Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032

Article *in* Estudios en Seguridad y Defensa · December 2017

DOI: 10.25062/1900-8325.253

3 authors:

Humberto Parra
Universidad de las Fuerzas Armadas-ESPE
27 PUBLICATIONS **454** CITATIONS
SEE PROFILE

Angie Fernández Lorenzo
Universidad de las Fuerzas Armadas-ESPE
76 PUBLICATIONS **844** CITATIONS
SEE PROFILE

Luis Recalde Herrera
Universidad de las Fuerzas Armadas-ESPE
7 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Cómo citar este artículo:

Parra, H., Fernández, A., & Recalde L. (2017). Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032. *Estudios en Seguridad y Defensa*, *12*(24), 99-111.

Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032[1]

Guidelines for the management of cybersecurity using the ISO / ECT standard 27032

Diretrizes para gestão da segurança cibernética utilizando o padrão ISO/ ECT27032

HUMBERTO PARRA CÁRDENAS, Ph.D.[2]

ANGIE FERNÁNDEZ LORENZO, Ph.D.[3]

LUIS RECALDE HERRERA, Mgs.[4]

Recibido:
30 de noviembre de 2016

Aprobado:
15 de diciembre de 2017

Palabras clave:
Ciberespacio, Ciberamenazas, Ciberseguridad, Internet, Gestión. ISO 27032.

Keywords:
Cyberspace, Cyber Threats, Cybersecurity, ISO 27032.

Palavras-chaves:
ciberespaço, ciberameaças, cibersegurança, internet, gestão, ISO 27032.

Resumen

Como consecuencia de la rápida evolución y desarrollo de los sistemas de telecomunicaciones y de información, en la última década gran parte de actividades tanto comerciales, financieras y comunicacionales se las realiza a través de las redes de internet, las cuales han dado origen a un espacio virtual y asimétrico denominado "Ciberespacio", es decir, que este es la autopista por donde circula información digital tanto de personas naturales como

1. Artículo de reflexión vinculado al proyecto de investigación del Departamento de Seguridad y Defensa de la Universidad de las Fuerzas Armadas ESPE, Ecuador.
2. Tcrnl. Humberto Parra Cárdenas, PhD. Director del Departamento de Seguridad y Defensa, Universidad de las Fuerzas Armadas ESPE. haparra@espe.edu.ec
3. Eco. Angie Fernández Lorenzo, PhD. Profesora del Departamento de Ciencias Económicas, Administrativas y de Comercio, Universidad de las Fuerzas Armadas ESPE. aafernandez2@espe.edu.ec
4. Mayor Luis Recalde Herrera, Mgs. Profesor del Departamento de Seguridad y Defensa, Universidad de las Fuerzas Armadas ESPE. llrecalde@espe.edu.ec

organizaciones de todos los Estados del mundo. Al paso que ha aumentado la tecnología van apareciendo y creándose nuevas amenazas que ponen en peligro la ciberseguridad de las naciones. Para analizar las amenazas cibernéticas es importante enfocarse en términos de su origen, es decir, de donde provienen. Las ciberamenazas pueden derivarse de un espectro amplio de fuentes, que van desde una sola persona como un hacker solitario, pasando por un empleado descontento, los cibercriminales y ciberterroristas y llegando hasta el empleo de las capacidades de una o varios Estados-nación para conducir un ataque encubierto, coordinado y dinámico a un adversario. El presente artículo está orientado a conceptualizar el enfoque, el alcance y las directrices de la norma ISO/ECT 27032 para la gestión de la ciberseguirdad, para lo cual se realizó un análisis de contenido cualitativo; fundamentándose en un estudio conceptual del origen del Ciberespacio. Además se estudió que al interactuar en este espacio virtual origina un creciente riesgo para mantener la confiabilidad, integridad y disponibilidad de la información, por la proliferación de las "Ciberamenazas" que han ido evolucionando de tal forma que sus irrupciones podrían afectar a todas las actividades humanas. Como resultado de este trabajo se determinó que la implementación de la Norma Internacional ISO 27032 proporcionará directrices para mejorar la seguridad cibernética (Ciberseguridad), mediante buenas prácticas para quienes gestionan sus actividades en el ciberespacio, a fin de asegurar la información, las redes, de internet y proteger las infraestructuras críticas.

Abstract

This article seeks conceptualizing the approach, scope and guidelines of the standard ISO / ECT 27032 for managing the cybersecurity, for which a qualitative content analysis was performed; it was based on a conceptual study of the origin of the Cyberspace. Additionally, it was studied that the interaction in this virtual space creates an increased risk for maintaining the reliability, integrity and availability of information, this occurred due to the proliferation of "Cyber Threats", which have evolved in such a way that their raids could affect all human activities. As a result of this work, it was determined that the implementation of the International Standard ISO 27032 will provide guidelines for improving cybersecurity, through good practice for those who manage their activities in the Cyberspace, in order to ensure information, networks, Internet and protect critical infrastructure.

Resumo

Como consequência da rápida evolução e o desenvolvimento do sistema de telecomunicações e de informação, na última década, grande parte das atividades,

tanto comerciais, como financeiras e de comunicações, são realizadas através das redes de internet, as quais deram origem a um espaço virtual e assimétrico denominado "ciberespaço", ou seja, esta é autopista por onde circula a informação digital, tanto das pessoas naturais, como das organizações de todos os Estados do mundo. Na medida em que tem aumentado a tecnologia, vão aparecendo e sendo criadas novas ameaças, que põem em perigo a "cibersegurança" das Nações. Para analisar as ameaças cibernéticas é importante focar em termos de sua origem, isto é, de onde provêm. As ameaças cibernéticas podem derivar de um aspecto amplo de fontes, que vão desde uma só pessoa, como um hacker solitário, passando por um funcionário descontente. Os cibercriminosos e os ciber-terroristas chegam até ao uso das capacidades de um ou vários Estados-Nação para conduzir um ataque encoberto, coordenado e dinâmico a um adversário.

Introducción

Como consecuencia de la rápida evolución y desarrollo de los sistemas de telecomunicaciones y de información, en la última década gran parte de actividades tanto comerciales, financieras y comunicacionales se las realiza a través de las redes de Internet, las cuales han dado origen a un espacio virtual y asimétrico denominado "Ciberespacio", es decir, que este es la autopista por donde circula información digital tanto de personas naturales como organizaciones de todos los estados del mundo. En este nuevo ambiente de dimensiones infinitas actualmente se producen ataques que aseguran el anonimato y pueden causar mayores efectos que un ataque con armas convencionales; dado que pueden inutilizar infraestructuras críticas de un país tales como centrales hidroeléctricas, refinerías, aeropuertos, sistemas de telecomunicaciones, aplicaciones financieras, etc.; además, pueden producir pánico financiero y sustracción de información altamente clasificada. A este tipo de atacantes se les conoce actualmente como amenazas cibernéticas, ya que estos no usan armas, ni municiones ni ejércitos, solo se infiltran en todos los sistemas tecnológicos y son capaces de someter gobiernos, quebrar economías y desquiciar a grupos sociales, a través de la inyección de un simple virus hasta sofisticados ataques realizados por un terrorista informático o por un Estado como parte de un plan estratégico para doblegar a otro país.

En este contexto, todos quienes interactúan en el espacio cibernético (personas, organizaciones y estados), deben tener un papel preponderante en la gestión de la seguridad de ciberespacio, a fin de proteger su privacidad, sus activos y sus infraestructuras críticas. En tal virtud surge la ISO/ECT 27032 como una Norma Internacional encargada de abordar la ciberseguridad desde un enfoque técnico con el fin de determinar los riesgos más comunes para la seguridad del espacio cibernético y establecer los controles más adecuados para mitigar dichos riesgos.

Adicionalmente, esta norma enfoca la necesidad de un eficiente intercambio de información entre todos los que interactúan en el ciberespacio, a fin de crear una base de conocimientos sólida de las amenazas y de los incidentes que permitan proteger la privacidad, integridad y disponibilidad de sus activos y su aplicabilidad en el ámbito empresarial.

Metodología

Para desarrollar el presente trabajo se realizó un estudio de contenido cualitativo, para lo cual se analizó el contenido de la norma ISO 27032, que básicamente se divide en dos partes: la primera que se enfoca al marco teórico de la ciberseguridad; y la segunda, que está orientada a la aplicabilidad de la norma y a las categorías y particularidades de todos los actores que intervienen en el ciberespacio.

Inicialmente se realizó el análisis de las definiciones de los elementos básicos que intervienen en la ciberseguridad a fin de comprender adecuadamente la concepción del ciberespacio en el ámbito de la seguridad: analizando las principales amenazas que utilizan el espacio cibernético para llevar a cabo acciones criminales, terroristas, de usurpación y uso ilícito de la información; también se realizado una aproximación a la conceptualización de la ciberseguridad como elemento clave para preservar los activos de una organización; y, finalmente se analizó el propósito, alcance y aplicabilidad de la norma ISO/ECT 27032 como referente de buenas prácticas tanto para proveedores como para usuarios de servicios de internet y de la infraestructura tecnológica de comunicaciones, a fin de preservar la integridad, confiabilidad y disponibilidad de la información que circula por el ciberespacio; y, finalmente se examinó como esta norma complementa el enfoque de la gestión de riesgos de otras normas de las familias ISO 27000 y la ISO 31000, mediante: la identificación de activos críticos, evaluación de riesgos tanto de proveedores como usuarios, la responsabilidad hacia otras partes interesadas al interactuar en el ciberespacio, proporcionando directrices para la implementación de controles: a nivel de aplicación, para protección de servidores, para usuarios finales, contra ataques de ingeniera social y otros controles a nivel de hardware.

Conceptualización de los elementos principales de la Ciberseguridad

Origen y definición del Ciberespacio

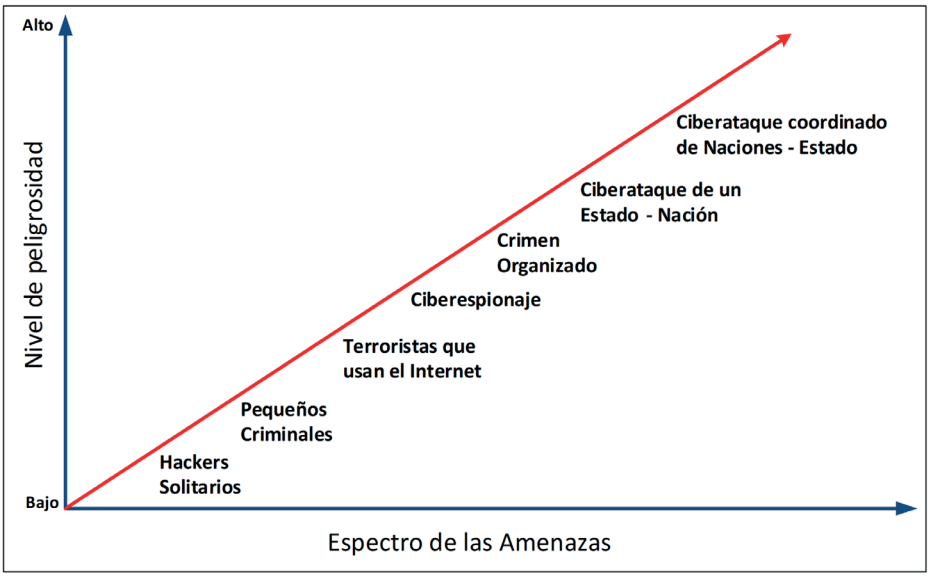
Rattray (2001) plantea que "El ciberespacio es un entorno artificial para la creación, transmisión y uso de la información en una variedad de formatos,

fundamentalmente constituido por el hardware electrónico, redes, sistemas operativos, estándares y políticas de transmisión" (p, 17). Por otro lado Aguirre (2010) define al ciberespacio como un espacio virtual de interacción, puesto que su realidad se materializa a través de un intercambio de información, surgiendo de una interacción entre el espacio y el medio en este caso la interacción entre redes de computadoras y personas.

De estas definiciones se podría abstraer que el ciberespacio es un ecosistema virtual que se forma de una combinación de la energía electromagnética, electrónica, las infraestructuras de red y la información, lo que lo hace único y asimétrico, y que básicamente sirve para el intercambio de información y conocimiento, sin importar la localización física, condición social, religiosa o económica de quienes interactúan en él. Está compuesto por una capa de física, que corresponde a la infraestructura y al hardware; una segunda capa que corresponde a las aplicaciones y al software; y, finalmente una capa que corresponde a la comunicación y generación de contenido, llamada capa cognitiva (Ventre, 2012).

La naturaleza y las fuentes de las Ciberamenazas

Figura 1: Fuentes y espectro de las ciberamenazas



Fuente: Elaboración propia. (IBM Global Business Service, 2010).

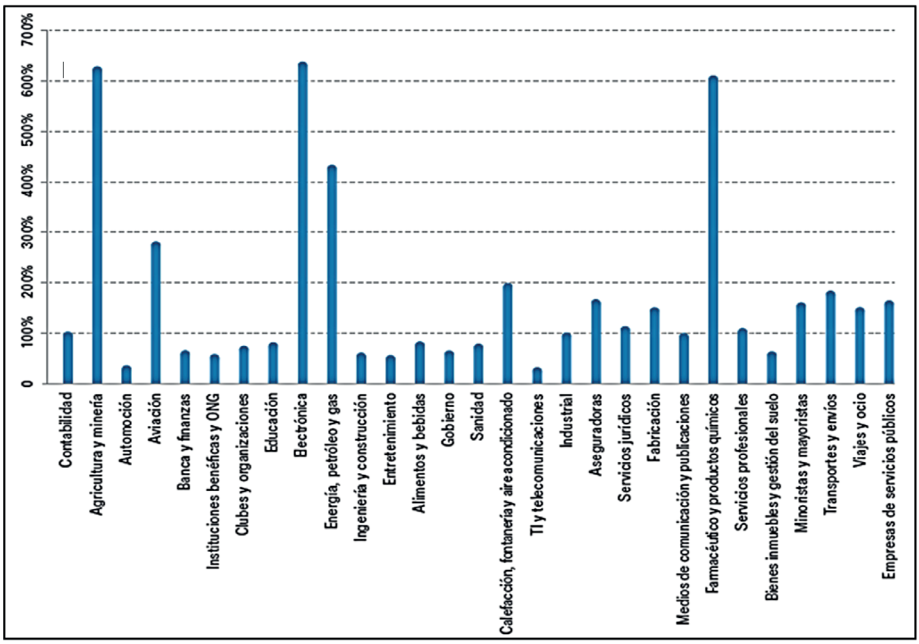
Para analizar las amenazas cibernéticas es importante enfocarse en términos de su origen, es decir, de donde provienen. Las ciberamenazas pueden derivarse de un espectro amplio de fuentes, que van desde una sola persona como un

hacker solitario, pasando por un empleado descontento, los cibercriminales y ciberterroristas y llegando hasta el empleo de las capacidades de una o varios Estados-nación para conducir un ataque encubierto, coordinado y dinámico a un adversario. En tal virtud el impacto potencial de este ataque cibernético aumenta y puede causar daños considerables a las infraestructuras tecnológicas de un país. Este espectro de amenazas se puede esquematizar en la figura 1, contrastando su nivel de peligrosidad, siendo los menos peligrosos los hacker solitarios que buscan más reconocimiento y notoriedad y llegando a amenazas promovidas por Estados que tienen un alto grado de sofisticación y destrucción.

Otra de las características importantes que se deben considerar al momento de categorizar e investigar las ciberamenazas son las técnicas y tecnologías utilizadas, partiendo desde la simple piratería para difundir información malintencionada hasta al ataque con la inyección de un virus que puede bloquear los sistemas computacionales de las infraestructuras críticas de un estado e inutilizar los sistemas de información y comunicaciones de cualquier tipo de organización sea esta pública o privada. Por lo tanto, la preparación de las organizaciones y de los Estados para hacer frente a este tipo de amenazas varía significativamente de acuerdo a sus medios y a sus capacidades estratégicas.

Por otro lado, la empresa multinacional de telecomunicaciones CISCO SYSTEMS, así como otras empresas y organizaciones que se dedican a la protección de la seguridad informática y de las comunicaciones han publicado estadísticas alarmantes del crecimiento exponencial de ataques a las infraestructuras tecnológicas de empresas de todo tipo en los cinco últimos años, tal como se puede observar en la figura 2, en la cual CISCO difunde el reporte del crecimiento de ataques de malware por tipo de industria en el 2013. Donde se puede observar que las industrias con un crecimiento de más del 600% en ataques son: las de agricultura y minería, las farmacéuticas y químicas y las de electrónica, mientras que con un crecimiento mayor al 400% están las industrias de energía, gas y petróleo. Por otro lado se puede ver que las industrias que han sufrido menos ataques de malware, son las de aviación y las de IT y telecomunicaciones.

Figura 2: Riesgos de los sectores y encuentros con malware web.



Fuente: Tomado del Informe de CISCO Cloub Web Security (CISCO, 2014)

La Ciberseguridad en el contexto empresarial

En el glosario de términos publicado por el NICCS (National Initiative for Cybersecurity Carrers and Studies, 2015), se define a la ciberseguridad como el conjunto de estrategias, políticas y normas orientadas a la seguridad de las operaciones en el ciberespacio. Ampliando este concepto se puede decir que se enfoca en minimizar las amenazas y las vulnerabilidades que podrían tener los sistemas de información de una organización, incluyendo las políticas y procedimientos para mitigar los riesgos, la disuasión, y la respuesta a incidentes en el ciberespacio.

Mientras que la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), define a la ciberseguridad de la siguiente manera:

> La Ciberseguridad comprende el conjunto de herramientas, políticas, conceptos de seguridad, medidas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, mejores prácticas, seguridad y tecnologías que se pueden utilizar para proteger en el entorno cibernético los activos de las organizaciones y de los usuarios. Los activos de la organización y de los usuarios incluyen dispositivos informáticos, recursos humanos, infraestructura,

> aplicaciones, servicios relacionados, sistemas de telecomunicaciones, y la totalidad de la información transmitida y/o almacenada en el entorno cibernético. La Ciberseguridad garantiza la consecución y el mantenimiento de la seguridad de los activos de propiedad de las organizaciones y de los usuarios, contra los riesgos de seguridad en el entorno cibernético. Los objetivos generales de seguridad comprenden los siguientes: disponibilidad; integridad, la cual puede incluir autenticidad y no repudio; y la confidencialidad. (ITU, 2008)

Esta definición en un sentido más amplio determina toda una amalgama de elementos que se consideran en la ciberseguridad, lo cual no solo corresponde a las directrices y políticas para proteger los activos de información de una organización y de los usuarios de los servicios de telecomunicaciones, sino que incluye a toda su infraestructura tecnológica, a las personas, y a las buenas prácticas de gestión de la seguridad de la información.

El Estándar ISO/ECT 27032

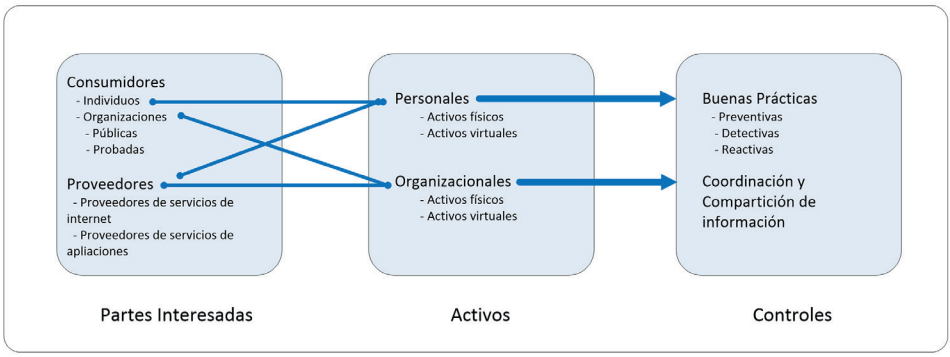
Enfoque

Esta norma internacional liberada el 16 de julio de 2012, propone un enfoque sistemático para la adecuada gestión de la ciberseguridad, proporcionado una orientación técnica en el análisis de los riesgos de la ciberseguridad causados por los ataques de la ingeniería social, la piratería informática, la proliferación de software malicioso o potencialmente no deseado, además proporciona controles para la detección, seguimiento, preparación y respuesta contra ataques provenientes del ciberespacio.

Otro aspecto significativo que abarca esta norma es la posibilidad que tanto proveedores como consumidores (personas y organizaciones) puedan intercambiar información sobre todo para el manejo de incidentes y proliferación de ciberamenazas.

Es importante destacar que en el año 2014, el Instituto Ecuatoriano de Normalización – INEN, publica la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27032, que una traducción idéntica de la norma internacional ISO 27032:2012. (INEN, 2014), cuyo enfoque general se puede resumir en la figura 3, que se muestra a continuación.

Figura 3: Vista general del enfoque.



Fuente: Traducido de la ISO/ECT 27032

Alcance

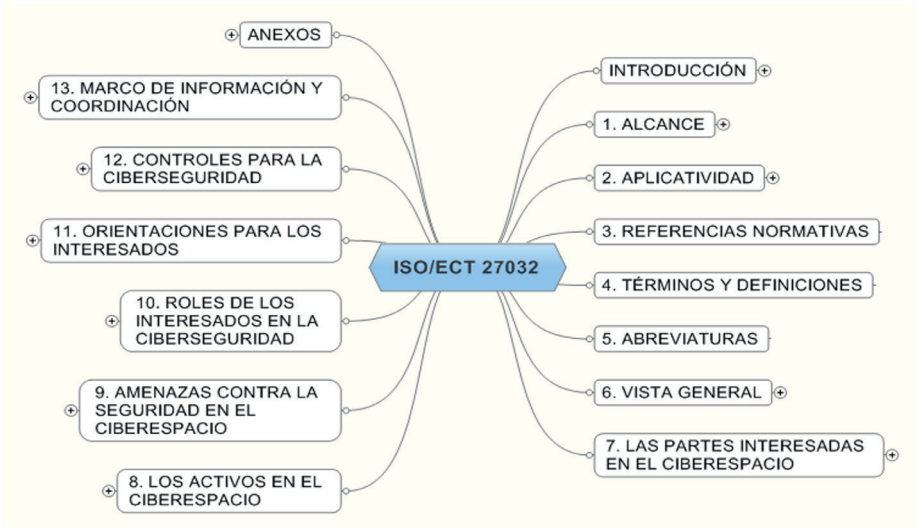
La ISO/ECT 27032 cubre las prácticas de seguridad desde el nivel más básico para quienes interactúan en el ciberespacio. Esta norma contempla una descripción integral de cómo mejorar la seguridad cibernética; una explicación de la relación entre la ciberseguridad y otros tipos de seguridades en el ámbito tecnológico; una definición de las partes interesadas (*stakeholders*) y una descripción de su papel en la seguridad cibernética; una orientación para abordar problemas comunes de seguridad cibernética y un marco que permite a las partes interesadas colaborar en la solución de problemas comunes en la ciberseguridad. Extrayendo los aspectos básicos de la ciberseguridad y de su dependencia en otros dominios de la seguridad, en forma concreta sobre: la seguridad de la información, la seguridad de las redes, la seguridad en Internet y la protección de la información de las infraestructuras críticas (CIIP, por sus siglas en inglés).

Estructura y contenido general de la Norma

En la figura 4 se ha esquematizado la estructura general de la norma ISO/ECT 27032; cuyo contenido se puede dividir en dos partes. En una primera parte, desde la sección uno hasta la sexta, se realiza un enfoque del marco teórico de la ciberseguridad, del alcance, aplicabilidad y enfoque general del contexto en el que se orienta la ciberseguridad como parte de la seguridad en general. Mientras que en la segunda parte, que va desde la sección siete hasta la decimotercera, se incluyen los aspectos fundamentales de ciberseguridad que enfoca esta norma, es decir, una descripción de los *stakeholders* y sus roles, así como una clasificación de los activos en el ciberespacio; también se hace una descripción de las amenazas contra la seguridad del ciberespacio y los controles para mitigar los riesgos de

dichas amenazas; y, finalmente se hace referencia a un marco de información y coordinación de los actores que intervienen activamente en el ciberespacio, tanto proveedores como consumidores.

Figura 4: Estructura General del estándar ISO/ECT 27032



Fuente: ISO/ECT 27032

Dentro del análisis específico de la segunda parte de la norma ISO/ECT 27032l en la sección 7 de esta norma, se establece que dentro de ciberespacio interactúan, por un lado los consumidores; sean estos personas naturales y organismos tanto públicos como privados; y por otro lado están los proveedores de servicios de Internet y de aplicaciones. Esta norma internacional a todos estos grupos descritos anteriormente los nombra en forma genérica como partes interesadas o *stakeholders*.

En la sección 8 se describen los activos que están expuestos en el ciberespacio; considerando como activo todo bien o servicio que tiene un valor tangible o intangible para las organizaciones y para los individuos y que cuya perdida, substracción o destrucción pueden causar deterioro en su patrimonio e inclusive en su credibilidad e imagen. En tal sentido la ISO/ECT 27032 establece dos grandes grupos relacionados a los bienes personales y a los activos de las organizaciones, sean estos físicos o virtuales.

La sección 9 en forma específica establece cuáles son las amenazas contra la seguridad en el ciberespacio. Por un lado se establecen las amenazas a los bienes de las personas e individuos; por otro lado, las amenazas latentes para los activos de las organizaciones. En esta sección además se analizan cuáles son los agentes de amenazas y sus principales motivaciones para irrumpir en el ciberespacio. Otro apartado importante que enfoca está sección es lo referente a las vulnerabilidades que potencialmente pueden aprovechar los ciberatacantes y sus principales mecanismos de ataque, los cuales pueden originarse tanto en el interior de un red privadas por individuos que pertenecen a la organización, como en forma externa a una red privada como por ejemplo los ataques que se realizan a través del Internet.

Los roles de las partes interesadas o *stakeholders*, es decir de los consumidores sean estos personas naturales u organizaciones y de los proveedores, básicamente se enfocan a su participación activa o pasiva para contribuir a la seguridad cibernética, están claramente estipulados en la sección 10 de la norma motivo del presente estudio.

La sección 11 de la norma internacional se enfoca a la evaluación y tratamiento de los riesgos; considerándose aspectos fundamentales como la identificación de activos críticos y los riesgos inherentes a dichos activos, para identificarlos y evaluarlos claramente. También se establecen las directrices de seguridad para consumidores y proveedores de servicios que intervienen activamente en el ciberespacio, complementadas con una serie de buenas prácticas que permitirán garantizar la seguridad de la información dentro de las organizaciones.

En la sección 12 de la ISO/ECT 27032, se trata como elemento clave de la aplicabilidad de esta norma los controles para una efectiva y eficiente seguridad cibernética; tanto a nivel de aplicaciones, de servidores (hardware) y de usuario final. También se establecen en forma explícita los controles en caso de ataques de ingeniería social y otros controles adicionales para fortalecer la ciberseguirdad.

Considerando que los incidentes cibernéticos pueden originarse en cualquier lugar del planeta, sin importar fronteras geográficas, sin que importe el tipo de amenazas y atacantes, las organizaciones y los individuos deben establecer normas y regulaciones para compartir la información que les permita responder efectivamente a cualquier evento o incidente que ponga en riesgo la seguridad de su información; en tal virtud, como en la sección 13 de esta norma se establecen las políticas generales y el marco de coordinación a todo nivel para crear un sistema global de ciberseguirdad, seguro, confiable y transparente.

Finalmente la norma ISO/ECT 27032 incluye tres anexos; el Anexo A, orientado a mejorar los controles para detectar y responder ante amenazas emergentes. Mientras tanto el Anexo B incluye fuentes adicionales en las cuales se pueden

ampliar aspectos técnicos y metodológicos para fortalecer la seguridad cibernética y el reporte de incidentes. El Anexo C incluye una serie de normas e informes técnicos que podrán ser de gran utilidad para la gestión integral de la ciberseguridad.

Conclusiones

El estándar o norma ISO/ECT 27032, como parte de la familia ISO 27000, propone un enfoque sistemático para la gestión de la ciberseguridad, considerando que en el ciberespacio no solo interactúan organizaciones para intercambiar información en forma lícita, sino que también conviven en este ecosistema virtual amenazas tanto internas como externas que potencialmente podrían dañar, sustraer, destruir o incluso usar con fines políticos, económicos y delictivos los activos de estas organizaciones y los bienes de las personas en general.

Esta norma proporciona directrices para que las partes interesadas evalúen los riesgos por el potencial deterioro o pérdida de sus activos e implementen controles efectivos tanto para las aplicaciones, como para los usuarios finales y los servidores de una organización. También proporciona lineamientos para la protección de la información contra ataques de ingeniería social, proveyendo estrategias, políticas, métodos y procesos para mitigarlos, además de una adecuada capacitación y entrenamiento de los usuarios y consumidores que interactúan en el ciberespacio.

Los incidentes que afectan la ciberseguridad traspasan las fronteras geográficas y las redes internas de las organizaciones lo cual limita la respuesta en forma individual ante estos incidentes, por lo que se plantea la necesidad de establecer directrices generales para compartir información acerca de las amenazas con el fin de ejecutar acciones coordinadas para responder adecuadamente ante cualquier tipo de amenaza a la ciberseguridad, por lo que esta norma proporciona un marco de referencia para implementar un sistema de información coordinado y compartido para un eficiente y efectivo control del espacio cibernético.

La norma ISO/ECT 27032 por sí sola no es certificable y constituye una directriz de buenas prácticas para la gestión de la ciberseguirdad en todo tipo de organizaciones, sean estás públicas o privadas e inclusive de las personas que interactúan permanentemente en el ciberespacio.

Referencias

Aguirre, J. (2010). *Ciberespacio y Comunicación:* Nuevas formas de vertebración social en el siglo XXI. Madrid: Biblioteca Virtual Universal

CISCO. (2014). *Informe anual de seguridad.* San José, CA: Cisco Systems, Inc.

IBM Global Business Service (2010). *Cyber defense*: *Understanding and combating the threat*. IBM Global Bussines Services, p.5

INEN (2014). *Tecnología de la información – Técnicas de seguridad – Directrices para ciberseguridad* (ISO/IEC 27032:2012, IDT), NTE INEN-ISO/IEC 27032

Instituto Español de Estudios Estratégicos (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacios*. Madrid: Ministerio de Defensa.

ISACA (2012). Information technology — Security techniques — Guidelines for cybersecurity. Genova: ISO/IEC 27032

ISACA (2013). *Transforming Cybersecurity*: Using COBIT. Illinois: ISACA org.

ITU (2008). *Recommendaion IUT-T X 1025. Section 3.2.5* - Overview of cybersecurity. Recuperado de: http://icto.dost.gov.ph/wp-content/uploads/2014/07/T-REC-X.1205_April2008.pdf

Klimburg, A. (2012). *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence

Kissel, R. (2013). Glossary of Key Information Security Terms. National Institute of Standards and Technology NIST

NICCS - National Initiative for Cybersecurity Carriers and Studies (2015). Recuperado de: http://niccs.us-cert.gov/glossary

Rattray, G. (2001, p.17, 65). *Strategic Warfare in Cyberspace*. Massachusetts: MITT Press

Ventre, D. (2012). *Cyber Conflic: Competing National Perpectives*. Engelska: Wiley-ISTE