UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

LA CONFIDENCIALIDAD, LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS EN LAS REDES DE TELECOMUNICACIONES: EL CASO MEXICANO

TESIS

Que para obtener el título de

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A

ALAIN SILVERS SALAS VÁZQUEZ

DIRECTOR DE TESIS

MTRO. ENRIQUE OCTAVIO DÍAZ CERÓN

Ciudad Universitaria, Cd. Mx., 2016.

AGRADECIMIENTOS.

Esta tesis se la dedico a Eva Vázquez, quien con su cariño, paciencia y amor ha logrado levantarme en los momentos más difíciles de mi vida personal y académica. Así mismo, por haberme guiado a lo largo de mi vida, por ser mi apoyo, mi luz y mi camino. Madre, todos los días agradezco el tenerte conmigo.

A Silverio Salas, gracias por tu apoyo y por haberme dado las herramientas necesarias para poder realizar mis estudios, agradezco los consejos que me diste para enfrentar la adversidad y salir adelante. Padre, gracias por ayudarme a cumplir mis sueños.

A Kareen Salas, gracias porque siempre has confiado y creído en mí; además, por todo el apoyo brindado cuando más lo he necesitado. Hermana, gracias por llenar mi vida de alegría y amor.

A Dios, por haberme dado a tan magnífica familia, además, de haberme puesto en el camino a todos los amigos que hicieron que la universidad fuera una excelente experiencia.

Al Mtro. Enrique Díaz Cerón, gracias por el apoyo, confianza y tiempo que me brindó para desarrollar la tesis, además, por la paciencia, atención y dedicación en la realización del trabajo.

A la U.N.A.M y la Facultad de Ingeniería, que fueron mi propósito desde que quise estudiar una carrera, han sido todo lo que pude haber imaginado; en ocasiones me pregunté por qué tenía que irme de aquí, pero ahora sé que todavía quedan experiencias que solo el mundo puede ofrecer.

Este es mi legado.

Índice de figuras.

Índice de tablas.

INTRODUCCIÓN.

La confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones modernas están comprometidas en muchas formas, las cuales, algunas están en nuestro control y otras no pueden estarlo. En este mundo cada vez más móvil, las medidas de seguridad en las redes de telecomunicaciones tradicionales enfocadas en plataformas de escritorio, pasan a ser más relevantes al nuevo entorno mundial de las tabletas y teléfonos inteligentes.

La estructuración de la red y la construcción del ciberespacio son características fundamentales del ambiente del siglo XXI, permite imaginar un mundo donde la interacción entre los individuos deja de estar influenciada por barreras geográficas y da acceso a otros requerimientos como la disponibilidad y el tiempo de acceso a la red de la información.

No cabe duda que el ciberespacio es un entorno virtual; donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Se ha convertido en un nuevo entorno que, junto con los tradicionales de tierra, mar, aire y espacio, es el medio donde se desarrollan las actividades económicas, productivas y sociales de las naciones modernas.

Debido al constante cambio del entorno de las redes de telecomunicaciones, organizaciones y compañías de todos los tamaños y niveles, se enfrentan a retos para mantenerse al frente del cambio que representan las amenazas modernas y emergentes. Estas deben adoptar programas de seguridad de redes, desarrollar políticas de red y seguridad, además de detectores de amenazas emergentes.

Como la tecnología ya no es exclusiva de las grandes empresas, organizaciones o agencias del gobierno, la red global de información se ha convertido en dominio de todos, desde conglomerados internacionales de millones de dólares hasta niños de primaria.

En la era de la información se generan cada vez más dependencias derivadas del funcionamiento en red. Por tanto, no es posible asegurar el desarrollo y el bienestar social, sin garantizar la seguridad y protección de las infraestructuras esenciales para el funcionamiento normal de la vida en sociedad.

La respuesta de la industria a las tecnologías desarrolladas era la típica adición de *hardware,* o la integración de paquetes de *hardware-software* para hacer frente a las amenazas identificadas. Esto dio lugar a un constante estado de costosas actualizaciones que añadieron complejidad a la red, aumentó la carga de trabajo y la dificultad para los administradores de la red y los usuarios finales, agravando el equilibrio entre la seguridad y la productividad. Y debido a que los nuevos productos no siempre fueron capaces de integrarse completamente en la red, esto dejo puntos ciegos que las amenazas han explotado sin ser detectados.

Basta un descuido para violar potencialmente la integridad y las redes de información. Por lo general, muchas personas fácilmente se dejan llevar por una falsa sensación de seguridad sobre la efectividad de códigos de accesos, verificación de identidad y políticas sobre el uso de las Tecnologías de la Información y la Comunicación. Debido a este error humano, ha sido importante asegurar que el esquema de la seguridad de la red sea claro y simple para los administradores de la red y los usuarios, con la necesaria complejidad para identificar, detectar o contener amenazas.

Con la explosión de las redes sociales como fuente primaria de conectividad; para la mayoría de la gente, direccionar las amenazas ocultas desde los sitios de las redes sociales ha sido un reto continuo, y más con las plataformas que continúan compartiendo e integrando dispositivos. América latina y el Caribe tenían 14 millones de usuarios de internet en el 2013, de ellos, casi 95% utilizaron sitios de redes sociales de forma activa y con mayor tiempo de uso.[1]

Hacia el año 2013, las violaciones de datos a gran escala fueron noticias destacadas en los medios internacionales, pusieron de manifiesto que los delitos cibernéticos siguen proliferando, y que la amenaza sigue acechando a gobiernos, empresas y usuarios finales. Además, no es fácil medir los costos por parte de los delitos cibernéticos, por lo que se estima que subieron, por lo menos, a 113,000 millones de dólares. Solamente en México, los costos de los delitos en las redes se cree que alcanzaron los 3,000 millones de dólares.[2]

A nivel mundial en el 2013, una de cada ocho violaciones de datos dio como resultado la exhibición de 552 millones de identidades, lo que permitió a los delincuentes acceder a información sobre identidad, domicilios particulares, historias clínicas, números de teléfono, información financiera y direcciones de correo electrónico.[3] Lo dicho anteriormente, fue consecuencia, en parte, de una débil actitud de los usuarios finales junto con la mayor adopción de dispositivos móviles.

Para tener en claro la magnitud de este problema, tenemos un ejemplo en donde las tarjetas de crédito robadas pueden venderse por un valor de hasta 100 dólares en el mercado negro, lo que hace de esta actividad -la violación de datos- una tarea sencilla y de bajo riesgo para los delincuentes.

[1] Organización de los Estados Americanos, Symantec. (2014, Junio). *Tendencias de Seguridad Cibernética en América Latina y el Caribe*. Recuperado de http://www.symantec.com/la/reporteOAS/
[2] Ibíd.
[3] Ibíd.

El objetivo principal de esta tesis es efectuar un diagnóstico que abarque aspectos políticos, sociales y tecnológicos de la situación actual de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones mexicanas.

Y si bien existen historias de éxito en otros países, la experiencias recientes confirman que los gobiernos no pueden ocuparse por sí solos de garantizar la seguridad, de ahí que destaquemos la cooperación que las entidades del sector privado y académico, que son las propietarias y operadoras de la mayoría de las infraestructuras y sistemas de la región, tienen en el intercambio de información y cooperación para garantizar la protección adecuada de la privacidad y confidencialidad, en esta era digital en continua evolución

Por lo que podemos aprovechar la experiencia y los conocimientos que estos han facilitado para la cooperación y el desarrollo a las necesidades de cada país, para plantear una propuesta con base en los resultados obtenidos en el diagnóstico.

Para el desarrollo de este estudio, utilizamos un diseño exploratorio, porque fue el más adecuado para entrar en contacto con la situación actual; utilizando la información obtenida en conjunto para brindar una imagen más clara, a la fecha, de la posición que ocupa México en materia de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones.

La presente investigación está estructurada de la siguiente manera:

En el primer capítulo se plantea el problema de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones; se identifican los problemas específicos a investigar, los objetivos que persiguen la investigación y se justifica la investigación.

Después se plantea la fundamentación teórica estableciendo los antecedentes históricos del caso, las bases teóricas necesarias para poder determinar la estructura del documento. Además, se desarrolla la metodología, presentando el diseño de la investigación, la población que se tomó en cuenta para la investigación, los instrumentos utilizados y los procedimientos. Finalmente, se plantea la hipótesis general.

En el segundo capítulo se analiza la evolución del sector de las telecomunicaciones, se describen algunos aspectos que marcan el desarrollo del sector desde finales de los años setenta, se tratan los aspectos de la convergencia más relevantes en su transformación, lo que ha llevado hasta al entorno actual, el cual muestra una concentración de más jugadores y de más mercados, un mayor crecimiento y penetración de los servicios.

En el tercer capítulo, se desarrolla una perspectiva general de la seguridad de las telecomunicaciones y las tecnologías de la información, se examinan algunas de las cuestiones prácticas asociadas y se indica cómo diversos aspectos de la seguridad de las TIC se abordan en los trabajos de normalización. Este capítulo reúne material, relacionado con la seguridad, extraído de las Recomendaciones UIT-T y contiene explicaciones sobre las relaciones entre diversos aspectos de los trabajos.

También se detalla el proceso de creación de un equipo de respuesta a incidentes de seguridad informática (CERT), en el que se integra a un grupo de personas selectas dedicado a la implantación y gestión de medidas tecnológicas, con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio.

Además, se presentan recomendaciones, orientaciones e iniciativas necesarias para proteger las diversas entidades que participan en la prestación, soporte y utilización de las tecnologías y servicios de la información y comunicación. Se presenta la norma ISO 27011, la cual, permite llevar a cabo el proceso de seguridad de la información de manera estructurada, organizada y documentada, basado en diferentes controles y políticas que se establecen.

En el cuarto capítulo, se presentan herramientas utilizadas por el sector privado, ya que más de 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por éste. Estas herramientas han surgido como consecuencia a que el sector de la infraestructura crítica, ha sido un blanco de ataques, debido a instalaciones antiguas y, el predominio de “medidas a medias e improvisadas”, en lugar, de sistemas de seguridad integrales.

A escala global, las dos principales tendencias en el crimen cibernético son el fraude con motivaciones económicas y los ataques contra la confidencialidad, la integridad y la disponibilidad. Por lo que se presentaron tecnologías, políticas y procedimientos que pueden ayudar a proteger las infraestructuras críticas e implementarlas en las organizaciones para que se encuentren preparados para enfrentar un posible ataque cibernético.

Finalmente, en el quinto capítulo se hace un análisis de la situación mexicana en lo referente a garantizar la protección adecuada de la privacidad y las libertades individuales. Se hace un análisis de la situación de Argentina y Uruguay, ya que son dos de los países con actividad criminal cibernética más alta del mundo. Así mismo, podemos observar otra manera distinta de abordar la ciberseguridad a partir de problemas totalmente diferentes, y de las características particulares de cada país, incluyendo Alemania y Canadá.

CAPÍTULO 1.
MARCO CONCEPTUAL Y METODOLÓGICO.

1.1 PLANTEAMIENTO

1.1.1 PROBLEMÁTICA

La confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones no están garantizadas para los usuarios; ya que la captación, registro y almacenamiento de información no se gestionan de manera ética, legal y responsable.

Actualmente ciudadanos de México y del mundo están viviendo una etapa trascendente, una revolución tecnológica que pretende ubicar a cada participante dentro de la sociedad de la información, la cual se basa en la creatividad, así como en la capacidad de producir, almacenar y distribuir información.

Países desarrollados con muy buenas condiciones de vida, infraestructura y con una economía estable han estado enfrentando constantes innovaciones tecnológicas, las cuales han generado inversiones, permitiendo el desarrollo de proyectos de suma importancia y, por consiguiente, contribuido al crecimiento, productividad, empleo y desarrollo social de los sitios involucrados.

Dicho crecimiento conlleva el intercambio masivo de información, incluidos los datos personales que describen aspectos como la identidad, precisan el origen, la residencia, la trayectoria académica y laboral de los individuos. También incluyen aspectos más sensibles, como lo son: salud, ideología y las características físicas de la persona, aspectos de fácil acceso a través de distintos medios electrónicos.

El uso de internet genera un intercambio masivo de datos, aparentemente, inofensivo, pero su manejo en grandes cantidades puede utilizarse ilegalmente: para predecir el comportamiento de una persona, tendencias políticas o creencias religiosas. Cualquier dato relacionado con las personas, posibilita la generación de perfiles que pueden afectar sus libertades, y tiene la capacidad de dañar derechos constitucionales, como la privacidad y la intimidad.

Otro problema radica en que las redes de telecomunicaciones son objeto de ataques perpetrados por personas mal intencionadas, que sirven a sus intereses personales o a los de los grupos de poder fácticos. Los datos que se transmiten en las redes de telecomunicaciones, en paquetes, desde la fuente hasta su destino pueden desviarse para crear negocios ilícitos basados en su compra y venta masiva, sin el consentimiento de los titulares; en consecuencia, no se rinden cuentas sobre su uso o el beneficio que generan.

La protección de datos personales en las redes de telecomunicaciones es una clave esencial para la defensa de los derechos humanos ante el imparable avance tecnológico. No sólo la intimidad o la vida privada están en juego cuando se trata de protección de datos, sino la Sociedad de la Información y la evolución tecnológica.

Organismos reguladores de diversos países han detectado la necesidad de legislar en materia de protección de datos, entendiendo que la libre circulación de la información en las redes de telecomunicaciones es un instrumento necesario para el progreso de las actividades económicas, sociales y políticas de cada participante; sin embargo, ésta debe darse con la debida protección de los derechos y libertades de los ciudadanos, sin que la custodia en torno a estos derechos sea un obstáculo al progreso tecnológico.

La presente investigación pretende esbozar soluciones tecnológicas que eviten tanto que la información sea robada en las redes de telecomunicaciones como que se ponga en peligro el derecho a la privacidad y a la intimidad.

Además, se desea detectar, a la luz del análisis de las experiencias de los países seleccionados, las posibles causas y efectos que, en el caso mexicano, podría tener la implementación de aquellas recomendaciones que respondan a las necesidades del país, de su infraestructura; la aplicación y el aprovechamiento de tecnologías de la información y las comunicaciones, en aras de facilitar el ingreso del país en la Sociedad de la Información en condiciones satisfactorias de confidencialidad, privacidad y protección de datos.

Luego de lo expuesto, las preguntas que guían esta investigación son:

¿Qué esfuerzos están haciendo las autoridades y los responsables de las redes de telecomunicaciones mexicanas para garantizar a los usuarios confidencialidad, privacidad y protección de sus datos en sus redes? ¿Qué recomendaciones han emitido los organismos internacionales y qué experiencias de países seleccionados se pueden considerar para el progreso de las actividades económicas, sociales, políticas y tecnológicas en este sentido?

1.1.2 OBJETIVO

Realizar un diagnóstico previo que abarque los aspectos políticos, sociales, jurídicos y tecnológicos de la situación actual de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones mexicanas, además de plantear una propuesta con base en los resultados obtenidos en el diagnóstico de la situación nacional, en las recomendaciones de organismos internacionales y en las experiencias de países seleccionados, con el fin de mejorar aspectos primordiales relativos a las telecomunicaciones nacionales.

1.1.3 JUSTIFICACIÓN

Se pretende que la presente tesis sea considerada como una sugerencia para fomentar regulaciones específicas en las telecomunicaciones que, en un momento dado, puedan influir en un marco de desarrollo tecnológico, en la seguridad jurídica, en el bien común y en el progreso de México; que pueda servir como orientación, referencia y consulta para mejorar los procesos de captación, transmisión, manejo, registro, conservación y comunicación de los datos relativos a las personas físicas y morales.

Se busca aportar conocimientos e información necesarios para que los entes públicos consideren adoptar medidas de carácter técnico y organizativo con el fin de poder evitar la vulneración de las redes de telecomunicaciones, a fin de garantizar la confidencialidad, la privacidad y la protección de datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Por otra parte, podría beneficiar a las inversiones en el sector de las tecnologías de información, brindar un panorama de libre circulación de la misma como instrumento necesario para el progreso de las actividades políticas y sociales de México, eventualmente permitir que las pequeñas y medianas empresas puedan realizar actividades de comercio electrónico en todos los niveles.

Inclusive, se podría beneficiar con cualquier persona física, sin importar su nacionalidad o residencia, así como la población vulnerable, los consumidores y el sector empresarial.

1.2 MARCO TEÓRICO

1.2.1 ANTECEDENTES HISTÓRICOS

Los datos personales, progresivamente, han cobrado cada vez mayor relevancia social y económica. Recientemente, han sido calificados como “el nuevo petróleo del internet y la nueva moneda del mundo digital”. (Meglena Kuneva, 2009, citado en Remolina-Angarita, 2010). [4]

La información se ha transformado en un recurso comercializado en el mercado nacional e internacional, es un insumo de los sistemas de información privados y gubernamentales. Por lo que, rápidamente, las empresas estadounidenses están ubicando sus esfuerzos en el aprovechamiento y obtención de utilidades de esta tendencia. (Schwartz, 2004, citado en Remolina-Angarita, 2010). [5]

Los gobiernos justifican la transferencia de datos por motivos de seguridad, de investigaciones, labores de inteligencia, cooperación internacional, etc. De la misma manera, las empresas requieren la información para brindar atención, administrar y proveer soporte técnico a las bases de datos de clientes y proveedores. La globalización y los procesos de interacción económica, tecnológica y social piden, entre otras actividades, la circulación internacional de información entre las empresas y los gobiernos.

[4] Meglena, K. (2009, Marzo). *European Consumer Commissioner, Roundtable: Keynote Speech*. Ponencia presentada en el I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores, Cartagena.
[5] Schwartz, Paul M. (2004). Property, Privacy and Personal Data. *Harvard Law Review*, *117*, 2055-2128

Al respecto, las Tecnologías de la Información y Comunicación (TIC)[6] han contribuido significativamente a acelerar el proceso del tratamiento y la transferencia internacional de datos personales.

Las organizaciones internacionales han emitido diversos documentos para verificar que los países importadores y exportadores garanticen, un nivel adecuado de protección de datos personales cuando son transferidos. Pablo Palazzi (2003) sostiene que las reglas deben evitar crear paraísos informáticos, es decir, sitios donde se puedan realizar tratamiento de datos y donde la falta de leyes de protección de los mismos viole las leyes de privacidad.[7]

A partir de 1970 se ha demostrado la necesidad de proteger los datos personales, para evitar lastimar los derechos de las personas, sin impedir su tratamiento. Esta problemática ha sido afrontada por organismos internacionales como las Naciones Unidas (ONU), la Organización de Cooperación y Desarrollo Económico (OCDE), además de numerosos países europeos y americanos.

Una de las primeras constituciones que se esforzó en hacer notar la necesidad de proteger los datos personales -frente al riesgo del progreso tecnológico, así como de adoptar normas y articular instituciones correspondientes, luego de considerar el manejo de datos y su protección como un derecho fundamental- fue la de Portugal, emitida en 1976. Este ordenamiento establece que el uso de la informática se debe gestionar con respeto la vida privada, familiar, los derechos, las libertades y las garantías del ciudadano. A pesar de ello, pasaron quince años para que se dictara la Ley N° 10, llamada “De protección de datos personales frente a la informática”.[8]

---

[6] Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información.

[7] Garriga-Domínguez, A. (2004). Tratamiento de datos personales y derechos fundamentales. Madrid: Dykinson.

[8] Bazán, V. (2005). *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*, 3 (2), 85-139.

En 1978 la Constitución de España estableció en el artículo 18.4 que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”; mientras que el artículo 105 menciona que la ley regulará “el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas”.[9]

En 1980, el consejo de la OCDE adopta la “Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales”. Después, en 1985 los gobiernos de países miembros de la OCDE adoptaron la “Declaración relativa a los flujos transfronterizos de datos no personales”.

En 1981, el Consejo de Europa establece el “Convenio para proteger a las personas respecto al tratamiento automatizado de datos de carácter personal” en Estrasburgo el cual, procura conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos, y se aplica a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.

En 1995, mediante la Directiva 95/46/CE24 del Parlamento Europeo y del Consejo de Europa, se estableció que la transferencia de datos personales sólo puede realizarse cuando el país en cuestión, garantice un nivel de protección adecuado.

[9] Bazán, V. (2005). *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*, 3 (2), 85-139.

El grupo determinó que, considerar a este “nivel adecuado de protección” como tal depende de diversos factores: unos de naturaleza regulatoria -que son una combinación de derechos del titular y de obligaciones para quienes procesan la información- y otros, de carácter instrumental e institucional -que comprenden la existencia de procedimientos judiciales que garanticen la eficiencia y que sancionen el tratamiento indebido de la información-.

También contempla la existencia de una autoridad independiente que controle, vigile y sancione a los que trabajan con datos personales.

En el 2000, se efectúa un cambio de gran trascendencia en cuestiones relacionadas con la protección de datos. La Carta de Derechos Fundamentales de la Unión Europea reconoce en su artículo 8° el derecho de protección de datos como una categoría diferente del derecho a la vida privada, en los siguientes términos:

“Toda persona tiene el derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente”.[10]

[10] Comisión Europea. (2000). *Carta de Derechos Fundamentales de la Unión Europea*. Recuperado de http://www.europarl.europa.eu/charter/pdf/text_es.pdf

1.2.2 BASE TEÓRICA

A continuación, se presentan las bases teóricas que sustentan nuestra investigación sobre la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones para sustentar la información contenida en todos los párrafos.

Con el propósito de que se entienda de manera adecuada la información que queremos transmitir en este diagnóstico, además de que pretendemos que la tesis sea un precedente para fomentar regulaciones específicas de las telecomunicaciones. Los siguientes temas definen un conjunto de conceptos y proposiciones jurídicos que constituyen un punto de vista o enfoque determinado, dirigido a explicar el fenómeno sobre la situación actual de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones mexicanas.

Por este motivo, el presente trabajo se relaciona con varias teorías que lo sustentan conceptualmente y que se relacionan con la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones.

1.2.2.1 DATOS PERSONALES

La definición de datos personales está contenida en la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 20 de junio de 1995, y dice así:

"Datos personales es toda información sobre una persona física identificada o identificable".[11]

Cuatro componentes importantes surgen de esta definición, por lo que se analizará por separado para alcanzar una definición común del concepto de datos personales.

[11] Parlamento europeo, Consejo de la Unión Europea. (2007, Junio). *Dictamen 4/2007 sobre el concepto de datos personales*.
Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

a) Toda información

El concepto de "toda información" incluye todo tipo de afirmaciones sobre una persona: desde información objetiva -como tipo de sangre- hasta información subjetiva, como opiniones. Cualquiera que sea la clase de datos que proporcione información es considerada como de "datos personales", incluyendo la relativa a la vida privada del sujeto, así como la que haga mención sobre cualquier actividad desarrollada por un sujeto.

Desde el punto de vista del formato donde la información está contenida, el concepto de datos personales incluye la información conservada en papel, la información almacenada en una memoria de una computadora -utilizando un código binario- en una cinta de video y hasta aquellos datos que consisten en sonidos e imágenes. Esto queda asentado en el fundamento 14 del artículo 33 de la Directiva, en el que se afirma:

"Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos".[12]

b) Sobre

Se puede considerar que la información es "sobre" una persona cuando se refiere a ella. Este componente de la definición determina con precisión cuáles son las relaciones, los vínculos que importan y cómo distinguirlos. Para considerar que los datos son "sobre" una persona debe haber un elemento "contenido", un elemento "finalidad" o un elemento "resultado".[13]

---

[12] Parlamento europeo, Consejo de la Unión Europea. (1995, Octubre). *Directiva 95/46/ relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*
Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_es.pdf

[13] Parlamento europeo, Consejo de la Unión Europea. (2007, Junio). *Dictamen 4/2007 sobre el concepto de datos personales*.
Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

El elemento contenido está presente en casos en los que se proporciona información sobre una persona concreta. Independientemente de la repercusión de esa información en el interesado, los datos se refieren sin lugar a dudas al mismo.

El elemento finalidad existe cuando los datos se utilizan con el propósito de evaluar o manipular, con el propósito de influir en la situación o comportamiento de una persona. Es decir, cuando la información se utilizará para tratar al sujeto de determinada manera.

La tercera categoría, resultado, hace que su uso influya en los derechos y los intereses del sujeto.

De estas categorías se determina como no necesario que los datos se centren en una persona para considerar que la describen. Es necesario analizar cada dato en función de sus características.

c) Identificada o identificable

Un sujeto es identificable cuando, dentro de un grupo de personas, se le distingue de los demás sujetos. La directiva en su definición del artículo 2 menciona:

"Se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".[14]

[14] Parlamento europeo, Consejo de la Unión Europea. (2007, Junio). *Dictamen 4/2007 sobre el concepto de datos personales*. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

Para aclarar más la idea, cuando se hace referencia a una persona directamente identificable, se apela al identificador más común: nombre y apellidos. Por otra parte, cuando se habla de una persona indirectamente identificable, se refiere a combinaciones únicas -sean grandes o pequeñas- como el número de seguridad social, el número de pasaporte, etcétera.

En algunos casos no es posible identificar al sujeto en una primera intención, por lo que se usan más identificadores, como elementos específicos o característicos de su identidad física, fisiológica, psíquica, económica, cultural y social, que pueden llegar a ser concluyentes en algunas circunstancias.

d) Persona física

Una persona física, para la directiva, son los seres humanos. Los Estados delimitan jurídicamente el concepto de *seres humanos*, al entenderlo como la capacidad de la cual están dotadas las personas para ser sujetos de relaciones jurídicas, desde su nacimiento hasta su muerte, por lo que la información referente a personas físicas también puede ser considerada en función de sus características, como información sobre personas jurídicas. Todo esto está incluido en el artículo 6 de la Declaración Universal de los Derechos Humanos:

"Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica".[15]

1.2.2.2 Hábeas data

El concepto de hábeas data depende de las características jurídicas del país que lo trate, puede ser una garantía constitucional, un procedimiento jurídico, un proceso constitucional o un derecho a la protección de los datos personales.

[15] Organización de las Naciones Unidas, UNESCO. (2008, Diciembre). Declaración Universal de los Derechos Humanos. Recuperado de http://unesdoc.unesco.org/images/0017/001790/179018m.pdf

De acuerdo con algunos autores, “hábeas data” es un concepto proveniente de la antigua forma “hábeas corpus”, donde la primera palabra significa “conserva o guarda tu”; y la segunda, proveniente del inglés “data”, “información o datos”. Entonces, la traducción literal sería “conserva o guarda tus datos” (Ekmekdjian, 1995).[16]

a) Etimología

Hábeas: Segunda persona singular del presente subjuntivo del verbo latino *habere*, que significa: aquí tengas en posesión.[17]

Data: Acusativo neutro plural de *datum*, de la misma raíz que el verbo latino *do, das, dedi, datum, dare* significa: “dar”, “ofrecer”.[18]

b) Definición

Hábeas data se define como “el derecho que permite que toda persona pueda acceder al conocimiento de los datos que consten de registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación”.[19]

Este concepto simula al “hábeas corpus”, que protege la libertad del individuo, mientras que el hábeas data protege la información que identifica al individuo.

---

[16] Bazán, V. (2005). *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*, 3 (2), 85-139.
[17] Chaname, O. R. (2003). *Hábeas data y el derecho fundamental a la intimidad de la persona*. Tesis de maestría no publicada, Universidad Mayor de San Marcos, Lima, Perú.
[18] Muñoz de Alba, M. M. (2006). Habeas Data. En Romero, R. M. (Eds.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Estudios de derecho público y política*. (pp. 1-21). México: Instituto de Investigaciones Jurídicas de la UNAM. Recuperado de http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf
[19] Pizzolo, C. (1996). *Hábeas data. El derecho a la intimidad*. Buenos Aires, Argentina: Desalma.

c) Características

El hábeas data se ocupa de proteger derechos que se ven amenazados por el progreso tecnológico, el cual hace que las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar datos sean más rápidas y que se extiendan hacia el mundo sin que exista un control real de la calidad, fidelidad ni de cómo y a quién se envía la información.

El hábeas data protege los derechos subjetivos de tipo privado, que son facultades jurídicas que se les reconocen a los sujetos de derecho por naturaleza, solo el titular puede saber si la información le causa daño o no, además de verificar si es cierta y está actualizada.

El hábeas data debe ser un proceso rápido, ya que los derechos son susceptibles de ser dañados, y si son lesionados, el daño seria amplio y probablemente no podría existir alguna reparación inmediata.

d) Tipos de Hábeas data

La clasificación de los diversos tipos de Hábeas data se relaciona directamente con el objetivo que cada uno persigue. Néstor Pedro Sagüés dice que conviene clasificarlo tomando en cuenta la experiencia jurídica (1995).[20] Entonces, podrían organizarse de la siguiente manera:

I.- Informativo

Es aquel que procura recabar información e indagar en registros o bancos de datos destinados a proveer informes. Existen tres subespecies (exhibitorio, finalista y autoral).[21]

[20] Sagüés, N. P. (1995). Subtipos de Hábeas Data. *Jurisprudencia Argentina*, 4,352-354

[21] Chaname, O. R. (2003). *Hábeas data y el derecho fundamental a la intimidad de la persona*. Tesis de maestría no publicada, Universidad Mayor de San Marcos, Lima, Perú.

I.I Exhibitorio

Toma conocimiento de los datos referidos a las personas y responde a la pregunta: ¿qué se registró?

I.II Finalista

Conoce la finalidad de los datos, establece saber para qué y para quién existen.

I.III Autoral

Persigue averiguar acerca de quién obtuvo los datos del registro.[22]

2.- Por omisión

Agrega más datos a los que deberían constar en el registro.

3.- Rectificador

Corrige datos falsos, inexactos e imprecisos en los registros.

4.- Reservador

Protege la confidencialidad de los datos para que su publicación no pueda causar daño.

5.- Cancelatorio

Elimina los datos almacenados en los registros en el caso de que se trate de datos "sensibles", en tanto que podrían lastimar la privacidad de las personas.

[22] Muñoz de Alba, M. M. (2006). Habeas Data. En Romero, R. M. (Eds.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Estudios de derecho público y política*. (pp. 1-21). México: Instituto de Investigaciones Jurídicas de la UNAM. Recuperado de http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf

1.2.2.3 Derecho a la privacidad

"Lo privado es todo lo que está afuera del ámbito del interés público, de los asuntos del Estado, de lo que involucra al conjunto de la sociedad. Lo privado es el ámbito restringido de lo doméstico y lo familiar, de aquellos asuntos del sujeto, que no necesariamente deben ser divulgados masivamente" (Sennett, 1978)[23]

La privacidad define la protección de las personas, impidiendo que terceros se ocupen de su vida privada, es una esfera de aislamiento donde el sujeto está fuera de los ojos de las demás personas. El derecho a la vida privada se manifiesta con la realización de actividades y comportamientos personales, familiares o de amistad en el que la persona decide coexistir manteniendo esa esfera.

La aproximación al concepto de privacidad depende de factores sociológicos, culturales y de la tradición jurídica del país.

La Declaración Universal de los Derechos Humanos de 1948 menciona que nadie será objeto de intromisiones en su vida privada, su domicilio, sus comunicaciones, ni de ataques a su reputación.[24]

Las personas tendrán derecho a la protección de la ley contra los ataques, lo que conlleva la necesidad de que el banco de datos sea privado para lograr confidencialidad y seguridad en la transmisión de los mismos. Es necesario establecer cuáles datos pueden ser proporcionados al banco, así como quién y para qué los posee, pudiendo oponerse a que éste los posea.

A pesar de esto, lo que caracteriza a la ley, como tener una vida privada, es el derecho a mantenerse ajeno a las intromisiones ilegitimas o legitimas infundadas.

---

[23] Sennett, R. (1978). El declive del hombre público.
Recuperado de http://www.ddooss.org/libros/Richard_Sennett.pdf

[24] Organización de las Naciones Unidas, UNESCO. (2008, Diciembre). Declaración Universal de los Derechos Humanos. Recuperado de http://unesdoc.unesco.org/images/0017/001790/179018m.pdf

Existe una gran relación entre intimidad y privacidad, la intimidad se refiere al ámbito personal que no debería ser conocido por los demás, y la privacidad se refiere a acciones que pueden ser conocidas por terceros. Cuanto más íntimo es el carácter de la cultura, mayor es el espacio que reclama; cuanto más social es la cultura, más se reduce el espacio hasta sus mínimas manifestaciones.[25]

Los individuos tienen derecho a la intimidad de sus comunicaciones, de los datos sobre su salud, su identidad, sus ideas, su patrimonio, sus creencias. El derecho a la intimidad se convierte entonces el pilar de los demás, ya que funda, alimenta y da razón de ser a otros: Se puede afirmar que sin intimidad no hay libertad.

Carlos Colautti (1996) dice que entre intimidad y privacidad podría establecerse una relación, al pensar que las acciones intimas están dentro de las acciones privadas. Por lo tanto, concluye que las acciones íntimas son privadas, pero no todas las acciones privadas son íntimas.[26]

El desarrollo de la tecnología cuestiona el derecho a la intimidad por los datos que se mueven a través de los medios informáticos. Javier Royo (2000) le da el nombre de intimidad informativa al derecho a poder determinar cuándo, cómo y con qué alcance se va a transmitir información sobre nosotros a los demás.[27]

[25] Locke, J. (1690). Del estado de la naturaleza. En Mellizo, C. (Eds.), *Segundo Tratado sobre el Gobierno Civil. Un ensayo acerca del verdadero origen, alcance y fin del Gobierno Civil*. (pp. 5-10). Recuperado de http://cinehistoria.com/locke_segundo_tratado_sobre_el_gobierno_civil.pdf
[26] Colautti, C. E. (1996). Reflexiones preliminares sobre el Hábeas Data, La Ley, 1996-C, 917 -922.
[27] Pérez Royo, J. (2000). *Curso de derecho constitucional*. Barcelona: Ediciones jurídicas y sociales.

Origen de la vida privada

Hace más de 120 años, Samuel D. Warren y Louis D. Brandeis, abogados de Boston, publicaron el ensayo titulado *The right to privacy*.

El aumento de avances tecnológicos y el desarrollo de la prensa de finales del siglo XIX, amenazaban con la difusión indiscriminada de información privada, las columnas de los periódicos divulgaban los más íntimos detalles para satisfacer la curiosidad de la población.

Las posibles invasiones tecnológicas hicieron sentir preocupación a Warren y Brandeis sobre los riesgos del crecimiento de la sociedad tecnológica del siglo XIX, en lo relativo a la protección de la vida privada. Este interés se ve reflejado en el siguiente párrafo de su ensayo:

"La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales» (Warren y Brandeis, 1995).[28]

El principal argumento que Warren y Brandeis emplean en su ensayo en defensa del derecho a la privacidad es, la obligación de toda persona de controlar su círculo privado y su propia información personal. El derecho a que toda persona proteja su integridad, pueda ejercer control sobre aquella información que afecte su autoestima y su personalidad individual.

[28] Warren, S. D. y Brandeis, L. D. (1995). The Right to Privacy. *The Harvard Law Review Association*, 4(5), 193-220.

Para Warren y Brandeis (1995), el derecho a la privacidad no impide la publicación de aquello que es de interés público o cuando la revelación de la información privada se realiza en circunstancias conforme al régimen jurídico. La protección del derecho decae cuando es el propio sujeto quien publica u otorga consentimiento.[29]

La intensidad y complejidad de la vida es consecuencia del progreso de la civilización, así que demanda cierto distanciamiento del mundo, convierte la soledad en algo fundamental para el individuo. Hace que la intromisión a través de medios tecnológicos a la esfera privada genere angustia y sufrimiento mucho mayor que el producido por daño físico. (Warren y Brandeis, 1995)[30]

Por esto mismo, Warren y Brandeis abogaron por un sistema que protegiera el derecho a la privacidad, ya que consideraron que, si la información sobre la vida privada de una persona es conocida por terceros, se perjudica la libertad del individuo.

La noción de privacidad formulada por Warren y Brandeis emerge como aproximación al momento de delimitar posibles invasiones tecnológicas, de tener el derecho al control sobre cómo la información personal es comunicada a otros en la sociedad tecnológica. Defiende fuertemente a la privacidad para contribuir al mantenimiento y al avance del sistema democrático, además de establecer los límites sobre los individuos y definir la esencia humana.

[29] Warren, S. D. y Brandeis, L. D. (1995). The Right to Privacy. *The Harvard Law Review Association*, 4(5), 193-220.
[30] Ibíd.

1.3 METODOLOGÍA DE INVESTIGACIÓN

La presente investigación utiliza un diseño exploratorio, es efectuada sobre un tema desconocido o poco estudiado, por lo tanto, los resultados constituyen una visión aproximada de dicho tópico. De la misma manera, es utilizada para aumentar el conocimiento del investigador sobre el problema y posteriormente poder realizar un estudio más estructurado.

Cada día se genera un intercambio masivo de datos en las redes de telecomunicaciones y hay necesidad de explorarlo a fin de encontrar soluciones tecnológicas que eviten el robo de información en las redes de telecomunicaciones.

Por otro lado, la investigación sirve para determinar las posibles causas y efectos que podría tener, en el caso mexicano, la implementación de las recomendaciones. Es un tema que no ha sido suficientemente estudiado.

Los estudios exploratorios aclaran y delimitan los problemas, además de permitir conocer las variables de interés de la confidencialidad, la privacidad y la protección de los datos.

Siendo la investigación cualitativa, el diseño más conocido de la investigación exploratoria, conviene al presente trabajo porque se concentró más en la profundidad y comprensión que en la medición de las variables.

1.3.1 POBLACIÓN Y MUESTRA

La población está conformada por organismos internacionales reguladores de telecomunicaciones, presentes en países europeos y en México.

Se realizó un muestreo de tipo general, no probabilístico de selección intencional, basado, principalmente, en la experiencia de la población y en los criterios de quien efectúa la investigación. El criterio de selección intencional se adecúa a la naturaleza y los objetivos de esta investigación, porque permite seleccionar a los participantes que mejor representen a la población por el hecho de tener amplio conocimiento del fenómeno a investigar.

Los criterios de inclusión y exclusión para la delimitación poblacional son los siguientes:

- Se comenzó por el Parlamento Europeo.
- Se utilizó organismos internacionales reguladores de telecomunicaciones para seleccionar los casos apropiados y ricos en información.
- La muestra se fue formando de manera seriada, es decir, el siguiente organismo o país se seleccionó con base en la información proporcionada por los que fueron seleccionados.
- La muestra fue ajustada al instante; la información obtenida orientó el proceso de muestreo.
- El muestreo continuó hasta alcanzar el “punto de saturación”, es decir, hasta que no hubo información diferente, sino solo “más de lo mismo”.

1.3.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El instrumento que se utilizó fue la revisión documental, ya que ésta es una investigación exploratoria y la muestra seleccionada de la población a estudiar requiere atención de los aspectos políticos, administrativos y tecnológicos que enfocan la situación actual la confidencialidad, la privacidad y protección de datos en las redes de telecomunicaciones mexicanas.

Se comprobó la validez y fiabilidad de la información mediante la comparación de los documentos. El punto de saturación, esto es, el punto en que ya no se obtiene nueva información y ésta comienza a ser redundante; guio la investigación y determinó el momento cuando ya no se requirió seguir investigando.

Debido a que la revisión fue documental, ésta se basó en información hallada que resultó relevante para conocer soluciones tecnológicas en el mundo que eviten que la información sea robada en las redes de telecomunicaciones.

1.4 HIPÓTESIS

Para fortalecer la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones es necesaria la cooperación entre las autoridades y los responsables de las redes de telecomunicaciones, es decir, los gobiernos de los países y los legisladores, además de los ingenieros y técnicos de seguridad que trabajan en la infraestructura de las redes de telecomunicaciones deben crear alianzas para fortalecer la capacidad de recuperar, prevenir, mitigar, responder, investigar y procesar el impacto de los posibles ataques.

Por consiguiente, la forma en que se equilibre y se enfrenten los desafíos en un futuro inmediato sobre la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones, deberá destacar la necesidad de trabajar en conjunto en cuatro niveles diferentes: internacional, nacional, sector privado e individual.

Al garantizar que la captación, registro y almacenamiento de información se administre de una forma ética, legal y responsable en las redes de telecomunicaciones, se convertirá en una poderosa herramienta para el desarrollo económico y social, la gobernanza democrática, la seguridad nacional y la de los ciudadanos.

CAPÍTULO 2
ANÁLISIS TEMÁTICO.

2.1 INTRODUCCIÓN

Antes de iniciar el diagnóstico sobre la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones, es conveniente definir aquellos aspectos importantes que juegan un papel fundamental en el mercado de las telecomunicaciones, para poder ubicarnos en el entorno actual de la regulación de las telecomunicaciones

Por ello, hay que entender el entorno, los procesos, el desarrollo, evolución y los organismos, ya que son pieza medular en el diagnóstico de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones mexicanas.

En este capítulo se consideran conceptos importantes para los avances que impactaron a las tecnologías de la información y las comunicaciones, tales como la convergencia en las redes y servicios, y la neutralidad de la red como pilar fundamental de esta última tendencia.

2.2 LA CONVERGENCIA DE LAS TELECOMUNICACIONES.

La convergencia se entiende como la posibilidad tecnológica para el usuario de servicios de telecomunicaciones de recibir en un mismo dispositivo múltiples servicios, como pueden ser, telefonía, internet, televisión, radio. También, como la posibilidad de los proveedores de transportar diversos servicios por medio de sus redes.[31]

La definición que da la Unión Internacional de Telecomunicaciones (UIT) es: "la transformación coordinada de redes que antes eran independientes hacia una igualdad que permita el soporte común de servicios y aplicaciones" (UIT, 2004).[32]

Existen elementos fundamentales en el desarrollo de la convergencia, como son: la digitalización, la capacidad y la calidad requeridas por cada servicio, y las vías que emplean. Los consumidores desarrollan un rol más activo, en la mayoría de los casos, son los que diseñan nuevos productos, demandan estándares de calidad e impulsan la innovación.

Dados estos nuevos formatos de comunicación y de internet, el modelo para hacer negocios y de relacionarnos, ha generado una transformación real en la vida digital. Esto supone también, que la delincuencia se adapte a este nuevo entorno con más medios económicos y más herramientas, así mismo, pueden obtener beneficios desde el anonimato a un mercado económico, político, religioso y social.

[31] Guerra de la Espriella, M. R. & Oviedo, J. D. (2011, Abril). De las telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09), Bogotá, Colombia: CEPAL.
Recuperado de http://repositorio.cepal.org/bitstream/handle/11362/4818/S110124_es.pdf?sequence=1
[32] Aldana, A. T. & Vallejo, A. C. (2010). Telecomunicaciones, convergencia y regulación. *Revista de Economía Institucional, 12*(23), 165-197. Recuperado de http://www.redalyc.org/articulo.oa?id=41915521008

De esta forma, la convergencia ha cambiado las formas de acceder a la información y esto, ha derivado en nuevos riesgos para la confidencialidad, la privacidad y la protección de datos.

La convergencia entre la seguridad física y lógica, precisa de la concienciación del sector de la seguridad de la información, o más bien en lo que ya se ha convertido en ciberseguridad.

Hay que mencionar además que, la formulación de políticas para el sector de las telecomunicaciones tiene un elemento importante en convergencia, pues asocia cambios tecnológicos y de mercado. Garantiza la equidad en el acceso y facilita la inversión para un nivel de competencia más profunda, con el fin de fomentar la regulación por mercado en lugar de la regulación por servicios.

Aldana & Vallejo (2010) afirman que la convergencia facilita la administración integral desde el punto de vista del consumidor y del regulador, cuando se integran todos los servicios tecnológicos al sector.[33]

2.2.1 EVOLUCIÓN

"Los avances que marcaron las tecnologías de la información y las comunicaciones, se realizaron en paralelo con decisiones de ajuste organizacional en materia de liberalización y privatización del sector de telecomunicaciones, la industria impulsó cambios en el mercado y señaló nuevas direcciones para la regulación que pueden ser analizados en un proceso de tres etapas" (UIT, 2007, 7-26).[34]

[33] Aldana, A. T. & Vallejo, A. C. (2010). Telecomunicaciones, convergencia y regulación. *Revista de Economía Institucional*, *12*(23), 165-197. Recuperado de http://www.redalyc.org/articulo.oa?id=41915521008
[34] Ibid

Primera etapa

En la primera etapa del cambio tecnológico, tres desarrollos tuvieron una influencia trascendental en la perspectiva del sector TIC y en el desenvolvimiento de nuevos servicios y aplicaciones. Estos son: la digitalización, la computarización y las tecnologías de conmutación de paquetes.

La digitalización permite convertir la información que es procesada, almacenada y transmitida en las redes de telecomunicaciones a un lenguaje binario, usando un ancho de banda mucho menor que el requerido originalmente para transmitir la misma información.

Esto amplió la posibilidad para los operadores de redes de ofrecer servicios distintos a los mismos usuarios e incluso a nuevos, por medio de las mismas redes, sin necesidad de desarrollar infraestructura adicional a aquella con la que ya se contaba, generando que los proveedores de servicios aumenten su oferta de servicio.

La computarización posibilitó el despliegue de infraestructuras y de nodos de red como sustitutos de los circuitos. Entonces, las computadoras se convirtieron en aparatos que agregan inteligencia a los nodos de red.

Por su parte, las tecnologías de conmutación de paquetes de datos, han permitido el establecimiento de plataformas de transmisión multiservicio en la misma red y el uso eficiente de los recursos en las diferentes infraestructuras de red, abriéndole paso a la convergencia.

Segunda etapa

En la segunda etapa de cambio tecnológico, las tecnologías permiten desarrollar nuevos servicios y aumentar la capacidad de la red, dando lugar a la convergencia de servicios. En ésta, tres diferentes tendencias pueden ser identificadas.

Primero, el surgimiento del protocolo IP que facilitó la separación esencial entre la capa de transmisión y la capa de servicios. Segundo, el surgimiento de nuevas infraestructuras la cual, se manifiesta a través de nuevas plataformas de redes de transporte de telecomunicaciones, como lo es la transmisión de telecomunicaciones sobre redes eléctricas, así como nuevas infraestructuras físicas que emplean tecnologías alámbricas e inalámbricas. Y finalmente, la convergencia.

La convergencia incrementa el uso de las redes, disminuye barreras de entrada y los costos de prestación del servicio, impulsa el surgimiento de nuevos modelos de negocio, ya que pueden emplearse indistintamente las redes de empresas de telefonía fija, móvil, de fibra óptica, para llevar todos los servicios a las comunidades a las que tengan acceso, incrementando la cobertura sin la necesidad de desarrollar una red para cada tipo de servicio.

Tercera etapa

En la tercera etapa de cambio tecnológico ocurren transformaciones que se fundamentan en la administración y la operación de los procesos, en la creación de nuevos productos y técnicas asociadas con la percepción de las sociedades de la información.

Los reguladores intentarán que las decisiones, las normas y los estímulos tomados en la segunda etapa generen nuevas formas de organización y de arreglos institucionales que permiten alcanzar beneficios sociales y tecnológicos, además de facilitar el desarrollo de políticas públicas.

Además, debido a la rápida innovación, se necesitarán políticas que puedan anticiparse a los avances del sector y que cubran aspectos tales como la regulación, el estímulo a la inversión en infraestructura y servicios, la seguridad de redes y contenidos, e igualmente la compatibilidad entre componentes.

2.3 NEUTRALIDAD DE LA RED

La idea de neutralidad de red se fundamenta en el concepto del internet abierto, está asociada a estándares abiertos, a la libertad de conexión de internet y al trato comercial que adoptan los usuarios por parte de los proveedores de internet (ISP).

La expresión “neutralidad de la red” se le atribuye al profesor Tim Wu, generada en el debate sobre las prácticas de la administración del tráfico de internet o calidad del servicio (QoS) en 2003. Planteaba una probable problemática entre los intereses de los proveedores de internet, los clientes y las empresas por un internet sin limitaciones.[35]

Las cuatro libertades de internet propuestas por el profesor Wu, que enfrentarían los intereses anteriormente señalados, son las siguientes:[36]

- Libertad para conectar dispositivos.
- Libertad para ejecutar aplicaciones.
- Libertad para recibir los paquetes de contenido que se deseen.
- Libertad para obtener información relevante del Plan de Servicio.

Estas libertades se ven favorecidas cuando los Estados garantizan la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones, por lo que la protección de la neutralidad de la red es fundamental para garantizar la pluralidad y diversidad del flujo informativo.

[35] Marsden, C. T. (2012, Febrero). Neutralidad de la Red: Historia, regulación y futuro. *Revista de los Estudios de Derecho y Ciencia Política de la UOC, ISSN 1699-8154*(13). 24-43.
[36] Ruiz, L. M. (2014, Enero). Neutralidad de red y desarrollo de las TIC. *Revista Universitaria Europea*, ISSN: 1139 -5796(20), 1-20

En algunos países empiezan a surgir iniciativas y acercamientos donde se debate si las disposiciones referentes a la neutralidad de la red son necesarias y si requieren de políticas de “no discriminación”, en las que se les prohíba a los proveedores de internet la administración del tráfico de internet para que, se concentren en ofrecer el contenido en igualdad de condiciones.

La popularización y el crecimiento poco planificado del internet en la actualidad, ha llevado a encontrar una rivalidad entre los intereses privados de los proveedores de internet y los desarrolladores de las TIC.

Los proveedores de internet (ISP) valoran que programas, servicios o datos no deben ser distribuidos a los clientes, y organizan sistemas para que éstos no lleguen a los usuarios, generando desprotección en estos últimos.

La tecnología actual permite a cualquier enrutador de un proveedor de internet observar, dentro de un paquete de datos, su contenido, mediante una inspección profunda de paquetes o *Deep Packet Inspection* (DPI). El *Deep Packet Inspection* permite al proveedor de internet determinar si un paquete de datos necesita un transporte de alta velocidad o un canal de transporte dedicado, y también permite reducir la velocidad de otros contenidos.

Los métodos de administración del tráfico no solo perjudican a la velocidad, sino que también los *Deep Packet Inspection* podrían bloquear por completo algún contenido si deciden que no favorece a los proveedores de internet.

La brecha digital y los problemas de desarrollo están fuertemente ligados con la neutralidad de la red. La conectividad a internet es costosa para la mayoría de países en desarrollo, convirtiendo éste servicio universal, en un servicio inaccesible. Cuando éste llegue a los países en desarrollo, los proveedores de internet lo estarán definiendo.

La neutralidad de la red debe contener valores sociales, económicos y políticos vinculados a los requerimientos de internet (Mueller, 2007)[37]

La neutralidad de la red hace referencia a algunos derechos y principios que aparecen en la Carta de Derechos Fundamentales de la Unión Europea, como son el respeto a la vida privada, a la libertad de expresión e información, y a la protección de los datos personales.[38]

Hoy en día, las redes neutrales deben operar según tres principios:

- No discriminación: Basado en el trato imparcial de todo el tráfico sobre la red
- Interconexión: Obligación y derecho de los operadores
- Accesibilidad: Cualquier contenido tiene derecho a ser enviado y recibido

La Unión Europea establece un marco regulatorio, explicado por directivas,[39] para tener una reglamentación común sobre la red. Dicho marco se indica a continuación:

- Directiva relativa al acceso a las redes y servicios de comunicación electrónicas.
- Directiva relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.
- Directiva relativa a la autorización de redes y servicios de comunicaciones electrónicas.
- Directiva relativa al servicio universal.
- Directiva relativa al tratamiento de los datos personales.

[37] Marsden, C. T. (2012, Febrero). Neutralidad de la Red: Historia, regulación y futuro. *Revista de los Estudios de Derecho y Ciencia Política de la UOC, ISSN 1699-8154*(13). 24-43.
[38] Ruiz, L. M. (2014, Enero). Neutralidad de red y desarrollo de las TIC. *Revista Universitaria Europea*, ISSN: 1139 -5796(20), 1-20.
[39] Ibíd.

De esta manera, el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) indica que los mandatos legales de las Directivas permiten una regulación más equilibrada de todos los proveedores, no solo de los dominantes; además explica que la regulación de la neutralidad de la red es importante, ya que están en juego tecnologías de censura, como se especifica a continuación:

"La libertad de expresión y los derechos ciudadanos, así como el pluralismo de los medios de comunicación y la diversidad cultural son valores importantes de la sociedad moderna y son dignos de ser protegidos en este contexto, en especial porque la comunicación de masas se ha convertido en más fácil para todos los ciudadanos gracias a Internet". (ORECE, 2010)[40]

Por ejemplo, en Noruega, la regulación de la neutralidad de la red ha sido más eficaz porque ha establecido que:

- Los usuarios deben recibir información completa y precisa sobre el servicio que adquieren, en específico sobre la capacidad y la calidad.
- Los usuarios pueden utilizar los servicios y aplicaciones de su preferencia, pueden enviar y transmitir el contenido que quieran y conectar cualquier hardware y software que no dañe la red.
- No puede haber discriminación basada en el servicio, el contenido, el remitente o el destinatario.

[40] Marsden, C. T. (2012, Febrero). Neutralidad de la Red: Historia, regulación y futuro. *Revista de los Estudios de Derecho y Ciencia Política de la UOC, ISSN 1699-8154*(13). 24-43.

CAPÍTULO 3
ANÁLISIS INTERNACIONAL.

3.1 INTRODUCCIÓN

Los organismos de normalización desempeñan un papel fundamental en el propósito de dar a conocer los problemas de seguridad de las TIC, cuidando que las consideraciones de seguridad conformen un aspecto esencial de las especificaciones, y proporcionando normas técnicas y orientaciones para ayudar a los proveedores y usuarios a tomar medidas de seguridad eficaces para proteger los sistemas de TIC.

Para comenzar con el análisis, el tema dos presenta una introducción general a los trabajos que realiza el UIT-T en materia de seguridad y cómo responde a los problemas de ciberseguridad, introduciendo arquitecturas de seguridad genéricas para sistemas de comunicaciones de extremo a extremo, junto con algunas otras, específicas de la aplicación.

El tema tres, describe la situación actual de la Unión Europea, relativa a la seguridad de las redes y la información. Se detalla el proceso de creación de un equipo de respuesta a incidentes de seguridad informática (CERT), que va desde perspectivas de gestión empresarial y de procesos, hasta puntos de vista técnicos.

Finalmente, el tema cuatro resalta aspectos importantes como la norma ISO 27011, que describe cómo gestionar la seguridad de la información en una empresa de telecomunicaciones mediante procesos de colaboración y controles que garanticen la reducción de riesgos en la prestación de servicios de telecomunicaciones.

3.2 UIT

En esta sección se tiene por objeto presentar las principales actividades de los trabajos que realiza la UIT en materia de seguridad y de protección de las tecnologías de la información y las comunicaciones.

Para garantizar que se cubra una amplia variedad de servicios de redes de telecomunicaciones, la UIT define perfiles de seguridad y normalización que facilitan la compatibilidad y reutilización de soluciones, de modo que se beneficien tanto fabricantes como proveedores de servicios, gracias a la compatibilidad entre los componentes.

La recomendación ITU-T X.1205 publicada en 2008, procura establecer fundamentos que permitan garantizar la seguridad de las redes, trata diversas formas de neutralizar amenazas, además considera principios de protección de red y analiza estrategias de gestión de riesgos.[41]

Por otra parte, la ITU-T en su recomendación identifica las partes implicadas que habrá que proteger:

- Clientes / Abonados.
- Comunidad / Autoridades.
- Operadores de red / Proveedores de servicio.

De igual modo, a los elementos siguientes:

- Los servicios de comunicaciones y de informática.
- La información y los datos.
- El personal, los equipos y las instalaciones.

[41] Sector de Normalización de las Telecomunicaciones de la UIT. (2012, Enero). *Seguridad de las telecomunicaciones y las tecnologías de la información*. Recuperado de http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf

Y también define qué son las amenazas, las vulnerabilidades y los riesgos de seguridad de los que se debe proteger al tratamiento de la información y a la red de telecomunicaciones.[42]

Amenaza

La amenaza de seguridad corresponde a una posible violación de la misma. Algunos ejemplos son:

- Divulgación de información no autorizada.
- Destrucción o modificación no autorizada de los datos y equipos.
- Robo, eliminación o pérdida de información.
- Interrupción o prohibición de servicios
- Usurpación de identidad.

Vulnerabilidad

La vulnerabilidad de seguridad es una imperfección o fragilidad que puede utilizarse para violar un sistema o la información que contiene. La UIT-T contempla cuatro tipos:

- Vulnerabilidades de tipo amenaza.
- Vulnerabilidades de diseño y especificación.
- Vulnerabilidades de aplicación.
- Vulnerabilidades de operación y configuración.

Riesgo

Un riesgo de seguridad es la probabilidad de que los resultados negativos puedan surgir de ejecutar una vulnerabilidad de seguridad.

[42] Sector de Normalización de las Telecomunicaciones de la UIT. (2012, Enero). *Seguridad de las telecomunicaciones y las tecnologías de la información*. Recuperado de http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf

Los organismos de normalización deben tener conocimiento de las amenazas, los riesgos y las vulnerabilidades asociadas; ligados al tratamiento de la información y las redes de telecomunicaciones para lograr una seguridad adecuada, además deben respaldar una gestión de seguridad y un procedimiento adecuado de incidentes -lo que comprende la asignación de responsabilidades y la especificación de las medidas que se deben tomar para prevenir, detectar, investigar y actuar frente a cualquier incidente de seguridad-.

3.2.1 CIBERSEGURIDAD

La ciberseguridad puede utilizarse para garantizar la disponibilidad, integridad, confidencialidad y el respeto a la privacidad del usuario.

Uno de los objetivos de la ciberseguridad es proteger el ciberentorno, el cual comprende a los usuarios, los dispositivos informáticos conectados, todas las aplicaciones, servicios y sistemas que puedan estar conectados a internet y al ambiente de las redes, ya sean públicas o privadas.[43]

La recomendación ITU-T X.1205 define a la ciberseguridad como una colección de instrumentos, políticas, conceptos de seguridad, directrices, planteamientos de gestión de riesgos, garantías y tecnologías que pueden utilizar para proteger el entorno, la organización y los usuarios.[44]

[43] Sector de Normalización de las Telecomunicaciones de la UIT. (2008, Abril). *Serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad. Seguridad en el Ciberespacio– Ciberseguridad*. Recuperado de https://www.itu.int/rec/T-REC-X/es

[44] Sector de Normalización de las Telecomunicaciones de la UIT. (2012, Enero). *Seguridad de las telecomunicaciones y las tecnologías de la información*. Recuperado de http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf

3.2.1.1 Estrategias de protección de la red

Para un diseño de redes seguras, éstas se segmentan por capas, lo que permite a la capa superior determinar sus condiciones de seguridad y a las inferiores utilizar los servicios de seguridad; de igual modo, facilita el desarrollo de soluciones flexibles y adaptables de seguridad en el nivel de la red, el nivel de aplicación y el nivel de gestión de las organizaciones.

Gestión de acceso uniforme

La gestión de acceso uniforme es utilizada para determinar sistemas que puedan emplear los servicios de autentificación y de autorización para verificar el uso de un recurso.

La autentificación, es el procedimiento por el cual, un usuario solicita a una red, la creación de una identidad; y la autorización decide el nivel de privilegios de acuerdo con el control de acceso de la identidad.

Dependiendo del tipo de empresa, pueden utilizarse uno o más métodos para autentificar a un usuario, inclusive una combinación de estos para la gestión de acceso; entre los cuales, se cuentan: el filtrado de IP, las contraseñas, los pases de validez limitada, las técnicas biométricas, las tarjetas inteligentes y los certificados.

La autentificación por contraseñas, debe emplearlas con al menos ocho caracteres, como mínimo un carácter alfabético, uno numérico y uno especial. Puede ser necesario unificar la autentificación por contraseñas con otros procesos y la autorización; los certificados, el protocolo de acceso al directorio (LDAP).

Las organizaciones deben plantear un sistema de gestión de acceso uniforme, con reglas que habrán de aplicarse adecuadamente en:

- Directorios y bases de datos de identidades.
- Múltiples sistemas de autentificación como contraseñas.
- Anfitriones, aplicaciones y servidores de aplicación.

Seguridad de profundidad variable

El nivel de seguridad por capas promete grados de seguridad variables, cada nivel de seguridad está apoyado en las capacidades de la capa inferior y ofrece una mayor seguridad.

Pueden recurrirse a las VLAN[45] para hacer una segmentación de la red, esto permite que las empresas incluyan y segmenten sus redes privadas de área local, además controlan y prohíben el intercambio de tráfico con otras VLAN. La separación del tráfico de datos en grupos específicos es un elemento importante para la seguridad sin que existan fugas entre las VLAN.

Se puede conseguir una segunda capa de seguridad utilizando *firewalls*[46], los cuales, posibilitan segmentar en zonas más pequeñas la red. Los *firewalls* restringen el acceso al tráfico interno y externo, ofreciendo conexiones seguras con la red, además los Firewalls son adaptables a las necesidades de las empresas.

A una tercera capa de seguridad se le puede agregar una VPN, la cual, da seguridad hasta el nivel del usuario y brinda acceso seguro a distancia para instalaciones distantes. Las VPN garantizan la integridad y la confidencialidad de los datos.

[45] Una VLAN (LAN virtual) es un grupo de dispositivos de red, tales servidores y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red

[46] Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

El implemento de VPN, VLAN y de los *firewalls*, permiten la restricción de acceso a usuarios o a grupos en la red, dependiendo de los criterios, de las políticas y las necesidades de la empresa.

Gestión de la seguridad

La gestión de la seguridad es una práctica o recomendación global que comprende zonas fundamentales de la infraestructura de la red y exhibe medidas para neutralizar las posibles amenazas sobre de ésta. Se consideran nueve dominios de gestión de red que necesitan atención para que el plano de gestión de la red se considere seguro:[47]

i. **Registros cronológicos de actividad seguros**

Se utilizan para mantener el inventario de las actividades de los usuarios o del administrador y de los sucesos generados por el dispositivo. Los datos reunidos se designan como “registros cronológicos de auditoría”, y el trayecto comprobable se denomina "rastro de auditoría".

Los registros cronológicos de auditoría se pueden utilizar para la reconstrucción de eventos, la detección de intromisión, el análisis de problemas y el pronóstico de tendencias a largo plazo.

Su información ayuda a reconocer la causa de un problema de seguridad y a evitar futuros incidentes.

ii. **Autentificación del operador de red**

Se debe apoyar en una autentificación centralizada de los operadores y administradores de la red. Una administración centralizada de contraseñas ayuda a la solidez de las contraseñas.

[47] Sector de Normalización de las Telecomunicaciones de la UIT. (2008, Abril). *Serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad. Seguridad en el Ciberespacio– Ciberseguridad*. Recuperado de https://www.itu.int/rec/T-REC-X/es

iii. Control de acceso para los operadores de red

En este caso, se han de seguir las prácticas adecuadas, por ejemplo, para determinar el nivel básico de control de acceso pueden utilizarse procedimientos basados en servidores RADIUS[48].

iv. Encriptación del tráfico de gestión de red

La encriptación del tráfico de gestión da una firme protección contra los usuarios, con excepción de aquellos que tienen acceso a las claves de encriptación. Es aconsejable la encriptación del tráfico de datos entero a fin de garantizar la confidencialidad e integridad de los datos.

v. Acceso a distancia seguro para los operadores

La mejor opción para dar seguridad a los administradores y operadores que gestionan la red a través de una red pública es, usar una red privada virtual segura con IPsec, esta red privada virtual garantizará la encriptación y autentificación de todos los administradores distantes.

vi. Firewall

Los *firewalls* controlan el protocolo, número de puerto, dirección de origen y destino del tráfico manejado para diversos dominios de seguridad. El tipo y las reglas de filtrado dependen específicamente de cada red.

vii. Detección de intrusión

Los sistemas de detección de intrusión se emplean para avisar sobre la probabilidad de que ocurra un incidente de seguridad a los administradores de red.

[48] RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

viii. Endurecimiento del OS

Todos los sistemas operativos usados en la gestión de la red -sean operativos generales o sistemas operativos en tiempo real- es recomendable que sean endurecidos.

ix. Software sin virus

El software debe ser examinado antes de ser instalado.

3.2.1.2 Tecnologías de la ciberseguridad

Las técnicas de ciberseguridad más importantes son las siguientes:

Criptografía

La criptografía ejerce un papel fundamental en la protección de la información almacenada y durante su transmisión como un enlace de comunicaciones. La criptografía cambia datos con un código secreto, también utiliza claves secretas para sus procesos, a este cifrado de datos con un código secreto se le denomina encriptación.

Las técnicas criptográficas básicas, pueden ser de dos tipos:

i. Clave simétrica

Utiliza algoritmos en los cuales la clave de encriptación y desencriptación son idénticas. Los algoritmos de clave simétrica pueden ser la norma de encriptación de datos triple (3DES, triple data Encryption Standard) y la norma de encriptación avanzada (AES, Advanced Encryption Standard).

ii. Clave asimétrica.

Utiliza algoritmos que utilizan distintas claves para encriptar y desencriptar el texto cifrado. El usuario tendrá una clave privada para él y una clave pública para los demás. La clave pública es utilizada para encriptar y la privada para desencriptar datos.

Las técnicas de criptografía de clave simétrica se destacan por ser más rápidas de aplicar, por otra parte, la distribución de sus claves es complicada, por lo que no se utilizan a gran escala. La criptografía de clave asimétrica radica en la utilización de certificados digitales para su gestión y como medio para intercambiar de manera segura una clave simétrica.

Tecnologías de control de acceso

El control de acceso posibilita analizar y entender la naturaleza de los ataques que sufre la red, además garantiza que sólo usuarios autorizados puedan acceder al sistema. Las técnicas que se utilizan para controlar el acceso se muestra a continuación:

1. **Protección del perímetro.**

   Instala una frontera lógica o física entre zonas protegidas para impedir el acceso a la red de cualquier usuario no autorizado. Las tecnologías de protección del perímetro comprenden:

   a) Software de filtrado del contenido o de gestión del contenido:

   El filtrado del contenido puede hacerse con filtros URL, que niegan el acceso de los usuarios a páginas web o dudoso contenido.

   b) *Firewalls*:

   Esta tecnología puede dividirse en cuatro categorías:

i. Filtros de paquetes:

Los filtros de paquetes comparan cada paquete IP con una regla previamente definida antes de mandarlo a su destino final. Las reglas pueden contener las direcciones IP de origen y destino, el número de puerto de origen y destino, así como el protocolo utilizado. Dependiendo de la comparación, el firewall puede eliminar, remitir o enviar el paquete.

ii. Pasarelas a nivel de circuito:

Las pasarelas a nivel de circuito trabajan en la capa TCP y supervisan la toma de contacto entre paquetes para descubrir si la sesión es legítima o no. Las pasarelas a nivel de circuito no filtran paquetes individuales.

iii. Pasarelas a nivel de aplicación:

Las pasarelas a nivel de aplicación filtran paquetes en la capa de aplicación del modelo OSI. Además, examinan los paquetes en la capa de aplicación para filtrar instrucciones específicas, no permiten que el tráfico no configurado alcance la aplicación.

iv. *Firewall* de inspección multicapa por estados:

Estos *firewalls* filtran paquetes en la capa de red, deciden si los paquetes de sesión son válidos y filtran el contenido de estos.

c) Traducción de dirección de red o *Network Address Translation* (NAT):

Establece la relación entre la dirección IP de un sistema de la red interna y una dirección IP externa. Con NAT es posible que varios sistemas detrás de los *firewalls* compartan la misma dirección IP externa.

d) Pasarelas a nivel de aplicación:

Las pasarelas a nivel de aplicación están diseñadas para restringir el acceso entre dos redes separadas, utilizan la inspección de paquetes apoyados en estados y los métodos de pasarela a nivel de aplicación para restringir el acceso a la red. Están constituidas por un dispositivo con hardware y software.

e) Intermediario de aplicación:

El intermediario de aplicación supervisa los intentos de conexión a nivel de aplicación a través de un examen de los paquetes en la capa más alta del protocolo. Los intermediarios de aplicación tienen completa visibilidad de los intercambios de datos en la capa de aplicación. Además, tienen la capacidad de poner fin a las conexiones e iniciar una nueva conexión con una red protegida interna.

2. Red Privada Virtual o *Virtual Private Network* (VPN)

Las VPN interconectan redes y usuarios lejanos a las redes, presentan un establecimiento de canal o canales de datos seguros en una red o en conexiones punto a punto. Pueden utilizarse como un servicio en el cual se proporciona conectividad a una infraestructura compartida, gestión y direccionamiento seguro y fiable semejante a los de una red privada.

Hay tres tipos principales de VPN:

a) Las VPN de capa 2: Imitan una LAN para conectar los sitios de una empresa o una organización al usar las conexiones VPN activas.

b) Las VPN de capa 3: Imitan una WAN usando las conexiones VPN activas con una infraestructura de red. Presenta la capacidad de usar esquemas de direccionamiento IP privado en una infraestructura pública.

c) Las VPN de capa 4: Se usan para garantizar las transacciones que se lleva a cabo en redes públicas. Se utiliza conexiones VPN para establecer un canal seguro entre las aplicaciones durante la transacción, así se garantía la confidencialidad y la integridad de los datos.

3. **Autentificación.**

   De acuerdo con el número de factores de identificación, los sistemas de autentificación se clasifican en:

   - De factor único: Utiliza combinaciones de ID de usuario o contraseña.
   - De doble factor: Para acceder al sistema requiere un testigo físico y el conocimiento de un secreto.
   - De triple factor: Añade otro factor como biométrico o medición de una parte del cuerpo.

4. **Autorización.**

   Después de realizar la autentificación, los dispositivos de autorización controlan el acceso a los sistemas. La autorización se clasifica en función del nivel con que se dividen los recursos del sistema, pueden ser:

   - Granularidad: sistema que maneja el acceso a puntos muy específicos.
   - Dependiente de la función: el acceso se basa en la función que se ha establecido al usuario dentro de la organización.
   - Dependiente de la regla: independientemente de la función de los usuarios dentro de la organización, el acceso se basa en reglas específicas ligadas a cada usuario.

Antivirus e integridad del sistema.

La tecnología antivirus ayuda a proteger sistemas contra ataques por gusanos, códigos maliciosos y caballos de Troya. Por otro lado, las técnicas de integridad del sistema emplean software que examina las actualizaciones autorizadas en el sistema.

Auditoría y supervisión.

Los procesos de auditoría y supervisión permiten determinar la seguridad global del sistema -después o durante un ataque- se puede analizar la debilidad del sistema.

El sistema de detección de intrusos compara el tráfico de red y las entradas del registro cronológico para encontrar firmas y perfiles de dirección, indicativos de piratas. Las actividades sospechosas arrojan alarmas de administrador y preguntas configurables, este sistema de detección de intrusos puede clasificarse en:

a) Plano de detección de incidentes:
   - Tiempo real.
   - Fuera de línea.

b) Tipo de instalación:
   - En red.
   - En anfitrión.

c) Tipo de reacción ante incidentes.

3.2.2 ARQUITECTURAS DE SEGURIDAD

En 2003 se aprobó la recomendación UIT-T X.805, dicha norma puede aplicarse a distintos tipos de redes y es independiente de la tecnología que utilice la red.

Esta arquitectura de seguridad, de la recomendación UIT-T X.805 ofrece una visión general, así como de extremo a extremo de la seguridad de la red para detectar, evaluar y reparar debilidades de seguridad.[49]

La arquitectura se divide en una serie de características de seguridad de red punto a punto en distintos componentes de la arquitectura, la figura 2.2 muestra esos elementos que permite examinar la seguridad de extremo a extremo de forma ordenada, de igual manera, diseña medidas en cada una de las dimensiones de seguridad para solucionar amenazas específicas.

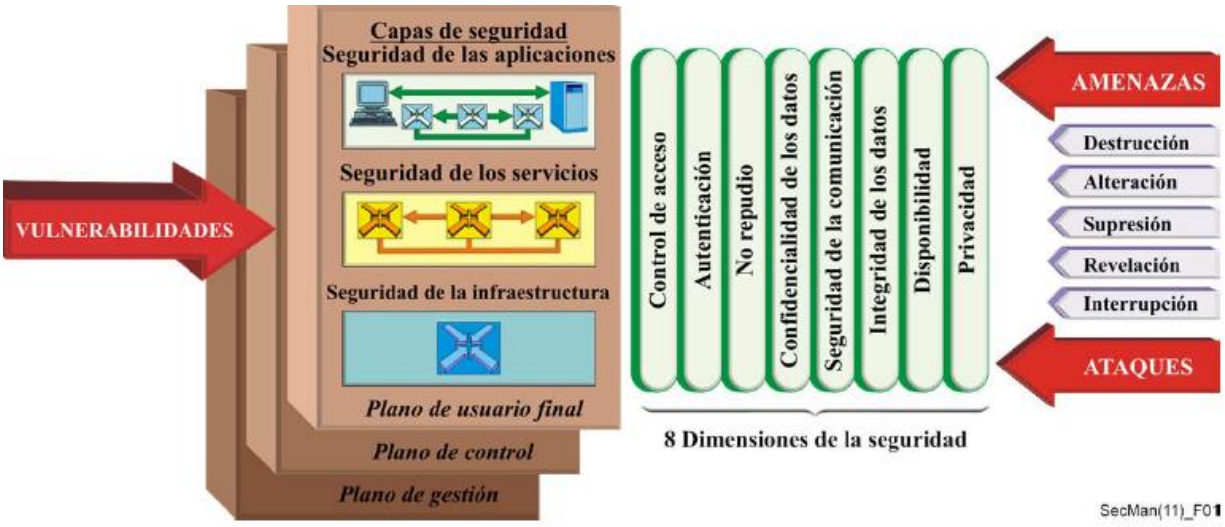

Figura Nª 1. Elementos de la arquitectura de seguridad.
Fuente: Seguridad de las telecomunicaciones y las tecnologías de la información, 2012.

[49] Sector de Normalización de las Telecomunicaciones de la UIT. (2012, Enero). *Seguridad de las telecomunicaciones y las tecnologías de la información*. Recuperado de http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf

Además, la recomendación UIT-T X.805 determina tres componentes principales de las arquitecturas: las capas de seguridad, los planos de seguridad y las dimensiones de seguridad, los cuales, se describen a continuación.

3.2.2.1 Dimensión de seguridad

Es un grupo de medidas de seguridad que responde a un definido aspecto de infalibilidad de la red. Brindan más protección para la red y la defienden de las amenazas de seguridad. En la recomendación se identifican ocho medidas contra las principales amenazas:

i. **Dimensión de seguridad control de acceso**

Garantiza que sólo los dispositivos y usuarios autorizados pueden acceder a los elementos de la red, a la información almacenada, a los servicios y las aplicaciones. Establece varios niveles para restringir el acceso; el control de acceso, está basado en las funciones RBAC (Role Based Acces Control).

ii. **Dimensión de seguridad autenticación**

Comprueba la identidad de las entidades de comunicaciones. De esta forma, garantiza la autenticidad de la identidad que se le asigna a personas, dispositivos, servicios o aplicaciones, de tal manera, que una entidad no usurpa la identidad de otra.

iii. **Dimensión de seguridad no repudio**

Evita que una entidad delegue su responsabilidad sobre la operación de tratamiento de datos, pues otorga pruebas de distintas acciones en la red. Asegura la disponibilidad de pruebas para demostrar que un determinado evento sí ha sucedido.

iv. Dimensión de seguridad confidencialidad de los datos

Impide que los datos sean difundidos sin autorización. Garantiza que entidades no autorizadas puedan descifrar el contenido de datos. Los procedimientos más utilizados son la encriptación, así como las listas de control de acceso y las autorizaciones de archivos.

v. Dimensión seguridad de la comunicación

Garantiza que la información solo circule, que no se intercepte o se separen entre puntos extremos autorizados.

vi. Dimensión de seguridad integridad de los datos

Protege los datos contra operaciones no autorizadas de modificación, supresión y creación. Garantiza la precisión y veracidad de los datos.

vii. Dimensión disponibilidad

Asegura que no se le niegue el acceso autorizado a la red, a causa de sucesos que afecten a la ley o a políticas establecidas: afectando a la información almacenada, a los servicios y las aplicaciones.

viii. Dimensión privacidad

Protege la información que pueda proceder de la observación de las actividades de la red.

3.2.2.2 Capas de seguridad

Son sistemas que permiten ejecutar soluciones seguras de red, además proporcionan una perspectiva secuencial de la red, que define dónde actúa en beneficio a la seguridad de los productos.

En esta recomendación, se definen tres capas de seguridad:

a) Capa de seguridad de infraestructura

Representa los bloques de construcción de las redes, sus servicios y aplicaciones. Engloba los dispositivos de transmisión de la red y los elementos que están protegidos por las distintas dimensiones de seguridad.

b) Capa de seguridad de servicios

Se utiliza para proteger a los proveedores de servicios y a los usuarios que están expuestos a amenazas contra la infalibilidad, los servicios pueden ser básicos como, transporte y conectividad hasta, servicios de valor añadido.

c) Capa de seguridad de aplicaciones

Ajusta la seguridad de las aplicaciones de red a las que acceden los usuarios. En esta capa hay cuatro tipos de ataques contra la seguridad: el usuario, el proveedor de la aplicación, los programas de terceros y el proveedor del servicio.

3.2.2.3 Planos de seguridad

Compete a necesidades de seguridad particulares, referentes a las actividades de: gestión de red, control de red, así como a las de usuarios finales. Las redes se diseñan de manera tal, que los sucesos de un plano de seguridad estén aislados de los otros planos de seguridad

Se definen tres planos de seguridad que representan a los tres tipos de funciones protegidas en la red:

i. Plano de seguridad de gestión

Se relaciona con las actividades de operaciones, administración, mantenimiento y suministro de un usuario o una red.

ii. Plano de seguridad de control

Tiene que ver con aspectos necesarios para proteger y establecer la comunicación punto a punto a través de la red, sin importar el medio y la tecnología usada. Permite determinar la mejor forma de conmutar el tráfico en la red.

iii. Plano de seguridad de usuario extremo

Se relaciona con la seguridad del tráfico de datos del usuario extremo cuando accede y utiliza la red del proveedor de servicios.

3.2.3 SEGURIDAD DE LA INFRAESTRUCTURA DE RED

La recomendación UIT-T M.3010 describe una red separada que transmite datos para supervisar y controlar el tráfico de gestión de la red, esta red es conocida como Red de Gestión de las Telecomunicaciones (RGT).[50]

Respecto a su finalidad, una Red de Gestión de las Telecomunicaciones soporta una extensa variedad de áreas de gestión que comprenden la planificación, la instalación, la operación, la administración, el mantenimiento y suministro de redes y servicios de telecomunicaciones.

Una Red de Gestión de las Telecomunicaciones proporciona una arquitectura organizada con el fin de obtener una interconexión entre diversos tipos de sistemas de operaciones y equipos de telecomunicaciones para el intercambio de información.

[50] Sector de Normalización de las Telecomunicaciones de la UIT. (2000, Febrero). *Serie M: RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales.* Recuperado de http://www.itu.int/rec/T-REC-M.3010/es

La Red de Gestión de las Telecomunicaciones se desprende y aísla de la infraestructura de la red pública, de esta forma, garantiza que no se contamine con la problemática que representan las amenazas a la seguridad en el plano de usuario de una red pública, ya que, el acceso a este plano, está condicionado a los administradores de red autorizados.

La Red de Gestión de las Telecomunicaciones se compone de tres arquitecturas diferentes e intercomunicadas: arquitectura funcional, de información y física.

3.2.3.1 Arquitectura funcional

Es un marco de gestión estructural y global de la Red de Gestión de las Telecomunicaciones,[51] la utilidad se puede explicar a través de los siguientes elementos fundamentales:

Bloques de función de la Red de Gestión de las Telecomunicaciones

El bloque funcional, es la unidad más pequeña de las propiedades de la gestión de la Red de Gestión de las Telecomunicaciones. Algunos bloques de función están dentro y parcialmente fuera, aquí la definición:

a) **Bloque de función de sistemas de operaciones (OSF, Operation System Function).**

   Procesa información con el propósito de supervisar, coordinar o controlar funciones y gestiones de telecomunicaciones.

[51] Sector de Normalización de las Telecomunicaciones de la UIT. (2000, Febrero). *Serie M: RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales.* Recuperado de http://www.itu.int/rec/T-REC-M.3010/es

b) Bloque de función de elemento de red (NEF*, Network Element Function*)

Proporciona las funciones de telecomunicaciones y de soporte solicitadas por la red que está siendo gestionada.

c) Bloque de función de estación de trabajo (WSF*, Workstation Function*)

Facilita el medio de interpretar información de la Red de Gestión de las Telecomunicaciones para el usuario y viceversa. Una parte del bloque encuentra fuera de la frontera a causa, de la responsabilidad del traslado, que tiene entre un punto de referencia y un punto de no referencia.

d) Bloque de función de transformación (TF, T*ransformation Function*)

Conecta dos entidades con mecanismos de comunicación incompatibles, los cuales, pueden ser protocolos o modelos de información. El bloque TF se puede usar en cualquier lugar o en cualquiera frontera de una RGT.

3.2.3.2 Arquitectura de la información de la Red de Gestión de las Telecomunicaciones

Está basada en modelos de gestión abiertos normalizados, que mantienen el modelado de la información que van a comunicar. La información de gestión desempeña un papel fundamental para las administraciones, por lo que se deben aplicar técnicas de seguridad en el entorno de la Red de Gestión de las Telecomunicaciones y debe asegurar la protección de la información a través de las interfaces.

La arquitectura de la información de la Red de Gestión de las Telecomunicaciones, se ordena e intercambia información a partir de los siguientes elementos fundamentales:

Modelo de interacción

Éste modelo proporciona las reglas y esquemas que dirigen el flujo de información entre los bloques de función de la Red de Gestión de las Telecomunicaciones.

Los procesos de gestión para el intercambio de información, aceptan una de las dos funciones posibles:

a) Función gestionada:

Técnica que gestiona los elementos de información de la Red de Gestión de las Telecomunicaciones, ligada con recursos gestionados. Revela un aspecto de los elementos de información y proporciona la información que refleja la conducta del recurso, por ejemplo: la fuente de información.

b) Función gestionante:

Técnica que crea directivas de operación de gestión y recibe la información del proceso, por ejemplo: el usuario de la información.

Modelos de información de gestión de la Red de Gestión de las Telecomunicaciones

Este modelo presenta el alcance de la información, que puede ser revelada e intercambiada en una forma normalizada. Tiene presencia, en el nivel de aplicación y presenta una variedad de aplicaciones de gestión, tales como: almacenamiento, extracción e información de procedimiento.

Elementos de información de gestión de la Red de Gestión de las Telecomunicaciones

Los elementos pueden ser normas conceptuales de los recursos, que han de ser gestionados, o pueden mantener determinadas funciones de gestión, supervisando desde sus propiedades hasta los fines de gestión.

Modelo de información de un punto de referencia

Este modelo de información, es la agrupación mínima de información de gestión revelada, que puede ser especificada en un bloque de función de la Red de Gestión de las Telecomunicaciones.

Puntos de referencia

Este concepto representa la suma de las capacidades con intercambio de información que un bloque de función requiere de otro bloque de función. Del mismo modo, unifica la arquitectura funcional y la de información de la Red de Gestión de las Telecomunicaciones, a través, de la interacción de los bloques de función de la Red de Gestión de las Telecomunicaciones. Los bloques de función, articulan la información de gestión sobre el punto de referencia.

3.2.3.3 Arquitectura física de la Red de Gestión de las Telecomunicaciones

La arquitectura física de la Red de Gestión de las Telecomunicaciones, está ordenada en bloques físicos e interfaces físicas. Los bloques físicos se designan de acuerdo al conjunto de bloques de función que puede contener cada uno, para cada bloque físico, hay un bloque de función característico que lo contiene.

a) **Sistema de operaciones (OS)**

Ejecuta funciones de sistemas de operaciones, proporciona ocasionalmente las funciones de adaptador y de estación de trabajo.

b) **Transformación**

Dispositivo que produce la conversión entre diferentes protocolos y formatos de datos para el intercambio de información entre bloques físicos. Existen dos tipos que se aplican a los puntos de referencia: la de adaptación y de mediación.

- Dispositivo de adaptación (AD):
  Proporciona la transformación entre un organismo físico no Red de Gestión de las Telecomunicaciones y un elemento de red o sistema de operaciones.

- Dispositivo de mediación (MD):
  Proporciona transformación entre bloques físicos de la Red de Gestión de las Telecomunicaciones que integran mecanismos de comunicación incompatibles.

c) Elemento de red (NE)

Constituido por equipos de telecomunicación y equipos de soporte.

d) Estación de trabajo (WS).

Las funciones que ejecuta la estación de trabajo es traducir la información ubicada en el punto de referencia a un formato visible.

3.2.3.4 Relaciones entre arquitecturas de la Red de Gestión de las Telecomunicaciones

En el marco de la arquitectura funcional y la arquitectura de información, se expresan las necesidades empresariales que deben llenar por medio de la implementación de la Red de Gestión de las Telecomunicaciones.[52] Estas implementaciones, pueden variar según las especificaciones funcionales y de información de la Red de Gestión de las Telecomunicaciones.

[52] Sector de Normalización de las Telecomunicaciones de la UIT. (2000, Febrero). *Serie M: RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales.* Recuperado de http://www.itu.int/rec/T-REC-M.3010/es

Cada implementación de la Red de Gestión de las Telecomunicaciones debe enfrentar distintas limitaciones, tales como: costos, calidad de funcionamiento y funciones suministradas, de esta forma, existe una diversidad de implementaciones de arquitecturas físicas.

Cada implementación debe satisfacer las necesidades reconocidas y especificadas de la arquitectura funcional y de información de la Red de Gestión de las Telecomunicaciones. Para explicarlo mejor, se expone en la figura 2.

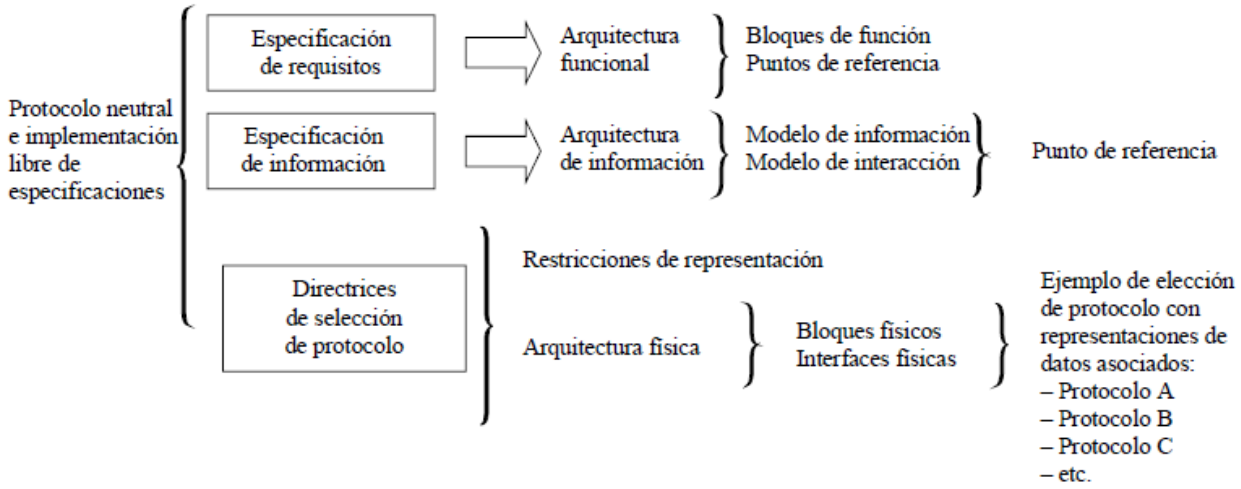

Figura Nª 2. Relación entre las arquitecturas de la RGT

Fuente: Serie M: RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales, 2000.

3.3 LA UNIÓN EUROPEA

En marzo de 2010 la Comisión Europea, puso en acción la estrategia "Europa 2020," la cual plantea estrategias para: conseguir una economía de baja emisión de carbono, altos niveles de empleo, productividad y unión social.

Entre las siete iniciativas emblemáticas de la estrategia Europa 2020, la que se expone en este capítulo es "La Agenda Digital para Europa", pues propone medidas para encaminar a Europa hacia un crecimiento inteligente, sostenible e incluyente. Las propuestas constituyen el marco que proyecta una sociedad y una economía digital.[53]

El objetivo de la Agenda Digital para Europa es dar prioridad al aprovechamiento de las tecnologías digitales, y en particular la de promover internet como base fundamental para hacer negocios, trabajar, jugar, comunicarse y expresarse en libertad. Dicha Agenda promoverá la innovación, el crecimiento económico y la mejora de la vida, tanto para los ciudadanos como, para las empresas.[54]

La Agenda Digital para Europa tiene en cuenta que, la confianza y seguridad en internet son importantes para mejorar la ciberseguridad, en consecuencia, a esto, incluye iniciativas que se enfocan en el combate contra la ciberdelincuencia y a la inclusión de mecanismos de protección para las infraestructuras criticas de información.

[53] Comisión Europea. (2010, Marzo). *Una estrategia para un crecimiento inteligente, sostenible e integrador*. Recuperado de https://www.sepe.es/contenidos/personas/formacion/refernet/pdf/Estrategia_Europa_2020.pdfn

[54] Comisión Europea. (2010, Marzo). *Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global*. Recuperado de http://eur-lex.europa.eu/procedure/ES/200304

Una infraestructura crítica está definida como:

"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas ". (Directiva europea: 2008/114/CE,8 de diciembre de 2008).[55]

La Comisión adoptó el Plan de Acción PICI o de Protección de Infraestructuras Críticas de Información (PICI), designado para proteger a Europa de ciberataques, aumentar la preparación, fortalecer la seguridad y la resistencia de las infraestructuras vitales de las Tecnologías de la Información y la Comunicación (TIC).

La Agenda Digital para Europa apunta que la cooperación entre entidades debe organizarse a nivel mundial, de esta manera, las peleas contra las amenazas a la seguridad serán realmente efectivas, además propone fortalecer la gestión mundial de los riesgos en el mundo físico y en el digital.

Dicho lo anterior, la Comisión define qué es amenaza, vulnerabilidad y riesgo, para que las personas involucradas en los diferentes procesos, procedimientos y operaciones de las Infraestructuras Críticas de Información, manejen claramente los conceptos.[56]

[55] Ministerio de defensa. (2014, Junio). Documentos de Seguridad y Defensa 60 Estrategia de la información y seguridad en el ciberespacio.
Recuperado de http://www.defensa.gob.es/ceseden/ealede/publicaciones/docSegyDef/

[56] Comisión Europea. (2010, Marzo). *Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global*. Recuperado de http://eur-lex.europa.eu/procedure/ES/200304

Amenazas

Se definen como los elementos causados por fuerzas extrañas o no extrañas, peligrosos para el hombre, comunidad o instalación.

Vulnerabilidad

Es el conjunto de condiciones y procesos originados por factores físicos, tecnológicos, sociales, económicos y ambientales, susceptibles de daños frente al impacto de peligros o amenazas.

Riesgos

Corresponden a la probabilidad de que una amenaza se convierta en un desastre, con graves consecuencias económicas, sociales y ambientales.

Y como complemento, la Comisión presentó una propuesta, con el objetivo de fortalecer y modernizar la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), la cual, ejerce como centro de conocimiento especializado de ciberseguridad en las redes de información de la Unión Europea y también, desempeña una labor importante en la coordinación de respuesta de los estados miembros.

Para hacer frente a los delitos cibernéticos, destaca la creación de equipos de respuesta a emergencias informáticas o CERT, que son las siglas en inglés para *Computer Emergency Response Team*.

3.3.1 COMPUTER EMERGENCY RESPONSE TEAM (CERT)

El primer CERT apareció a finales de los 80 en E.U.A., debido a su éxito y a las recomendaciones internacionales de organismos ligados con la seguridad de las redes de telecomunicaciones, han hecho que los CERT se hayan multiplicado en el mundo.

Europa cuenta con la mitad de los CERT del mundo, los que encabezan la lista con mayores CERT son: Alemania con 21, Reino Unido con 17 y Holanda con 10.

Un CERT está conformado por un equipo de expertos en seguridad de las TI, encargados de los incidentes de seguridad y de ayudar a los clientes a recobrarse después de sufrir uno. Además, ofrece servicios preventivos y educativos para minimizar o disminuir los riesgos.[57]

Algunas ventajas importantes de tener un CERT:

- Se dispone de una organización centralizada para asuntos de la seguridad de las TI.
- Trata de un modo centralizado y especializado los incidentes con las TI.
- Tiene los conocimientos necesarios para asistir a los usuarios que se recuperan de un incidente de seguridad.
- Fomenta la colaboración en la seguridad de las TI entre los clientes.

3.3.1.1 Servicios posibles de un CERT

El manual del CERT define varios servicios que pueden ser prestados y por el momento ningún CERT presta todos los servicios. La selección de servicios conocidos es:

- **Servicios básicos:**
  Se distinguen 2 tipos, servicios reactivos y servicios proactivos.

[57] European Network and Information Security Agency. (2006, Diciembre). Cómo crear un CSIRT paso a paso. Recuperado de http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-spanish

Los proactivos están enfocados a la prevención de incidentes, aquí se expone una visión general:

- Comunicados
- Observatorio de tecnología
- Evaluaciones o auditorias de la seguridad
- Configuración y mantenimiento de la seguridad
- Servicios de detección de intrusos
- Desarrollo de herramientas de seguridad

Los reactivos se orientan en el tratamiento de incidentes y la disminución de los daños resultantes.
Los servicios más conocidos son:

- Alertas y advertencias
- Tratamientos de incidentes
- Análisis de incidentes
- Apoyo a respuestas de incidentes
- Tratamiento de vulnerabilidad
- Análisis de la vulnerabilidad
- Respuesta de la vulnerabilidad

- **Servicios de gestión de la seguridad y la calidad:**
  Sus objetivos son a largo plazo y comprenden la consultoría y medidas de tipo educativo.

  - Análisis de riesgos
  - Continuidad del negocio y recuperación tras un desastre
  - Consultoría de seguridad
  - Sensibilización
  - Educación/Formación

- **Manejo de instancias**

  Hace la difusión y el tratamiento de la información proveniente de proveedores e interesados, lo servicios que hace son:

  - Análisis de instancias
  - Respuesta a las instancias
  - Coordinación de la respuesta a las instancias

3.3.1.2 Generación de alertas, advertencias y comunicados

Aquí se describen los procedimientos básicos y métodos de trabajo de los CERT en el esquema de la información como se muestran en la figura 3, la cual, detalla la recopilación de información procedente de diferentes fuentes, la comprobación y su autenticidad, así como la devolución al grupo de clientes.

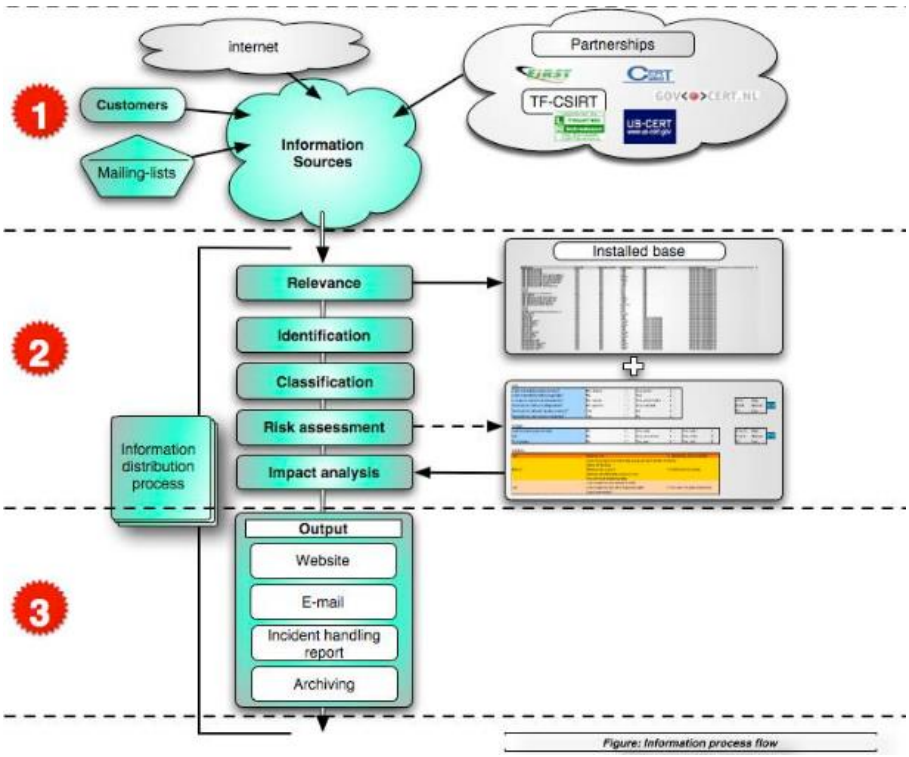

Figura Nª 3. Esquema de la información.
Fuente: Cómo crear un CSIRT paso a paso,2006.

PASO 1- Recopilación de información sobre la vulnerabilidad

La información recolectada aumenta el nivel de entendimiento sobre las vulnerabilidades de los sistemas de TI.

Existen dos tipos de fuentes información que aportan conocimientos a los servicios:

- Información sobre la vulnerabilidad de los sistemas de TI.
- Informes sobre incidentes.

Dependiendo de la empresa y de la infraestructura de TI se encuentran diversas fuentes de información sobre vulnerabilidad, ya sean fuentes públicas o privadas:

- Listas de correo públicas o cerradas.
- Información facilitada por los proveedores de los productos.
- Sitios web.
- Información pública en internet.
- Información sobre vulnerabilidad proporcionada por socios públicos y privados.

PASO 2: Evaluación de la información y valoración del riesgo

En este paso, se realiza un estudio de la vulnerabilidad de la infraestructura de TI en el grupo de clientes.

Identificación

Siempre la información sobre vulnerabilidad entrante ha de ser identificada y se ha de determinar si la fuente es de confianza. En caso de no serlo, se generarían alertas que provocarían molestias en los procesos y perjudicarían a los CERT.

Pertinencia

Se utiliza el hardware y el software para filtrar la información sobre vulnerabilidad respondiendo a dos preguntas: ¿es esta información pertinente para dicho grupo? y ¿el grupo atendido utiliza este software?

Clasificación

Se puede clasificar la información recibida, teniendo en cuenta las indicaciones del remitente y la política de seguridad de la información que se maneja.

Evaluación del riesgo y análisis de las consecuencias

Para determinar el riesgo y las consecuencias de una vulnerabilidad, existen diferentes métodos.

Para tener una idea de la gravedad de la vulnerabilidad se tienen en cuenta las siguientes preguntas:

- ¿La vulnerabilidad es conocida?
- ¿Está muy desarrollada?
- ¿Es fácil de explotar?

En el caso de riesgo se recurre a la fórmula:

- Impacto= Riesgo X Daños potenciales

Los daños potenciales pueden ser:

- Acceso no autorizado a los datos
- Negación de servicios
- Ampliación de permisos

PASO 3: Distribución de la información

La posibilidad de elección entre diversos métodos de distribución, cada CERT elige el de su preferencia, basados en el grupo de cliente o en su estrategia de comunicación:

- Sitio web.
- Correo electrónico
- Informes
- Archivo e investigación

Un aviso de seguridad debe seguir una misma estructura, de esta forma, mejorará la legibilidad y el lector, encontrará rápidamente la información pertinente; la siguiente figura 4 muestra la información mínima que debe contener:

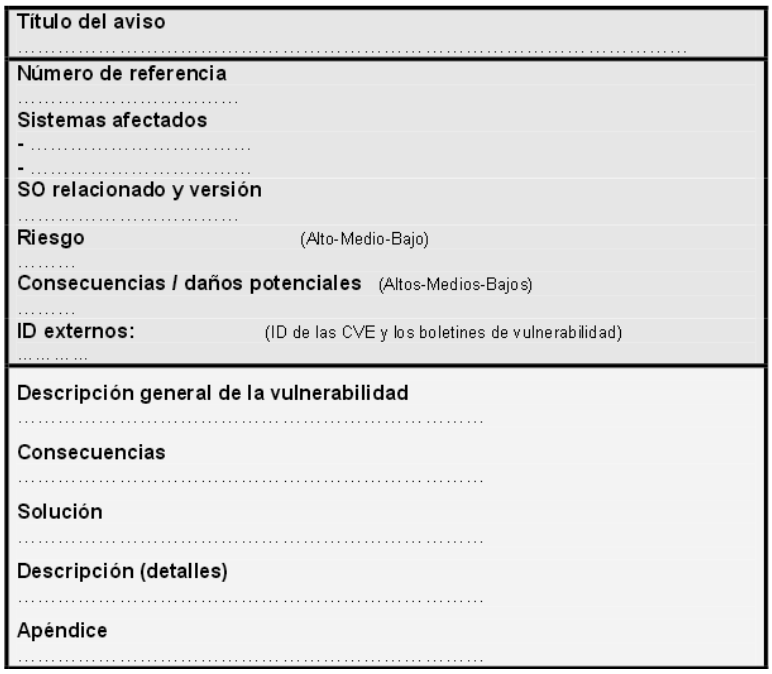

Figura Nª 4. Ejemplo de aviso de seguridad.
Fuente: Cómo crear un CSIRT paso a paso, 2006.

3.3.1.3 Tratamiento de los incidentes

El tratamiento de los incidentes lleva el mismo proceso que el tratamiento de información, la diferencia radica en el proceso de recopilación de la información. En la siguiente figura 5 se describe el proceso de tratamiento de incidentes:

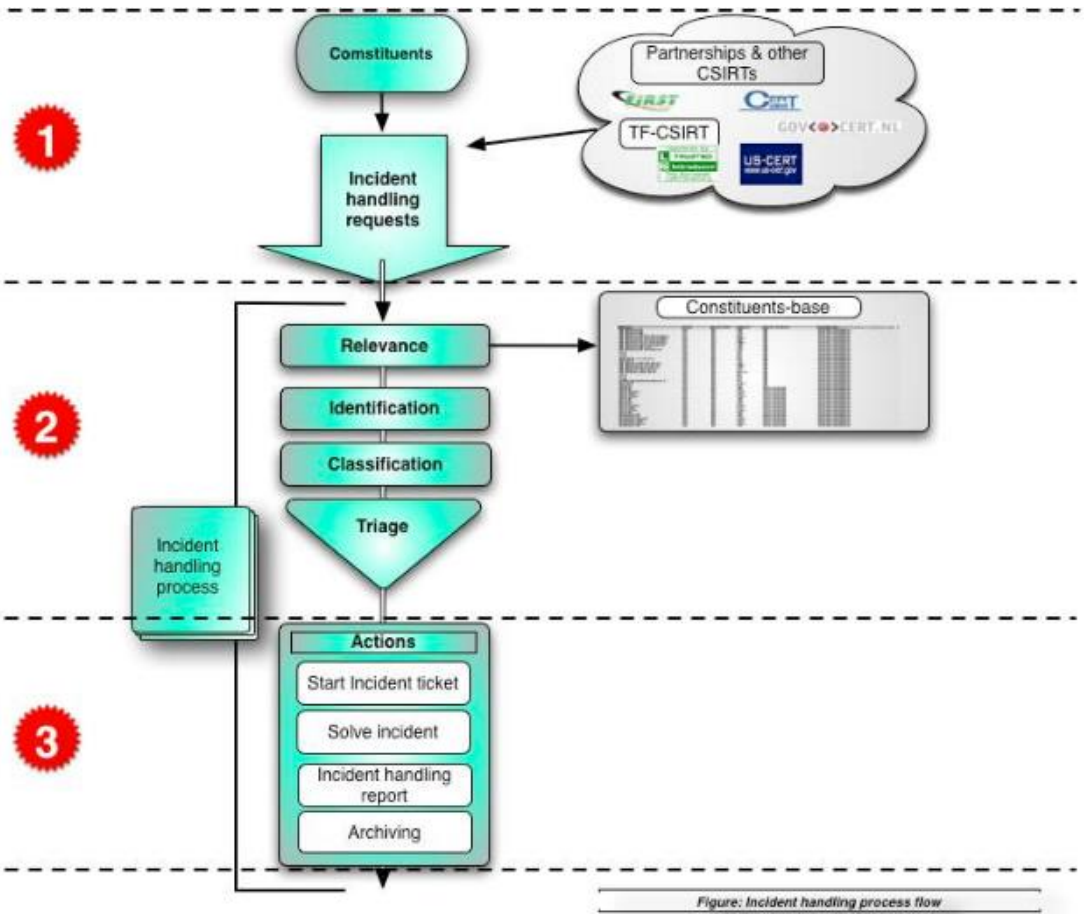

Figura Nª 5. Esquema de tratamiento de incidentes.
Fuente: Fuente: Cómo crear un CSIRT paso a paso, 2006.

PASO 1: Recepción de los informes de incidentes

Las notificaciones de incidentes llegan por diversos canales al CERT, ya sea por teléfono, fax o e-mail. Se recomienda anotar todos los detalles cuando se recibe la notificación del incidente con un formato parecido al de la figura 6:

FORMULARIO DE COMUNICACIÓN DE INCIDENTE

Sírvase rellenar este formulario y enviarlo por fax o correo electrónico a: ……
Las líneas marcadas con un asterisco (*) son de respuesta obligatoria.

Nombre y organización
1. Nombre*:
2. Nombre de la organización*:
3. Sector:
4. País*:
5. Ciudad:
6. Dirección de correo electrónico*:
7. Número de teléfono*:
8. Otros:

Ordenador(es) afectado(s)
9. Número de ordenadores:
10. Nombre del ordenador e IP*:
11. Función del ordenador*:
12. Zona horaria:
13. Hardware:
14. Sistema operativo:
15. Software afectado:
16. Ficheros afectados:
17. Seguridad:
18. Nombre del ordenador e IP:
19. Protocolo/puerto:

Incidente
20. Número de referencia:
21. Tipo de incidente:
22. Inicio del incidente:
23. El incidente aún no se ha resuelto: Sí NO
24. Hora y método de descubrimiento:
25. Vulnerabilidades conocidas:
26. Ficheros sospechosos:
27. Medidas:
28. Descripción detallada*:

Figura Nª 6. Contenido de un formato de incidente.
Fuente: Cómo crear un CSIRT paso a paso, 2006.

PASO 2: Evaluación del incidente

En este paso confirma la autenticidad, congruencia del incidente y se clasifica.

Identificación

Comprueba que el creador del aviso es auténtico y que pertenece al grupo de clientes, así se evita acciones innecesarias.

Congruencia

Confirma que la petición de tratamiento del incidente procede del grupo de clientes; o si afecta a sistemas TI.

Clasificación

Ordena el incidente según su gravedad y se prepara el "triage", el cual, permite realizar una evaluación inicial de un informe entrante, además de ser el punto de partida para trabajar con documentación y datos de una petición.

PASO 3: Acciones

El tratamiento de incidentes sigue estos pasos:

Resguardo de incidente

El primer paso es, crear el número de resguardo del incidente para poderlo utilizar en comunicaciones posteriores.

Ciclo de vida del incidente

Al incidente se le aplica una serie de procesos repetidamente hasta que se resuelve, esta estructura es llamada ciclo de vida, porque cada paso es consecutivo, dichos procesos son:

- **Análisis:**
  Se estudian todos los detalles del incidente.

- **Información de contacto:**
  Todas las partes implicadas son informadas sobre los datos del incidente.

- **Asistencia técnica:**
  Se recoge información sobre el ataque y se ayuda a los afectados a recuperarse rápidamente.

- **Coordinación:**
  Se informa a otras partes implicadas del sistema TI.

Informe de tratamiento de incidente

Se escribe un documento sobre las lecciones aprendidas para evitar errores en el tratamiento de futuros incidentes.

3.3.1.4 Herramientas disponibles para CERT

A continuación, se presentan recomendaciones sobre herramientas comunes que usan los CERT.

- **Software de encriptación de correos electrónicos y mensajes**

  GNUPG

  Es un software que permite encriptar y firmar los datos y comunicaciones. Su utilidad principal es la combinación con el cliente de correo, además evita el uso de algoritmos patentados para mantener libertad e independencia.

  PGP

  Son las siglas para *Pretty Good Privacy* o privacidad bastante buena. Sirve para cifrar contenido y acceder a él mediante una clave pública y firmar documentos digitalmente para autentificarlos.

- **Herramientas de tratamiento de incidentes**

  Request Tracker for Incident Response **(RTIR)**

  Es un sistema que responde a las necesidades de los CERT y equipos de respuesta a incidentes para el tratamiento de incidentes.

- **Herramientas de Administración basada en la relación con los clientes o *Customer Relationship Management* (CRM)**

  Son una base de datos CRM para un grupo amplio y necesitado de localizar los detalles, algunos ejemplos son:

  - *SugarCRM.*
  - *Sugarforce.*

- **Verificación de la información**

  Websitewatcher

  Detecta actualizaciones y cambios en los sitios web.

  Watchthat page

  Envía por e-mail información sobre cambios en páginas web.

3.4 International Organization for Standardization (ISO)

ISO/IEC 27000 publicado en mayo de 2009, es un conjunto de estándares internacionales para Sistemas de Gestión de la Seguridad de la Información (SGS), desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission)* proporcionan un marco de gestión de seguridad sobre la información usada por cualquier tipo de organización: pública o privada, grande o pequeña.[58]

El conjunto de estándares que aportan información a la familia 27000 son los siguientes:

- **ISO 27001.**
  Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Este estándar ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

- **ISO 27002.**
  Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

- **ISO 27003.**
  Es una guía de implementación de SGSI e información acerca del uso del modelo PDCA (*Plan, Do, Check, Act*) y de los requerimientos de sus diferentes fases.

[58] Gutiérrez, C. S.; Liceaga, C. J.; Baker E. T. & Aguilar, R. G. (2009, Diciembre). *Manual de normas y políticas de seguridad informática.* México: UVM.

- **ISO 27004**

  Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

- **ISO 27005.**

  Establece las directrices para la gestión del riesgo en la seguridad de la información. Está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, es aplicable a todo tipo de organizaciones, que tengan la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información.

- **ISO 27006**

  Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

En este capítulo, la norma que vamos a analizar es la ISO 27011, ya que es una guía de gestión de seguridad de la información en Telecomunicaciones, elaborada en conjunto con la ITU.

3.4.1 ISO/IEC 27011.

La norma ISO 27011 garantiza la seguridad de la información a través de los controles adecuados, por lo que estos controles, han de ser dirigidos, especificados e implementados, para llevar a cabo el cumplimiento de los objetivos de seguridad.[59]

[59] Telecommunication standardization sector of ITU. (2008, Febrero). *Series X: data networks, open system communications and security. Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.* Recuperado de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43751

La elección de estos controles va a depender de la identificación y evaluación continua de los posibles riesgos de seguridad que tengan las organizaciones de telecomunicaciones. La implementación de esta norma recomienda a las organizaciones dedicadas a las telecomunicaciones ejecutar lo siguiente:

- Proteger la integridad, confidencialidad y disponibilidad de las infraestructuras y servicios.
- Organizar los recursos para que las actividades sean más eficientes.
- Admitir un principio global relacionado con la seguridad de la información.
- Reforzar la disminución de los riesgos de los servicios que ofrecen las empresas de telecomunicaciones.

A continuación, se exponen puntos destacables en el ámbito de la protección de las telecomunicaciones sobre la norma ISO 27011:

3.4.1.1 Comunicaciones y operaciones de gestión

Su objetivo es asegurar el funcionamiento óptimo y correcto del proceso de la información. Establece las responsabilidades y procedimientos para la gestión de la información, que incluyen el desarrollo de procedimientos adecuados operativos.

Documentación de procedimientos operativos

La documentación de procedimientos debe estar preparada para las actividades del sistema, así como asociada con el procesamiento de la información e instalaciones de comunicación; tales como: computadoras de inicio, copias de seguridad, mantenimiento de equipos, manejo de medios, cuarto de informática, gestión de manejo y seguridad del correo.

Los procedimientos operativos y de documentación, deben ser tratados como documentos formales, donde puedan ser manejados e implementados los mismos procedimientos, herramientas y utilidades.

Los procedimientos operativos deben especificar detalladamente las instrucciones para la ejecución de cada trabajo incluyendo:

- Proceso y manejo de la información
- Respaldo
- Requerimientos de horario
- Instrucciones para el manejo de errores
- Contactos de soporte en caso de dificultades técnicas
- Procedimientos de reinicio y recuperación en caso de fallo

Gestión del cambio

La gestión del cambio controla los cambios en las instalaciones y sistemas de procesamiento de información. Los sistemas de operación y de software deben estar sujetos a una gestión estricta de control de cambio, así como a los siguientes elementos:

- Identificación y registro de cambios significativos
- Planificación y pruebas de cambio
- Evaluación de impactos potenciales
- Procedimiento de aprobación de cambios
- Comunicación de los detalles de cambio para todas las personas involucradas

Una causa común de fallas en la seguridad es el inadecuado control de cambios en las instalaciones y sistemas de procesamiento de información. Los cambios en el entorno operacional pueden causar un impacto en la fiabilidad de las aplicaciones.

Separación de instalaciones de desarrollo, de pruebas y operativas

En las organizaciones de telecomunicaciones, los datos usados en un ambiente de prueba y desarrollo, deben ser adecuados en los sistemas y servicios de telecomunicaciones para ser probados en situaciones reales. Cuando la información incluye datos sensibles, los controles deben ser apropiados para evitar la fuga de información causada por errores del programa o errores operativos.

Además, la mayoría de los datos deben ser manejados apropiadamente tomando en cuenta su ciclo de vida, desde la recolección hasta la producción; y en la destrucción de datos, después de las pruebas. Solo el personal de desarrollo puede tener acceso a las contraseñas de operación, desde donde controla la emisión de contraseñas para el apoyo de sistemas operativos. Después del uso de las contraseñas, es necesario garantizar su cambio.

El nivel de separación entre las instalaciones de desarrollo, de pruebas y operativas; se debe identificar y adecuar para evitar problemas operacionales. Algunos elementos que deben ser considerados son:

- Reglas para la creación de software, desde el desarrollo hasta su funcionamiento, deben ser definidos y documentados.
- Software de desarrollo y operación, deben ejecutarse en diferentes sistemas o procesadores de computadoras, en diferentes dominios o directorios.
- Compiladores, editores y otras herramientas de desarrollo o utilidades del sistema, no deben ser accesibles desde los sistemas operativos.

Gestión de la seguridad de la red

El manejo de la seguridad de la red requiere minuciosos cuidados al flujo, monitoreo y a la protección de datos. Por otro lado, algunos controles pueden ser requeridos para proteger información sensible que pasa por redes públicas. Algunas de estas medidas pueden ser:

i. Protección de las instalaciones de red

Las instalaciones de la red, deben ser protegidas para evitar interferencias en los servicios de telecomunicaciones causados por comportamientos inesperados o provocados por servicios o instalaciones de telecomunicaciones de otras organizaciones.

Con el fin de proteger de ciberataques a las instalaciones de red, las organizaciones de telecomunicaciones deben tener mecanismos que filtren o limiten direcciones IP, puertos de comunicaciones y protocolos de aplicación. Dependiendo de los servicios de telecomunicaciones, esos mecanismos de filtros, deben ser implementados en conjunto con procesamiento de señales, autentificación de usuarios y control de accesos.

ii. Medidas contra la suplantación

Con el fin de prevenir la suplantación, deben ser implementados controles apropiados de seguridad contra accesos no autorizados, estos controles que pueden aplicarse son:

- Introducción de control de contraseñas.
- Funciones estrictas de autentificación.
- Introducción de contraseñas de una sola vez y autentificación por *token*.

iii. Mecanismos de detección y restricción de congestión de la red

Las instalaciones de telecomunicaciones deben tener mecanismos para detectar congestión en la red y evitar la concentración de las comunicaciones en caso de que se congestione la red.

Los organismos de telecomunicaciones deben reconocer el límite de rendimiento de sus servicios e implementar mecanismos de control para manejar el número de solicitudes antes de llegar a sus límites.

iv. Recolección adelantada de información que pueda causar congestión

Deben establecerse reglas para la recolección de información relativa a desastres y eventos planeados que puedan causar congestión de la red, por los organismos de telecomunicaciones.

v. Identificación y preferencia de comunicaciones esenciales

Las comunicaciones esenciales deben ser la primera consideración. En casos donde estén interconectadas las organizaciones de telecomunicaciones con otras organizaciones, el arreglo para el trato esencial de comunicaciones deben hacerlo con medidas apropiadas.

Seguridad de los servicios de red

Se debe determinar y monitorear regularmente la capacidad del proveedor de la red para gestionar servicios de manera segura. También deben ser identificadas las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requerimientos de gestión.

Los servicios de red incluyen conexiones, servicios privados de red, redes de valor añadido y gestión de soluciones de seguridad. Estos servicios pueden ir desde la administración de ancho de banda hasta los servicios de valor agregado.

Las características de seguridad de los servicios de red pueden ser:

- Tecnología aplicada para la seguridad de los servicios de red, tales como: autenticación , encriptación y controles de conexión a la red.
- Requerimientos técnicos para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión.
- Procedimientos para restringir el acceso a los servicios de red o aplicaciones.

3.4.1.2 Control de acceso

El acceso a la información, instalaciones de procesamiento de información y procesos de negocios, deben ser controlados basándose en los requerimientos del negocio y la seguridad.

Las reglas de control de acceso y derechos de cada usuario o grupo, deben estar claramente definidas en la política de control de acceso, estos controles de acceso son lógicos y físicos. Los usuarios y proveedores de servicios, deben dar una declaración clara de los requerimientos del negocio para cumplir con los controles de acceso.

Las políticas deben tener en cuenta lo siguiente:

- Requerimientos individuales de seguridad del negocio.
- Identificación de toda la información relacionada a las aplicaciones del negocio y los riesgos que enfrenta.
- Políticas para la difusión de la información y la autorización.
- Coherencia entre las políticas de control de acceso y clasificación de la información de diferentes sistemas y redes.
- Gestión de los derechos de acceso en un ambiente de red que reconoce todas las conexiones disponibles.

Gestión de acceso de usuario

Garantizar el acceso a los usuarios autorizados e impide los accesos no autorizados a los sistemas de información, mediante procedimientos establecidos para controlar la asignación de accesos a los sistemas y servicios.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida de los accesos de los usuarios, desde del registro inicial de los nuevos usuarios, hasta su baja, cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Control de acceso a la red

El objetivo es impedir el acceso no autorizado a los servicios de la red, garantizando el acceso de usuarios a los servicios y redes sin comprometer su seguridad mediante:

- Interfaces adecuadas, entre la red de la organización y las redes públicas o privadas de otras organizaciones.
- Mecanismos de autenticación adecuados, los cuales se aplican a los usuarios y equipos.
- El cumplimiento de control de los accesos de los usuarios a los servicios de información.

Control de acceso a las aplicaciones

Impide el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones. Utiliza dispositivos de seguridad para restringir el acceso a las aplicaciones y a sus contenidos, además de restringir el acceso lógico a las aplicaciones e información.

Por lo que los sistemas de aplicación deben:

- Controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones.
- Proporcionar protección contra accesos no autorizados derivados del uso de cualquier software del sistema operativo y software malicioso que puedan traspasar los controles del sistema o de las aplicaciones.
- No comprometer otros sistemas con los que se compartan recursos de información.

3.4.1.3 Adquisición, desarrollo y mantenimiento de sistemas de información

El diseño e implementación de los sistemas de información, pueden ser decisivos para la seguridad, los requisitos de seguridad son previamente identificados, manejados, justificados, aceptados y documentados como parte del proceso para el desarrollo o implementación de los sistemas.

Seguridad de las aplicaciones del sistema

Para evitar errores, perdidas, modificaciones no autorizadas o el mal uso de la información en las aplicaciones, se deben diseñar controles apropiados que incluyan la validación de los datos de entrada, el tratamiento y los datos de salida. Dichos controles deberían ser determinados en función de los requisitos de seguridad y la estimación del riesgo.

Cuando sea posible, se deben utilizar librerías y funciones estándar para necesidades como validación de datos de entrada, restricciones de rango y tipo, así como: integridad referencial. Para una mayor confianza con datos sensibles, se construyen e incorporan funciones adicionales de validación y chequeo cruzado.

Controles criptográficos

Con la ayuda de la criptografía, se protege la confidencialidad, autenticidad e integridad de la información. Con el establecimiento de políticas de uso de controles criptográficos y una adecuada gestión de claves para dar soporte al uso de esas técnicas, utilizando estándares formales.

Seguridad en los procesos de desarrollo y soporte

En el control estricto de los entornos de desarrollo de proyectos y de soporte, mantienen la seguridad del software del sistema de aplicaciones e información. Los directivos responsables deben garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometan la seguridad del sistema o del entorno operativo.

El desarrollo e implementación de software debe incorporar la seguridad de la información al ciclo de vida de desarrollo de los sistemas en todas sus fases, desde la concepción hasta la desaparición, también tiene que integrar las mejoras de seguridad en las actividades de gestión de cambios.

Gestión de las vulnerabilidades técnicas

Se debe seguir un método efectivo, sistemático y cíclico, tomando medidas que confirmen su efectividad para la gestión de debilidades técnicas.

El seguimiento de parches de seguridad mediante herramientas de gestión de vulnerabilidades, con la evaluación de la relevancia o urgencia en su entorno tecnológico. La prueba y aplicación de parches críticos deben ser medidas de protección rápidas y extensas para que las vulnerabilidades de seguridad no afecten a los sistemas.

3.4.1.4 Gestión de Incidentes de Seguridad de la Información

Garantiza que los eventos y debilidades en la seguridad se comuniquen para que puedan realizar acciones correctivas en los sistemas de información. Tanto empleados, como contratistas, deben conocer los procedimientos para informar de los diferentes eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales, y si se presenta un nuevo evento, deben informar lo más rápido posible.

Algunos ejemplos de incidentes o eventos de seguridad para reportar son:

- Perdida de servicio, equipos o instalaciones.
- Mal funcionamiento del sistema.
- Errores humanos.
- Infracciones físicas de seguridad.
- Cambios no controlados del sistema.

Gestión de incidentes y mejoras en la seguridad de la información

Deben ser delimitadas las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información, además deben aplicar procesos de mejora continua para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información

Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales.

CAPÍTULO 4
ANÁLISIS DE LA PARTICIPACION DEL SECTOR PRIVADO.

4.1 INTRODUCCIÓN

Con el objetivo de conocer las actividades desarrolladas por el sector privado en este campo, el capítulo cuatro presenta las herramientas más comunes que utiliza dicho sector en materia de seguridad en las redes modernas.

Como ya se mencionó, los gobiernos deben trabajar conjuntamente con el sector privado y las organizaciones de la sociedad civil y reconocer que la seguridad cibernética es una responsabilidad compartida.

Los esfuerzos realizados por el sector privado para invertir en capacitación y en desarrollo de habilidades , han mostrado resultados tangibles, pues las autoridades responsables de la gestión de incidentes o la investigación de delitos cibernéticos han respondido con más rapidez y eficacia, lo que ha permitido mitigar el impacto de los ataques y aprehender a más delincuentes.

La información reunida a continuación ofrece una perspectiva importante de las herramientas, estrategias de infraestructura y nuevos métodos para reforzar la red que el sector privado ofrece, debido al crecimiento de la tecnología en el ambiente empresarial.

4.2 DATA CENTER FIREWALLS.

El *data center*[60] provee un nuevo campo para las tendencias de la informática y las redes de telecomunicaciones, maneja las estrategias de infraestructuras de las tecnologías de la información, así como nuevas estrategias y nuevos métodos para reforzar la seguridad de la red.[61]

Las tendencias de los consumidores influencian el desarrollo del *data center*, a su vez, el sector empresarial también juega un papel decisivo en el progreso. Con la evolución de la tecnología, las empresas han tenido que aprender a caminar al borde de la innovación con el propósito de salir adelante o mantenerse frente a las empresas competidoras, los cambios en las prácticas comerciales que han influido el desarrollo del *data cente*r son:

- Virtualización:
  Crea una versión virtual del dispositivo o recurso, como puede ser un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo en donde el marco puede dividir el recurso en uno o más entornos de ejecución.

- Computación en la nube:
  Es la computación en la que grandes grupos de servidores remotos están conectados en una red que permite el almacenamiento centralizado de datos y el acceso en línea a los servicios o recursos informáticos.

[60] Data Center o en español centro de datos, son salas especiales equipadas con mecanismos de control eléctrico, ambiental y de incendios en donde se alojan los sistemas de proceso, comunicación y almacenamiento de datos.
[61] Fortinet Network Security Solutions (2015, Enero), *Data Center Firewalls*. Recuperado de https://partners.fortinet.com

- Software-Defined Networks (SDN):
  Es una aproximación a la creación de redes en las cuales el control se desacopla desde el software y está dado a la aplicación del software llamado controlador. Es dinámico, manejable, rentable y adaptable, haciéndolo ideal para el gran ancho de banda de la naturaleza dinámica de las aplicaciones actuales.

- BYOD:
  Se refiere a los empleados que usan un dispositivo personal en el trabajo, ya sea laptop, tabletas o teléfonos inteligentes, con el fin de interactuar con la red corporativa.

- Big data:
  Un volumen masivo de datos, tanto estructurados como no estructurados, los cuales son tan enormes que son difíciles de procesar utilizando bases de datos tradicionales y técnicas de software.

- The Internet of Things (IoT):
  Es el concepto en el cual los objetos cotidianos tienen la capacidad de conectarse a la red e identificarse en otros dispositivos. *The Internet of Things* es significativo porque un objeto que puede representarse digitalmente se convierte en algo más grande que el objeto por sí mismo.

4.2.1 INTEGRACIÓN DE LA INFRAESTRUCTURA.

Enfrenta el crecimiento del *data center* mientras se mantiene la capacidad que requiere el uso de integración de la tecnología para reducir la posibilidad de señal perdida y disminución de velocidad debido a las barreras de seguridad entre los acuerdos de aplicaciones independientes. Existen dos campos que deben ser el corazón de un moderno *firewall*, con dos tipos de diseño hibrido:

- CPU + OTS ASIC.
  Un diseño mediante el cual una Unidad de Procesamiento Central o en inglés *Central Processing Unit* (CPU) es aumentada por un procesador fuera el estante o en inglés *off-the-shelf* (OTS)[62] .

- CPU + Custom ASIC.
  Es el más difícil pero el mejor diseño. Reúne un CPU general que está ligado cercanamente a un número de Circuitos Integrados para Aplicaciones Específicas o en inglés *Application-Specific Integrated Circuits* (ASICs)[63]. Haciendo coincidir el ASIC, que son diseñadas específicamente para manejar tareas para cada procesador y dispositivos; la habilidad para procesar datos se mejora y el rendimiento des sistema se optimiza.

4.2.2 EDGE VS. CORE DATA CENTER FIREWALLS.

4.2.2.1 Edge Firewall.

Implementado en el borde de una red con el fin de protegerla en contra de potenciales ataques del tráfico externo. Además de los deberes de un controlador de accesos, el *Edge Firewall* puede tener capacidades adheridas como otros dispositivos de seguridad. Este método, sin embargo, conduce a una compleja arquitectura que resulta en una red, seguridad y control complicado.

[62] Off-The-Shelf (OTS) se refiere a todos los elementos que están disponibles en el mercado, se pueden comprar y conectar libremente en un sistema.
[63] ASIC es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general, los cuales son usados para una función específica.

4.2.2.2 Data Center Firewall

Además de ser un controlador de accesos, el *Data Center Firewall* ejerce un sin número de funciones. Dependiendo de la configuración y tamaño de la red, el *Data Center Firewall* también puede proveer funciones adicionales a la seguridad, tales como segregar recursos internos de acceso para personas maliciosas y asegurarse del cumplimiento de la norma de protección a consumidores y usuarios con datos sensibles.

Estas funciones son conocidas como Multicapa de Seguridad y pueden incluir:

- Seguridad IP
- Firewall
- Sistema de detección de intrusos/ Sistema de prevención de intrusos
- Antivirus/Antispyware
- Filtro web
- Anti spam

Además, trabajan en conjunto, proporcionando seguridad integrada para el centro de datos, al mismo tiempo, proveen un consolidado control para administradores mientras presentan complejas barreras ante las amenazas potenciales.

4.2.3 CARACTERÍSTICAS DEL DATA CENTER FIREWALLS

Así como los dispositivos y actividades de los usuarios finales evolucionan, los *data center* también deben evolucionar para garantizar el servicio y mantener la seguridad. Algunas tendencias del mercado afectan al *data center*, incluyendo el uso de dispositivos móviles, de dispositivos de portabilidad del empleado o *BYOD*, la consolidación del *data center* a través de la virtualización de servidores, computación en la nube y el *Software-Defined Networks*.

Cuando una empresa u organización crece, el acceso a la red empieza a crecer en múltiples ubicaciones y con miles de usuarios, la opción para considerar usar un firewall de la empresa puede convertirse en una inversión necesaria.

Mientras la capacidad para manejar miles de usuarios y múltiples locaciones puede realizarse con el *firewall* de la empresa, la compensación está en la necesidad de redundancia para asegurar confiabilidad, que resulta en significativos aumentos de los costos y con equipos más complejos, así como la necesidad de una amplia formación si las organizaciones tienen la intención de manejar el *firewall* de la empresa.

Mediante el diseño y la implementación de infraestructuras de red que combinan alto rendimiento con *Software-Defined Networks* (SDN), el *Data Center Firewall* provee la capacidad de evolucionar con las tendencias de la industria y el usuario. Para lograr esto, el *Data Center Firewall* debe enfocarse en tres áreas principales de fundamentos de la seguridad: rendimiento, segmentación y simplificación.

- Rendimiento:
  El *data center* ésta a la vanguardia del diseño de red, lo que permite un mayor rendimiento a través de alta velocidad y capacidad y baja latencia en los firewalls. Actualmente, lo mínimo que requiere el *Data Center Firewall* es 10 Gbps, que permite un alto rendimiento requiere un puerto de conectividad de 10 Gigabits para cada puerto Ethernet del *Data Center Firewall*, con la capacidad de ampliación del rango de la gama de 40 a 100 Gigabit.

- Segmentación:
  Con la evolución de los dispositivos de las TI y la evolución de las amenazas de red, las organizaciones que utilizan el *data center* han adoptado la segmentación de la red como una buena práctica para aislar los datos críticos en contra de las amenazas potenciales. Para apoyar el uso de la segmentación de la red en el esquema de seguridad de la red, el *Data Center*

Firewall debe proveer alta densidad y abstracción lógica apoyando tanto como física y virtualmente la segmentación. Los beneficios incluyen mantener los datos sensibles con particiones desde accesos no autorizados, con fines de seguridad y cumplimiento -limitando el movimiento lateral de las amenazas avanzadas- además de asegurar que los empleados y los usuarios tengan acceso solo a los servicios y aplicaciones para las que estén autorizadas.

- Simplificación:
  Debido a que los *data center* se extienden a usuarios externos de diferentes niveles de confianza, se necesita extender un modelo de "cero-confianza" para el acceso a los datos más allá del tradicional *data center* y de la segmentación del núcleo en la red. Esto requiere de una plataforma de seguridad consolidada y simplificada que puede gestionar múltiples funciones, mientras apoya a las operaciones de red de alta velocidad. A fin de simplificar aún más las operaciones del *Data Center Firewall*, se integran funciones de enrutamiento y conmutación dentro del *firewall*.

4.2.3.1 Firewall Virtual

A diferencia de las máquinas y redes físicas, las máquinas virtuales operan en un entorno virtual aislado en un huésped, pero actuando como si fuera una red o sistema independiente; sin embargo, la red puede ser objeto de amenazas e intrusiones desde fuentes externas.

Las redes virtuales (VLAN) se pueden usar para segmentar múltiples subredes lógicas en el mismo *switch* para asegurar que los datos sean transmitidos entre las máquinas virtuales en la red virtual. Un *firewall* virtual es simplemente un servicio de *firewall* funcionando completamente con el ambiente virtual, proporcionando el típico filtrado y monitoreo de paquetes que podrían esperarse

cuando se utiliza un dispositivo físico en una red física. El *firewall* virtual puede tomar varias formas, puede ser cargado como software tradicional en la máquina del huésped virtual, puede ser integrado dentro del ambiente virtual o puede ser un *switch* virtual con capacidades adicionales.

Los *firewalls* virtuales pueden ser operados de dos formas posibles, dependiendo de cómo sea desarrollado, ya sea en el modo puente o en el modo hipervisor[64]. Un *firewall* virtual que opera en modo puente actúa como un firewall físico, normalmente situado en un *switch* entre redes o en el puente para interceptar el tráfico de la red que necesita viajar a través del puente; de esta forma, el *firewall* virtual puede decidir permitir el pasaje, dejar, rechazar, seguir o reflejar el paquete.

En el modo hipervisor, el *firewall* virtual no es del todo parte de la red virtual, más bien, reside en el huésped de la máquina virtual o hipervisor, con el fin de capturar y analizar los paquetes destinados para la red virtual. Desde que los *firewalls* virtuales operan en modo hipervisor ya no son parte de la red virtual en una máquina virtual; ellos son capaces de correr más rápido dentro del núcleo a velocidades del hardware original.

4.2.4 SERVICIOS DEL FIREWALL DE CENTRO DE DATOS.

4.2.4.1 Aplicaciones de Sistemas.

Los sistemas típicos de aplicación consisten de interfaces de usuarios, programación y base de datos. Una interface de usuario es el control o método por el cual los usuarios interactúan con la computadora, sistema o la red.

[64] Los hipervisores son aplicaciones que presentan a los sistemas operativos virtualizados una plataforma operativa virtual, a la vez que ocultan a dicho sistema operativo virtualizado las características físicas reales del equipo sobre el que operan.

4.2.4.2 Aplicaciones de servicios.

Con el creciente uso de la nube para habilitar el uso global de aplicaciones y accesos a la base de datos de las organizaciones, se han desarrollado servicios tecnológicos enfocados para llenar las necesidades de varias industrias desde pequeñas y medianas empresas hasta corporaciones internacionales. En el mercado actual y muy previsiblemente en el futuro, los servicios de la nube continuaran creciendo rápidamente. Existen tres servicios principales de esta gama: Infraestructura (IaaS), Plataforma (PaaS) y Software (SaaS).

- **Infraestructura como servicio o *Infrastructure as a Service* (IaaS).**
  Este el servicio más básico de los tres servicios de la nube. El proveedor crea la infraestructura, la cual se convierte en una plataforma de autoservicio para el usuario, para acceder, monitorear y administrar remotamente los servicios del centro de datos.

- **Plataforma como servicio o *Platform as a Service* (PaaS)**
  El modelo PaaS provee al usuario un nivel adicional del servicio del modelo IaaS. En éste, el proveedor no solo construye la infraestructura, sino también proporciona servicios de monitoreo y mantenimiento para los usuarios.

- **Software como servicio o *Software as a Service* (SaaS).**
  El modelo SaaS representa el más largo del mercado de la nube. Éste tiene el paso final de llevar la aplicación del software en el conjunto de funciones administradas por el proveedor y con el usuario que tiene una interfaz de cliente.

  Debido a que la aplicación reside en la nube, la mayoría de SaaS puede operar a través de un navegador web sin la necesidad de descargar o instalar software en los sistemas físicos. Este permite a las empresas a desarrollar software y requerimientos de la misma operación.

- **La responsabilidad de seguridad compartida o *The Shared Security Responsibility* (SSR).**

  Al usar los servicios en la nube para aplicaciones y accesos a la base de datos, estos trabajos conllevan una responsabilidad compartida para la seguridad y la operación divididas entre el proveedor y el inquilino de la nube. Dependiendo de cuál modelo sea elegido para la operación, ya sea IaaS, PaaS o SaaS, el nivel de responsabilidad de la seguridad cambia.

4.3 NEXT GENERATION FIREWALL (NGFW).

Los principales beneficios del NGFW son la visibilidad y el control del tráfico que entran a los puertos del *firewall*. Con el NGFW, los administradores proveen granularidad más fina que proporciona una visión más profunda en el tráfico que intenta acceder a la red. Esto incluye profunda visibilidad de los usuarios y dispositivos, así como la habilidad de permitir o limitar el acceso basado en contenido y aplicaciones específicas en lugar de rechazar o aceptar cualquier tráfico usando un particular protocolo de transmisión.[65]

Con un *firewall* tradicional, el tráfico es aceptado con base en los criterios de identificación de los puertos designados y su dirección IP. Por el contrario, con NGFW el tráfico es aceptado basado en ID del usuario, tanto la dirección IP como el contenido del tráfico.

4.3.1 CAPACIDADES DEL NGFW.

El NGFW proporciona soluciones en contra de una amplia gama de amenazas avanzadas contra aplicaciones, datos y usuarios. Con el fin de defender a las redes en contra de amenazas recientes, el NGFW debe tener la habilidad para identificar y controlar aplicaciones que se ejecutan en la red, deben integrar un sistema de prevención de intrusos (IPS) con capacidad de escaneo y la habilidad de verificar la identidad de usuarios y dispositivos para hacer cumplir las políticas de acceso.

[65] Fortinet Network Security Solutions (2015, Enero), *Next Generation Firewall (NGFW*). Recuperado de https://partners.fortinet.com

- **Sistema de Prevención de Intrusiones o *Intrusion Prevention System* (IPS).**

  El Sistema de Prevención de Intrusiones detecta amenazas, pero no alerta al firewall para que tome acción en contra de amenazas identificadas o trafico desconocido.

- **Inspección Profunda de Paquetes o *Deep Packet Inspection* (DPI).**

  La Inspección Profunda de Paquetes identifica y clasifica el tráfico de la red que pasa a través del firewall u otros dispositivos de seguridad basada en firmas, como errores de protocolos, virus, spam, intrusiones, o violaciones de políticas.

- **Control e Identificación de las Aplicaciones de red o *Network Application Identification & Control.***

  El NGFW con control de aplicaciones permite identificar y controlar aplicaciones de la red sin importar el puerto, protocolo o la dirección de la IP utilizada. Le da un visibilidad y control inigualable sobre el tráfico de las aplicaciones, inclusive aplicaciones desconocidas de fuentes desconocidas, además de inspeccionar el tráfico de aplicaciones encriptadas.

- **Identidad del Usuario o *User Identity.***

  Cuando un usuario intenta acceder a los recursos de la red, el NGFW permite la identificación desde la lista de nombres, direcciones IP y del directorio activo que se mantiene a nivel local. La solicitud de conexión solo se permitirá si el usuario pertenece a uno de los grupos permitidos y las políticas del firewall asignado se le aplicaran a todo el tráfico que maneje ese usuario.

- **Inteligencia *Extra Firewall.***

  Esta inteligencia *extra firewall* proporciona la habilidad de crear listas para accesos o para negar el tráfico externo de la red. Estas listas pueden ser diseñadas por la dirección IP como:

- **Listas Blancas:** Diseñan fuentes consideradas confiables que permiten el acceso a la red.
- **Listas negras:** Diseñan fuentes consideradas no confiables y niegan el acceso a la red.

- **Red Virtual Privada o *Virtual Private Network* (VPN).**
  La tecnología de la red virtual privada permite a las organizaciones establecer comunicaciones seguras y privadas entre múltiples redes y huéspedes, usando IPS y Capas de Conexión Segura o *Security Sockets Layer* (SSL).

4.3.1.1 Funciones del NGFW.

La mejor forma de detectar amenazas consiste en desarrollar un Sistema de Detección de Intrusiones (IDS) como parte de la arquitectura de la red. Con el fin de prevenir amenazas identificadas a partir de la explotación de vulnerabilidades, debe desarrollarse un Sistema de Prevención de Intrusiones (IPS). El propósito del IPS es reaccionar ante las amenazas detectadas en una red con el fin de bloquear el intento de intrusión del tráfico que se aprovecha de las vulnerabilidades del sistema, desviaciones desde protocolos estándar o ataques generados por fuentes confiables.

Otra función del NGFW es proveer Inspección de Tráfico Encriptado de Capas de Conexión Segura (SSL). Este tipo de inspección protege clientes finales, así como servidores y aplicaciones web de amenazas ocultas potenciales. La Inspección de Capas de Conexión Segura (SSL) intercepta e inspecciona el tráfico encriptado antes de enrutarlo a su destino y se puede aplicar tráfico orientado al cliente y como usuarios a través de la nube.

El uso de la Inspección de Capas de Conexión Segura (SSL) permite las aplicaciones de políticas en contenido web encriptado para prevenir intrusiones potenciales, como el tráfico malicioso oculto en el contenido de Capas de Conexión Segura (SSL).

4.3.2 CAPACIDADES EXTENDIDAS DEL NGFW.

Dentro de la infraestructura de seguridad de la red de la empresa, se necesita proteger en contra de las nuevas clases de ataques altamente diseñados, dirigidos y adaptados para eludir defensas comunes. Debido a estas desarrolladas y avanzadas amenazas, son necesarias defensas adicionales como: antivirus, *anti-malware*, *anti-botnet*, filtrado web y *sandboxing*.

- **Antivirus/malware:**
  Es responsable por detectar, remover y reportar código malicioso. Al interceptar e inspeccionar el tráfico y el contenido de las aplicaciones, la protección del antivirus se encarga de que las amenazas maliciosas ocultas dentro del contenido de las aplicaciones legítimas, sean identificadas y removidas antes de puedan causar daño.

- **Anti-botnet:**
  Responsable de detectar y reaccionar ante ataques Distribuidos de Negación del Servicio o *Distributed Denial of Service* (DDoS) u otros ataques coordinados a la red. Las organizaciones pueden prevenir, descubrir y bloquear actividades de *botnet* usando el diseño de detección y regulación de servicios IP *anti-botnet*.

- **Filtrado Web.**

  El filtrado web permite o bloquea el tráfico Web basado en el tipo de contenido, comúnmente definido por categorías. El filtrado web protege dispositivos finales, redes y la información sensible contra amenazas Web, previniendo al usuario de acceder a sitios de *Phishing* o *Malware*.

- **Sandboxing.**

  El *sandboxing* aísla códigos desconocidos y potencialmente maliciosos para ejecutar todas las funciones antes de permitir el tráfico de descarga dentro de la red. El *sandboxing* tiene la capacidad de detectar ataques del día cero.

4.3.3 PROTECCION AVANZADA CONTRA AMENAZAS O *ADVANCED THREAT PROTECTION* (ATP).

Para proteger contra modernas y futuras amenazas, herramientas de defensa como ATP están siendo incorporadas dentro de la infraestructura de la red de seguridad. Esta protección proporciona un incremento en la seguridad en todas las redes, desde pequeñas y medianas empresas hasta las más grandes. Las capacidades críticas que ejerce el ATP son:

- **Control de acceso:**

  Gestión de vulnerabilidades, dos factores de identificación

- **Prevención de amenazas.**

  Prevención de intrusión (IPS), control de aplicación, filtrado web, filtrado de correo y antimalware.

- **Detección de amenazas.**

  Sandboxing, detección de *botnet*, reputación del cliente y análisis del comportamiento de la red.

- **Respuesta a incidentes.**
  Registros consolidados, servicios profesionales, cuarentena de usuarios o equipos y actualización de prevención de amenazas.

- **Monitoreo Continuo.**
  Vistas en tiempo real, reportes de seguridad e inteligencia de amenazas.

4.4 GESTIÓN UNIFICADA DE AMENAZAS O UNIFIED THREAT MANAGEMENT (UTM).

La Gestión de Amenazas Unificadas es un acercamiento a la gestión de seguridad que provee a los administradores la habilidad para monitorear y administrar múltiples aplicaciones y componentes de infraestructura de seguridad a través de una consola de administración. La Gestión de Amenazas Unificada (UTM) proporciona al administrador la destreza de proteger a las oficinas y sucursales ante amenazas potenciales, en lugar de tener dependencia con los administradores de sitios remotos o los paneles de control múltiples.[66]

Similar al NGFW, una de las fortalezas de la Gestión de Amenazas Unificadas es la integración de componentes y funciones dentro de los accesorios del hardware y las aplicaciones asociadas al software de seguridad. La ventaja de la Gestión de Amenazas Unificadas es que va más allá del NGFW, concentrándose en el alto rendimiento de la protección de los centros de datos, incorporando una gama más amplia de capacidades de seguridad, proporcionando administración amistosa y de amenazas hostiles.

4.4.1 CARACTERÍSTICAS DE LA GESTIÓN DE AMENAZAS UNIFICADA (UTM)

La Gestión de Amenazas Unificada (UTM) son generalmente adquiridas ya sea como servicios de la nube o aplicaciones de la red, *firewall* integrado, sistema de detección de intrusos (IDS), *anti-malware*, spam y filtrado de contenido. Estas pueden ser instaladas y actualizadas tantas veces sea necesario mantener la paz con las amenazas emergentes.

[66] El siguiente capítulo fue sacado de Fortinet Network Security Solutions (2015, Enero), *Unified Threat Management (UTM)*. Recuperado de https://partners.fortinet.com

- **Firewall:**

  La más necesaria e implementada tecnología de la seguridad en la red, la cual usa reglas o políticas para determinar cuál trafico está permitido dentro o fuera del sistema o la red.

- **Sistema de detección de intrusos o *Intrusion Detection System* (IDS).**

  Es capaz de detectar amenazas potenciales en la red, pero no reacciona enviando un mensaje al *firewall* para bloquear la amenaza.

- **Antivirus/malware**:

  Proporciona protección multicapas en contra de virus, *spyware* y otro tipo de ataques de *malware*. También puede aplicar la protección de antivirus al tráfico de Protocolo de Transferencia de Archivos o *File Transfer Protocol* (FTP), Mensajería instantánea y contenido web en el perímetro de la red.

- **Antispam:**

  Este es un módulo que detecta y remueve correo no requerido aplicando el criterio de verificación para determinar si los correos encajan en los parámetros definidos como trafico spam.

- **Filtrado de contenido:**

  Estos dispositivos bloquean el tráfico de y para la red por la dirección IP, nombre de dominio/URL, tipo de contenido. Ellos mantienen una lista blanca de sitios confiables y una lista negra de sitios prohibidos para prevenir a los usuarios de ser expuestos de contenido malicioso.

- **VPN.**

  Una red virtual privada usa protocolos especiales para mover paquetes de información a través de internet seguro. En general, los protocolos de la VPN encriptan el tráfico haciendo que el intercambio sea ilegible a todos los que quieren interceptar y examinar esos paquetes mientras van sobre el internet.

4.4.2 CARACTERÍSTICAS EMPRESARIALES AVANZADAS DISTRIBUIDAS

Los clientes empresariales pueden tener acceso a más características avanzadas, como puede ser identidad basada en el control de acceso, prevención de intrusiones (IPS), calidad del servicio (QoS) e inspección de SSL/SSH.

- **Control de Acceso.**
  La aplicación de control puede identificar y controlar aplicaciones, programas de software, servicios de red y protocolos. El sistema de Gestión de Amenazas Unificada da seguimiento a nombres de usuarios, direcciones de IP y un directorio activo de grupos de usuarios; cuando el usuario intenta acceder a los recursos de la red, la Gestión de Amenazas Unificada aplica las políticas del *firewall* basadas en aplicaciones de pedido o de destino.

- **Sistema de prevención de intrusiones (IPS).**
  Un sistema de prevención de intrusiones actúa como un perro guardián, buscando por patrones de la actividad y tráfico de la red, y registra eventos que pueden afectar a la seguridad.

- **Calidad del servicio (QoS),**
  La calidad del servicio se refiere a la habilidad de lograr maximizar el ancho de banda y manejar con otros elementos de desempeño de la red como: latencia, tasa de error y tiempo de actividad. La calidad del servicio también controla y maneja recursos de la red ajustando prioridades para tipos específicos de datos sobre la red.

- **Inspección de Capas de Conexión Segura (SSL)/ intérprete de órdenes segura (SSH).**
  La inspección provee la habilidad de inspeccionar contenido encriptado por las aplicaciones, usando una técnica de encriptación de Capas de Conexión Segura (SSL).

4.4.3 CARACTERÍSTICAS DE LA GESTIÓN DE AMENAZAS UNIFICADA (UTM)

Con el enfoque que tiene la gestión de amenazas unificada (UTM) de ser flexible y preparado para el futuro, existen tecnologías que están siendo integradas a los dispositivos de la gestión de amenazas unificada (UTM). En medio de estas capacidades de adaptarse a diversos tamaños de redes, encontramos Conmutación, Red de Área Local Inalámbrica (WLAN) y Alimentación a través de Ethernet o *Power-Over-Ethernet* (POE).

Conmutación.

Integrando la conmutación dentro de la gestión de amenazas unificada (UTM), esto reduce el número de dispositivos de hardware y monitores de control necesarios para manejar el sistema la gestión de amenazas unificada (UTM). Desde este panel de control integrado, los puertos individuales pueden ser conmutados para activar o desactivar el tráfico de red físicamente aislado.

Red de Área Local Inalámbrica (WLAN)

Integrando la Red de Área Local Inalámbrica (WLAN), proporciona un método para asegurar que cada red en toda la infraestructura física pueda ser controlada para mantener políticas de seguridad consistentes y controles en toda la red de las interfaces de control. Esta aproximación también detecta y elimina posibles puntos ciegos, además de mejorar la prevención de acceso inalámbrico a la red combinada.

Alimentación a través de *Ethernet o Power-over-Ethernet* (POE).

La alimentación a través de Ethernet permite proporcionar energía a los dispositivos externos. Se puede alimentar a través del cable de datos Ethernet a lo largo de extensas longitudes, ya sea en los mismos conductores datos o en un conductor dedicado en el mismo cable. Las aplicaciones de la gestión de amenazas unificada (UTM) utiliza la alimentación a través de Ethernet (POE) que permite la conexión de Redes de Áreas Locales Inalámbricas (WLAN), extensores de 3G/4G, Voz sobre Protocolo de internet (VoIP) y cámaras IP de la plataforma de seguridad de la red.

4.5 APLICACIONES DE SEGURIDAD.

Con el aumento de la confianza de las empresas en las aplicaciones que están en la nube, enfocarse en las vulnerabilidades de las aplicaciones de la web es esencial para la seguridad del sistema y de la red. Estas aplicaciones residen en la capa 7 del modelo OSI, pero aún siguen siendo vulnerables a ataques dirigidos, de éstos: Negación de Servicio o *Denial of Service* (DoS) o uno peor, Negación de Servicio Distribuido o *Distributed Denial of Service* (DDoS) son diseñados para inhibir el uso de las aplicaciones.[67]

4.5.1 CAPAS DE APLICACIÓN; EL MODELO DE CONEXIÓN DE SISTEMAS ABIERTOS U *OPEN SYSTEMS INTERCONNECTION* (OSI)

El modelo de conexión de sistemas abiertos u *Open Systems Interconnection* (OSI) define a las redes por niveles. A medida que el nivel incrementa, también la complejidad y la naturaleza crítica de los datos contenidos.Las aplicaciones son las que permiten a los usuarios realizar tareas usando sistemas y redes sin tener que aprender lenguajes complejos para escribir sus códigos.

4.5.2 VULNERABILIDADES DE LAS APLICACIONES.

El amplio uso de las aplicaciones proporciona comodidad entre los usuarios y consumidores privados, haciendo a las amenazas de aplicación un problema con el potencial de casos repetidos. Esto puede ocurrir de fuentes inofensivas, como pueden ser clientes o aquellos que usan el modelo BYOD, los cuales regularmente fallan en cumplir con los exámenes de seguridad en sus equipos. También puede ocurrir como un esfuerzo de la competencia o un hacker para afectar negativamente el éxito de la compañía

[67] El siguiente capítulo fue obtenido de Fortinet Network Security Solutions (2015, Enero), *Application Security*. Recuperado de https://partners.fortinet.com

4.5.2.1 OWASP.

Existe un proyecto global que ayuda a desarrolladores de aplicaciones y sistemas y a los administradores de sistemas de seguridad de la red a identificar y entender a las amenazas emergentes de las aplicaciones de seguridad. Este proyecto llamado Proyecto Abierto de Seguridad de Aplicaciones Web u *Open Web Application Security Project* (OWASP).

Del 2010 al 2013, el Proyecto de Seguridad de Aplicaciones Abiertas de la Web (OWASP) encontró una consistencia de las cuatro principales amenazas de la seguridad del sistema y la red:

1. **Inyección de Lenguaje de Consulta Estructurado o *Structured Query Language* (SQL)**:
   Este tipo de irrupciones permite a los atacantes falsificar identidades, alterar o suprimir datos, cambiar o evitar transacciones de varios tipos, también permiten la divulgación completa, la destrucción o hacer inaccesible la base de datos del sistema, hasta inclusive convertirse en administradores de la base de datos. La severidad del ataque depende de la creatividad y habilidades del atacante; la inyección de Lenguaje de Consulta Estructurado (SQL) es una amenaza de alto impacto.

2. ***Cross-site scripting* (XSS).**
   También conocido como inyección XXs, son maliciosos scripts inyectados en los sitios web confiables, generalmente son usados en forma de una secuencia de comandos secundarios en el navegador para ser transmitidos a los usuarios finales. Debido a que los navegadores de los usuarios finales lo consideran como un sitio de confianza, se ejecutara el script, lo que permite acceder a las cookies, sesiones u otra información retenida por el navegador y usada con el sitio. Algunos scripts son capaces de reescribir el contenido de las paginas HTML.

3. **Pérdida de Autenticación y Gestión de Sesiones.**

   Esta área incluye todos los aspectos de autenticación de usuarios y manejo de sesiones activas, incluso los protocolos de autenticación pueden ser adentrados por la deficiente gestión de credenciales, como el cambio de contraseñas, las opciones de “olvide mi contraseña” y “recordar mi contraseña”, opciones de actualización cuentas, entre otras. La complejidad de este problema viene con el hecho de que muchos desarrolladores prefieren crear sus propias sesiones simbólicas, las cuales pueden o no pueden estar adecuadamente protegidas, dependiendo de la habilidad del desarrollador los pasos pueden no estar en el lugar para protegerlos a través del ciclo de vida de las aplicaciones.

4. **Referencia Insegura y Directa a Objetos.**

   Cuando una aplicación proporciona acceso directo a objetos debido a los accesos basados en usuario, los atacantes pueden pasarse directamente los accesos y los recursos del sistema. También permite a los atacantes a eludir autorización y obtener accesos a los recursos mediante la modificación de los parámetros usados para apuntar directamente a los objetos. Este método simplemente toma los accesos suministrados por el usuario y los usa para recuperar los datos como si el atacante fuera un usuario autorizado.

4.5.3 SOLUCIONES DE SEGURIDAD PARA APLICACIONES.

Una herramienta importante en la protección de la red es el sistema de prevención de intrusiones (IPS), el cual busca más allá del puerto y del protocolo para examinar la firma o el contenido del tráfico de la red para identificar y detener a las amenazas. NGFW y UTM utilizan capacidades como ATP, que protegen las regiones de la capa tres y la capa cuatro contra ataques DDoS, mediante la combinación de hardware y software programable para dirigir amenazas modernas y emergentes.

Además de las capacidades del NGFW y UTM, el uso de estas dos en conjunto con otras capacidades de seguridad de la red presenta una protección adicional de extremo a extremo. Las siguientes capacidades se suman a las soluciones de seguridad crítica para proteger en contra de ataques DDoS y proteger a las capas 3, 4 y 7.

4.5.3.1 Aplicación de Controladores de Entrega o *Application Delivery Controllers* (ADC).

Las aplicaciones de controladores de entrega (ADC) son dispositivos de red que manejan interfaces de clientes para aplicaciones web y empresariales. Una función primaria es como equilibrador de carga del servidor, que resulta en un rendimiento optimizado del sistema del usuario final y un aumento en la fiabilidad Gbps a través de la capa 4, accesibilidad a los recursos del centro de datos y seguridad en las aplicaciones empresariales. Los controladores de Entrega (ADC) son implementados en los centros de datos, colocados detrás del firewall y enfrente de los servidores, que actúa como un punto de control para la aplicación de seguridad y proporciona autenticación, autorización y contabilidad.

4.5.3.2 Aplicación de Red de Entrega o *Application Delivery Network* (ADN).

La aplicación de Red de Entrega (ADN) está dividida en tres elementos:

- **Servidor:**
  Cuando las aplicaciones exceden un solo servidor, la aplicación de red de entrega (ADN) gestiona múltiples servidores para permitir aplicaciones más allá de un simple servidor, crean un servidor virtual. Una vez que se selecciona los mejores servidores para la aplicación, la aplicación de red de entrega utiliza conexión de persistencia para mantener una conexión con el servidor original donde se inició la transacción.

- **Seguridad del núcleo:**
  Este elemento es donde las herramientas y servicios residen para defender las aplicaciones de amenazas. Las capacidades incluyen un fuerte *firewall*, VPN, escaneo de antivirus/*malware*, además pueden incluir NGFW con IPS, control de aplicación y también políticas de acceso de usuario para mejorar la protección.

- **Perímetro exterior:**
  El Enlace de Equilibrio de Cargas o *Basic Link Load Balancing* (LLB) gestiona el ancho de banda y la redundancia utilizando múltiples enlaces WAN. Si la aplicación incluye el acceso de múltiples centros de datos para operaciones como recuperación de desastres, el Servidor Global de Balance de cargas o *Global Server Load Balancing* (GSLB) utiliza DNS basados en una plataforma de resolución para enrutar tráfico entre múltiples centros de datos, permitiendo que cualquier centro de datos automático o programable pueda rutear basado en las necesidades de rendimiento de la infraestructura.

4.5.4 CARACTERÍSTICAS DE LAS APLICACIONES WEB DEL FIREWALL.

Las aplicaciones web del *firewall* (WAF) implementan protección en el centro de datos, balance de carga y aceleración de contenido de y para los servidores web. El principal uso de las aplicaciones web del *firewall* (WAF) es proteger aplicaciones web de ataques que intentan explotar vulnerabilidades. Ellas protegen aplicaciones web asociadas al contenido de la base de datos mediante el escaneo de vulnerabilidades de las aplicaciones web del *firewall* (WAF), mitigando amenazas prevalentes como XSS, desbordamiento de buffer, denegación de servicio (DoS), inyección SQL y envenenamiento de cookies.

La respuesta a la pregunta de por qué los NGFW o los IPS no pueden mitigar estas amenazas, es porque las IPS sólo detectan problemas conocidos que pueden producir falsos positivos, no protegen contra amenazas incrustadas en el trafico SSL. Los firewalls básicos buscan ataques basados en la red y no por ataques basados en aplicaciones.

4.5.4.1 Heurística.

Una de las claves que permiten a las aplicaciones web del firewall (WAF) contrarrestar las amenazas DDoS es la heurística o análisis basado en el comportamiento. Algunas de las protecciones de amenazas incluyen configurar sistemas para identificar ataques potenciales, basados en el volumen de la fuente (intención vs contenido), *ping rates* (*hardcoded*[68] vs costumbre), dimensión de paquetes (gruesa vs granular) y tendencia a emparejar (fijo vs adaptativo).

4.5.4.2 WAF y conformidad PCI DSS

En el estilo de vida del siglo XXI, la habilidad para proveer transacciones seguras de datos no se limita a la corrupción de datos y programas, limitaciones de rendimiento o parámetros operacionales de la red en el estricto sentido de proporcionar almacenamiento y vías digitales. Consideraciones adicionales respecto a la información personal identificable (PII), seguridad del crédito, otras cuentas personales y seguridad de los datos son regulados desde fuera del sector de la tecnología.

[68] Hard-code, término del mundo de la informática hace referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente en el código fuente del programa, en lugar de obtener esos datos de una fuente externa como un fichero de configuración o parámetros de la línea de comandos, o un archivo de recursos.

Los Estándares de Seguridad de Datos en la Industria de la Tarjeta de Pago o *Payment Card Industry Data Security Standards* (PCI DSS) establecen requisitos para las prácticas de seguridad que aplican a cualquier vendedor u organización que procesan, almacenan o transmiten datos de los tarjetahabientes.

Los Estándares de Seguridad de Datos en la Industria de la Tarjeta de Pago (PCI DSS) atienden 12 requerimientos que cubren seis metas comunes que reflejan las mejores prácticas de seguridad. De los seis objetivos mencionados, el número 3 influye más a la capacidad de la red para mantener operaciones seguras y un control efectivo contra DDoS y otras amenazas maliciosas para seguridad de la red. A continuación, se muestra los estándares actuales para el cumplimiento de la seguridad de datos PCI.

1- Instalar y mantener una configuración del firewall para proteger los datos del tarjetahabiente
2- No utilizar valores predeterminados para las contraseñas de los sistemas y otros parámetros de seguridad
3- Proteger los datos de titulares de la tarjeta
4- Encriptar la transmisión de datos a través de redes públicas y abiertas de los tarjetahabientes
5- Usar y actualizar regularmente programas y antivirus
6- Implementar y mantener aplicaciones y sistemas de seguridad
7- Restringir acceso a los tarjetahabientes
8- Asignar una única ID para cada persona con una computadora de acceso
9- Restringir el acceso físico a los datos del tarjetahabiente
10- Seguir y controlar todos los accesos a los recursos de la red y a los datos del tarjetahabiente
11- Probar regularmente los sistemas y procesos de seguridad
12- Mantener una política que dirija seguridad de la información para empleados y contratistas.

CAPÍTULO 5
ANÁLISIS DEL CASO MEXICANO

5.1 INTRODUCCIÓN

En México existe una regulación respecto a la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones, lamentablemente no está coordinada ya que encontramos diferentes leyes que hacen referencia a actividades que ocurren en Internet, por ejemplo en materia penal existe una pequeña sección de delitos informáticos en el titulo noveno del Código Penal Federal; por otra parte la Secretaría de Seguridad Pública del Distrito Federal (SSPDF) creó el agrupamiento de la Policía Cibernética, pero no existe un solo marco normativo que hable del tema de la ciberseguridad.

En el artículo 6° de la Constitución Política De Los Estados Unidos Mexicanos se menciona que:

> "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes..."[69]

Si bien este derecho establece pautas para proteger los datos personales y se enfoca principalmente en el derecho al libre acceso a la información, no menciona directamente a Internet y a las infraestructuras críticas de la información como herramienta de comunicación entre el gobierno y la ciudadanía.

Igual sucede con el artículo 16 de la Constitución Política De Los Estados Unidos Mexicanos donde se menciona que:

[69] Constitución Política de los Estados Unidos Mexicanos, artículo VI.

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley[70]

Por otra parte, la Ley Federal de Telecomunicaciones y Radiodifusión que entró en vigor el 13 de agosto de 2014, presentó una disposición, la cual menciona que los concesionarios de telefonía deben llevar un registro de las comunicaciones de los usuarios; este registro debe contener datos como: nombre, domicilio, tipo de comunicación, número de destino, fecha, hora, y duración de la comunicación. Además, las empresas estarán obligadas a conservar esos registros durante dos años; en el primero la autoridad podrá consultarlos en un sistema en tiempo real, en el segundo tendrán que pedir al concesionario que le dé acceso.[71]

Finalmente, existe la Ley Federal de Protección de Datos Personales publicada en julio de 2010, la cual brinda garantías para proteger los datos personales en posesión de las empresas, así como de garantizar la privacidad y el derecho a la libertad informativa de las personas. Esta ley otorga cuatro derechos a las personas que entregan sus datos personales:[72]

- Acceso a sus datos
- Rectificación de datos erróneos o incompletos
- Cancelación de datos
- Oposición o exclusión de los datos de cualquier tipo de tratamiento.

---

[70] Constitución Política de los Estados Unidos Mexicanos, artículo XVI.
[71] ANADE, Colegio de Abogados. (2014, Agosto) *Resumen de la nueva Ley Federal de Telecomunicaciones Radiodifusión*. Recuperado de http://anademx.com/files/2014/08/4-AGOSTO-2014.-NOTA-DECRETO-LFTR.pdf
[72] Carrillo D'Herrera, Juan Carlos. (2011, Mayo*). Ley Federal de Protección de Datos Personales en Posesión de Particulares.* Seguridad. Cultura de Prevención TI. Num 10. Recuperado de http://revista.seguridad.unam.mx/numero-10/ley-federal-de-protecci%C3%B3n-de-datos-personales-en-posesi%C3%B3n-de-particulares

Y establece ocho principios que deberán seguir los responsables del tratamiento de los datos personales:

- Licitud
- Consentimiento
- Calidad
- Finalidad
- Proporcionalidad
- Responsabilidad
- Información
- Lealtad.

Además de estos artículos, no hay más referencias al Internet; mucho menos a la ciberseguridad ni a la protección de la infraestructura crítica del país, como los sectores de energía, telecomunicaciones, finanzas, transporte y servicios médicos.

Por otro lado, México pertenece a un grupo de trabajo internacional denominado *Anti-Phishing Working Group*[73], el cual reúne a más de dos mil empresas, compañías de productos y servicios de seguridad, agencias gubernamentales, organizaciones multilaterales y corporaciones de telecomunicaciones.

Además, existe el Proyecto Sombra, formado por voluntarios que reúnen, monitorean y reportan *malware*, *bots* informáticos que distribuyen códigos maliciosos y propician el fraude electrónico.

Para los crímenes cibernéticos en México, en el año 2000 se creó la Policía Cibernética que es la principal autoridad encargada de la seguridad y el delito cibernético. Dentro de la Policía Federal se encuentra la División Científica que mantiene una unidad responsable de coordinar actividades para investigar, prevenir y procesar conductas consideradas delictivas mediante el uso de medios

[73] http://www.antiphishing.org/

electrónicos y cibernéticos. La División Científica de la Policía Federal está integrada por el principal equipo de especialistas mexicanos abocados a dar respuesta a incidentes de seguridad cibernética (CSIRT), el CERT-MX.

Se sabe que en México varias dependencias federales, a pesar de la existencia del CERT, han sufrido ataques cibernéticos, entre los que destacan: el realizado por la Agencia de Seguridad de EU, la cual pudo tener acceso al correo del expresidente Felipe Calderón y de varios de miembros de su gabinete; también se informó que se violó el correo del presidente Peña Nieto, además del *hackeo* de Anonymus al portal de la SEDENA, la Cámara de Diputados y el INE.

Según datos de la División Científica de la Policía Federal, hubo un aumento de 113% en incidentes de seguridad cibernética en 2013 comparado con el año anterior. De los incidentes denunciados, aproximadamente 31% fueron contra instituciones gubernamentales, 26% contra entidades del sector privado, 39% contra organizaciones académicas y 4% contra otras entidades. Los incidentes de acceso lógico no autorizado aumentaron aproximadamente 260%, las infecciones de malware 323% y los incidentes de *phishing* un 409%, mientras que los ataques de denegación de servicio disminuyeron 16%.[74]

El reporte de la OEA sobre Seguridad Cibernética en América Latina y el Caribe evaluó a 100 países usando una escala de 0 a 100, en la cual México ocupa la posición 18, esto implica que se encuentra 12.3 puntos por debajo del promedio global, a la par de Perú, Vietnam y Burkina. Y los mejores países evaluados son EU (82.4), Canadá (79.4) y Australia (76.6).[75]

[74] Organización de los Estados Americanos, Symantec. (2014, Junio). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado de http://www.symantec.com/la/reporteOAS/
[75] Organización de los Estados Americanos, Symantec. (2014, Junio). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado de http://www.symantec.com/la/reporteOAS/

Hasta ahora, por medio de las recientes reformas en materia de telecomunicaciones y la Estrategia Digital Nacional, se ha dado preferencia en México a la digitalización de los servicios públicos y a la formación de una parte de la población en TI, pero el tema de la ciberseguridad no ha recibido el mismo impulso.

Durante los últimos años, México ha realizado esfuerzos en políticas públicas y regulación, con el fin de reformar el sector y de adoptar un escenario de mejores prácticas. En el 2013, surge la Estrategia Digital Nacional en el marco del Plan Nacional de Desarrollo 2013-2018, pretendiendo ser transversal para favorecer la apertura y la transparencia en todas las instancias del gobierno; sin embargo, en la Estrategia Digital Nacional y en el Plan Nacional de Desarrollo de la actual administración el tema de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones es prácticamente inexistente.

Dicho lo anterior, la Estrategia Digital Nacional se analiza a continuación en sus puntos más destacados.

5.2 ESTRATEGIA DIGITAL NACIONAL

En noviembre de 2013, el Gobierno Federal Mexicano dentro de su Plan Nacional de Desarrollo presentó la Estrategia Digital Nacional, documento que contiene acciones para implementar el uso de las telecomunicaciones para el desarrollo económico, social y gubernamental del país durante los próximos años.[76]

Esta estrategia es una respuesta a la necesidad de aprovechar las telecomunicaciones y a las Tecnologías de la Información y Comunicación, para impulsar el desarrollo del país. La integración de las Tecnologías de la Información y Comunicación, deberían traer múltiples beneficios a las personas, organizaciones y al gobierno.

La meta que tiene la Estrategia Digital Nacional es que -dentro de 5 años, o para el 30 de noviembre del 2018- México ocupe el primer lugar en los indicadores que miden el grado de digitalización de las naciones, la innovación y la apropiación social de la tecnología en América Latina, ya que ahora, se encuentra en los últimos lugares.[77]

5.2.1 MARCO ESTRUCTURAL DE LA ESTRATEGIA

La Estrategia Digital Nacional tiene cinco objetivos que se describen a continuación:

[76] El Economista. (2013, Noviembre). Estrategia Digital potenciará desarrollo de México: Peña Nieto. Recuperado de http://eleconomista.com.mx/sociedad/2013/11/25/estrategia-digital-potenciara-desarrollo-mexico-pena-nieto

[77] El Economista. (2013, Noviembre). Estrategia Digital potenciará desarrollo de México: Peña Nieto. Recuperado de http://eleconomista.com.mx/sociedad/2013/11/25/estrategia-digital-potenciara-desarrollo-mexico-pena-nieto

1. **Transformación gubernamental.**

   Desarrollar políticas para un Gobierno Digital, mediante la construcción de una nueva relación entre el gobierno y el ciudadano, que se base en la experiencia del ciudadano como usuario de servicios públicos a través de la ayuda de las Tecnologías de la Información y Comunicación.

2. **Economía digital**

   Incorporar las nuevas tecnologías en el desarrollo económico para democratizar la productividad, e incrementar el crecimiento y la generación de empleos.

3. **Educación de calidad**

   Integrar las Tecnologías de la Información y Comunicación en la formación de niños y jóvenes y ampliar la oferta educativa a través de medios digitales. Llevar a cabo la digitalización de archivos y colecciones de contenidos con base en una Agenda Digital Cultural.

4. **Salud universal y efectiva.**

   Aprovechar a las telecomunicaciones para aumentar la cobertura de los servicios y hacer más eficiente la infraestructura en la construcción de un Sistema Nacional de Salud Universal[78]. Crear también mecanismos de telesalud o telemedicina para facilitar la prestación de servicios remotos a zonas geográficamente apartadas y de mayor marginación en distintas regiones del país.

5. **Seguridad ciudadana**

   Usar las nuevas tecnologías y las telecomunicaciones para promover la comunicación e intercambio de información entre ciudadanos y autoridades para prevenir la violencia, y también para mitigar los posibles daños causados por desastres naturales.

[78] http://portal.salud.gob.mx/contenidos/sala_prensa/mexico_sano/pdf/MS10.pdf

5.2.2 HABILITADORES

Los habilitadores que se definen en la Agenda Digital Nacional son cualidades necesarias para alcanzar las metas de la estrategia digital nacional y, además, son instrumentos que se vinculan con los objetivos planteados. A continuación, se mencionan aspectos importantes de los cinco habilitadores:

1) **Conectividad**

   Describe aspectos para el desarrollo de las redes, la realización de una mejor infraestructura de telecomunicaciones y el aumento de las redes a nivel nacional, mediante el fortalecimiento del marco institucional regulatorio y el establecimiento de los tres siguientes aspectos:

   a) Construcción de una red troncal de telecomunicaciones
   b) Instalación de una red compartida de servicios móviles
   c) Conexión de sitios públicos

   Para conseguir este objetivo y, al mismo tiempo, asegurar la cobertura universal de los servicios de tv, radio, telefonía y datos para todo el país, se toman en cuenta para esta tesis, las siguientes iniciativas de la Agenda:

   i. **Ampliación de la red troncal de fibra óptica.**

      Aumentar la capacidad nacional de transporte de información y vincular a mercados que no han sido atendidos, para lograr que estos mercados sean atractivos para operadores de servicios móviles.

   ii. **Despliegue de una red compartida de servicios móviles al mayoreo.**

      Promover la estructura de operadores de telecomunicaciones locales y regionales que atiendan a las poblaciones que no cuenten con oferta de servicios.

iii. **Acceso a Internet de banda ancha a través del Programa México Conectado.**
Garantizar la conectividad de banda ancha en los sitios públicos hasta alcanzar la cobertura nacional.

iv. **Agilización y reducción de costos en el despliegue de las redes de los operadores de telecomunicaciones.**
Poner a disposición de los operadores de telecomunicaciones, los derechos de infraestructuras pasivas del Estado, para reducir costos del despliegue de redes.

v. **Mecanismos de coordinación entre los tres órdenes de gobierno para el aprovechamiento conjunto de sus redes.**
Establecer una coordinación para evitar el despliegue de infraestructura innecesariamente redundante.

vi. **Instalación de puntos de intercambio de tráfico de datos.**
Optimizar el uso de las redes troncales para que el trafico nacional no utilice cruces transfronterizos.

vii. **Centros de distribución de contenidos y centros de datos conectados a las redes troncales y a los IXP con banda ancha.**
Crear centros de distribución de datos y promover la transición ordenada a la versión del protocolo IPv6.

2) Inclusión y habilidades digitales

Para promover el desarrollo justo de habilidades para operar tecnologías y servicios digitales en todos los sectores sociales, mediante las siguientes iniciativas:

a) Incentivos para la cobertura social

b) Campaña Nacional de Inclusión Digital.

c) Inclusión y habilidades digitales con equidad de género.

d) Red nacional de centros comunitarios de capacitación y educación digital.

e) Habilidades para la Seguridad Digital.

3) Interoperabilidad.

Describe la capacidad de los sistemas para intercambiar información del gobierno a través de cuatro aspectos:

- Técnico
- Semántico
- Organizacional
- Gobernanza

Había que decir también, que cuenta con las siguientes iniciativas:

i. Lineamientos y políticas de interoperabilidad, intercambio y validación de la información en poder del Estado.

Instaurar documentos normativos que faciliten el uso de software de procesamiento de datos.

ii. Interoperabilidad de los documentos de identificación.

Para hacer más eficaces los procesos en la administración pública, se debe impulsar el Certificado de Nacimiento, el registro y expedición de Acta de Nacimiento, la Clave Única de Registro de Población (CURP), y la Firma Electrónica Avanzada.

iii. **Simplificación de la relación entre ciudadanos y gobierno mediante la interoperabilidad.**

Mejorar los trámites gubernamentales para simplificar y facilitar la experiencia del ciudadano en dichos trámites.

4) Marco Jurídico.

Su finalidad es proporcionar un ambiente de seguridad y confianza jurídica favorable para la adopción y fomento de las Tecnologías de las Información y la Comunicación, mediante el análisis de los siguientes:

- Protección de los derechos humanos
- Gobernanza de Internet
- Privacidad y protección de datos personales
- Seguridad de la información y delitos informáticos
- Firma Electrónica Avanzada
- Comercio electrónico
- Propiedad intelectual
- Gobierno digital
- Educación y salud digitales
- Economía digital

5) Datos Abiertos[79].

Los datos irán creando un valor con base en los servicios que genere, los datos deberán ser:

a) Accesibles de manera universal
b) Información pública
c) Disponibles en formatos libres y legibles por maquinas
d) Con licencias claras

[79] Datos abiertos (open data, en inglés) es una filosofía y práctica que persigue que determinados tipos de datos estén disponibles de forma libre para todo el mundo, sin restricciones de derechos de autor, de patentes o de otros mecanismos de control.

e) Primarios y oportunos
f) Reutilizables.

Al igual que los otros habilitadores, cuentan con las siguientes iniciativas para el cumplimiento de los objetivos de la Estrategia Digital Nacional:

i. **Política Nacional de Datos Abiertos.**
Hacer que la información se convierta en un bien público.

ii. **Participación social en la planeación y evaluación de políticas públicas mediante la apropiación, uso y re-uso por terceros de la información pública.**
Impulsar la participación ciudadana mediante el uso y re-uso de información para el diseño de políticas públicas.

iii. **Economía de nuevos productos, aplicaciones y servicios mediante los Datos Abiertos.**
Promover la economía digital, la invención de productos y aplicaciones por medio de la difusión de información pública.

iv. **Mecanismos de evaluación en materia de Datos Abiertos en la Administración Pública Federal.**
Fomentar un mecanismo de monitoreo y evaluación de la política de Datos Abiertos, conforme con los estándares internacionales.

5.3 CASOS NACIONALES

Aunque México cuenta con una agenda digital recientemente publicada y hace diversos esfuerzos para la construcción de un ecosistema digital más sólido en todos los sectores, la OEA estableció que México está “medianamente preparado” para enfrentar un ataque a su infraestructura critica.

En el 2013 algunos países de América Latina lograron importantes avances en la elaboración de sus políticas y marcos jurídicos, en el desarrollo de su capacidad técnica y en el entendimiento de los riesgos de los ciberataques; entre ellos Argentina y Uruguay efectuaron progresos significativos en lo que respecta a establecer un equipo u organismo nacional de respuesta ante incidentes cibernéticos. Las inversiones que realizaron en capacitación y desarrollo de capacidades les permitieron responder con mayor rapidez y eficacia; lo que permitió aminorar el impacto de los ataques y detener más delincuentes; por ello, la OEA los considera como “preparados” para enfrentar un ciberataque.

Por otra parte, existen dos marcos normativos sobre protección de datos en el mundo: el de Canadá y Alemania, los cuales fueron pioneros a nivel mundial y cuentan con grandes avances en comparación con los países latinoamericanos. Por lo que, primeramente, se analizaron los principios establecidos en sus directrices de privacidad y protección de datos, además de los fundamentos de sus estrategias de ciberseguridad.

Más adelante, se analizaron los casos de Argentina, Uruguay, Canadá y Alemania con base en la experiencia y conocimientos adquiridos hasta el año 2013 en cuanto al desarrollo de habilidades técnicas, investigación, leyes, políticas y cooperación con otras partes interesadas en seguridad cibernética.

5.3.1 CANADÁ.

Cuando México adoptó su nueva Ley Federal de Protección de Datos Personales en Posesión de Particulares en el 2010, Canadá celebraba el décimo aniversario de su Ley de Protección de la Información Personal y Documentos Electrónicos conocida en inglés como PIPEDA[80].

Canadá tiene dos leyes federales de privacidad; la Ley de Privacidad (The *Privacy Act*) y la Ley de Protección de Información Personal y de Documentos Electrónicos. La Ley de Privacidad impone obligaciones a los departamentos del gobierno federal, constituido por cerca de 250 agencias encargadas de hacer respetar los derechos de privacidad de las personas al limitar la recopilación, uso y divulgación de información personal. La Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), establece reglas de juego para las organizaciones del Sector Privado que recogen, utilizan o divulgan información personal en el curso de sus actividades comerciales. [81]

La normativa descrita en la PIPEDA se basa en diez principios relativos a la equidad en el procesamiento de la información que a su vez se conforman a los principios de la OCDE generalmente relativos a la responsabilidad, los fines, el consentimiento y las medidas de seguridad. Recientemente esta ley federal canadiense fue reformada en abril del año 2011.[82]

La Ley aborda la protección de datos personales y otorga nuevos derechos a las personas físicas para que puedan protegerse de la acumulación, uso o revelación de la información personal en la actividad comercial del sector privado. Además, la norma crea un código de información justo para garantizar una mayor

[80] PIPEDA, Personal Information Protection and Electronic Documents Act.
[81] Saltor, C. E. (2013). *La Protección de Datos Personales*. Tesis de grado doctoral sin publicar, Universidad Complutense De Madrid, Madrid, España.
[82] Bernier, Ch. (2010, Septiembre). *La ley federal canadiense des sector privado: Diez años después*. Ponencia realizada en el VIII Encuentro de Autoridades Iberoamericanas sobre Protección de Datos.

protección jurídica de los datos de carácter personal que usa y procesa el gobierno. De esta forma, la ley otorga mayor control a los individuos en cuanto al derecho para examinar la información sobre ellos en secciones gubernamentales federales y agencias.

El Gobierno Federal canadiense tiene límites impuestos por la ley para la recolección y publicación de datos, además tiene la obligación de solicitar, en lo posible, los datos en forma directa de la persona afectada. Se exige que la autoridad comunique a la persona cuando la información está siendo reunida y cómo se usará. También se prohíbe el uso de la información para otros propósitos que no sean permitidos por la ley.

La estrategia de Ciberseguridad canadiense se basa en conocer y combatir las ciberamenazas y fue presentada en el año 2010, con el compromiso de trabajar con provincias y sus gobiernos además del sector privado para implementar la estrategia y proteger así su infraestructura crítica de datos.

La estrategia de Ciberseguridad canadiense está construida sobre tres pilares:[83]

1. **Aseguramiento de los sistemas de gobierno.**
   El gobierno aportará las estructuras, las herramientas y el personal necesario para cumplir sus obligaciones en Ciberseguridad.

2. **Asociación para asegurar los sistemas cibernéticos fuera del Gobierno Federal.**
   El gobierno apoyará iniciativas y tomará medidas para fortalecer la capacidad de recuperación cibernética, incluyendo la de sus sectores de infraestructuras críticas.

[83] Gobierno de Canadá, (2010). *Canada´s Cyber Security Strategy: For a stronger and More Prosperus Canada.* Recuperado de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

3. **Ayudar a los canadienses a estar seguros en línea.**

   El gobierno asistirá a los canadienses para obtener la información que necesiten para protegerse en línea, y fortalecer la capacidad de la ley para combatir la cibercriminalidad.

Así mismo la estrategia refleja valores canadienses como el estado de derecho, la rendición de cuentas y la privacidad; permite mejoras continuas para enfrentar a las amenazas emergentes, integra actividades a través del gobierno de Canadá, además de enfatizar la alianza con la ciudadanía, las provincias, los territorios, las empresas y universidades.

5.3.2 ALEMANIA.

La *Bundesdatenschutzgesetz* (BDSG) es la Ley Federal de Protección de Datos, que actúa en conjunto con la ley de protección de datos de los estados federales alemanes y otras regulaciones específicas de diferentes áreas. Esta ley debe proteger los derechos individuales susceptibles de ser afectados a través del manejo de su información personal.

La BDSG contiene siete principios de protección de datos:[84]

1. **Prohibición sin permiso condicional.**

La recolección, procesamiento, y uso de datos personales está estrictamente prohibido a menos que el involucrado de su consentimiento.

2. **Principio de inmediatez.**

Los datos personales deben ser recolectados directamente de la persona involucrada.

3. **Prioridad a leyes especiales.**

La BDSG sustituye a cualquier ley que refleje información personal y su publicación.

4. **Principio de proporcionalidad.**

La creación de estándares limita los derechos fundamentales de la persona afectada. Por lo tanto, esas leyes y procedimientos deben ser apropiadas y estrictamente necesarias; esto es, justificadas.

[84] Bundesdatenschutzgesetz. (2015) En Federal Data Protection Act. Recuperado el 12 de Diciembre de 2015 http://germanlawarchive.iuscomp.org/?p=712

5. **Principio de anulación y economía de datos.**

Cada sistema de procesamiento de datos debe alcanzar la meta de no usar o procesar tan poco como sean posible los datos de identificación personal.

6. **Principio de transparencia.**

Si los datos personales son recolectados, la entidad responsable debe informar a la persona involucrada sobre el propósito de la recolección, procesamiento o su uso.

7. **Principio de destino.**

Si los datos son permitidos para ser recolectados para un propósito, su uso está limitado a este propósito.

La estrategia de ciberseguridad en Alemania debe estar garantizada en un nivel acorde con la importancia y protección requerida por la conexión de la infraestructura de información, sin obstaculizar las oportunidades y la utilización del ciberespacio. El nivel de ciberseguridad logrado es la suma de todas las medidas internacionales y nacionales tomadas para proteger la disponibilidad de las tecnologías de la información y comunicación, además de la integridad, autenticidad y confidencialidad de los datos en el ciberespacio.

La estrategia de ciberseguridad del gobierno alemán adapta sus medidas a las amenazas actuales y se centrará es diez áreas estratégicas:[85]

1. **Protección de las infraestructuras críticas de la información.**

Los sectores público y privado deben crear una estrategia y organización base para una coordinación más estrecha basada en el intercambio de información. Con la participación del Consejo Nacional de Ciberseguridad Alemán[86], la integración de sectores adicionales y de nuevas tecnologías se

[85] Federal Minister of the Interior. (2010). *Cyber Security Strategy for Germany.* Recuperado de
[86] The German National Cyber Security Council.

examina en mayor medida. Además, se examinará la necesidad de armonizar reglas para mantener las infraestructuras críticas durante las crisis.

2. Asegurar los sistemas IT en Alemania.

El gobierno alemán organizará iniciativas en conjunto con grupos de la sociedad para juntar consecuentemente información y asesoramiento. Además, examinará si los proveedores tienen que asumir mayor responsabilidad y asegurarse que un grupo básico de productos de seguridad y servicios están a disponibles a los usuarios.

3. Fortalecimiento de la seguridad IT en la administración pública.

La autoridad creará una común, uniforme y segura infraestructura de red en la administración federal, como una base para la comunicación de audio y datos. Por otra parte, para facilitar la implementación a través de una acción uniforme se realizarán inversiones dentro de la seguridad IT del gobierno federal con base a las posibilidades presupuestarias. Además de la cooperación operacional con los CERT se intensificará más por el Consejo de Planificación de TI[87].

4. Centro Nacional de Respuesta Cibernética.

El gobierno alemán estableció el Centro Nacional de Respuesta Cibernética para optimizar la cooperación entre las autoridades estatales y mejorar la coordinación de protección y respuesta a incidentes de TI.

5. Consejo Nacional de Ciberseguridad.

El Consejo Nacional de Ciberseguridad está destinado a coordinar las herramientas preventivas y los acercamientos interdisciplinarios de Ciberseguridad en los sectores públicos y privados. Además, complementará y unirá la gestión de TI a nivel federal y el trabajo del Consejo de Planificación de TI en el área de la ciberseguridad en un nivel político y estratégico.

[87] The IT Planning Council

6. **Control eficaz del delito también en el ciberespacio.**

Las autoridades alemanas, para enfrentar los crecientes desafíos globales de las actividades de cibercrimen, harán un esfuerzo para lograr la armonización mundial de la ley basada en la Convención del Consejo Europeo de Cibercrimen.

7. **Acción coordinada para asegurar la Ciberseguridad en Europa y todo el mundo.**

En Alemania se establecerá una política externa de Ciberseguridad de manera que los intereses e ideas relativas a la Ciberseguridad Alemana estén coordinadas con las organizaciones internacionales, como las Naciones Unidas, el Consejo de Europa, la OCDE y la OTAN. Así mismo, un código de conducta debe ser establecido para el ciberespacio, el cual deberá ser firmado por el mayor número de estados.

8. **Uso seguro y confiable de las Tecnologías de la Información.**

El gobierno alemán continuará e intensificará la investigación en materia de seguridad en TI y de protección de infraestructuras críticas. Además, se fortalecerá la soberanía tecnológica alemana y la capacidad económica de las competencias estratégicas de TI.

9. **Desarrollo de personal en autoridades federales.**

Como una política de Estado, en Alemania se analizará como una prioridad si el personal adicional es necesario en las agencias gubernamentales que se interesan en la ciberseguridad.

10. **Herramientas para responder los ciberataques.**

Las autoridades alemanas deben crear un conjunto coordinado e integral de herramientas para las autoridades con el fin de responder los ciberataques. Por encima de todo, los objetivos, mecanismos e instituciones deben ser incorporados en los procesos federales, así como con en los empresariales.

5.3.3 ARGENTINA.

Argentina cuenta actualmente con más del 76% de la población total conectado a internet, además de más de 22 millones de computadoras personales lo que hace que Argentina se encuentre entre los primeros países de la región en términos de adopción de las Tecnologías de la Información y Comunicación.[88]

Un componente importante de su rápido crecimiento ha sido el número de políticas y programas como Argentina Conectada[89] y Conectar Igualdad[90], los cuales buscan elevar la conectividad del ancho de banda en todo el país y promover la inclusión digital entre estudiantes de las escuelas sin importar su condición socioeconómica.

Además, las instituciones gubernamentales se han preocupado por tecnificar su infraestructura crítica y han digitalizado muchos de sus servicios; por ello, gran cantidad de sus procedimientos y transacciones se realizan actualmente por internet.

Dichos desarrollos han aumentado el riesgo de ser un blanco para el crimen cibernético, además de otras actividades maliciosas. Para enfrentar estas amenazas, el Gobierno Nacional creó el Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC)[91], el cual fue diseñado para apoyar la creación y adopción de un marco regulatorio que proteja a las infraestructuras estratégicas y críticas.

---

[88] Organización de los Estados Americanos, Trend Micro Incorporated. (2015, Abril). *Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas.* Recuperado de www.oas.org/cyber/
[89] http://www.argentinaconectada.gob.ar/index.html
[90] http://www.conectarigualdad.gob.ar/
[91] http://www.icic.gob.ar/

Entre los objetivos que planteó el ICIC están:

- Sensibilizar a los ciudadanos y a las instituciones sobre el riesgo que plantean las nuevas tecnologías.
- Fortalecer los niveles de seguridad cibernética en el Sector Público Nacional mediante la creación de estrategias comunes para proteger la información.
- Fomentar la colaboración entre diferentes sectores de la sociedad para adoptar un marco común de lineamientos para fortalecer los niveles de ciberseguridad e infraestructuras de información.
- Contribuir al mejoramiento de la ciberseguridad y la infraestructura de información crítica a escala internacional.

El Gobierno argentino se entrena de forma continua con el propósito de prepararse ante las amenazas cibernéticas emergentes. Desde 2012 se han llevado a cabo Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC), los cuales se realizan de forma anual.[92]

[92] Organización de los Estados Americanos, Symantec. (2014, Junio). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado de http://www.symantec.com/la/reporteOAS/

5.3.4 URUGUAY

La autoridad principal en materia de seguridad cibernética es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), donde opera el Centro de Respuesta a Incidentes de Seguridad Cibernética del Uruguay (CERTuy).[93]

Desde la creación del CERTuy, el gobierno uruguayo ha coordinado e implementado la respuesta al análisis de incidentes de seguridad, atendido la recuperación en desastres, elaborado pruebas de penetración y auditorias de seguridad. Además, ha fomentado y difundido normas, políticas y mejores prácticas que incrementan los niveles de seguridad.

Además, mediante la emisión de una serie de decretos oficiales, se instauró un marco regulatorio aplicable a las iniciativas sobre seguridad cibernética en el plano nacional. El Decreto 452 indica que el gobierno debe tener una política de seguridad cibernética, así como de poseer estándares de seguridad para el centro de datos, correos electrónicos y nombres de dominio pertenecientes a la administración central.

El sector privado no está obligado a reportar información sobre ataques cibernéticos ante las autoridades uruguayas. Los únicos que sí tienen la obligación de reportar son las instituciones y los organismos públicos, cuando un incidente de alto impacto pueda afectar al estado.

[93] Organización de los Estados Americanos, Symantec. (2014, Junio). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado de http://www.symantec.com/la/reporteOAS/

Los objetivos y obligaciones del CERTuy son:[94]

- Crear conciencia sobre las amenazas cibernéticas entre la sociedad.
- Proteger y regular los recursos de información críticos del Estado.
- Mejorar los estándares de seguridad para las bases de datos, el correo electrónico y los nombres de dominio.
- Integrar a todos los actores nacionales y regionales tales como Poder Judicial, Poder Legislativo, el Ministerio de Defensa Nacional, los sectores privado y financiero, la academia, los proveedores de servicios de Internet, la sociedad civil y los CSIRTs.

En noviembre de 2013, el CERTuy emitió la campaña Seguro te conectas, la cual busca crear conciencia sobre los problemas que puede producir el uso de las TIC, además de unir la campaña de concientización PARA, PIENSA, CONÉCTATE.

El éxito en los programas para combatir el cibercrimen y otras amenazas a la ciberseguridad necesitará de la capacidad de Uruguay de resolver tres problemas principales que han impedido su progreso: la falta de conciencia sobre la seguridad en las instituciones gubernamentales, los recursos financieros y la falta de personal capacitado.

[94] Organización de los Estados Americanos, Trend Micro Incorporated. (2015, Abril). *Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas.* Recuperado de www.oas.org/cyber/

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES.

6.1 CONCLUSIÓN.

A la vista de los resultados de este Proyecto de Tesis, se trató de cubrir la mayor posible cantidad de situaciones sobre la ciberseguridad, pero considero que existen puntos que están más allá de mis posibilidades, por lo que más adelante podrían realizarse otras tesis para abordarlos en profundidad.

A lo largo de la presente tesis referente a la confidencialidad, la privacidad y la protección de los datos, he llevado a cabo un análisis sobre características que consideré fundamentales en el ciberespacio y que determinarán el futuro a corto y mediano plazo del entorno de las redes de telecomunicaciones en nuestro país.

Para ello, hemos partido del análisis de la situación en aspectos sociales, jurídicos, políticos y tecnológicos, para así determinar los problemas actuales a los que ciudadanos de México y del mundo se enfrentan en esta materia y justificar las razones que han motivado las recomendaciones de organismos internacionales y las acciones de países que se seleccionaron para esta investigación.

En este sentido, hemos visto que uno de los problemas fundamentales que aborda esta investigación, y que hemos considerado justificadamente el pilar central de la misma: la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones no están garantizadas para los usuarios. Vimos que esta escasa protección ocasiona que los delitos cibernéticos sigan creciendo y las amenazas acechen a gobiernos, empresas y usuarios finales.

Dada esta situación, y teniendo en cuenta la enorme importancia que tiene y tendrá el sector de la ciberseguridad en el acontecer económico, social, político y tecnológico de los países, decidimos tomar las recomendaciones, normas y estándares de la Unión Internacional de Telecomunicaciones, la Unión Europea, y la Organización Internacional de Normalización con el fin de llevar a cabo un proceso de seguridad de la información de manera estructurada, organizada y documentada y de ese modo, beneficiarnos de las ventajas de la cooperación de las organizaciones para enfrentar de manera eficaz las amenazas y vulnerabilidades cibernéticas.

El análisis realizado enfoca la importancia de que los equipos de seguridad de la información (CERTs) intercambien sus conocimientos para atender las vulnerabilidades y, asimismo, que los operadores de infraestructuras de las organizaciones cumplan con los estándares de seguridad en sus productos y servicios e instauren un sistema de notificación donde bancos, empresas energéticas, de infraestructura de transporte y de internet puedan informar a los CERTs de ciberataques significativos.

Además, para asegurar la continuidad e integridad funcional del sistema de ciberseguridad, la norma ISO 27011 garantiza proteger la integridad, confidencialidad y disponibilidad de las infraestructuras críticas y los servicios, planteando controles previamente identificados tras la evaluación de riesgos de seguridad en los distintos procesos como a través de la preparación y capacitación del personal según su participación en materia de ciberseguridad.

En relación con el sector privado, es necesario que cada empresa tenga un programa estratégico de seguridad propio para su red de telecomunicaciones, además de incluir un programa de monitoreo 24/7 con análisis periódicos de la efectividad y de las posibles mejoras de la seguridad de la red, ya que existen numerosas herramientas tecnológicas utilizadas por la mayoría de empresas encargadas de la confidencialidad, privacidad y protección de datos de sus usuarios,

que proporcionan las condiciones necesarias para hacer más rentable el desafío que plantean las amenazas emergentes.

Actualmente en la legislación mexicana no existen mecanismos para garantizar la confidencialidad, la privacidad y la protección de los datos personales, que permitan frenar el uso excesivo de aquellos datos que sean falsos, desactualizados o caducos y se violente así el derecho a la intimidad consagrado en la Constitución. La ciberseguridad en México no está regulada como garantía o como un proceso específico dentro de la Estrategia Digital Nacional y en el Plan Nacional de Desarrollo vigente y no está mencionado expresamente en la Constitución del país.

Mi visión respecto del tema es que, por una parte, no se ha puesto el interés adecuado, no se entienden y tal vez ni se conocen los riesgos relativos a la seguridad de la información; por otra parte, se ha buscado la inclusión de la población mexicana a las telecomunicaciones en red, pero no se analizan las repercusiones de estar conectado, no se valora totalmente la prevención de amenazas y la protección de los recursos, ni se prevén las consecuencias que podrían traer al usuario y al país el robo de la identidad y de los datos confidenciales.

Las conclusiones resultan especialmente interesantes por varias razones: por un lado, porque la ciberseguridad y la protección de los datos son dos aspectos inseparables. Además, la seguridad personal, empresarial y nacional en el ciberespacio son retos que solo se pueden superar a través de una cooperación internacional, además de una normativa y regulación universal; ya que deben garantizar la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones, así como el cumplimiento de derechos y valores similares a los establecidos en La Carta de Derechos Fundamentales de la Unión Europea.

Por otro lado, es esencial que los gobiernos trabajen muy de cerca con el sector privado para ayudar a enfrentar las amenazas y a encontrar soluciones importantes para las infraestructuras de información críticas. El trabajo en conjunto del gobierno con el sector privado se puede convertir en una fuerte barrera de entrada para los ataques cibernéticos, en vista de que consideramos que compartir la información acerca de amenazas, vulnerabilidades e incidentes es esencial para mejorar la seguridad cibernética.

Con base en lo analizado con las normas, estándares y herramientas tecnológicas, queda en manos de los responsables en materia de política económica y de regulación de nuestro país el que se incentive, si fuere necesario, este tipo de estrategias con vistas a flexibilizar el mercado con el fin de incentivar un efectivo y rápido despliegue de este tipo de tecnologías en nuestro territorio y se preparen de la mejor manera para generar estrategias de prevención para poder actuar en un escenario de contingencia y tener los recursos y la capacidad para enfrentarse a estas amenazas de manera informada y responsable.

De los resultados de nuestro trabajo se desprende que se debería promover una Estrategia Nacional de Ciberseguridad y Ciberdefensa, ya que es fundamental para el desarrollo económico, social, político y tecnológico del país.

Por todas estas razones a continuación se presenta una propuesta con puntos que considero importantes a tomar en cuenta para la Estrategia Nacional de Ciberseguridad y Ciberdefensa.

6.2 PROPUESTA.

Garantizar a los usuarios que la captación, registro y almacenamiento de información se gestionen de manera ética, legal y responsable no es un tema exclusivo de México, sino que es un tema de importancia global. Un mal manejo de la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones en un país termina afectando a todos los demás ya que es precisamente una red interconectada.

Aquí se expondrán algunas líneas de acción que nos servirán para la estructuración de una nueva estrategia nacional de Ciberseguridad y Ciberdefensa, con el propósito de que sirvan como ejemplo para regular la captación, el registro y el almacenamiento de información de manera ética, legal y responsable.

Para juzgar el papel del gobierno mexicano en cuanto a la confidencialidad, la privacidad y la protección de datos en las redes de telecomunicaciones y para proponer soluciones respecto al tema, es útil hacer un comparativo sobre las prácticas internacionales en materia de ciberseguridad. Con este motivo se escogió a Canadá, Alemania, Uruguay y Argentina que en capítulos anteriores se analizó su situación.

En la tabla 1 pueden apreciarse las cinco áreas que conforman las categorías de mayor relevancia en algunos ejemplos de políticas de ciberseguridad[95], detallando el porcentaje de avance que cada país lleva desarrollado en sus estrategias nacionales de ciberseguridad y el ranking internacional del Índice Global de Ciberseguridad, la tabla 1 la obtuvimos de las publicaciones de la ITU y nos ayuda para obtener la conclusión.

[95] ITU, National Cybersecurity Commitment (2014, Diciembre). Global Cybersecurity Index (GCI). New York, USA.

Tabla Nª 1. Porcentaje de avance en políticas de ciberseguridad.

	México	Canadá	Alemania	Uruguay	Argentina
MEDIDAS LEGALES	25%	75%	100%	100%	100%
MEDIDAS TÉCNICAS	50%	100%	100%	67%	30%
MEDIDAS ORGANIZACIONALES	12.5%	87.5%	62.5%	62.5%	37.5%
GENERACIÓN DE CAPACIDAD	37.5%	87.5%	62.5%	50%	50%
COOPERACIÓN	37.5%	50%	50%	50%	12.5%
RANKING MUNDIAL	18°	2°	5°	8°	15°

Fuente: Elaboración propia.

En el cuadro mostrado se puede observar que los temas de mayor relevancia y atención en cuanto a estrategias nacionales de Ciberseguridad y Ciberdefensa son:

- Medidas legales:
  Es una medida del número de disposiciones legales y regulatorias disponibles.

- Medidas técnicas:
  Es una medida de los recursos dedicados a la ciberseguridad. El índice se compone de la cantidad de equipos informáticos de respuesta (CERT) existentes, el número de estándares desarrollados y el número de certificaciones efectuadas.

- Medidas organizacionales:
  Es una medida de las estrategias de coordinación a nivel nacional. El índice se compone de las políticas de ciberseguridad nacionales, los mapas de ciberseguridad, las agencias especializadas a cargo y las modalidades de su rendición de cuentas.

- Generación de capacidad:

  Se refiere a la formación de recursos humanos, principalmente mediante programas de enseñanza y entrenamiento. El índice se compone del nivel de estandarización empleada, la promoción del conocimiento, así como de la certificación y las agencias encargadas de la misma.

- Cooperación:

  Se refiere a la cooperación entre todos los sectores y disciplinas, nacional e internacional. El índice se compone de cooperación entre agencias, relación sector público – privado y lo relativo a la cooperación internacional.

En la tabla anterior se identifican las áreas de oportunidad en el trabajo para la estructuración de una nueva estrategia nacional de Ciberseguridad y Ciberdefensa en México.

A partir de las temáticas presentadas a lo largo del documento se planteó una propuesta de aspectos a desarrollar basados en las cinco áreas ya mencionadas que pueden contribuir al fortalecimiento de una estrategia nacional de Ciberseguridad y Ciberdefensa:

1. **Medidas legales.**

   En medidas legales se proponen las siguientes:

   - Armonizar el marco legal interno respecto a leyes internacionales
   - Incorporar a los delitos cibernéticos como tema fundamental de las políticas, normas, actos administrativos y otras figuras jurídicas
   - Regular el manejo de la información contenida en bases de datos personales, en especial la financiera, la crediticia, la comercial, la correspondiente a los servicios y la proveniente de terceros
   - Reglamentar el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales

- Reglamentar los procedimientos de cesión de datos a las autoridades y garantizar los derechos fundamentales de habeas data, de intimidad y de privacidad
- Modificar el Código Penal para preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
- Tipificar las siguientes conductas penales en las siguientes modalidades: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales
- Establecer que cuando el Juez tenga motivos razonables para deducir que alguien está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a la policía la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital del sospechoso para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen
- Fortalecer las medidas jurídicas existentes, y fomentar la adopción de estándares con referentes internacionales para garantizar redes de telecomunicaciones más seguras, como la recomendación ITU TX.1205.

2. Medidas técnicas:

Las medidas técnicas que se proponen son las siguientes:

- Ampliar y mejorar las capacidades del CERT de Seguridad e Industria, con la colaboración y coordinación con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado

- Implementar modelos de seguridad de acuerdo con las características y necesidades de los proveedores de redes y servicios de telecomunicaciones que vayan con los marcos de seguridad definidos por la UIT-T X-800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805)
- Reforzar la red de telecomunicaciones para proteger la confidencialidad, la privacidad y la disponibilidad de los datos a través de las herramientas del sector privado, las cuales son la data center firewall, NGFW, UTM y aplicaciones de seguridad
- Garantizar la integridad, confidencialidad y disponibilidad de las infraestructuras críticas y los servicios de las organizaciones de telecomunicaciones para que sean seguros y resistentes a amenazas en el ciberespacio mediante el cumplimiento con la ISO 27011.

3. Medidas organizacionales:

Las medidas organizacionales que se proponen son las siguientes

- Crear una Agencia Nacional de la Delincuencia Cibernética.
- Crear un Centro Integrado para el Delito Cibernético.
- Crear un Consejo de Seguridad Cibernética Nacional.
- Crear el mecanismo de coordinación intersectorial para emitir los lineamientos rectores del CERT.
- Destinar recursos humanos con conocimientos técnicos o jurídicos en el tema de ciberseguridad para apoyar a las actividades del CERT.
- Emitir un documento con las directrices en temas de ciberseguridad basada en estándares internacionales para ser implementadas por entidades mexicanas que manejen datos.

- Elaborar un documento en el que se analice la normatividad actual y se propongan las modificaciones necesarias en materia de ciberseguridad, para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación.

4. Generación de capacidad:

Las medidas de generación de capacidad que se proponen son las siguientes:

- Diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos para la policía judicial, los jueces y los fiscales
- Formar recursos humanos especializados en la materia de ciberseguridad
- Proporcionar los conocimientos necesarios, capacitación y otros recursos a los países que buscan construir la capacidad técnica y la ciberseguridad.
- Implementar asignaturas en seguridad de la información, ciberdefensa y ciberseguridad (teórico-prácticas) en las escuelas de formación y de capacitación.
- Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional
- Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación
- Sensibilizar a la población sobre las acciones para incrementar la seguridad en el acceso a internet.

5. Cooperación:

Finalmente, proponemos los aspectos siguientes relativos a la cooperación:

- Impulsar el establecimiento de canales internacionales de información, detección y respuesta
- Generación de políticas orientadas a fortalecer las alianzas y los acuerdos de cooperación y colaboración internacionales.
- Asociación con los estados, municipios, regiones, el sector privado y los sectores de infraestructura crítica. Promover la participación coordinada de instituciones públicas y del sector privado en simulacros y ejercicios internacionalesImplementación de mecanismos de múltiples niveles para el intercambio de informaciónPromover la armonización legislativa y la cooperación judicial y policial nacional e internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo

6.3 RECOMENDACIONES.

El objetivo principal de este trabajo es que pueda servir de guía de referencia y consulta para poder garantizar a los usuarios confidencialidad, privacidad y protección de datos en las redes de telecomunicaciones. Por ello consideramos imprescindible añadir una serie de recomendaciones finales, las cuales están basadas en las recomendaciones de la Organización de Estados Americanos (OEA)[96], el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas[97] y la Estrategia de Ciberseguridad Nacional de España [98] para poder realizar los análisis teniendo como referencia ciertos aspectos reflejados en la guía.

Antes, dejar constancia de que hay que considerar este trabajo como un apoyo genérico, ya que no se ha podido profundizar en todos los temas que abarca la temática de la ciberseguridad. De hecho, la primera recomendación que hacemos es que, si el análisis que se pretende realizar es muy específico en ciberseguridad, será necesario contar el apoyo de fuentes especializadas en esos temas. La guía tiene verdadera utilidad como posible nexo de unión entre diversas temáticas relacionadas y, por supuesto, como apoyo para poder acometer un análisis genérico de confidencialidad, privacidad y protección de datos en las redes de telecomunicaciones.

A continuación, se expondrán recomendaciones tomadas de la experiencia en políticas de ciberseguridad, marcos constitucionales, investigación y legislación de delitos cibernéticos, ciberdefensa y cooperación internacional de los Expertos internacionales:

---

[96] OEA. (2015, Abril). *Misión de Asistencia Técnica en Seguridad Cibernética". Conclusiones y Recomendaciones.* Colombia.
Recuperado de http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf

[97] Organización de los Estados Americanos, Trend Micro Incorporated. (2015, Abril). *Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas.* Recuperado de www.oas.org/cyber/

[98] Gobierno de España. (2013). *Estrategia de Ciberseguridad Nacional.* España. Recuperado de www.lamoncloa.gob.es

Al gobierno:

- **Desarrollar una visión global para la ciberseguridad**

La visión debe ser liderada por el más alto nivel de gobierno, debe formular objetivos y definir por qué son esenciales para la nación. Los objetivos distinguirán la prosperidad económica y social, la defensa del país y la lucha contra el cibercrimen también reconocerán la necesidad de respetar los valores establecidos en la constitución e incluir la cooperación internacional.

- **Adoptar un enfoque global de la gestión de riesgos de ciberseguridad**

Establecer un programa nacional de gestión de riesgos, tales como evaluación, tratamiento, preparación, recuperación y técnicas para que todos los actores evalúen y gestionen los riesgos de ciberseguridad.

- **Establecer un marco institucional**

El marco debería establecer un organismo coordinador con autoridad y responsabilidad legal para actuar, además de tener la responsabilidad de dirigir la formulación de una política pública y desarrollar una evaluación integral de los riesgos de ciberseguridad nacional.

- **Establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación**

Consultar con todas las partes interesadas sobre la forma de organizar el diálogo, establecer reglas para consultar durante la elaboración de políticas, además de crear foros para la ejecución de la visión y finalmente desarrollar un plan a corto, mediano y largo plazo para llegar a todos los actores gubernamentales y no gubernamentales.

- **El Gobierno debe adoptar una política para la protección de la infraestructura crítica**

La política para la protección de las infraestructuras critica debe girar en torno a que la coordinación debe liderar este proceso para asegurar los objetivos y se equilibren entre sí para el máximo beneficio del país.

A las autoridades de procuración e impartición de justicia:

- Definir la unidad policial que se encargará de la prevención, investigación y persecución de los delitos informáticos
- Establecer un punto de contacto disponible las 24 horas del día, los 7 días de la semana para garantizar la prestación de ayuda inmediata para fines de investigación, procedimientos u obtención de pruebas electrónicas
- Crear en la fiscalía una unidad especializada para la investigación de los ciberdelitos
- Proteger las garantías individuales durante el procedimiento para la investigación de delitos informáticos
- Adoptar medidas procesales para posibilitar la preservación de la evidencia digital
- Verificar que todas las actividades internacionales que involucren el intercambio de datos personales respeten las leyes internacionales de derechos humanos (derecho a la privacidad)
- Instaurar un marco para simplificar el intercambio directo de información entre equipos de respuesta e incidentes cibernéticos de otros países

A las organizaciones Públicas o Privadas:

- **Utilizar estrategias de defensa profunda**

Incluir la implementación de firewalls, así como antivirus de puertas de enlace, sistemas de protección contra intrusiones (IPS), escaneos de vulnerabilidad de sitios web con protección contra malware y soluciones de seguridad de puertas de enlace web en toda la red.

- **Monitorear para detectar intentos de penetración en la red y vulnerabilidades**

Intercambiar alertas sobre nuevas vulnerabilidades y amenazas en las plataformas para tomar medidas proactivas de reparación.

- **Usar un producto integral para seguridad en los dispositivos finales**

Implementar y usar un producto integral de seguridad que tenga capas adicionales de protección incluyendo:

- Prevención contra intrusión
- Protección del explorador
- Soluciones de reputación de cualquier aplicación y sitio web
- Funciones de prevención conductual de las aplicaciones
- Configuración del control de las aplicaciones y complementos del explorador
- Configuración del control de los dispositivos.

- **Proteger claves privadas.**

Obtener certificados digitales de una autoridad reconocida y confiable, usar infraestructuras independientes de firma de prueba y firma de versión, además de proteger las claves en dispositivos de hardware, criptográficos y a prueba de alteraciones.

- **Usar encriptación para proteger datos sensibles**

Implementar una política de seguridad que requiera que los datos sensibles sean encriptados, esto debe incluir una solución de Protección Contra Perdida de Datos (DLP) capaz de descubrir donde reside la información sensible, monitorear su uso y los proteja contra las perdidas.

- **Asegurar que todos los dispositivos con acceso a la red tengan protecciones de seguridad**

Avalar que exista un perfil mínimo de seguridad para todo dispositivo que acceda a la red.

- **Tomar medidas de actualización y aplicación de parches**

Hacer actualizaciones, cambios y migraciones desde exploradores, aplicaciones y complementos obsoletos. Siempre que sea posible se debe automatizar las implementaciones de parches para mantener la protección contra vulnerabilidades.

- **Aplicar una política de contraseñas**

Asegurar que las contraseñas cuenten con un mínimo de 8-10 caracteres de largo con una combinación de letras y números, además de reutilizar las mismas contraseñas en distintos sitios web.

- **Hacer copias de seguridad regularmente.**

Crear y mantener copias de seguridad de los sistemas críticos y de los extremos en caso de emergencia de seguridad o de datos.

- **Restringir los archivos adjuntos de correo electrónico**

Configurar los servidores de correo para bloquear o eliminar mensajes que contengan archivos adjuntos que se usan para difundir virus, como, por ejemplo: VBS, .BAT, .EXE, .PIF y .SCR.

- **Contar con procedimientos de respuesta a infecciones e incidentes**

Implementar un procedimiento de respuesta a infecciones e incidentes que incluya:

  - Contar con copias de seguridad y restauración para recuperar datos perdidos o comprometidos
  - Utilizar las funciones de detección de los firewalls y soluciones de seguridad de puertas de enlace web y endpoint para identificar sistemas infectados
  - Aislar las computadoras infectadas para prevenir el riesgo de infectar otros equipos
  - Bloquear el acceso de los servicios red si son víctimas de una amenaza hasta aplicar un parche.

- **Educar a los usuarios acerca de protocolos básicos de seguridad**

Los usuarios deben tener cuidado al hacer click en las URL de mensajes de correo electrónico o programas, además de no abrir datos adjuntos si no se esperaba recibirlos o si no provienen de una fuente conocida o confiable a menos que la descarga haya sido escaneada para detectar virus y malware.

A la Universidad:

- Establecer una academia de cibernética profesional para capacitar profesionales en ciberseguridad y promover la certificación en el país
- Impartir capacitación a los ministerios públicos, procuradores, jueces, fiscales y policías en materia de ciberdelitos y en aspectos técnicos y jurídicos del tratamiento de la evidencia digital
- Fortalecer el conocimiento académico en ciberseguridad
- Orientar y asesorar sobre normas, marcos y sobre las mejores prácticas de ciberseguridad

- Establecer un punto de contacto disponible las 24 horas del día, los 7 días de la semana para garantizar la prestación de ayuda inmediata para fines de investigación, procedimientos u obtención de pruebas electrónicas
- Establecer centros de innovación donde la población pueda buscar iniciativas empresariales en ciberseguridad
- Instaurar un mecanismo de cooperación formal entre el gobierno y el sector privado, que sea seguro para el intercambio de información de incidentes de ciberseguridad nacional e internacional.

Finalmente, a los ingenieros en telecomunicaciones:

- Obtener certificaciones en ciberseguridad
- Capacitarse en ciberseguridad en la academia de cibernética
- Promover el conocimiento académico en ciberseguridad
- Utilizar responsablemente las normas y marcos, además de aplicar las mejores prácticas de ciberseguridad ya que, estos asuntos pueden resultar vitales en la operación de las soluciones que ellos aporten a la sociedad.

BIBLIOGRAFÍA Y REFERENCIAS

1. Aldana, A. T. & Vallejo, A. C. (2010). Telecomunicaciones, convergencia y regulación. Revista de Economía Institucional, 12(23), 165-197. Recuperado de http://www.redalyc.org/articulo.oa?id=41915521008

2. Aldana, A. T. & Vallejo, A. C. (2010). Telecomunicaciones, convergencia y regulación. Revista de Economía Institucional, 12(23), 165-197. Recuperado de http://www.redalyc.org/articulo.oa?id=41915521008

3. ANADE, Colegio de Abogados. (2014, Agosto) Resumen de la nueva Ley Federal de Telecomunicaciones Radiodifusión. Recuperado de http://anademx.com/files/2014/08/4-AGOSTO-2014.-NOTA-DECRETO-LFTR.pdf

4. Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado, 3 (2), 85-139.

5. Bernier, Ch. (2010, Septiembre). La ley federal canadiense des sector privado: Diez años después. Ponencia realizada en el VIII Encuentro de Autoridades Iberoamericanas sobre Protección de Datos.

6. Bundesdatenschutzgesetz. (2015) En Federal Data Protection Act . Recuperado el 12 de Diciembre de 2015 http://germanlawarchive.iuscomp.org/?p=712

7. Carrillo D'Herrera, Juan Carlos. (2011, Mayo). Ley Federal de Protección de Datos Personales en Posesión de Particulares. Seguridad. Cultura de Prevención TI. Num 10. Recuperado de http://revista.seguridad.unam.mx/numero-10/ley-federal-de protecci%C3%B3n-de-datos-personales-en-posesi%C3%B3n-departiculares

8. Chaname, O. R. (2003). Hábeas data y el derecho fundamental a la intimidad de la persona. Tesis de maestría no publicada, Universidad Mayor de San Marcos, Lima, Perú.

9. Colautti, C. E. (1996). Reflexiones preliminares sobre el Hábeas Data, La Ley, 1996-C, 917 -922.

10. Comisión Europea. (2000). Carta de Derechos Fundamentales de la Unión Europea.
Recuperado de http://www.europarl.europa.eu/charter/pdf/text_es.pdf

11. Comisión Europea. (2010, Marzo). Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global. Recuperado de http://eur-lex.europa.eu/procedure/ES/200304

12. Comisión Europea. (2010, Marzo). Una estrategia para un crecimiento inteligente, sostenible e integrador. Recuperado de https://www.sepe.es/contenidos/personas/formacion/refernet/pdf/Estrategia_Europa_2020.pdfn

13. Constitución Política de los Estados Unidos Mexicanos, artículo VI.

14. Constitución Política de los Estados Unidos Mexicanos, artículo XVI.

15. El Economista. (2013, Noviembre). Estrategia Digital potenciará desarrollo de México: Peña Nieto. Recuperado de http://eleconomista.com.mx/sociedad/2013/11/25/estrategia-digital-potenciara-desarrollo-mexico-pena-nieto

16. El Economista. (2013, Noviembre). Estrategia Digital potenciará desarrollo de México: Peña Nieto. Recuperado de http://eleconomista.com.mx/sociedad/2013/11/25/estrategia-digital-potenciara-desarrollo-mexico-pena-nieto

17. European Network and Information Security Agency. (2006, Diciembre). Cómo crear un CSIRT paso a paso. Recuperado de http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-spanish

18. Federal Minister of the Interior. (2010). Cyber Security Strategy for Germany. Recuperado de https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

19. Fortinet Network Security Solutions (2015, Enero), Application Security. Recuperado de https://partners.fortinet.com

20. Fortinet Network Security Solutions (2015, Enero), Data Center Firewalls. Recuperado de https://partners.fortinet.com

21. Fortinet Network Security Solutions (2015, Enero), Next Generation Firewall (NGFW). Recuperado de https://partners.fortinet.com

22. Fortinet Network Security Solutions (2015, Enero), Unified Threat Management (UTM). Recuperado de https://partners.fortinet.com

23. Garriga-Domínguez, A. (2004). Tratamiento de datos personales y derechos fundamentales. Madrid: Dykinson.

24. Gobierno de Canadá, (2010). Canada´s Cyber Security Strategy: For a stronger and More Prosperous Canada. Recuperado de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

25. Gobierno de España. (2013). Estrategia de Ciberseguridad Nacional. España. Recuperado de www.lamoncloa.gob.es

26. Guerra de la Espriella, M. R. & Oviedo, J. D. (2011, Abril). De las telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09), Bogotá, Colombia: CEPAL. Recuperado de http://repositorio.cepal.org/bitstream/handle/11362/4818/S110124_es.pdf?sequence=1

27. Gutiérrez, C. S.; Liceaga, C. J.; Baker E. T. & Aguilar, R. G. (2009, Diciembre). Manual de normas y políticas de seguridad informática. México: UVM.

28. ITU, National Cybersecurity Commitment (2014, Diciembre). Global Cybersecurity Index (GCI). New York, USA.

29. Locke, J. (1690). Del estado de la naturaleza. En Mellizo, C. (Eds.), Segundo Tratado sobre el Gobierno Civil. Un ensayo acerca del verdadero origen, alcance y fin del Gobierno Civil. (pp. 5-10).

Recuperado de http://cinehistoria.com/locke_segundo_tratado_sobre_el_gobierno_civil.pdf

30. Marsden, C. T. (2012, Febrero). Neutralidad de la Red: Historia, regulación y futuro. Revista de los Estudios de Derecho y Ciencia Política de la UOC, ISSN 1699-8154(13). 24-43.

31. McCarthy Tétrault. (2000, Noviembre). Manual de reglamentación de las telecomunicaciones. (ISBN 0-9697178-7-3). Washington, Estados Unidos: Banco Mundial. Recuperado de http://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/Handbook_A4_S.pdf

32. Meglena, K. (2009, Marzo). European Consumer Commissioner, Roundtable: Keynote Speech. Ponencia presentada en el I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores, Cartagena.

33. Ministerio de defensa. (2014, Junio). Documentos de Seguridad y Defensa 60 Estrategia de la información y seguridad en el ciberespacio. Recuperado de http://www.defensa.gob.es/ceseden/ealede/publicaciones/docSegyDef/

34. Muñoz de Alba, M. M. (2006). Habeas Data. En Romero, R. M. (Eds.), Estudios en homenaje a Marcia Muñoz de Alba Medrano. Estudios de derecho público y política. (pp. 1-21). México: Instituto de Investigaciones Jurídicas de la UNAM. Recuperado de http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf

35. OEA. (2015, Abril). Misión de Asistencia Técnica en Seguridad Cibernética". Conclusiones y Recomendaciones. Colombia. Recuperado de http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_S

PA.pdf

36. Organización de las Naciones Unidas, UNESCO. (2008, Diciembre). Declaración Universal de los Derechos Humanos. Recuperado de http://unesdoc.unesco.org/images/0017/001790/179018m.pdf

37. Organización de los Estados Americanos, Symantec. (2014, Junio). Tendencias de Seguridad Cibernética en América Latina y el Caribe. Recuperado de http://www.symantec.com/la/reporteOAS/

38. Organización de los Estados Americanos, Trend Micro Incorporated. (2015, Abril). Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas. Recuperado de www.oas.org/cyber/

39. Parlamento europeo, Consejo de la Unión Europea. (1995, Octubre). Directiva 95/46/ relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_es.pdf

40. Parlamento europeo, Consejo de la Unión Europea. (2007, Junio). Dictamen 4/2007 sobre el concepto de datos personales. Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

41. Pérez Royo, J. (2000). Curso de derecho constitucional. Barcelona: Ediciones jurídicas y sociales.

42. PIPEDA, Personal Information Protection and Electronic Documents Act.

43. Pizzolo, C. (1996). Hábeas data. El derecho a la intimidad. Buenos Aires, Argentina: Desalma.

44. Ponencia presentada en el I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores, Cartagena.
45. Reglamento (ce) N° 1211/2009. Por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), Parlamento europeo, 25 de noviembre de 2009.

46. Resolución Nª 447. Estatuto de la comisión interamericana de telecomunicaciones (CITEL), Asunción, Paraguay, 5 de junio de 2014.

47. Ruiz, L. M. (2014, Enero). Neutralidad de red y desarrollo de las TIC. Revista Universitaria Europea, ISSN: 1139 -5796(20), 1-20

48. Sagüés, N. P. (1995). Subtipos de Hábeas Data. Jurisprudencia Argentina, 4,352-354

49. Saltor, C. E. (2013). La Protección de Datos Personales. Tesis de grado doctoral sin publicar, Universidad Complutense De Madrid, Madrid, España.

50. Schwartz, Paul M. (2004). Property, Privacy and Personal Data. Harvard Law Review, 117, 2055-2128

51. Sector de Normalización de las Telecomunicaciones de la UIT. (2000, Febrero). Serie M: RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales. Recuperado de http://www.itu.int/rec/T-REC-M.3010/es

52. Sector de Normalización de las Telecomunicaciones de la UIT. (2008, Abril). Serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad. Seguridad en el Ciberespacio– Ciberseguridad. Recuperado de https://www.itu.int/rec/T-REC-X/es

53. Sector de Normalización de las Telecomunicaciones de la UIT. (2012, Enero). Seguridad de las telecomunicaciones y las tecnologías de la información. Recuperado de http://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf

54. Sennett, R. (1978). El declive del hombre público. Recuperado de http://www.ddooss.org/libros/Richard_Sennett.pdf

55. Telecommunication standardization sector of ITU. (2008, Febrero). Series X: data networks, open system communications and security. Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Recuperado de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43751

56. Telefónica I+D. (s.f.). Las telecomunicaciones de nueva generación. Recuperado de http://catalogo.rebiun.org/rebiun/record/Rebiun10386440

57. Warren, S. D. y Brandeis, L. D. (1995). The Right to Privacy. The Harvard Law Review Association, 4(5), 193-220.

GLOSARIO.

A continuación, se muestran conceptos y definiciones claves que tiene el informe de la investigación.

ISP, son las siglas en inglés de *Internet Service Provider*, es la empresa que brinda conexión a Internet a sus clientes.

IXP, son las siglas en inglés de *Internet Exchange Point*, una infraestructura física a través de la cual los proveedores de servicios de Internet intercambian el tráfico de Internet entre sus redes.

3DES, son las siglas en inglés de *Triple Data Encryption Standard*.

AD, Dispositivo de adaptación.

ADC, son las siglas en inglés de Application *Delivery Controllers*.

AES, son las siglas en inglés de advanced encryption standard.

AES, son las siglas en inglés de *Advanced Encryption Standard*.

AGESIC, Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

AND, son las siglas en inglés de *Application Delivery Network.*

Anonymus, es un movimiento internacional de ciberactivistas, formado por un número indeterminado de personas que reciben ese nombre porque no revelan su identidad.

Anti-spam, aplicación o software informática que se encarga de detectar y eliminar el spam y los correos no deseados.

Antispyware, es una tecnología de seguridad que ayuda a proteger a un equipo contra spyware y otro software potencialmente no deseado.

Antivirus, son programas que buscan prevenir, detectar y eliminar virus informáticos.

Asequibilidad, que puede conseguirse o alcanzarse.

ASIC, son las siglas en inglés de *Application-Specific Integrated Circuits*.

ATP, son las siglas en inglés de *Advanced Threat Protection*.

Botnet, es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Por lo general, los *bots*, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas como "*botnet*", que comúnmente está compuesta por máquinas víctimas de todo el mundo.

Brecha digital, hace referencia a la desigualdad entre las personas que pueden tener acceso o conocimiento en relación a las nuevas tecnologías y las que no.

BYOD, son las siglas en inglés de Bring *Your Own Device*.

Caballos de Troya, es una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño.

Carta de Derechos Fundamentales, reconoce una serie de derechos personales, civiles, políticos, económicos y sociales de los ciudadanos y residentes de la UE, consagrándolos en la legislación comunitaria.

Centro de datos, son salas especiales equipadas con mecanismos de control eléctrico, ambiental y de incendios en donde se alojan los sistemas de proceso, comunicación y almacenamiento de datos.

CERT, son las siglas en inglés de *Computer Emergency Response Team*.

CERTuy, Centro de Respuesta a Incidentes de Seguridad Cibernética del Uruguay.

CESI, Comité Especializado en Seguridad de la Información.

Ciberentorno, incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

Ciberespacio, es un entorno virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes.

Cibernético, ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas.

Ciberseguridad, como una colección de instrumentos, políticas, conceptos de seguridad, directrices, planteamientos de gestión de riesgos, garantías y tecnologías que pueden utilizar para proteger el entorno, la organización y los usuarios.

CITEL, Comisión Interamericana de Telecomunicaciones.

Convergencia, puede ser entendida como el continuo desarrollo y provisión de servicios de voz, video y datos, ya sea individual o conjuntamente sobre redes basadas en Internet Protocolo (IP) usando diversos dispositivos fijos y móviles.

Cookies, son usualmente son pequeños archivos de texto y se almacenan en el directorio del navegador de tu ordenador o en las subcarpetas de datos de programa.

CPU, son las siglas en inglés de Central *Processing Unit*.

Criptografía, es la ciencia que resguarda documentos y datos que actúa a través del uso de las cifras o códigos para escribir algo secreto en documentos y datos que se aplica a la información que circulan en las redes locales o en internet

CRM, son las siglas en inglés de Customer *Relationship Management.*

DDoS, son las siglas en inglés de *Distributed Denial of Service*.

Deep Packet Inspection, es una forma de filtraje de paquetes en redes de computación que examina la sección de datos de paquetes, al pasar por un punto de inspección.

Derechos humanos, son derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición. Todos tenemos los mismos derechos humanos, sin discriminación alguna. Estos derechos son interrelacionados, interdependientes e indivisibles.

Digitalización, es el proceso de convertir información analógica en formato digital, mediante el cual un mensaje se convierte en una sucesión de impulsos eléctricos, equivalente a dígitos combinados (código binario), el 0 ó el 1.

Directivas, norma que fija a los Estados los objetivos que en determinada materia han de alcanzar, reservándoles la facultad de decidir sobre la forma y los medios de conseguirlos

DPI, son las siglas en inglés de Deep *Packet Inspection*.

ENRIC, Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos.

ENSI, Estrategia Nacional de Seguridad de la Información.

Ethernet, también conocido como estándar IEEE 802.3, es un estándar de transmisión de datos para redes de área local.

FCC, son las siglas en inglés de *Federal Communications Commision*.

Filtro web, es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo.

Firewalls, es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

Gigabits, es una unidad de medida de información normalmente abreviada como Gb, que equivale a 109 bits.

GSLB, son las siglas en inglés de Global *Server Load Balancing*.

Gusanos, es un programa que se reproduce por sí mismo, que puede viajar a través de redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware para difundirse.

Hacking, el término hackear significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red

Hardcoded, término del mundo de la informática hace referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente (a fuego) en el código fuente del programa, en lugar de obtener esos datos de una fuente externa como un fichero de configuración o parámetros de la línea de comandos, o un archivo de recursos.

HTML, es el lenguaje que se emplea para el desarrollo de páginas de internet. Está compuesto por una serie de etiquetas que el navegador interpreta y da forma en la pantalla.

Hypervisor, son aplicaciones que presentan a los sistemas operativos virtualizados (sistemas invitados) una plataforma operativa virtual (hardware virtual), a la vez que ocultan a dicho sistema operativo virtualizado las características físicas reales del equipo sobre el que operan.

IaaS, son las siglas en inglés de *Infraestructure as A Service*.

ICIC, Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad.

IDS, Sistema de Detección de Intrusiones.

IEC, son las siglas en inglés de International *Electrotechnical Commission*.

IoT, El internet de las cosas o The Internet of Things.

IP, son las siglas en inglés de Internet Protocol, un número único e irrepetible con el cual se identifica una computadora conectada a una red

IPS, son las siglas en inglés de Intrusion *Prevention System*.

IPsec, abreviatura de Internet *Protocol security*, un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

IPv6, son las siglas en inglés de *Internet Protocol version 6*, es una versión del *Internet Protocol* (IP)

La nube, que viene del inglés *Cloud computing*, es el nombre que se le dio al procesamiento y almacenamiento masivo de datos en servidores que alojen la información del usuario

LDAP, son las siglas en inglés de *Lightweight Directory Access Protocol,* es un conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de la red. Está basado en el estándar X.500 para compartir directorios, pero es menos complejo e intensivo en el uso de recursos.

LLB, son las siglas en inglés de *Basic Link Load Balancing*.

MD, Dispositivo de mediación.

Monopolístico, es una situación en el mercado en la que la fabricación y/o comercialización de un producto, un bien o un servicio está en manos de una única empresa.

NAT, son las siglas en inglés de *Network Address Translation.*

NE, Elemento de red.

NEF, son las siglas en inglés de *Network Element Function*.

Neutralidad, es un principio que establece que los paquetes de datos (el tráfico) recibido o generado en Internet no debe ser manipulado, tergiversado, impedido, desviado, priorizado o retrasado en función del tipo de contenido, del protocolo o aplicación utilizado, del origen o destino de la comunicación ni de cualquiera otra consideración ajena a la de su propia voluntad.

Normas, es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades.

OMC, Organización Mundial del Comercio.

ORECE, Organismo de Reguladores Europeos de las Comunicaciones Electrónicas.

OS, son las siglas en inglés de *Operating System*, es un programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes

OSF, son las siglas en inglés de *Operation System Function*.

OSI, son las siglas en inglés de *Open Systems Interconnection* o Interconexión de Sistemas Abiertos. Es un modelo o referente creado por la ISO para la interconexión en un contexto de sistemas abiertos. Se trata de un modelo de comunicaciones estándar entre los diferentes terminales y host. Las comunicaciones siguen unas pautas de siete niveles preestablecidos que son Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación.

OTS, son las siglas en inglés de *Off-The-Shelf*.

OWASP. son las siglas en inglés de *Open Web Application Security Project* o Proyecto abierto de seguridad de aplicaciones web, es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro

PaaS, son las siglas en inglés de *Plataform as A Service*.

PCI DSS, son las siglas en inglés de *Payment Card Industry Data Security Standards*.

PDCA, son las siglas en inglés de Plan*, Do, Check, Act*.

Phishing, es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

PICI, Protección de Infraestructuras Críticas de Información.

PII, Informacion Personal Identificable.

POE, son las siglas en inglés de *Power-over-Ethernet*.

PTT, son las siglas en inglés de *Post Telegraph&Telephone*.

QoS, son las siglas en inglés de *Quality of Service,* un conjunto de tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo determinado a uno o varios dispositivos.

RBAC, son las siglas en inglés de *Role Based Acces Control*.

Red troncal, es una red utilizada para interconectar otras redes, es decir, un medio que permite la comunicación de varias LAN o segmentos.

Reguladores de telecomunicaciones, tienen por objetivo primordial asesorar la coherencia legislativa y reglamentaria en materia de Telecomunicaciones, velar por el cumplimiento de las normas en dicha materia y proponer reformas institucionales para la defensa de la competencia en materia de Telecomunicaciones

RGT, Red de Gestión de las Telecomunicaciones.

Router, Dispositivo que proporciona conectividad a nivel de la red o a nivel tres en el modelo OSI.

RTIR, son las siglas en inglés de *Request Tracker for Incident Response.*

SaaS, son las siglas en inglés de *Software as a Service*.

Sandboxing, mecanismo que implementan varias aplicaciones para ejecutar aplicaciones y programas con seguridad y "aislarlas" del resto del sistema dentro de una especie de contenedor virtual desde el cual controlar los distintos recursos que solicita dicha aplicación

SDN, son las siglas en inglés de *Software-Defined Networks*.

SGS, Sistemas de Gestión de la Seguridad de la Información.

SGSI, Sistema de Gestión de Seguridad de la Información.

Software, se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

SQL, son las siglas en inglés de *Structured Query Language.*

SSL, son las siglas en inglés de *Security Sockets Layer*.

SSR, son las siglas en inglés de *Shared Security Responsibility*.

Switch, es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.

TCP, son las siglas en inglés de *Transmission Control Protocol*, es uno de los principales protocolos de la capa de transporte del modelo TCP/IP.

Tecnologías de la Información y Comunicación (TIC), son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes

TF, son las siglas en inglés de *Transformation Function*.

UIT, Unión Internacional de Telecomunicaciones.

UIT-D, Unión Internacional de Telecomunicaciones, Sector de Desarrollo.

UIT-R, Unión Internacional de Telecomunicaciones, Sector de Radiocomunicaciones.

UIT-T, Unión Internacional de Telecomunicaciones, Sector de Normalización.

Universalidad, que comprende o es común a todos en su especie, sin excepción.

URL, son las siglas en inglés de *Uniform Resource Locator*, que sirve para nombrar recursos en Internet.

UTM, son las siglas en inglés de *Unified Threat Management*.

VLAN, es un grupo de dispositivos de red, tales servidores y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red.

VoIP, Voz sobre Protocolo de internet.

VPN, son las siglas en inglés de *Virtual Private Network*, son un tipo de red en el que se crea una extensión de una red privada.

WAF, Web del Firewall.

WAN, son las siglas en inglés de *Wide Area Network*, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes.

WS, Estación de trabajo.

WSF, son las siglas en inglés de *Workstation Function*.

XSS, Cross-site scripting.