REVISTA

URVIO

Revista Latinoamericana de Estudios de Seguridad

PRESENTACIÓN DE ARTÍCULOS
URVIO No. 20
Revista Latinoamericana de Estudios de Seguridad

TEMA CENTRAL: CIBERSEGURIDAD

Coordinación: Carolina Sancho Hirane, Academia Nacional de Estudios Políticos y Estratégicos-ANEPE.
Envío de artículos: hasta el 13 de febrero de 2017
Publicación: junio 2017
Envío de artículos: revistaurvio@flacso.edu.ec

URVIO, Revista Latinoamericana de Estudios en Seguridad es una publicación electrónica semestral de FLACSO Sede Ecuador. Fundada en el año 2007, la revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y consulta sobre temas vinculados a la seguridad, delito organizado, inteligencia y políticas públicas sobre seguridad en la región.

La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización. En este sentido, de acuerdo a cifras de la Unión Internacional de Telecomunicaciones (UIT), en 2015 a nivel mundial la cantidad de usuarios de Internet se estimó en un 40% de la población y los abonados a banda ancha móvil 3.500 millones de personas. Todos los días crece la cantidad de aparatos conectados el ciberespacio en el marco de la internet.

No obstante, el incremento en el uso del ciberespacio ha generado ventajas y desventajas para los usuarios porque sus cualidades de facilidad en el acceso, rapidez en la transmisión de la información y bajo costo se ha visto afectado por la existencia de vulnerabilidades y amenazas que han afectado la confianza para la generación, almacenamiento y transmisión de información. En este contexto, periódicamente los ciudadanos reciben información sobre nuevos ciberdelitos ante los cuales están desprotegidos, como es el caso del robo de información en formato electrónico, el cryptoLocker, el phishing, entre otros. Hay frecuentes noticias sobre ciberataques a diversas organizaciones afectando su normal funcionamiento, por ejemplo cuando se produce un ataque de denegación distribuida de servicio (DDoS) o cuando un malware afecta los sistemas de supervisión, control y adquisición datos (SCADA) en la infraestructura crítica, como ocurrió con el gusano informático en el sistema de control de los reactores nucleares de Natanz en Irán.

Situaciones como las descritas obligan a reconocer que este ambiente no es ajeno a ciberdelitos que pueden perjudicar a las personas y ciberataques que pueden dañar a las organizaciones. De esta manera, los gobiernos deben tener presente que el adecuado funcionamiento del ciberespacio requiere garantizar condiciones mínimas de seguridad según estándares internacionales. Por este motivo, la existencia de ciberdelitos, ciberataques, ciberespionaje y posiblemente la ciberguerra, obliga a las máximas autoridades nacionales a contar con políticas públicas regulatorias, que ofrezcan seguridad y garanticen el respeto a los derechos de las personas. Asimismo, resulta necesaria la formulación de estrategias nacionales de ciberseguridad que requieren ser elaboradas en un marco de participación que contemple al sector público,

privado, académico y la sociedad civil, como también, la promoción de la coordinación interagencial y la cooperación internacional.

De acuerdo a lo expuesto, el próximo número buscará aportar elementos para debatir sobre este tema mediante la selección de artículos que respondan a cualquiera de los siguientes lineamientos:

- Ciberespacio como bien público: desafíos nacionales e internacionales.
- Gobernanza de internet: estado del debate.
- Organismos internacionales multilaterales: su aporte en el debate sobre ciberseguridad y logros alcanzados.
- Ciberseguridad como política pública y estrategias nacionales sobre el tema.
- El rol del sector privado y/o la comunidad internacional en la formulación de una política nacional de ciberseguridad.
- Infraestructura crítica en el ciberespacio y sector privado: rol y desafíos en el marco de una política nacional de ciberseguridad
- Ciberdefensa como parte de la ciberseguridad: características y desafíos.
- Manual de Tallin: aporte, limitaciones y desafíos.
- Ciberguerra: ¿es posible la guerra en el ciberespacio?, principales aproximaciones en torno al tema.
- Ciberdelitos: características, principales tendencias y desafíos en su persecución.
- Convención de Budapest: aporte para enfrentar el ciberdelito, limitaciones y desafíos en Latinoamérica.
- Arquitectura nacional de ciberseguridad: estudio de caso y lecciones aprendidas
- Arquitecturas nacionales de ciberseguridad: estudio comparado y buenas prácticas que pueden ser exportadas
- Ciberinteligencia: anticipando amenazas, vulnerabilidades y riesgos en el ciberespacio.
- Infraestructura crítica en el ciberespacio: metodología de identificación, estudios de casos y/o análisis comparado.
- Protección de la infraestructura crítica de la información en el ciberespacio: identificación de buenas prácticas.
- Incidentes en el ciberespacio: experiencias enfrentadas, medidas tomadas y lecciones aprendidas.
- Cultura en ciberseguridad: desafíos a enfrentar para promover una la ciudadanía informada.
- Cooperación internacional en ciberseguridad: posibilidades, limitaciones y desafíos.
- Coordinación interagencial en ciberseguridad: desafíos nacionales.

Los artículos deberán ajustarse a las directrices para autores de nuestra revista (descargar). Para la selección de artículos se utiliza un sistema de evaluación por lectores pares (peer review).

Las personas interesadas en participar deberán enviar sus trabajos a través de la plataforma de la revista URVIO.

Informes:
revistaurvio@flacso.edu.ec – (593 2) 2946800 ext. 3673

URVIO

RELASEDOR