UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“SGSI BAJO EL MARCO NORMATIVO ISO 27001 EN EL PROCESO DE CONTROL DE ACCESOS PARA UNA EMPRESA: una revisión científica de los últimos 9 años”

Trabajo de investigación para optar al grado de:

Bachiller en Ingeniería de Sistemas Computacionales

Autor:

Elisban Enrique Ríos Miranda

Asesor:

Mg. Ing. Carlos Ramos Gonzales

Lima - Perú

2019

DEDICATORIA

A mi madre de quien aprendí a ser perseverante, a mi padre que con su ayuda y fortaleza me educó con mucha sapiencia, a mi novia quien me da la fuerza y me motiva para seguir adelante, a mis amistades que con su apoyo y la manera de compartir conocimiento me llevó a esforzarme cada vez más.

AGRADECIMIENTO

A las personas que me guiaron y aconsejaron en la elaboración de este trabajo de investigación de la cuales me siento orgulloso y bendecido.

A mi tutor que con su experiencia y concejos brindados pude realiza esta investigación de manera correcta.

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En resumen, el trabajo de investigación se basa en el análisis de una de las normativas de prevención más conocidas contra ataques informáticos, y su implementación en una empresa.

Mostraremos de forma gráfica y estadística la información donde se detalla los métodos y prácticas que se usaron para contrarrestar los ataques informáticos que en estos últimos años aumentaron exponencialmente.

PALABRAS CLAVES: Seguridad de la información, SGSI, ISO 27001, Auditoria Informática y Herramientas de Seguridad de la Información.

CAPÍTULO I. INTRODUCCIÓN

Los ataques cibernéticos evolucionan y no se detienen con el pasar de los años y a su vez la evolución de la seguridad se moderniza y mejora, teniendo como resultado una carrera entre el bien el mal, donde uno ya no puede estar seguro hasta qué punto nuestra información es privada y segura, por ello, evolucionar es una obligación en las empresas de hoy. Una de las prácticas más importantes es la implementación de controles para asegurar la información, y una de las más conocidas es el SGSI (Sistema de Gestión de Seguridad de la Información) bajo la normativa ISO 27001 que tiene un total de 14 controles dedicados a medidas de "Control de Accesos".

La implementación de políticas de control de accesos es necesaria porque ayudaría a establecer que usuarios tienen accesos y que usuarios no, a los servicio o recurso que se tienen en la empresa. La no implementación de esta normativa ocasionaría que los usuarios tengan acceso a servicios o recursos que no le corresponde, lo que podría ocasionar la perdida de la información o estar propensos a ataques informáticos.

> "¿Cómo puede un usuario indicarle a un sistema que él está autorizado a usar determinados servicios computacionales? ¿Cómo puede el propietario de un sistema marginar a los usuarios no autorizados, mientras provee acceso cómodo a los usuarios autorizados? El trasfondo a estos dos interrogantes es: con las fallas de seguridad en los diferentes protocolos y aplicaciones, y con un entorno de Internet público hostil, debería existir algún mecanismo mediante el cual un usuario autorizado pueda usar los recursos a los que tiene derecho, dejando a los usuarios no autorizados sin acceso. Éste es el propósito de la autenticación, autorización y auditoría" (Arana, 2013).

"Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CID) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario.
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
- Permitir a un atacante hacerse pasar por otra entidad.
- Permitir a un atacante realizar una negación de servicio" (Symantec, 2017).

El objetivo de esta investigación es identificar los beneficios que se generan cuando se implementa la SGSI bajo la normativa ISO 27001 en un proceso de control de accesos, analizando las mejoras en el tratamiento de la Información para así impedir la perdida de información y contrarrestar ataques informáticos.

Sobre la normativa ISO/IEC 27001:2013 la cual tiene 14 dominios 35 objetivos de control y 114 controles, teniendo en cuenta esta información nosotros estaremos enfocados en el dominio "Control de Acceso" la cual tiene 14 controles, la norma no obliga a usar todos los controles solo los que más se adapten a la empresa, pero si obliga a cumplir los controles que se escogieron.

La seguridad de la información se basa en una serie de procedimientos, en el uso correcto de la información y mantener concientizado a los usuarios. Debemos saber que la evolución es necesaria, aún más en estos tiempos donde nuestra información se encuentra extendida en entornos conectados a Internet y entender que la perdida de la información puede ocasionar daños cuantiosos. Si nos damos cuenta cómo ha evolucionado la tecnología, tanto las herramientas para protegernos como las herramientas para realizar ataques, nos

preguntamos: ¿Cuál es el impacto de la implementación de la SGSI bajo la normativa ISO 27001 en el proceso de control de accesos en una empresa?

CAPÍTULO II. METODOLOGÍA

Esta investigación es una revisión científica que nos dará una visión de cuáles son sus beneficios de la implementación de la norma, comparados con no implementarlo y como se puede reducir el riesgo de ataques informáticos o perdida de información, utilizando la información encontrada como resultado de las búsquedas de las palabras claves: Seguridad de la información, SGSI, ISO 27001 y Control de Accesos.

Como estrategia de búsqueda se utilizó las palabras claves y conectores: "Seguridad de la Información", SGSI, "ISO 27001",27001 y "control de acceso".

Esta búsqueda se realizó en las bases de datos de: Redalyc, Ebsco y Scielo, utilizando sus mismos buscadores y en algunos casos se usó Google Académico.

Para el análisis se examinará los documentos con una antigüedad no mayor de 9 años teniendo como corte los documentos publicados a partir del 2010. Se utilizarán datos anteriores de hace 9 años para la revisión de conceptos y revisión de los primeros reportes de implementación de seguridad informática, los posteriores desde el 2015 será la información actualizada y de proyección al futuro, tanto en inglés como en español.

Nuestro criterio de búsqueda incluirá cualquier documento de corte empresarial de cualquier parte del mundo, se incluirá estudios, libros, revistas y tesis sólo dedicados a empresas teniendo en cuenta que las empresas son las que almacenan la mayor información importante, se excluirá búsquedas que se enfoquen sólo en comercial o ventas.

CAPÍTULO III. RESULTADOS

Como resultado de la búsqueda de las palabras claves se obtuvo para analizar una cantidad suficiente de información, sin embargo, es necesario descartar información de revistas tecnológicas, libros, publicaciones, trabajos monográficos, tesis, etc.

Se obtuvieron acceso a 443 documentos entre libros, publicaciones científicas y tesis de los cuales nos quedamos con 19 de ellos para plasmar la base de nuestra investigación, 7 de ellos responden a la pregunta, realizando la búsqueda en los portales web de Ebsco, Redalyc, Scielo y Google Académico, se excluyó documentos que mostraban información de otros temas similares, temas alejados de nuestro objetivo y otros que no contenían información relevante para la investigación. El siguiente cuadro da los resultados de búsquedas en los últimos 9 años:

Tabla 1: Resultados de búsqueda con la palabra: "ISO 27001" o "27001".

Fuente:	Cantidad de artículos	Cantidad seleccionada	Fechas	Idioma	¿Responde a la pregunta?
Ebsco.com	0	0	2011-2019	Español	-
Ebsco.com	3	0	2011-2019	Inglés	-
Redalyc.org	15	8	2011-2019	Español	3
Redalyc.org	4	0	2011-2019	Inglés	0
Scielo.org	5	4	2011-2019	Español	1
Scielo.org	0	0	2011-2019	Inglés	0

Fuente: (https://scielo.org/; https://www.redalyc.org/; https://www.ebsco.com/), Consultado el: 22 de octubre del 2019.

Tabla 2: Resultados de búsqueda con la palabra: SGSI.

Fuente:	Cantidad de artículos	Cantidad seleccionada	Fechas	Idioma	¿Responde a la pregunta?
Ebsco.com	0	0	2011-2019	Español	-
Ebsco.com	0	0	2011-2019	Inglés	-
Redalyc.org	15	2	2011-2019	Español	2
Redalyc.org	1	1	2011-2019	Inglés	0
Scielo.org	2	1	2011-2019	Español	1
Scielo.org	0	0	2011-2019	Inglés	0

Fuente: (https://scielo.org/; https://www.redalyc.org/; https://www.ebsco.com/), Consultado el: 22 de octubre del 2019.

Tabla 3: Resultados de búsqueda con la palabra: "Control de Acceso".

Fuente:	Cantidad de artículos	Cantidad seleccionada	Fechas	Idioma	¿Responde a la pregunta?
Ebsco.com	0	0	2011-2019	Español	-
Ebsco.com	0	0	2011-2019	Inglés	-
Redalyc.org	375	2	2011-2019	Español	0
Redalyc.org	6	0	2011-2019	Inglés	0
Scielo.org	15	1	2011-2019	Español	0
Scielo.org	2	0	2011-2019	Inglés	0

Fuente: (https://scielo.org/; https://www.redalyc.org/; https://www.ebsco.com/), Consultado el: 22 de octubre del 2019.

Se analizó los documentos y se concluye que una de las tácticas de seguridad que más implementan en las empresas es la de "Control de Accesos" en un 86.96% de las empresas.

Tabla 4. Tácticas para la seguridad de la información - Empresas (Elaboración propia).

Tácticas	F. Muestreo	Uso de las tácticas
Auditorias	20	86.96%
Control de accesos	20	86.96%
Encriptación	18	78.26%
Antivirus y Antimalware	17	73.91%
Respaldo de información	17	73.91%
seguridad perimetral	16	69.57%
Filtrado de contenido Web	15	65.22%
Redes privadas virtuales	14	60.87%
Contraseñas seguras	11	48.70%
Hacking	2	8.70%
Inteligencia Artificial	1	4.35%

Muestreo de alrededor de un total de 19 muestras de la búsqueda entre tesis y revistas científicas.

Se revisó los resultados indicados en los documentos y todos encuentran muchos beneficios tales como: Reducción de Incidencias, se aplica a cualquier tamaño de empresa, brinda las pautas para las auditorias y mejoras y reducción de riesgos.

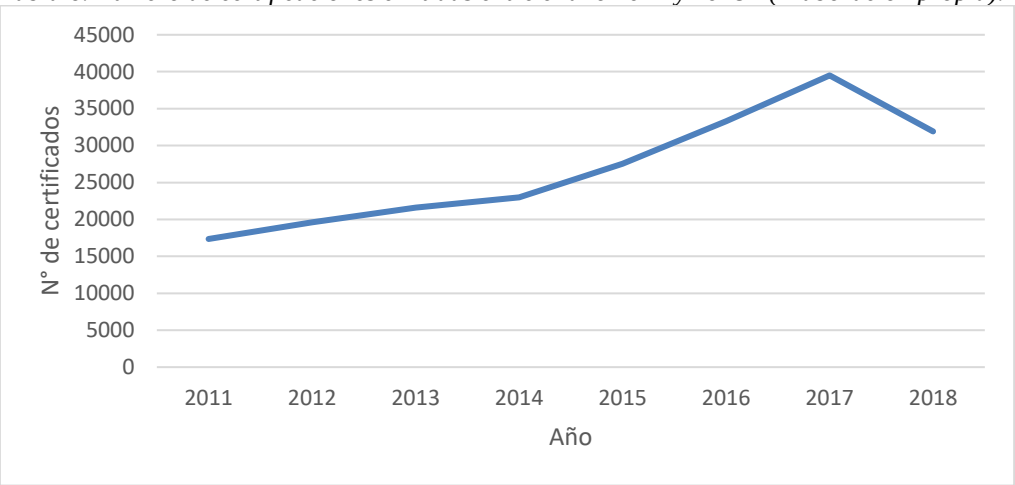
Tabla 5. Costo - Beneficio en la implementación de ISO 27001 en las empresas (Elaboración propia).

Beneficios:	**Costos:**
✓ Reduce los riesgos de la seguridad de la información. ✓ Reduce la probabilidad y el impacto de los incidentes de seguridad. ✓ La certificación de un estándar internacional. ✓ Ventajas de marketing /marca. ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial. ✓ Enfoque coherente y estructurado. ✓ Evaluación integral de riesgos. ✓ Focaliza el gasto en seguridad de la información donde produce mayor ventaja. ✓ Los clientes tienen acceso a la información a través medidas de seguridad. ✓ Los riesgos y sus controles son continuamente revisados. ✓ Posibilidad de integrarse con otros sistemas de gestión ISO. Confianza y reglas claras para las personas de la organización. ✓ Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad. ✓ Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.	• Gestión de proyectos, recursos del proyecto. • El cambio organizacional requiere de recursos de la organización. • Diseño, desarrollo, pruebas, implementación. • Certificación y visitas de seguimiento. • Operación y mantenimiento en curso.

Muestreo de alrededor de un total de 19 muestras de la búsqueda entre tesis y revistas científicas.

También se elaboró un cuadro donde se aprecia la cantidad de certificados emitidos en ISO 27001 en durante desde el año 2011 al 2018, donde se puede apreciar el auge de la demanda de la certificación, salvo el año 2018:

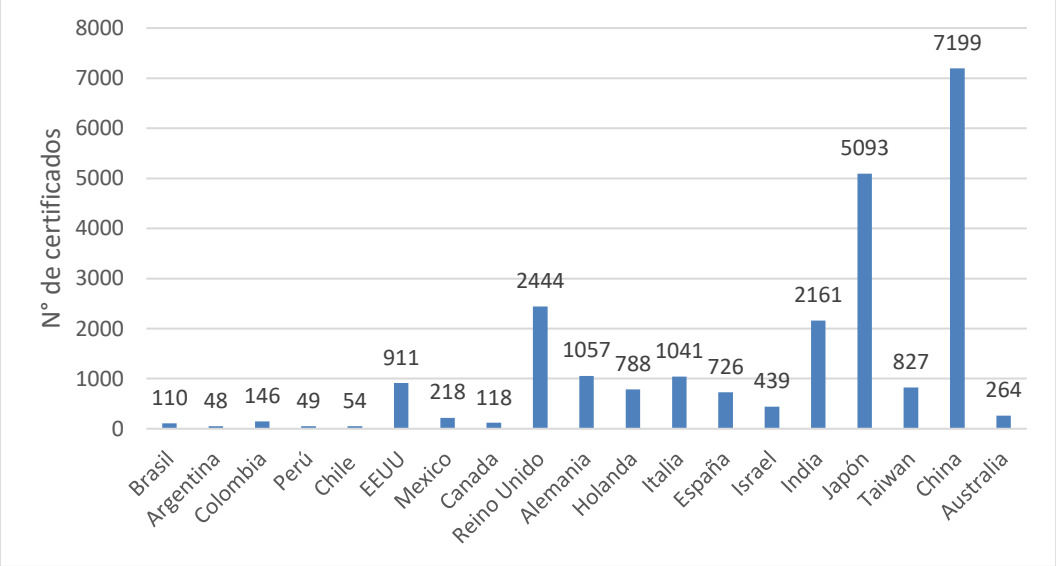
Tabla 6. Numero de certificaciones emitidas entre el año 2011 y 2018 - (Elaboración propia).



Fuente: (https://www.iso.org/), Consultado el: 22 de octubre del 2019.

Se elaboró un cuadro donde se halla la cantidad de empresas certificadas en ISO 27001 en durante el año 2018, en las principales ciudades del mundo:

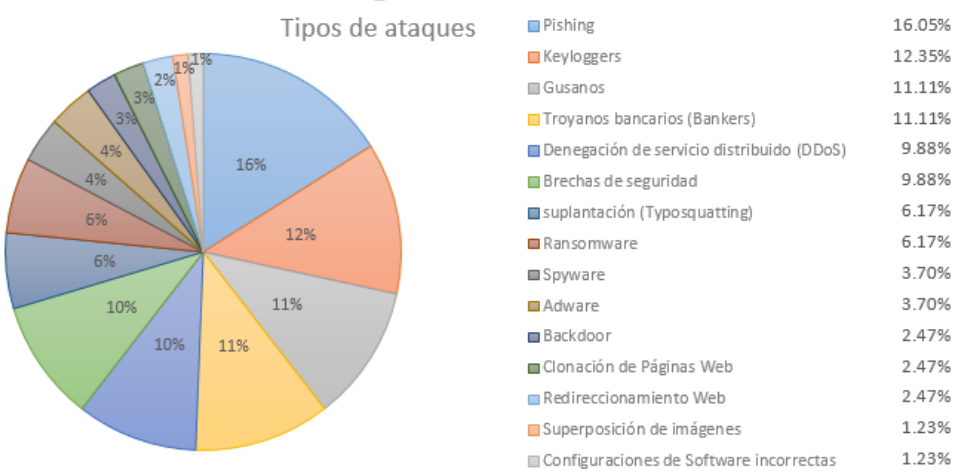
Tabla 7. Numero de certificaciones emitidas en el año 2018 por países - (Elaboración propia).



Fuente: (https://www.iso.org/), Consultado el: 22 de octubre del 2019.

En cuanto a las prácticas más usadas para perpetrar ataques son: Pishing, Keyloggers, Gusanos, Troyanos bancarios y últimamente DDoS (Denegación de Servicios); este último está siendo usado con mayor frecuencia en estos dos últimos años.

Figura 1. Los tipos ataques registrados según el porcentaje de uso (Elaboración propia).



Lista de los tipos de los tipos de ataques obtenidos de la búsqueda entre tesis, libros y revistas científicas.

Adicionalmente se halló información e igual de importante ya que surge en estos últimos años el término Ciberataque y Ciberseguridad. Los ciberataques con mayor número de afectados hasta el momento son:

Figura 2. Los mayores ataques registrados en orden de la gravedad de los daños (Elaboración propia).

Tipo de Ataque	afectados	fecha	descripción	Solución o como se contrarresto
DDoS (Ataque por denegación de servicios)	28 millones de personas	05/03/2018	La plataforma de desarrollo *GitHub* fue saturada hasta que recibió mayor trafico del que puede gestionar 1,35 terabits por segundo, no estaba accesible por 10 minutos. A nivel mundial.	El software Prolexic, comenzó a desviar el tráfico para separar los paquetes de información de los que eran simplemente usuarios que intentaban ingresar.
Ransomware: WannaCry	360 000 computadoras atacadas	12/05/2017	WannaCry uso una vulnearbilidad de Windows, para "secuestrar" encriptando los documentos y exigiendo al usuario un pago de 300 dolares para decifrar los archivos. 180 paises.	El malware intentaba conectarse a un dominio no registrado, si no lo lograba, cifraba el equipo; si lo lograba, se detenía. Un experto en seguridad registró el dominio y el ataque se detuvo.
Malware: Petya y NotPetya	Aproximadamente 80 Empresas	27/06/2017	Usando el mismo método que el WannaCry y ayudandosé de una debilidad de protocolos para compartir en red, secuestró Disco Duros (MBR) y se propagó en redes, afectando a entidades de Ucrania, Rusia y España.	Dos ingenieros registraron el dominio y el ataque se detubo, la misma solución aplicada al WannaCry
3° ciberataque a Yahoo	32 millones de cuentas	15/02/2017	Robo de información de usuarios, el metodo de utilización de cookies usado por dos años.	Las cookies fueron invalidadas.
Ataque a CloudBeed	sin calcular	27/02/2018	Se filtraban los datos personales de usuarios de millones de plataformas existentes en la base de datos de la compañía de servicios web y seguridad CloudFare, incluyendo contraseñas, direcciones IP, cookies, datos y chats privados. Las principales aplicaciones afectadas fueron Uber, Fitbit, Reddit o Medium.	Sin solución

Información de ataques recientes extraída de revistas científicas de este año 2019 (Elaboración propia).

La calidad se limita al desarrollo de acciones correctivas sin la identificación de las causas raíces que originan los problemas y la adaptación de medidas tales como el SGSI, orientadas

a la eliminación preventiva de dichas causas (Arévalo, 2015); la información está en la memoria del personal con experiencia, exponiéndose a la pérdida de información esencial en el caso de despido del empleado (Murphy, 2013).

CAPÍTULO IV. CONCLUSIONES

Concluimos que la SGSI más usada es la normativa ISO 27001, utilizada para reducir riesgos informáticos y contrarrestar los ataques informáticos.

La implementación de la normativa ISO 27001 en el proceso de control de accesos, según el cuadro costo beneficio (*Tabla 5*) estaría dándonos mayores beneficios comparadas con los costos de implementación y mantenimiento.

La seguridad de la información en estos últimos años ha evolucionado de la misma manera y casi en paralelo con los ataques informáticos (*figura 2*) realizar mejoras en el proceso de control de accesos en las empresas es unos de los principales puntos por donde se debe comenzar a implementar la normativa ISO 27001 y porque no, en todos los procesos de la empresa.

REFERENCIAS

Lievano, F. (2016). *Sistema de Gestión de la Seguridad de la Información*. Trabajo de Fin de Máster. Universidad Abierta de Cataluña, Barcelona, España.

Instituto Nacional de Ciberseguridad (2016). *Protección de la Información*. Madrid, España: INCIBE.

C, Ormella. (2009). *¿Seguridad informática vs Seguridad de la información?* Revista Carlos Ormella Meyer y Asoc, (1 - 3).

C, Ormella. (2014). *Normas ISO de Seguridad de la Información*. Revista Carlos Ormella Meyer y Asoc, (2 - 12).

Denning, J. y Denning, E. (2016). Las dificultades de la ciberseguridad. *Investigación y ciencia - Edición española de SCIENTIFIC AMERICAN,* N° 481.

Soriano, M. (2012). *Seguridad en Redes y Seguridad de la Información*. Praga, República Checa: Improvet.

Bravo, O. y Chávez, R. (2017, octubre). *Seguridad de la Información en Ecuador*. Deloitte, 4-20.

Asqui, R. (2018). *Análisis Comparativo en Términos de Seguridad de la Información y Rendimiento entre Sistemas Operativos Android e IOS en Teléfonos Móviles.* (Proyecto de Titulación) Universidad De Guayaquil, Ecuador.

Castro, A., Cipriano, M., García, E., Liporace, J., Maiorano, A., Malvacio, E. y Tapia, N. (2018). *Herramientas de Criptoanálisis*. Proyecto de estudio. Instituto Universitario del Ejército, Buenos Aires, Argentina.

González, S. y Julián, A. (2016). *Análisis y Diseño de Estrategias para Incrementar la seguridad de las contraseñas*. Tesis para obtener el título de Ingeniero en Comunicaciones y Electrónica. Instituto Politécnico Nacional - Escuela Superior de Ingeniería Mecánica y Eléctrica, Ciudad de México, México.

Quevedo, F. Y Sesme, J. (2018). *Análisis de Vulnerabilidades en los Servicios Active Directory, DNS Y DHCP Instalados en los Sistemas Operativos Windows Server (2008, 2012, 2016) Utilizando Herramientas de Test de Intrusión*. Proyecto De Titulación para la Obtención del Título de Ingeniero en Networking y Telecomunicaciones. Universidad De Guayaquil, Guayaquil, Ecuador.

Castellanos, W. (2010, diciembre). *Evolución de la seguridad de la información. Una revisión desde la Perspectiva de Negocio*. Bogotá, Colombia.

Cedeño, R. (2018, marzo). *La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar*. Trabajo de investigación presentado en el I Congreso Internacional Multidisciplinario de Educación Superior. Miami, Estados Unidos.

Cadena, A. (2017). *Riesgos de Seguridad Asociados al uso de Dispositivos Móviles Personales (SmartPhone - Android) en Entornos BYOD - Bring Your Own Device*. Trabajo Fin de Máster. Universidad Internacional de la Rioja, Bogotá, Colombia.

Murga, W. (2018). *Sincronización de los Sistemas de Investigación de la DIRINCRI con Recursos Móviles (Smartphone).* Tesis para optar el Título Profesional de Ingeniero Redes y Comunicaciones. Universidad Tecnológica del Perú, Lima, Perú.

Alonzo, S. (2014). *Seguridad de la información*. Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, Guatemala. (pp7- pp15)

Giménez, J. (2014). *Seguridad en Equipos Informáticos*. Málaga, España: IC Editorial.

Marín, M. (2012, marzo). *La Importancia de la Seguridad Informática en las Empresas*. Universidad San Martin de Porres. Lima, Perú.

Gené, J., Gallo, P. y De Lecuona, I. (2018, enero). *Big data y seguridad de la información*. Universidad de Barcelona, 50, 1-3.

Rodríguez, A. y Cruz, J. (2016). *Modelo de un Sistema de Gestión de la Seguridad de la Información Aplicada a una Empresa de Software*. Tesis para optar al título de Ingeniero en Telemática. Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Marcela, D. y Martínez, J. (2016). *Propuesta de un Sistema de Gestión de la Seguridad de la Información para Entidades Dedicadas al Servicio de Outsourcing de IT*. Tesis para optar al título de Ingeniero en Telemática. Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Ramos, B. y Ribagorda, A. (2004). *Avances en Criptología y Seguridad de la Información*. Madrid, España: Diaz de Santos.

Pabón, J. (2010). *La Criptografía y la Protección a la Información Digital*. Revista La propiedad Inmaterial, 14, 10-32.

Álvarez, R., Tortosa, L., Vicent, J. y Zamora, A. (2009, junio). *A Non–abelian Group Based on Block Upper Triangular Matrices with Cryptographic Applications*, International Symposium Applied Algebra Algebraic Algorithms and Error–Correcting Codes. Tarragona, España.

Velasco, A. (2008). *El Derecho Informático y la Gestión de la Seguridad de la Información una Perspectiva con Base en la Norma ISO 27001*. Revista de Derecho Articulo de divulgación. 29, 5-31.

Taranilla, C. (2018). *Criptografía: Los Lenguajes Secretos a lo Largo de la Historia*. León, España: Almuzara.

Díaz, G., Alzórriz, I. Sancristóbal, E. y Castro, M. (2014). *Procesos y Herramientas para la Seguridad de Redes*. Madrid, España: UNED.

Mina. L. (2015). *Auditoria de Seguridad de la Información e Infraestructura de TI, al Área de TI de la Empresa de Energía de Arauca ENELAR E.S.P. del Departamento de Arauca*. Universidad Cooperativa De Colombia, Arauca, Colombia.

García, J. (2017). *Auditoría al Sistema de Gestión de Seguridad Información en el Proceso de Desarrollo de Software de acuerdo con la Norma ISO/IEC 27001:2013 en la Empresa IT Stefanini Colombia*. Trabajo de grado para optar por el título

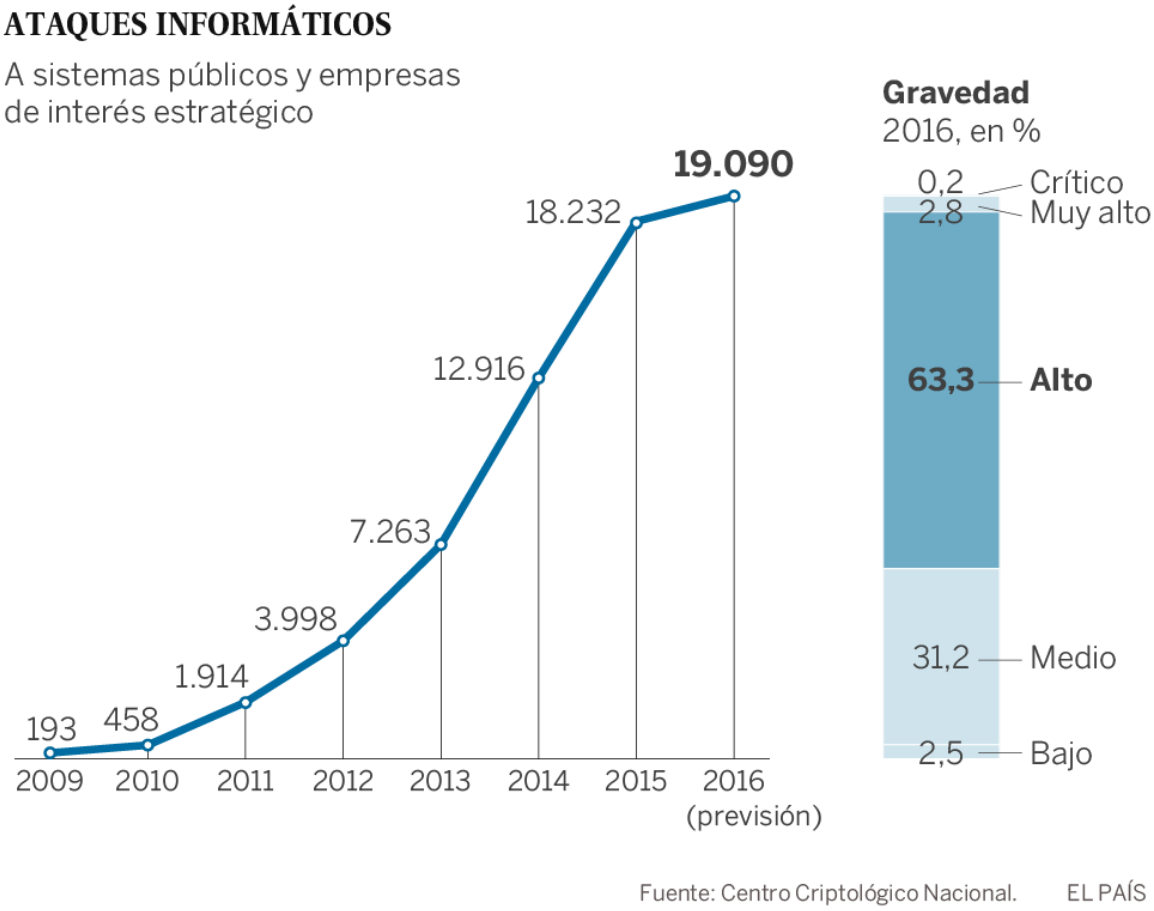
de especialista en seguridad Informática. Universidad Nacional Abierta y a Distancia, Bogotá, Colombia.

Muñoz, M. (2015). *Guía de implantación de un SGSI basado en la norma: UNE-ISO/IEC 27001*. Trabajo de final de la carrera: Ingeniería Técnica Informática de Sistemas. Universidad Abierta de Cataluña, Barcelona, España.

Mieres, J. y Borghello, C. (2008). *Robo de Información personal online*. Revista ESET, 3-13.

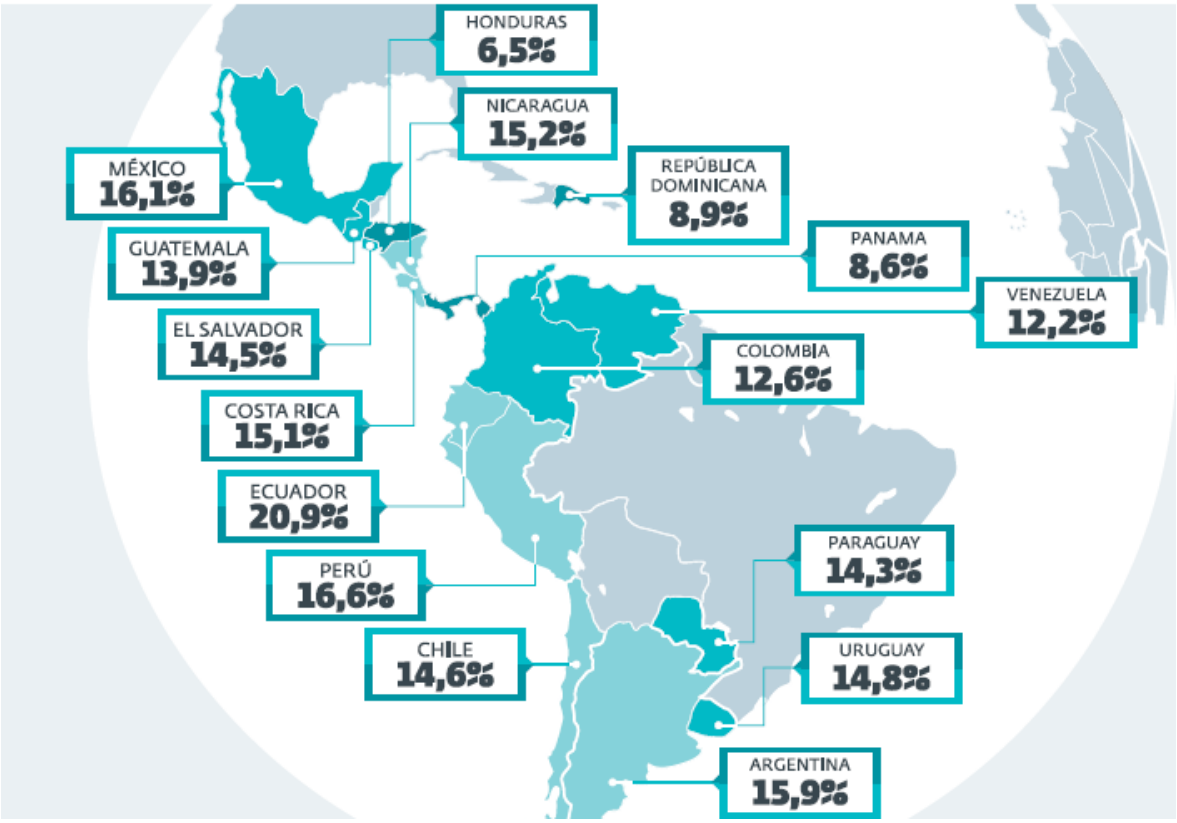
APWG (2018, 15 de mayo). Phishing Activity Trends Report. Unifying the Global Response To Cybercrime. Recuperado el 15 de Julio de 2018, de la página web: https://www.antiphishing.org/resources/apwg-reports/

ANEXOS


ATAQUES INFORMÁTICOS
A sistemas públicos y empresas de interés estratégico
193
458
1.914
3.998
7.263
12.916
18.232
19.090
2009
2010
2011
2012
2013
2014
2015
2016 (previsión)
Gravedad
2016, en %
0,2 Crítico
2,8 Muy alto
63,3 Alto
31,2 Medio
2,5 Bajo
Fuente: Centro Criptológico Nacional.
EL PAÍS

Estadísticas de mayor infección de malware y phishing en la región

Según la empresa ESET en su informe "Eset Security Report Latinoamérica 2017" (ESET, 2017b) indica que el Perú se encuentra entre los países con más incidentes de Phishing en la región:



CONTROLES: SOBRE CONTROL DE ACCESO DE LA ISO/IEC 27001/27002

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Acceso a las redes y a los servicios de red.

9.2 Gestión de acceso de usuario.
- 9.2.1 Registro y baja de usuario.
- 9.2.2 Provisión de acceso de usuario.
- 9.2.3 Gestión de privilegios de acceso.
- 9.2.4 Gestión de la información secreta de autenticación de los usuarios.
- 9.2.5 Revisión de los derechos de acceso de usuario.
- 9.2.6 Retirada o reasignación de los derechos de acceso.

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información secreta de autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Sistema de Gestión de contraseñas.
- 9.4.4 Uso de utilidades con privilegios del sistema.
- 9.4.5 Control de acceso al código fuente de los programas.