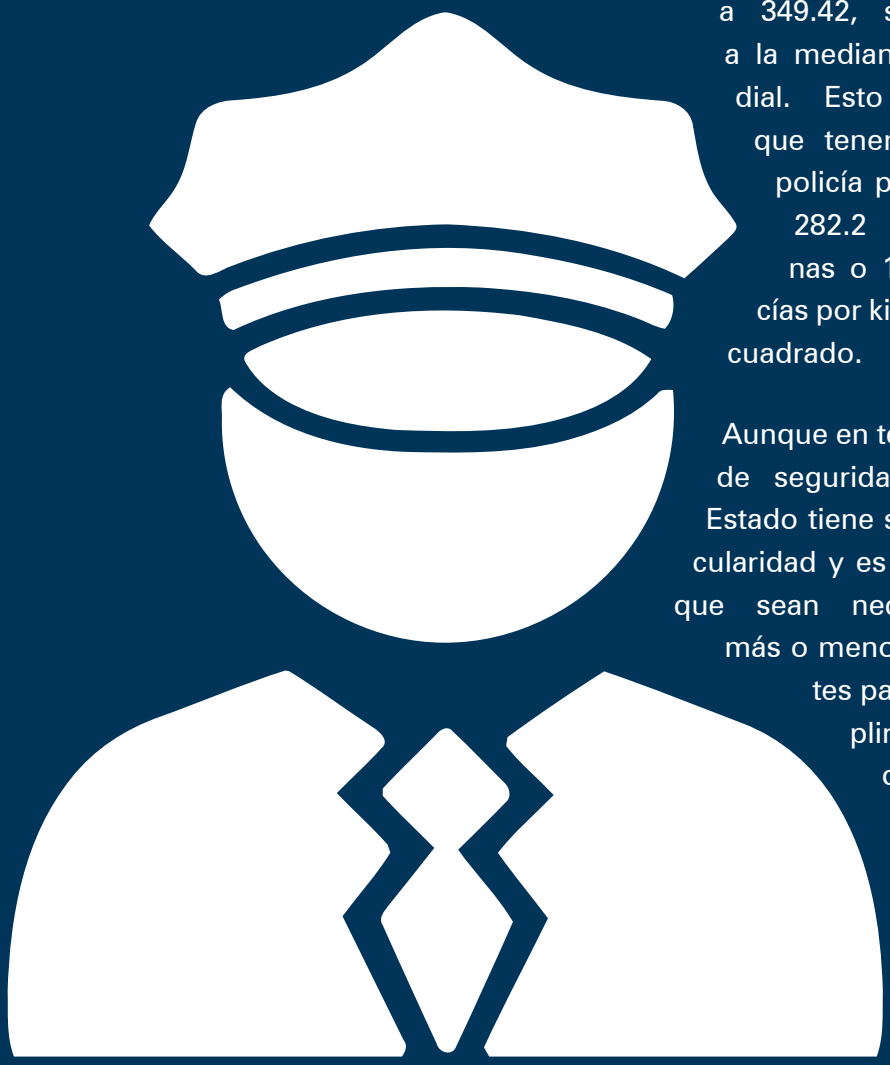
¿Es aconsejable integrar a la Policía Municipal a la Seguridad Ciudadana?

El escenario ideal es tener una estructura operativa de seguridad ciudadana que integre a las autoridades de los municipios, que garantice el cumplimiento de las leyes y las resoluciones o normativas emitidas por cada ciudad en sus diferentes aspectos (seguridad, medio ambiente y salubridad, etc.), así como para apoyar a la Policía Nacional.

Sin embargo, en las condiciones actuales integrar a la policía municipal en un rol de seguridad ciudadana, es una decisión peligrosa, que debe pensarse bien. Hay que entender que el problema de la seguridad en nuestro país no es de cantidad de oficiales de policía, sino de calidad: competencias, equipos y organización.

Actualmente contamos con unos 36,822 policías (PN, 2019), y alrededor de unos 50 mil militares. Esto quiere decir que tenemos a disposición un aproximado de 86 mil hombres con capacidad de trabajar en labores de seguridad ciudadana, sin agregarle más de 33 mil vigilantes privados y personas informales que realizan función de seguridad en entidades públicas y privadas.

Explicamos. Si tomamos la proyección estimada de habitantes para finales del 2019 de 10,538,320 (ONE, 2019) y realizamos un ejercicio matemático respecto a la cantidad necesaria de policías y comparamos con la mediana mundial tendríamos lo siguiente:



- Mediana mundial de acuerdo con las Naciones Unidas (NU, 2006) es de 300 agentes por cada 100 mil habitantes.

- Agentes policiales por cada 100 mil habitantes necesarios en República Dominicana es de 31,614.96. Esto quiere decir que tenemos unos 5,207 policías por encima de la mediana mundial.

- Agentes policiales por cada 100 mil habitantes en República Dominicana es igual a 349.42, superior a la mediana mundial. Esto indica que tenemos un policía por cada 282.2 personas o 1.3 policías por kilómetro cuadrado.

Aunque en términos de seguridad cada Estado tiene su particularidad y es posible que sean necesarios más o menos agentes para cumplir el rol de protección (esto tendría que estudiarse más a fondo), las estadísticas mundiales sirven de base referencial importante.

Parte del problema.

Los municipios de nuestro país ni siquiera reciben los fondos necesarios para sostenerse, mucho menos para destinar recursos para reclutar y formar policías con las competencias profesionales necesarias, ni para adquirir equipos y herramientas que les puedan apoyar en el combate a la delincuencia. Otro problema es lograr que no se reproduzca el escenario actual, donde los policías son asignados a tareas que no son propias de su profesión ¿Cómo se controlaría eso en los municipios? Eso sería todo un reto, partiendo de la histórica mala práctica.

El paso aconsejable.

Más que integrar a la Policía Municipal en este rol y crear un nuevo problema, ya que sus acciones demuestran que no cuenta con las competencias necesarias, lo más viable desde mi punto de vista es reformar la Policía Nacional y después trabajar con la municipal, llevándola al estándar deseado.

Es por eso por lo que mi respuesta a la pregunta inicial de si ¿Es aconsejable integrar a la Policía Municipal a la seguridad ciudadana? es: “no en las condiciones actuales”.

Fuente:
http://www.policianacional.gob.do/
https://www.one.gob.do/

Melvin Pérez
Magíster en Defensa y Seguridad Nacional
Certificado SSP, Asesor y Consultor de Seguridad

Certificaciones para profesionales de Auditoría, Seguridad, Gobierno y Control de Riesgos de TI.

ISACA es una organización internacional de Auditoría y controles en los sistemas de información computarizados.

Beneficios:

- Le da una ventaja competitiva
- Le ayuda a lograr un alto nivel profesional
- Confirma y demuestra su conocimiento y experiencia
- Cuantifica y comercializa su experiencia
- Proporciona el reconocimiento mundial como una marca de excelencia
- Aumenta su propio valor para su organización
- Certificaciones mejores pagadas

A continuación, se presenta el resultado obtenido mediante **encuesta anual de habilidades y sueldos en dolares de Global Knowledge :**

RAKING	CERTIFICACION	SUELDO
1	AWS Certified Solutions Architect – Associate	$50.143
2	CRISC: Certified in Risk and Information Systems Control (ISACA)	$48.694
3	CISM: Certified Information Security Manager (ISACA)	$46.051
4	Project+ (CompTIA) -	$45.433
5	CISSP: Certified Information Systems Security Professional (ISC) 2	$44.504
6	CISA: Certified Information Systems Auditor (ISACA)	$44.088
7	AWS Certified Developer – Associate	$42.917
8	PMP®: Project Management Professional	$42.353
9	COBIT 5 Foundation (ISACA)	$40.713
10	CGEIT: Certified in the Governance of Enterprise IT (ISACA)	$40.430

En este orden, con el objetivo de brindarte suficiente información para que tomes la decisión de acuerdo a tus metas profesionales, a continuación, se proporciona una leve descripción de cada una de las cuatro (4) certificaciones core de ISACA. Cabe destacar estas certificaciones están acreditada por ANSI, bajo ISO/IEC 17024: 2012.

CRISC: Certified in Risk and Information Systems Control

Esta certificación es la más joven y con mayor número de personas acreditadas. Está diseñada para profesionales cuyo trabajo comprende la identificación y gestión de riesgos de TI y de negocio, por medio de controles en los sistemas informáticos, cubriendo todo el ciclo de vida

Certificación Profesional en SEGURIDAD INTEGRAL CORPORATIVA

CERTIFIED CISEM CORPORATE INTEGRAL SECURITY MANAGER

CISEM®

La certificación "Gerente de Seguridad Integral Corporativa Certificado", de sus siglas en inglés (CISEM), consta de cinco dominios.

DOMINIO I – LA SEGURIDAD Y LAS INVESTIGACIONES
DOMINIO II – SEGURIDAD INDUSTRIAL, SALUD Y MEDIO AMBIENTE
DOMINIO III – GESTION DE LA SEGURIDAD DE LA INFORMACION
DOMINIO IV – GESTION DE RIESGOS, CRISIS Y EMERGENCIAS
DOMINIO V – GERENCIA DE SEGURIDAD

AVALADO POR:

CEXDE
CENTER FOR EXECUTIVE DEVELOPMENT

UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

MACROSeguridad
La Seguridad es el centro del desarrollo en un mundo global.

809-373-1729 y 809-350-6555
info@macroseguridadrd.com
https://www.revistamacroseguridad.com/contacto

de la gestión de riesgos y controles, desde el diseño, implementación y mantenimiento.

CISM - Certified Information Security Manager

La certificación está centrada exclusivamente en la gestión del sistema de seguridad de la información, promueve prácticas de seguridad internacional y reconoce a la persona que administra, diseña, supervisa y evalúa la seguridad de la información de una empresa.

Requiere al menos 5 años de experiencia en sistemas de información, 3 de los cuales deben ser en gerencia de seguridad.

CISA Certified Information Systems Auditor

Es la certificación más antigua de ISACA (desde 1978) y con mayor número de profesionales certificados. Está dirigida a profesionales del área de auditoría, monitoreo, contraloría, evaluación de sistemas y TI.

Diseñada para demostrar habilidades del candidato en gestión de vulnerabilidades, asegurar cumplimiento de estándares, proponer controles, procesos y actualizaciones a las políticas organizacionales. Requerido mínimo de 5 años de experiencia profesional en auditoría, control o seguridad de sistemas de información.

CGEIT: Certified in the Governance of Enterprise IT

La certificación CGEIT está diseñada para profesionales con responsabilidades relacionadas con la gobernabilidad de TI, tanto de asesoría como de aseguramiento.

Cómo obtenerlas

Para obtener una de estas certificaciones el candidato deberá cumplir con los siguientes lineamientos:

1. Pasar el examen.
2. Presentar una solicitud (dentro de los cinco años siguientes a la fecha de aprobación del examen) con pruebas fehacientes de tener experiencia laboral acumulada realizando las tareas propias de los dominios que abarca cada certificación.
3. Adherirse al Código de Éticas Profesionales de ISACA.
4. Aceptar cumplir con la política de educación continua
5. Cumplir con los Estándares de Auditoría de SI (CISA)

El punto 4 se refiere a que los profesionales que obtengan esta certificación para mantener la certificación deberán acumular créditos de educación continua anualmente.

El Capítulo de ISACA de Santo Domingo, en cumplimiento a su misión y visión, tiene la responsabilidad de proporcionar los medios para que más profesionales obtengan estas certificaciones y se apliquen las buenas prácticas en las empresas. Es por esto que se imparten programas de preparación para obtener estas certificaciones, orientados a preparar al candidato para tener éxito en el examen.

El programa incluye Información sobre el examen y la certificación CISA, la cobertura detallada del conjunto de conocimientos requeridos, preguntas de discusión del examen, considerando las experiencias de los instructores, los cuales están acreditados para impartir dichos cursos.

Adicional a estas cuatros (4) certificaciones, el Capítulo imparte cursos de preparación para COBIT 2019 y CSX Fundamental, los cuales se realizan de acuerdo a la demanda que se tenga. Para los mismos, se solicitan entrenadores certificados de otros capítulos de la región LATAM.

Asimismo, desarrolla eventos, conferencias, reuniones de networking y webinars que les permiten a los miembros y no miembros certificados obtener los CPE´s, así como oportunidad de voluntariado. Para más información puedes seguirnos en nuestras redes sociales como ISACA Santo Domingo Chapter en Lindklind, Facebook, YouTube. Entrar a nuestro portal: https://engage.isaca.org/santodomingochapter/home.

"El programa incluye Información sobre el examen y la certificación CISA, la cobertura detallada del conjunto de conocimientos requerido, preguntas de discusión del examen, considerando las experiencias de los instructores, los cuales están acreditados para impartir dichos cursos."

ISACA Capítulo Santo Domingo.

Consultoría:
PROGRAMA DE SEGURIDAD Y SALUD EN EL TRABAJO.

MACROSeguridad

La Seguridad es el centro del desarrollo en un mundo global.

Nosotros le desarrollamos el programa de seguridad y le acompañamos para la certificación.

"Somos proveedores de servicios de seguridad y salud avalados por el Ministerio de Trabajo"

MINISTERIO DE TRABAJO
República Dominicana

CERTIFIED CISEM CORPORATE INTEGRAL SECURITY MANAGER

info@macroseguridadrd.com
www.macroseguridad.edu.do
www.revistamacroseguridad.com

809-373-1729
809-350-6555

La Video Vigilancia en la Seguridad Ciudadana en República Dominicana

Antes de iniciar un plan de instalación de cámaras de seguridad, el primer paso que se debe dar es sincerar los datos estadísticos sobre los niveles de criminalidad, para poder determinar las zonas de mayor incidencia criminal, de modo que el proyecto impacte efectivamente en la reducción de los niveles de delincuencia.

Otro factor importante para tomar en cuenta antes de adquirir equipos de video vigilancia es identificar el tipo de tecnología a utilizar, que deberá guardar relación con: el objeto de protección, el nivel de crimen y las condiciones físicas de la zona a proteger. En definitiva, es imprescindible realizar un análisis previo y un diseño tecnológico que se ajuste a la realidad de cada zona en particular.

Es necesario que quien haga el diseño y quien lo reciba o apruebe conozcan sobre el tema a profundidad, es decir, sea un experto, con capacidad de poder elegir las cámaras, servidores o equipos de comunicación que se ajustan de mejor manera a las realidades particulares de cada zona a proteger.

Se instalarán las cámaras, pero ¿qué haremos con ella?

Se debe contar con un protocolo de actuación y uno de administración. El protocolo de actuación debe contener la manera en que se dará respuesta a los hechos detectados con los niveles de escalamiento necesarios para la toma de decisiones. El de administración establecerá de qué manera se gestionan los recursos tecnológicos instalados (quienes deben tener acceso, quienes autorizan la extracción de videos para garantizar la privacidad de los ciudadanos, entre otros).

Otro elemento importante es cómo se protegen los videos desde el punto de vista físico: protección contra incendios, inundaciones, sabotajes, controles de acceso y plan de contingencia; y desde el punto de vista lógico: acceso a los sistemas, jerarquía de usuarios, corta fuegos (firewall), protección o encriptación de la comunicación; de modo que sea un sistema robusto que dificulte la intrusión de un Hacker. En tal sentido, deben intervenir no sólo expertos en instalación de sistemas de video vigilancia, sino también, expertos en redes de comunicaciones y seguridad informática.

Dependiendo del objetivo que se desee, la inversión en este tipo de tecnologías puede ser alta, pues existen sistemas de gestión de videos o videos inteligentes que permiten reconocimiento facial, reconocimiento de placas de vehículos o identificar cualquier acción como el robo de cualquier bien público al que las cámaras estén vigilando. La última tecnología que tiene disponible el mercado consiste en cámaras que se manejan con el protocolo de internet o IP, permitiendo que las cámaras sean autogestionable, con calidad de imágenes manejable en el ámbito de los Megapíxeles, cuyo costo puede rondar entre los 1300 dólares hasta los 5 mil dólares cada cámara, independiente de los equipos de comunicaciones, sistema de energía alternativa, servidores, entre otros.

Como complemento a todo el aspecto tecnológico y de procesos, es aconsejable evaluar al personal involucrado en el proyecto y de ser necesario, elevar su nivel de competencias técnicas para garantizar su adecuada implementación, desarrollo y mantenimiento en el tiempo.

Melvin Pérez
Magíster en Defensa y Seguridad Nacional
Certificado SSP, Asesor y Consultor de Seguridad

La presencia rusa en América Latina:

RUS

América Latina, fuente de deseos imperiales, una región con países que bordean la semi-periferia y periferia, se encuentra, con recursos vitales, en la mira de las potencias que confrontan los intereses de una zona geográfica históricamente advertida, anunciada y hasta reconocida por muchos como de interés y alta influencia de los Estados Unidos.

En un mundo anárquico, multipolar y sin árbitros con capacidad de imponer las reglas del juego, los Estados entrelazan alianzas en sus diferentes campos de acción, operando en razón de lograr el mayor rédito de sus intereses. De ese mismo mundo forma parte América Latina, una región insertada en el mercado global, convertida en un actor de vital importancia por sus características geopolíticas, económicas, de seguridad (en distintos aspectos) y el interés que genera en las grandes economías del mundo.

Una de las potencias interesadas a las que nos referimos es la Federación de Rusia, que con sus 17 millones de km2 es conocida como la nación más grande del mundo, ubicada en Eurasia y reconocida por ser, no solo heredera de los zares y también de la Unión de Repúblicas Socialistas Soviéticas (URSS) (cuyo desmembramiento ocurrió en 1991), sino por ser una potencia militar dominante, de incalculable valor geoestratégico, con muy pocos rivales en el mundo, y uno de los actores principales del escenario geopolítico mundial.

Actor extra-regional con gran peso:

Si hubo un hecho con el que los realistas no contaban tras el fin de la Guerra Fría, era con el efecto de la globalización y su colateral efecto de interdependencia global, provocando un relativo declive de la preponderancia militar y su alcance extra-regional, así como un rápido surgimiento de nuevos actores "No Estatales". Hecho este que aún persiste, a pesar de que el unipolarismo ya pasó y el fin de la historia, por parafrasear a Fukuyama, es una ilusión.

Es un actor consciente de la dinámica internacional y de la nueva realidad de su nación, que en palabras de Iván Giménez en su obra El nuevo Gran Juego en Asia Central: Geopolítica en el Mar Caspio (2009:123): "Rusia está recuperando su papel como gran potencia des-

pués de la debilidad demostrada con el desmembramiento de la URSS" y lo hace emulando acciones audaces, y atreviéndose a llegar más lejos en procura de sus intereses y de lograr nuevos aliados estratégicos. Por eso observamos que, en pleno siglo XXI, Rusia se mueve en la región con pasos silentes, pero firmes e incuestionables.

En una entrevista realizada para la Revista Mexicana de Política Exterior, por Edgar Rebollar Sáenz, el viceministro de Asuntos Exteriores de la Federación de Rusia, Sergéi Ryabkov, expuso no solo la realidad actual de la presencia rusa en la región, sino las perspectivas a corto, mediano y largo plazo. Planteó que su misión en el mundo es garantizar la seguridad, soberanía e integridad de su nación, a tiempo que se fortalezca el Estado de Derecho y las instituciones democráticas, claro está, observándose a sí mismos como un centro de poder.

Habló de la importancia de reconocer que el sistema internacional actual es policéntrico y que la mejor manera de enfrentar los nuevos retos es a través del multilateralismo, de ahí se deriva entonces la importancia de regiones como la nuestra, justificando con ello la presencia política y el intercambio económico con la región, logrado a través de un ambiente de respeto a los principios del Derecho Internacional.

Lo anterior quizás justifica la actual presencia de la Federación de Rusia en la región, en sus 3 consulados y 18 embajadas, muchas de ellas concurrentes, lo que ayuda a abarcar prácticamente la totalidad de la zona que le corresponde con la presencia de 20 embajadas de países latinoamericanos.

¿Qué busca Rusia en América Latina?

Podríamos colegir que la presencia rusa en la región tiene por objetivo contrarrestar el peso geopolítico de los Estados Unidos en el mundo, forzando un balance que, debido a las grandes diferencias y realidad política, no puede cubrir.

En ese sentido, a pesar de que reconocen el valor geopolítico de algunos Estados y el potencial económico con otros, buscan establecer una relación que según Sergéi Ryabkov:

"Se apoya en principios comunes, valores objetivamente compartidos y la filosofía política basada en la protección y el

Una de las potencias interesadas a las que nos referimos es la Federación de Rusia, que con sus 17 millones de km2 es conocida como la nación más grande del mundo, ubicada en Eurasia y reconocida por ser, no solo heredera de los zares y también de la Unión de Repúblicas Socialistas Soviéticas (URSS) (cuyo desmembramiento ocurrió en 1991)

fortalecimiento de la soberanía nacional, el compromiso con el derecho internacional, incluidos los principios de no injerencia en los asuntos internos y la devoción a la diplomacia multilateral, así como el mantenimiento del equilibrio de intereses en los asuntos internacionales y el fortalecimiento de la seguridad y la estabilidad internacionales".

A lo anterior, el viceministro Ryabkov agrega el interés ruso de que "la región sea fuerte, políticamente unida y económicamente estable. Nos proponemos no considerar el mundo latinoamericano a través del paradigma de "amigo o enemigo" y "aliado u opositor".

América Latina en el escenario estratégico del Kremlin:

Hoy, América Latina es el escenario perfecto para realizar una diplomacia de baja intensidad, si es que una nación como Rusia puede pasar desapercibida. La región latinoamericana despierta de un letargo político y económico al que fue sometido por potencias regionales, ha permitido la cosecha del impulso dado por la política exterior rusa, hacia el último lustro del pasado siglo, de la mano del ex canciller ruso Eugenio Primakov, quien avizoró establecer un cambio de percepción de América Latina hacia Rusia.

Dos décadas después, conocemos de la relación comercial y política de Rusia en naciones como Venezuela, Nicaragua, Bolivia y Cuba, pero el interés ruso abarca más que sus aliados tradicionales e ideológicos. Su participación es escasa pero sustancial, su involucramiento es mínimo pero notorio. Se abstiene de aparentar una participación intrusiva, pero no reniega de su presencia.

Al día de hoy, las relaciones ruso-latinoamericanas se orientan hacia los puntos en común, no a las diferencias, pues, según Davydov, "Actualmente, a Rusia y Latinoamérica las une el rechazo al proteccionismo vulgar, la provocación de guerras comerciales y la práctica de sanciones basadas en percepciones unilaterales y actitudes agresivas que destruyen el ámbito de competencia civilizada."

Voz e imagen rusa en la región:

Podríamos decir que tanto la distancia como el idioma son obstáculos para el fortalecimiento de las relaciones oficiales; imaginémonos entonces lo que sería para los ciudadanos. Pues, recordando la línea Primakov, los rusos han identificado tanto el personal idóneo como el esencial para llevar a cabo estos acercamientos oficiales, para todo lo demás, está Russia Today , medio por el cual, no solo promueven la imagen de Rusia, sino que también se muestran al mundo desde sus perspectivas e intereses. A esto le añadimos que rápidamente se han convertido, no sin detractores , en un medio de referencia en la población latinoamericana, "diciendo su verdad, a su manera".

En definitiva, Rusia hace y hará lo que tenga que hacer, cuando lo tenga que hacer. Aplicará la Real Politik, su influencia política y económica, aún si esto conlleva la participación como observador en organismos regionales o papeles más activos como el de la crisis de Venezuela, o de más baja intensidad como en Cuba, Bolivia y Nicaragua sin ignorar a grandes naciones como México, Brasil, Chile o Argentina, por citar algunos casos, pues para la otrora nación zarista representan alianzas estratégicas de alto valor y que pueden ser aprovechadas a largo plazo.

Ib ídem. Pág. 10.

Canal oficial de la Federación rusa.

Erglanger, Steven. New York Times: artículo "¿Periodismo o propaganda? En el caso de RT, la distinción no es clara. 12 de marzo de 2017. Visto en:

Joel Delgado, Internacionalista
Magíster en Seguridad y Defensa Nacional
Catedrático de varias Universidades

Una nueva certificación ante las nuevas amenazas cibernéticas

Los Ciberataques se están convirtiendo en parte del día a día, aun no existen suficientes profesionales capacitados para ayudar a las compañías y organizaciones a proteger y defender sus activos digitales de forma adecuada. A medida que el paisaje cibernético continúa evolucionando rápidamente, no es suficiente confiar únicamente en el conocimiento y la teoría. Para ayudar en la crisis global de capacidades en la materia, ISACA ha creado el programa de preparación y certificación Cybersecurity Nexus (CSX).

CSX está ayudando a modelar el futuro de la Ciberseguridad mediante el desarrollo de un pensamiento de vanguardia, así como con programas de entrenamiento y certificación para los diferentes perfiles de profesionales que necesita el mercado. Construido con base en las fortalezas en procesos de capacitación y mejores prácticas que desarrolla ISACA Internacional, ofrece a los profesionales de Ciberseguridad un enfoque efectivo para mantener más seguros las organizaciones, su información y entornos digitales. Un programa holístico desarrollado por ISACA que está diseñado para ayudarlo, sin importar dónde se encuentre en su carrera, y sirve como una fuente única e integral para todo lo relacionado con la Ciberseguridad.

La certificación está alineada con la Iniciativa Nacional de Educación Cibernética (NICE) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), que es compatible con temas de ciberseguridad, actividades y roles laborales a nivel mundial. La certificación también está alineada con el Marco de Habilidades para la Era de la Información (SFIA).

Programa de Certificaciones CSX:

El programa está organizado en estas certificaciones, comprendidas por un plan de estudio, entrenamientos y examen de certificación:

CSX Cybersecurity Fundamental: ofrece una certificación en los conceptos introductorios que enmarcan y definen los estándares, directrices y prácticas de la industria de Ciberseguridad. Estas habilidades tienen una gran demanda, ya que las amenazas continúan plagando a las empresas de todo el mundo.

CSX Cybersecurity Practitioner: es una certificación basada en desempeño que valida habilidades técnicas en ciberseguridad, así como la preparación para el trabajo, globalmente diseñada para profesionales en ciberseguridad. Esta certificación le permite servir como un primer respondiente, en el seguimiento de procesos y procedimientos establecidos, y en la resolución de problemas en diferentes sistemas.

CSX Cybersecurity Audit: es un programa de certificación de Auditoría de Ciberseguridad que brinda a los profesionales de auditoría/aseguramiento el conocimiento necesario para sobresalir en las auditorías de ciberseguridad. Proporciona a los profesionales de la seguridad un entendimiento del proceso de auditoría, y a los profesionales de riesgos de TI un entendimiento del riesgo cibernético y los controles de mitigación.

Para mas información:

https://cybersecurity.isaca.org/csx-certifications

Por: Lic. Máximo Patiño Lalane, CISM CSX

Consultor y Docente en Seguridad de la Información.

Certificación Profesional en SEGURIDAD INTEGRAL CORPORATIVA

CERTIFIED CISEM CORPORATE INTEGRAL SECURITY MANAGER

ATENCION SANTIAGO 16 de noviembre

CISEM®

La certificación "Gerente de Seguridad Integral Corporativa Certificado", de sus siglas en inglés (CISEM), consta de cinco dominios.

DOMINIO I – LA SEGURIDAD Y LAS INVESTIGACIONES
DOMINIO II – SEGURIDAD INDUSTRIAL, SALUD Y MEDIO AMBIENTE
DOMINIO III – GESTION DE LA SEGURIDAD DE LA INFORMACION
DOMINIO IV – GESTION DE RIESGOS, CRISIS Y EMERGENCIAS
DOMINIO V – GERENCIA DE SEGURIDAD

AVALADO POR:

CEXDE
CENTER FOR EXECUTIVE DEVELOPMENT

UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

MACROSeguridad
La Seguridad es el centro del desarrollo en un mundo global.

809-373-1729 y 809-350-6555
info@macroseguridadrd.com
https://www.revistamacroseguridad.com/contacto

“El sistema Operativo Aurora OS (Avrora OS) que podría utilizar Huawei, desarrollado por la empresa ruso Jolla Ltd”

El 15 de mayo 2019, el presidente de Estados Unidos, Donald Trump, firma una orden ejecutiva que declara “emergencia nacional” por amenazas contra la tecnología estadounidense. La orden prohíbe el uso de equipos de telecomunicaciones fabricados por compañías consideradas como una amenaza para la seguridad nacional de EE.UU., lo que allana el camino para una prohibición total de los productos fabricados por Huawei Technologies de China.

La promulgación de esa orden suscitaría aún más tensiones en las relaciones entre Washington y Pekín, las dos economías más grandes del mundo, que ya se encuentran enfrascadas en una batalla por las prácticas comerciales chinas, consideradas por las autoridades norteamericanas como ‘desleales’. En particular, EE.UU. afirma que la empresa Huawei actúa bajo órdenes del Gobierno chino y que sus equipos podrían ser usados para el espionaje. Por su parte, la compañía ha negado en reiteradas ocasiones las acusaciones de Washington. (Fuente RT)

En particular, la medida proscribe la compra o uso de cualquier tecnología de comunicaciones producidas por entidades que están controladas por “un adversario extranjero” y que puedan crear un “riesgo indebido de sabotaje” de los sistemas de comunicaciones de EE.UU. o “efectos catastróficos” para la infraestructura estadounidense.

Podemos decir que, con esta medida de boicot impuesto por Estados Unidos al gigante chino Huawei, y que impide a sus teléfonos y clientes recibir la nueva versión de Android, estas medidas obligan a Huawei a acelerar un proyecto iniciado en el 2012 para el desarrollo de su propio sistema operativo que llevaría por nombre ‘Hongmeng OS’, y serviría tanto para ordenadores personales como para dispositivos móviles. Aunque los expertos indican que dicho sistema operativo ya habría sido testeado en distintos móviles desde el 2012, pero no se tiene una versión definitiva que permita sustituir Android y su Play Store.

Es oportuno indicar que al gigante chino Huawei no tener una fecha cierta de cuándo puede tener la versión definitiva para su salida a producción del sistema operativo 'Hongmeng OS', esto ha creado los rumores que indican que Huawei apostaría por un sistema operativo ruso desarrollado por Jolla Ltd, empresa que está formada por muchos antiguos exempleados de Nokia, los cuales fueron los encargados de desarrollar Sailfish OS, un sistema operativo sencillo para smartphones pequeños cuya función más interesante es que es compatible con aplicaciones Android.

"Huawei cerca de abandonar Android; ya negocia con Rusia para usar el sistema Aurora OS"

Con el acercamiento de China a Rusia Huawei estaría cerca de abandonar Android. Esta difícil situación que está pasando la empresa china la ha llevado a buscar una alternativa que se llama Aurora OS (Avrora OS) y procede de Rusia. El sistema operativo es en realidad una versión de Sailfish OS, una plataforma que desarrolló Jolla y que ha quedado casi totalmente ensombrecida por el duopolio Android/iOS. Ahora podría salir de las sombras, y sus opciones son desde luego interesantes. (Fuente Washington Post).

Según la página web Xataca.com, Huawei no ha confirmado esta circunstancia, pero sí sabemos que su plan B se llama Hongmeng OS (también conocido como ArkOS) y que por lo visto estaría ya instalado en un millón de dispositivos que probablemente sirvan como campo de pruebas para esa plataforma de Huawei. (Fuente RT).

Finalmente podemos decir que lo que está viviendo en este momento el gigante chino Huawei ya sucedió a finales de 2017, cuando el Departamento de Seguridad Nacional de EE.UU. (DHS) ordenó a todas las agencias gubernamentales del país prescindir de productos de Kaspersky Lab, el mayor proveedor ruso de seguridad cibernética y antivirus, debido a los supuestos "riesgos de seguridad" y a la preocupación de que ciertos directivos de Kaspersky podrían tener vínculos con la inteligencia rusa y otras agencias gubernamentales. El Departamento de Seguridad Nacional de EE.UU. no proporcionó ninguna prueba que confirmara sus afirmaciones, como en este momento tampoco ha podido hacerlo con Huawei.

Alfonso de los Santos
Auditor de TI
Certificado en CISA, COBIT, ITIL
Catedrático de varias Universidades

> *"En particular, la medida proscribe la compra o uso de cualquier tecnología de comunicaciones producidas por entidades que están controladas por "un adversario extranjero" y que puedan crear un "riesgo indebido de sabotaje" de los sistemas de comunicaciones de EE.UU. o "efectos catastróficos" para la infraestructura estadounidense."*

CERTIFIED CISEM CORPORATE INTEGRAL SECURITY MANAGER

UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

Certificación CISEM

CISEM

CISEM

QUINTIN
CONSULTING

quintinrd quintin_rd
Av. 27 de febrero, Plaza Central
Piso 4, local A-404-4, Sto. Dgo, R.D.

809-379-0407 809-214-1178
felix@quintin.do quintin.do

OFRECEMOS LOS SIGUIENTES SERVICIOS:

Asesoría y Consultas en el ámbito Jurídico Corporativo.

Representación ante las autoridades administrativas: Laborales, Marítimas y demás.

Representación ante los órganos jurisdiccionales del Estado, Civiles, Comerciales, Larolares, entre otros.

Instrumentación y redacción de Defensa y Demandas, según sea su caso.

Evaluación y estudio previo de todo tipo de contrato: Civiles, Comerciales, Laborales, Marítimos, etc.

Representación gratuita a los trabajadores y Gente del Mar.

Diligencias de conciliación y advenimiento amistoso.

CURSO
ANÁLISIS DE RIESGOS DE SEGURIDAD Y APLICACIÓN DE CONTROLES

Porque el riesgo de seguridad debe ser gestionado...

"Toda decisión en el ámbito de la Seguridad debe basarse en un análisis de riesgos"

Av. Winston Churchill, 4to nivel, Local 404, Plaza Central
809-350-6555 y 809-373-1729
info@macroseguridadrd.com
https://www.revistamacroseguridad.com/contacto

AVALADO POR:

UNIVERSIDAD INTERAMERICANA DE PUERTO RICO

CEXDE
CENTER FOR EXECUTIVE DEVELOPMENT

MACROSeguridad
La Seguridad es el centro del desarrollo en un mundo global.

info@macroseguridadrd.com
MacroSeguridad
www.revistamacroseguridad.com
809-373-1729