Retos de Seguridad Informática y Seguridad de la Información

Garantivá Ortiz, Edgar Mauricio.
maur73@hotmail.com
Universidad Piloto de Colombia

Resumen - El documento describe la visión conceptual de la seguridad informática y seguridad de la información, y la perspectiva respecto al panorama reciente y las tendencias de ciberdefensa teniendo en cuenta los retos que ello supone.

Abstract - The paper describes the conceptual vision for IT security and information security, and perspective regarding the recent scenario and trends of cyber considering the challenges that entails.

Palabras Clave- Seguridad, Ciberdefensa, Amenazas, Gestión, Ciberataques.

I. INTRODUCCIÓN

Tanto en Colombia como a nivel global, se han identificado los alcances de la seguridad de la información y la seguridad informática, y aunque cada tema es muy extenso, tienen puntos comunes que se relacionan por la creciente tendencia de la digitalización de la información para facilitar su almacenamiento y tratamiento. La situación reciente respecto a ciberataques ha dejado expuestos algunos de los errores en los que se ha incurrido en el manejo de dichos incidentes. El futuro cercano refleja que la seguridad debe asumir nuevos retos.

Es claro que la industria de seguridad de la información (y seguridad informática) es una de las pocas que tiene una industria paralela trabajando en contra, lo cual exige tener esquemas y políticas dinámicas que no limiten e interfieran con las acciones que se deben llevar a cabo.

II. SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA SEGURIDAD INFORMÁTICA

Una de las situaciones más recurrentes y que genera debate entre profesionales y especialistas de ambos campos, es la diferenciación de seguridad informática (IT Security) con seguridad de la información (Information Security). De antemano se sabe que su significado, implicaciones y alcance no son los mismos, pero sí están relacionados por un fin común: proteger la información. Ambos campos buscan alcanzar este objetivo de manera distinta. Los siguientes son aspectos representativos de cada campo, que permiten diferenciarlos de manera preliminar:

A. Seguridad Informática

Se concentra en proteger los componentes de infraestructura tecnológica y de comunicación que soportan la operación de una organización enfocándose básicamente en hardware y software, favoreciendo la utilización de las herramientas informáticas de manera apropiada. Se puede decir que el análisis de riesgos se orienta principalmente en identificar vulnerabilidades de hardware y/o software sobre la infraestructura, con el fin de mitigar y llevar el riesgo a un nivel aceptable a través de acciones preventivas y correctivas. La seguridad informática se basa principalmente en implementar herramientas para necesidades específicas de seguridad, generar procedimientos basados en requerimientos orientados a seguridad TIC[1], lograr cumplimiento normativo, mejorar indicadores de seguridad entre otros.

B. Seguridad de la Información

Tiene como propósito proteger la información, independientemente del medio que la contenga. Material impreso, medios magnéticos o el conocimiento de las personas son ejemplos claros de activos que contienen información que es valiosa para una organización.

[1] TIC: Tecnologías de la Información y las Comunicaciones

La seguridad de la información tiene tres principios fundamentales que son confidencialidad, integridad y disponibilidad de la información. Basados en el aseguramiento de estos principios se ejecutan las acciones a nivel estratégico que buscan mantener el riesgo en la gestión de la información por debajo del nivel asumible.

C. Comparativo de Conceptos de Seguridad Informática y de la Información

Haciendo una evaluación del alcance de los dominios del anexo A del estándar ISO27001:2013 se puede ver de una manera más clara la aplicabilidad de la seguridad Informática y de la seguridad de la información. Aunque todos los dominios hacen parte de un sistema de gestión de seguridad de la información, hay unos ampliamente ligados a seguridad informática. Los dominios resaltados en color naranja son abarcados principalmente dentro del alcance de la seguridad informática:

Fig. 1. Dominios de ISO27001:2013.[8]

A juicio de experto, se tiene la siguiente definición para seguridad informática o IT Security: *"Es la distinción táctica y operacional de la seguridad. Es la forma como se detallan las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo"*[1] mientras que para seguridad de la información o information security se tiene la siguiente definición: *"Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información"*. [1]

En conclusión, la dirección o gerencia de la organización se encarga de marcar las directivas y/o estrategias en materia de seguridad, y mediante un plan determinar las medidas tanto técnicas como procedimentales que permiten garantizar el cumplimiento de los objetivos marcados por la política de seguridad que está dentro del alcance de la seguridad de la información. Las medidas técnicas (tácticas y operacionales) que apoyan el cumplimiento de dicha política están dentro del alcance de la seguridad informática. En la siguiente figura se ven aspectos estratégicos y operativos dentro de un marco dirección/operación:

Fig. 2. Marco de IT Security vs Information Security. [9]

III. CIBERSEGURIDAD, SGSI Y CIBERATAQUES

A. Conceptos de CSIRT y SGSI

Actualmente el concepto de ciberseguridad es de uso común para entidades gubernamentales, entidades privadas y para el ciudadano en general. Todos de una u otra forma desarrollan sus actividades del día a día a través de Internet, en muchas ocasiones careciendo del nivel adecuado en materia de seguridad, comprometiendo la información de los ciudadanos y en algunas ocasiones la seguridad nacional. En Colombia los aspectos de ciberseguridad[2] y ciberdefensa[3] son tratados en el documento CONPES 3701 de 2011[4].

En el documento CONPES 3701 están relacionadas las interacciones y cooperaciones entre distintos entes dispuestos en una estrategia de ciberseguridad organizada.

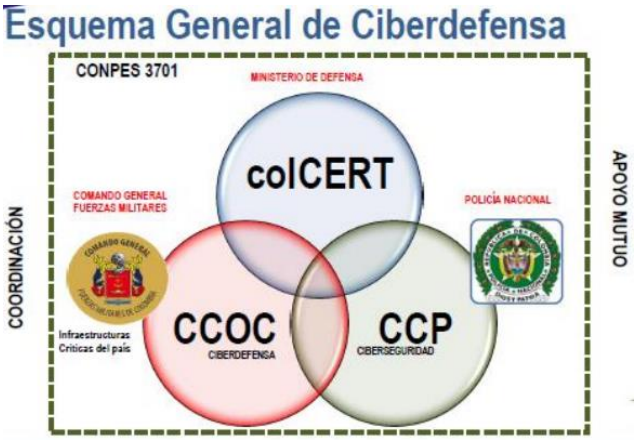

Fig. 3. Esquema de Ciberdefensa Nacional. [5]

En cualquier organización tener implementado un SGSI definido da el marco y la directriz a nivel normativo necesaria para una acción efectiva de un CSIRT[5]. A través del SGSI se promueve la cultura de seguridad y la sensibilización requerida para que los funcionarios dentro de las organizaciones puedan identificar y responder ante un incidente de seguridad [2].

Se puede entender entonces que un CSIRT efectivo requiere una madurez de otros procesos del SGSI, así mismo como el SGSI requiere un CSIRT para dar una respuesta coordinada, efectiva y documentada ante un incidente, creando una retroalimentación eficaz entre ambos.

B. Situación reciente y consecuencias de Ciberataques

A partir de un estudio realizado a nivel global, el Ponemon Institute expone como se han generado altísimos costos como consecuencia de ciberataques en el reporte global del costo de cibercrimen 2014 [3]. Este estudio permite observar como los delitos cibernéticos siguen en aumento para las organizaciones. La Figura 4 muestra el crecimiento de los costos respecto al año 2013 en 257 compañías de 7 países:

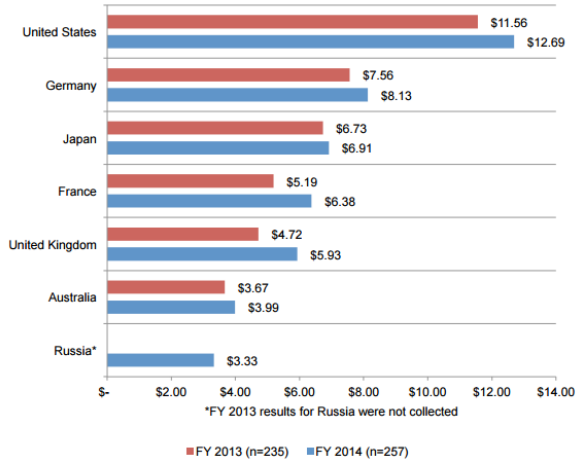

Fig. 4. Costos Totales de Cibercrimen en 7 países - 2014. Costo expresado en dólares (000,000). [3]

Se encontró que el promedio de costo anual para 257 organizaciones como punto de referencia es $7,6 millones por año (2014) respecto al costo de $7,2 millones del año anterior (2013).

El costo de la ciberdelincuencia varía según el tamaño de la organización. Los resultados revelan una relación positiva entre el tamaño de la organización y el costo anual. Sin embargo, sobre la base de empleados de las empresas, se determinó que las organizaciones pequeñas tienen un costo per-capita significativamente mayor al de organizaciones más grandes (U$1.601 frente a U$437 dólares).

Todas las industrias son víctimas de la delincuencia informática, pero en diferentes grados. El costo promedio anualizado de los delitos

[2] Capacidad del estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
[3] Capacidad del estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.
[4] Conpes 3701 Lineamientos de política para ciberseguridad y ciberdefensa.
[5] Centro de Respuesta a Incidentes de Seguridad Informática, según sus siglas en inglés.

cibernéticos parece variar según el segmento de la industria, donde las organizaciones del sector energético y de servicios financieros experimentaron sustancialmente mayores costos por delincuencia cibernética que las organizaciones del sector de medios de comunicación, ciencias de la vida y la salud.

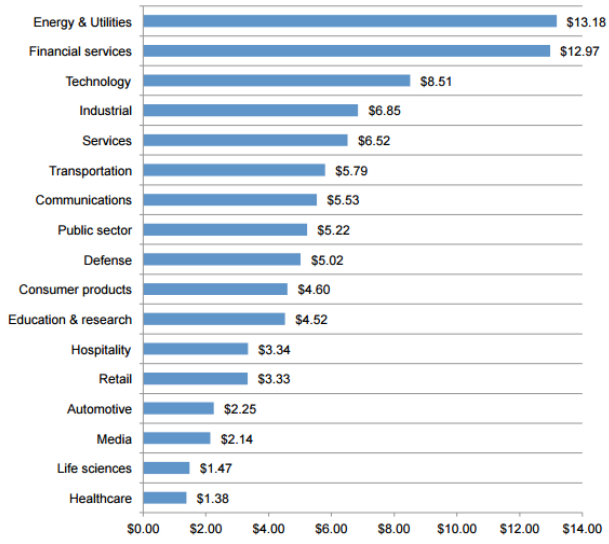

Fig. 5. Promedio de costos de Cibrecrimen por año en cada sector de la industria - 2014. Costo expresado en dólares (1,000,000). [3]

Los delitos cibernéticos más costosos son aquellos causados por actores internos con fines maliciosos, denegación de servicios y ataques vía web. Estos representan más del 55% de todos los costos asociados a delincuencia cibernética por organización sobre una base anual.

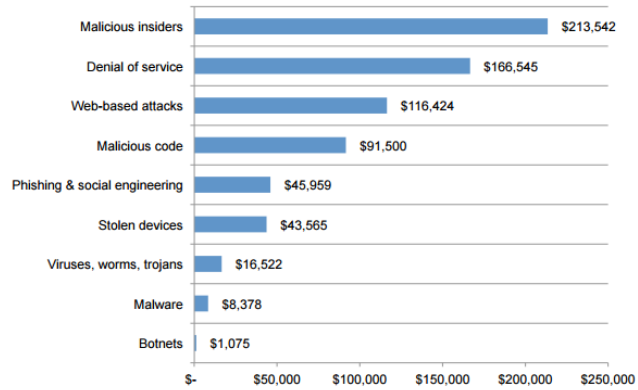

Fig. 6. Promedio de costos de Cibrecrimen por tipo de ataque - 2014. Costo expresado en dólares. [3]

Los ataques cibernéticos pueden ser aún más costosos si no se contienen rápidamente. El tiempo promedio para contener un ataque cibernético fue de 31 días, con un costo promedio de participar organizaciones de U$639.462 (U$20.758 por día). Esto representa un aumento del 23% de costo promedio estimado respecto al año anterior.

Las interrupciones en el negocio representan el costo externo más alto, seguido por los costos asociados con pérdida de información. La interrupción del negocio representa el 38% de costes externos totales por año, que incluyen los costos asociados con fallas en los procesos de negocio y pérdida de productividad de los empleados.

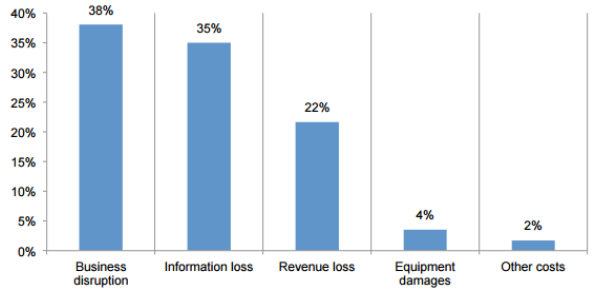

Fig. 7. Porcentaje de costo por consecuencias externas - 2014 [3]

Según el estudio internet security threat report realizado por Symantec [4] los ataques dirigidos hacen uso de técnicas sofisticadas y están diseñados con fines económicos habitualmente. Para el top 5 de vulnerabilidades de dia-0[6] se necesitaron cerca de 19 días para generar parches de seguridad y 4 días más para realizar la distribución. Debido a este comportamiento los atacantes pueden durar mucho tiempo en ser detectados al utilizar distintas vulnerabilidades de dia-0 en el mismo ataque.

[6] Vulnerabilidades no difundidas y/o conocidas.

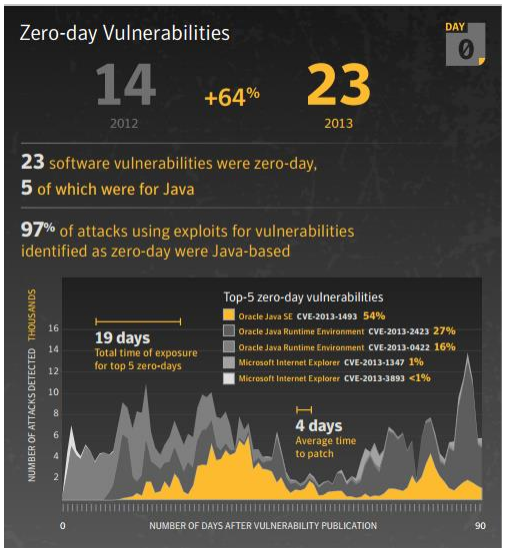

Fig. 8. Estadísticas de Vulnerabilidades dia-0[4]

En Estados Unidos durante el año 2014 varias empresas de gran renombre fueron víctimas de incidentes divulgados en todos los medios en las siguientes fechas:

1) *Enero 2014 – Target (Retail):*Robo de datos financieros de 40 millones de Clientes.
2) *Enero 2014 – Yahoo Mail (Comunicaciones):* Fueron hackeadas 273 millones de cuentas de correo.
3) *Abril 2014 - AT&T (Comunicaciones):* Personal interno hackeó durante dos semanas información confidencial de usuarios.
4) *Mayo 2014 – eBay (Retail):* Credenciales de empleados comprometidas con privilegios para ver información de usuarios.
5) *Junio 2014 – Evernote (comunicaciones):* 100 millones de usuarios fueron víctimas de un ataque de denegación de servicios.
6) *Agosto 2014 - Community Health Service (Salud):* Información clínica de 4,5 millones de pacientes comprometida a través de un ataque con malware sofisticado generado en china.
7) *Agosto 2014 - UPS (Servicios):* La información de clientes de más de 60 establecimientos fue comprometida.
8) *Agosto 2014 - Industrias de Defensa (Defensa):* Compañías dedicadas al sector fueron hackeadas intentando robar programas de defensa de jets militares.
9) *Septiembre 2014 - Google (comunicaciones):* 5 millones de credenciales de Gmail fueron comprometidas.
10) *Septiembre 2014 - Apple iCloud (Tecnología):* Hackers utilizando ataques de fuerza bruta extrajeron fotografías de celebridades.
11) *Octubre 2014 – JP Morgan Chase (Financiero):* La información de 76 millones de propietarios de hogares y 7 millones de pequeñas empresas fueron comprometidos por un ataque desplegado en Rusia.

C. Tendencias para 2015

En el año 2014 vulnerabilidades como HeartBleed y Poodle [7] pusieron en evidencia el que era considerado uno de los protocolos seguros para utilizar aplicaciones y sitios web en general.

Los analistas de seguridad de Symantec basados en estudios y tendencias del mercado tecnológico hacen las siguientes predicciones respecto a lo que viene para el 2015:

Los ataques a tecnologías IoT[8] van a hacerse comunes, sobre todo con equipos caseros para automatización como cámaras y dispositivos de control remoto de luces y equipos de calefacción entre otros.

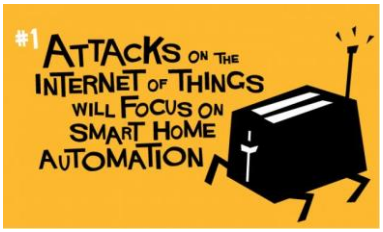

Fig. 9. Ataques IoT[6]

Los dispositivos móviles siguen siendo uno de los principales blancos de los atacantes por la información personal que contienen, además de los métodos de pago que utilizan NFC[9].

[7] Vulnerabilidades de seguridad asociadas a protocolo SSL.
[8] IoT: Internet of Things de sus siglas en Internet: Interconexión Digital de objetos cotidianos.
[9] NFC: Near-Field Communication por sus siglas en ingles.

Fig. 10. Dispositivos móviles [6]

La convergencia entre el aprendizaje a nivel de máquina y el análisis de grandes cantidades de datos serán importantes en el combate contra el cibercrimen con el fin de generar medidas proactivas.

Fig. 11. Maquinas aprendices [6]

La privacidad de la información en móviles seguirá siendo difícil de alcanzar, por la descarga de aplicaciones que se camuflan y hacen extracción de información,

Fig. 12. Móviles: Extracción de información. [6]

Los estafadores seguirán utilizando ransomware[10] con fines económicos a través de medios de pago electrónicos.

Fig. 13. Estafadores utilizan ransomware.[6]

[10] Programa informático malicioso que solicita dinero a cambio de desbloqueo de almuerzo y/o papa.

Las fugas de información constante seguirán siendo un riesgo latente.

Fig. 14. Fugas de datos[6]

Los ataques de denegación de servicio distribuido crecerán por la facilidad de despliegue y por las motivaciones de hacktivismo principalmente.

Fig. 15. Ataques DDoS[6]

Las soluciones de múltiples factores de autenticación llegaran al siguiente nivel a través de la evaluación del comportamiento del usuario.

Fig. 16. Evaluación de comportamiento de usuario [6]

Las soluciones en la nube seguirán creciendo, así como las dudas suscitadas sobre la gobernabilidad de la información, los niveles de acceso y la protección de los datos privados.

Fig. 17. Amenazas sobre soluciones en la nube.[6]

La lucha contra la delincuencia informática seguirá avanzando, a través de las estrategias colaborativas entre la industria de seguridad, los proveedores de telecomunicaciones y gobiernos de todo el mundo.

Fig. 18. Ciberseguridad y colaboración entre gobierno e industria.[6]

IV. Nuevos retos a nivel de seguridad informática: Falencias técnicas

Después de revisar conceptos, antecedentes y situaciones futuras, es claro que la seguridad de la información afrontará distintos retos. Es una tendencia general en bastantes organizaciones colombianas de diferentes sectores manejar la seguridad de la información con prácticas desacertadas que debilitan los esquemas dispuestos y exponen los eslabones más débiles a amenazas como el cibercrimen. Algunas prácticas de este tipo son:

1) Sistemas de gestión de seguridad de la información preparados solo para épocas de auditoria.
2) Procesos de papel que difieren de los objetivos de negocio y marcos normativos a los que deben estar alineados.
3) Orientación de esfuerzos únicamente a tareas estratégicas dejando de lado las iniciativas de orden táctico.
4) Destinación de recursos enfocada a gobierno de TI[11] y falta de recursos para liderazgo operacional que se ve reflejada en falencias de formación y capacitación de personal operativo.
5) Gestión de proyectos de seguridad enfocada al cumplimiento de cronogramas por encima de aseguramiento de calidad.
6) Análisis de riesgos deficientes a nivel técnico que resultan en controles mal implementados.
7) Omisión de políticas y controles para usuarios con altos privilegios que en algunas ocasiones resultan generando brechas de seguridad.
8) Procesos productivos asociados a rentabilidad que no tienen en cuenta el ROSI[12] que permite visualizar la seguridad como una inversión y no como un gasto.

Este tipo de situaciones generan falencias técnicas que difícilmente pueden ser controladas durante un incidente de seguridad.

Por ejemplo Sony, Microsoft entre otras grandes corporaciones han sufrido recientemente ataques que han afectado por días enteros sus servicios de entretenimiento, y han dejado en evidencia las falencias técnicas que poseen, a pesar de que ya han tenido situaciones similares en ocasiones anteriores. Seguramente cuentan con procesos y áreas dedicadas a gobierno y gestión de SI, pero para contener esos ataques no fue suficiente. Este tipo de incidentes generan afectación de imagen y financiera considerable para las organizaciones

V. Conclusiones

Para evitar situaciones de ciberataques sin respuestas acertadas en las organizaciones en las que cada profesional de seguridad desempeña sus labores, se deben considerar acciones correctivas:

1) Definir indicadores claros en materia de TI, que permitan ajustar las herramientas de seguridad informática basadas en su estado

[11] TI: Tecnologías de la Información
[12] ROSI: Retorno sobre la inversión en Seguridad, extensión del conocido concepto financiero ROI.

actual y el estado deseado.

2) Generar la sensibilización y capacitación sobre conceptos de seguridad de la información para todos los actores dentro de una organización, de forma similar en la que se generan las sesiones de prevención de riesgos laborales.

3) Destinar los recursos que se puedan para implementar y/o incluir controles tecnológicos basados en nuevas herramientas de protección perimetral de nueva generación y análisis de malware avanzado y amenazas persistentes que permitan estructurar un CSIRT con una mayor efectividad.

4) Contar con un director de seguridad informática y un gerente de seguridad de la información que puedan interactuar con el fin de alinear la estrategia (seguridad de la información) con las acciones técnicas (seguridad informática).

VI. REFERENCIAS

[1] Cano Jeimy J. "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes" , ISACA, 2011.[Online].Disponible:http://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx

[2] Ciberataques y ciberamenazas. GITS Informática, [Online]Disponible:http://www.gitsinformatica.com/ciberataques.html

[3] Ponemon Institute Research Report. 2014 Global Report n the Cost of Cyber Crime. Octubre 2014.

[4] Symantec Corporation. Internet Security Threat Report. Vol 19. April 2014. [Online]Disponible: http://www.itu.int/en/itu_d/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

[5] Huertas Leonardo. 1er Foro de Seguridad y Defensa Cibernética: Una estrategia de país: Visión del Sector Defensa en Ciberseguriad. 27 y 28 de Mayo de 2014. [Online]Disponible:https://device.virtual.uniandes.edu.co/images/forosisis/foros/fsi1/2Leonardo-Huertas.pdf

[6] Symantec Connect. The Threat Landscape in 2014 and Beyond: Symantec and Norton Predictions for 2015, Asia Pacific & Japan. 25 de Noviembre de 2014. [Online] Disponible:http://www.symantec.com/connect/blogs/threat-landscape-2014-and-beyond-symantec-and-norton-predictions-2015-asia-pacific-japan .

[7] Walters, Riley. Cyber Attacks on U.S. Companies in 2014. The Heritage Fundation. [Online].Disponible: :http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014 .

[8] González, Dulce. ISO-27001:2013 ¿Qué hay de nuevo? [Online].Disponible:http://www.magazcitum.com.mx/?p=2397

[9] ¿Seguridad Informática o Seguridad de la Información? [Online].Disponible:http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Autor

Edgar Mauricio Garantivá Ortiz
Ingeniero Electrónico, Universidad de Cundinamarca
Estudiante candidato a Grado de Especialización en Seguridad Informática, Universidad Piloto de Colombia
2015