Sistema de Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la seguridad nacional

National Cyber Security System Against the Cyber Attacks as threat to National Security

Daniel Iván Taipe Dominguez[1]

Calle Monte Coba 1015, Edificio B, departamento 2020 - Surco. Lima, Perú. +51985032866.

d_taipe@hotmail.com **HTTPS://ORCID.ORG/0000-0002-4673-323X**

PP. 43 -48

Recibido: 04/10/2019 Aceptado: 29/01/2020 Publicado: 17/02/2020

Resumen

En el desarrollo de la investigación se tuvo como objetivo analizar el Sistema de Seguridad Cibernética Nacional frente a los Ciberataques como amenaza a la Seguridad Nacional; desde luego el estudio lo que pretende es generar aportes que contribuyan a la solución de la problemática que se presenta; En cuanto a la metodología utilizada, se puede señalar que ha sido de tipo descriptiva, diseño no experimental descriptiva correlacional, como resultados se aprecia que es necesario buscar desarrollar el reforzamiento de la educación, la capacitación y el desarrollo de las líneas de formación profesionales de los especialistas de ciberseguridad, adicionalmente se debe establecer una concientización en materia de ciberseguridad en todas las fases de la formación académica y profesional del ciudadano.

1 Magíster en Doctrina y Administración aeroespacial. Escuela Superior de Guerra Aérea.

Abstract

The objective of the investigation was to analyze the National Cyber Security System against Cyber attacks as a threat to National Security; Of course, the study is intended to generate contributions that contribute to the solution of the problem presented; Regarding the methodology used, it can be noted that it has been descriptive, non-experimental descriptive correlational design, as results it is appreciated that it is necessary to seek to develop the strengthening of education, training and development of professional training lines of Cybersecurity specialists, in addition, awareness of cybersecurity should be established in all phases of the academic and professional training of the citizen.

KEYWORDS: IT SECURITY AUDIT, CYBERSECURITY, ETHICAL HACKING, INFORMATION SECURITY, CYBER SECURITY.

Introducción

El riesgo cibernético es una amenaza creciente para los ecosistemas financieros nacionales e internacionales. Las innovaciones tecnológicas y la sofisticación de las redes del delito cibernético, así como la interconectividad un sistema financiero global plantean desafíos a los responsables de la formulación de políticas para prevenir, detectar y mitigar las consecuencias de los ciberataques.

La protección contra el riesgo cibernético depende en gran medida de la conciencia y la cultura entre el personal de las instituciones. A nivel mundial, los ciberataques han demostrado que el factor humano es decisivo. Se debe promover una mayor colaboración transfronteriza para intercambiar información relevante y armonizar prácticas, con el fin de mejorar el entorno de ciberseguridad global.

El uso del ciberespacio está transformando los negocios, haciéndolo más eficiente y efectivo. Está abriendo mercados, lo que permite que el comercio tenga lugar a un costo menor, y permite a las personas hacer negocios desde cualquier lugar. Ha promovido una nueva forma de pensar, modelos de negocios innovadores y nuevas fuentes de crecimiento y oportunidades comerciales para empresas establecidas y empresarios emergentes por igual. Permite a las empresas ofrecer una experiencia de compra mejor, más barata y más conveniente a los clientes. También ayuda a las personas a "darse una vuelta", comparar precios y encontrar lo que quieren.

Para abordar los desafíos de la seguridad cibernética de frente, y aprovechar las oportunidades que ofrece el ciberespacio, se requiere liderazgo y gobernanza del ciberespacio en los niveles más altos

El presente trabajo pretende presentar propuestas a la realidad del Perú respecto de la Gestión de la Ciberseguridad y el desarrollo de Cibercapacidades haciendo un análisis de realidades comparadas a nivel mundial, así como utilizar herramientas como el Informe Bid/OEA 2017 "Ciberseguridad Estamos Preparados en América Latina" en donde se presentan diversos puntos de mejora para países de la región, en ese sentido esta investigación pretende presentar propuestas a la realidad del Perú respecto de la Gestión de la Ciberseguridad y el desarrollo de Cibercapacidades haciendo un análisis de realidades comparadas a nivel del hemisferio en donde se presentan diversos puntos de mejora para países de la región.

Ahora bien, según Emanuel Abraham (2014), menciona que, es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

En ese sentido, la Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en sus procesos. Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre la los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

El servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que "Para atrapar a un intruso, primero debes pensar como intruso" (UNAM, 2011).

La Ciberseguridad se encuentra comprendida dentro de la seguridad de la información, en la cual se busca garantizar la confidencialidad, integridad y disponibilidad de los activos de la información digital y de la infraestructura que la soporta (CCFFAA, 2018).

Materiales y Métodos

La presente investigación se ha abordado con un enfoque cualitativo, desde el paradigma hermenéutico y solo desde esa perspectiva se aborda el tema de la Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la Seguridad Nacional, en ese sentido, partiendo de una análisis crítico reflexivo con la búsqueda de referencias alineadas al tema del ciberespacio, el cual está constituido por hardware, software, internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socio-económica de cualquier nación, y en especial aquellos ligados a sus infraestructuras críticas, siendo estos los materiales que constituyen gran parte de la investigación efectuada.

Análisis y Resultados

Al fortalecer la cooperación nacional se pretende con esta línea de acción, establecer el liderazgo y la gobernanza para definir en forma clara la filiación, líneas de comunicaciones, roles. y responsabilidades, de igual manera la de liderar la colaboración y promover el intercambio de información a través de las entidades gubernamentales nacionales, ahora bien, para establecer esta Política, es conveniente la participación de un

amplio espectro de actores relacionados con esta temática, sea como parte de un Consejo ampliado ad hoc, o como parte de una Comisión temporal o permanente en Ciberseguridad.

Una vez establecida la Política Nacional de Ciberseguridad, creemos que el mejor escenario para que la normativa necesaria para el cumplimiento de las políticas nacionales de ciberseguridad pueda emitirse al margen de factores coyunturales políticos, y que asegure la continuidad y constante actualización que en este campo es ineludible, es que esta responsabilidad esté en manos de un organismo constitucional autónomo como son por ejemplo el Banco Central de Reserva (BCR), la Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones (SBS) y la Oficina Central de Lucha contra la Falsificación de Numerario (OCN). (Web Peru.gob.pe).

El Convenio sobre Ciberdelincuencia, conocido como Convenio de Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet, buscando armonizar las leyes nacionales, la mejora de técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa el 8 de noviembre de 2011, entrando para la firma de los Estados el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

Discusión

Es importante precisar que en el contexto internacional, se considera oportuno mencionar que los países como Estados Unidos, China, Israel, Rusia e Irán, así como la OTAN plantean la creación de Organizaciones que permitan enfrentar eficientemente estas amenazas, ya que son capaces de afectar todos los ámbitos del poder y potencial nacional. Esto ha derivado en la creación de organismos dedicados a la Seguridad de la Información, los cuales deberán hacer frente a las amenazas actuales y futuras siendo parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad.

De manera contundente se vislumbra el impulso de aplicabilidad del estándar propuesto por el Convenio en materia de Derecho Penal, Delitos relacionados a las infracciones a la propiedad intelectual, no solo alcanza a personas naturales sino hace responsables a las personas jurídicas. Por otro lado el Convenio establece mecanismo de resguardo de información y cooperación entre Estados respecto del tráfico de información.

Conclusiones

El estado peruano puede enfocarse en desarrollar una sólida estrategia de residencia cibernética. Esto significa el desarrollo de la capacidad para detectar y resistir como parte de los mecanismos de "pre interrupción" que permiten a las organizaciones detectar los riesgos emergentes.

A su vez, el estado peruano debe establecer una línea base de seguridad en cada una de sus instituciones, pero también deben reconocer que no pueden cumplir con la protección de manera individual. Se debe trabajar en conjunto con sus pares para proteger el ecosistema digital del estado.

A su vez, aumentar la seguridad en las instituciones de educación básica y superior, a través del enriquecimiento del talento de ciberseguridad del estado mejorando y ampliando las oportunidades educativas.

Referencias

Abad, W., Cañarte, T., Villamarin, M., Mezones, H., Delgado, A., Toala, F., Figueroas, J., y Romero, V. (2019). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. Alicante, España: 3Ciencias.

Aguilera, P. (2010). Seguridad informática. Madrid, España: Editex, S.A.

Andina (31 de agosto de 2018). ¿Cuáles son los ciberataques más comunes en el Perú? Andina. Recuperado de https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html.

Areitio, J. (2009). Seguridad de la información. Madrid, España: Paraninfo S.A.

Armas, J. (2018). Ciberseguridad: cómo adoptar medidas para proteger sus activos de información. Review of Global Management, 4(2), 20-21.

Baca, G. (2016). Introducción a la seguridad informática. México D.F., Grupo Editorial Patria S.A.

Cano, J., y rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. RISTI, 32(6), 7-9.

Chicano, E. (2014). Auditoría de seguridad informática. IFCT0109. Málaga, España, IC Editorial.

Cortés, R. (2015). Estudio actual de la política pública de ciberseguridad y ciberdefensa en Colombia. Revista de derecho común y nuevas tecnologías, 14, 1-17.

Dordoigne, J. (2015). Redes informáticas. Nociones fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP, V6...). Barcelona, España: Ediciones Eni.

El Peruano (14 de enero de 2019). Ciberataques en crecimiento. El Peruano. Recuperado de https://elperuano.pe/noticia-ciberataques-crecimiento-74748.aspx.

Espinoza, J. (2018). Entre la figura electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. Revista del Instituto de Ciencias Jurídicas de Puebla, México, 12(41), 241-266.

Fundación Telefónica (2011). Realidad aumentada: una nueva lente para ver el mundo. Barcelona, España: Editorial Ariel.

Gestión (11 de junio de 2019). Radiohead responde a hackers: libera sesiones robadas de música inédita. Gestión. Recuperado de https://gestion.pe/tecnologia/radiohead-responde-hackers-libera-sesiones-robadas-musica-inedita-269828-noticia/.

Gomes, C. (2017). La nueva era de la información como poder y el campo de la ciberinteligencia. URVIO: Revista Latinoamericana de Estudios de Seguridad, (20), pp. 94-109.

González, P. (2015). Ethical Hacking: Teoría y práctica para la realización de pentesting. Madrid, España: OxWORD Computing.

Guerrero, L. (2007). Los derechos humanos como política pública: Colombia, una salida democrática en un país violento. Bogotá, Colombia: Universidad Nacional de Colombia.

Hernández, G. (2010). Actualidad y futuro del derecho procesal: principios, relgas y pruebas. Bogotá, Colombia: Editorial Universidad del Rosario.

Hinarejos, A., y De la Peña, J. (2017). I+D+i y ciberseguridad: análisis de una relación de interdependencia. Cuadernos de estrategia, (185), 247-290.

Joyanes, L. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, (185), 19-64.

Joyanes, L. (2015). Sistemas de información en la empresa. El impacto en la nube, la movilidad y los medios sociales. México D.F.: Alfaomega.

Medina, M., y Molist, M. (2015). Cibercrimen. Barcelona, España: Tibidabo Ediciones.

Pacheco, F., y Jara, H. (2012). Hackers al descubierto. Madrid, España: Usershop.

Poma, A., y Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. Sciéndo, 22(4), 275-282.

Pons, V. (2017). Internet, la nuuva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO: Revista Latinoamericana de Estudios de Seguridad, (20), 80-93.

Sánchez, H. (2009). Metodología y diseño de la investigación científica. Lima, Perú: Editorial Visión Universitaria.

San-Martín, C. (2006). Derecho Penal. Lima, Perú: Grijiley.

Santos, M., Barrios, A., y Gonzáles, P. (2019). El hacking como comportamiento típico en las nuevas formas de delincuencia organizada. Espirales: revista multidisciplinaria de investigación, 3(26), 60-70.

Stel, E. (2014). Seguridad y defensa del ciberespacio. Buenos Aires, Argentina: Editorial Dunken.

Touhil, G., y Touhil, J. (2014). Cibersecurity for Executives. A Practical Guide. New Jersey. EE.UU.: Wiley.