DETERMINACIÓN DE LOS RIESGOS Y PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN DEL TELETRABAJO EN LAS ORGANIZACIONES.

JHULIE ANDREA BORDA CRUZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

DETERMINACIÓN DE LOS RIESGOS Y PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN DEL TELETRABAJO EN LAS ORGANIZACIONES.

JHULIE ANDREA BORDA CRUZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Yenny Stella Núñez
Director Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 15 de marzo del 2021

DEDICATORIA

Esta monografía la dedico a mi mamá, quien es mi motor principal y mi más grande apoyo en los momentos vertiginosos de la vida, quien con amor y comprensión me ha brindado las herramientas para convertirme en la persona y profesional que soy hoy en día y a Dios le doy gracias por ello.

AGRADECIMIENTOS

Mi más cordial agradecimiento hacia las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes nos forman profesionales completos a través de un sistema de gestión implementado que facilita el desenvolvimiento de sus estudiantes de manera óptima hasta el cumplimiento de sus logros. Asimismo, agradecer a cada uno de mis tutores y asesores que de una u otra forma han compartido sus conocimientos hacia mi persona para lograr disipar dudas acerca de los procedimientos respectivos para cumplir con los objetivos de esta monografía.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

IPS: Sistema de prevención de intrusos [1] el cual es un software que permite controlar el acceso a los portales informático, generando protección a la información de los ataques y los intrusos.

WEBSITES: sitios web [2].corresponde a una disposición de la comunicación y la información existente en una plataforma digital (internet), lo cuales se encuentran conformados por acciones de los sujetos y el contenido que se publica.

PASSWORDS: son contraseñas para acceder de forma segura a los sistemas de información [3].

JAVASCRIPT: conocido como un lenguaje de programación [4].para crear páginas web dinámicas, el cual cuenta con características como que los programas se pueden probar en cualquier navegador y no necesita de la compilación de programas para probarlo, mediante las "n" cantidad de líneas codificadas que emite JAVA, es lo que permita la formación un script

URL: Localizador uniforme de recursos[5].representa la dirección de internet en la cual los sitios web organizan la información que se encuentran en los portales de internet, por lo cual permite manejar recursos identificados a través de la plataforma digital, y facilitar la localización de la información

---

[1] ESCOBAR, Frank Sistema de Prevención de intrusos [en línea]. Publicación de articulo en blog del informatico. 2015 [consultado 10 mayo 2020]. Disponible en http://franyagami28.wixsite.com/blog-del-informatico/single-post/2015/09/13/Sistema-de-Prevenci%C3%B3n-de-Intrusos-IPS

[2] JAIMES, Alonso. Web site as a basic device for information and communication. Theoretic approach: definition and essential elements [en línea]. Revista científica de información y comunicación Tesis de Maestría. 2008 [consultado 10 mayo 2020]. Disponible en http://institucional.us.es/revistas/comunicacion/5/07alonso.pdf

[3] CASTRAÑON DELGADO, Ernesto. Sistemas de control de acceso alternativo a passwords.[en línea]. Trabajo especial de grado 2012 [consultado 10 mayo 2020]. Disponible en http:// oa.upm.es>PFC_ERNESTO…PDF Sistemas de control de acceso alternativos a passwords-Archivo DIGITAL UPM-Universidad…

[4] EGUILUZ PEREZ, Javier Introduccion a JavaScript [en línea]. Publicación de investigación 2008 [consultado 10 mayo 2020]. Disponible en http:// www.google.com/url?sa=t&source=web&rct=j&url=http://www.librosweb.es/javascript

[5] ZAMORA LUCIO, Marco Antonio. Internet [en línea]. Publicación técnica 2014 [consultado 10 mayo 2020]. Disponible en http:// www.google.com/url?sa=t&source=web&rct=j&url=http://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/Presentaciones_Enero_Junio_2014/Definiciones%2520de%2520Internet.pdf&ved=2ahUKEwiG0ufc5NnqAhUgMUakhtr6c0iqfJaJegQICRA&usg=A0vVaw1pVGTHeu8s1CJjl8A-eo8X

VPN: Redes virtuales privadas: [6].corresponde a la privacidad que existe entre el emisor y receptor cuanto establece una línea de comunicación, a través de un medio inseguro.

[6] FERNANDEZ HERNANDEZ, Jesús; ALONSO, BERROCAL, Jose, FIGUEROLA PANIAGUA, Carlos, ZAZO RODRIGUEZ, Angel, Redes ptivadas virtuales [en línea]. Informe técnico 2006 [consultado 10 mayo 2020]. Disponible en http:// www.google.com/url?sa=t&source=web&rct=j&url=http://eprintd.rclis.org/13992/1/fernandez2006redes.pdf&ved=2ahKEwiDt7KS4tnqAhXqguAKHaZzDoQQFjACegQIBRAB&usg=AOvVaw1rGSF7hFLCan6IBMbrWkon

RESUMEN

La presente monografía tiene como finalidad determinar los riesgos en la seguridad informática de las organizaciones en modalidad de teletrabajo, los cuales son de carácter imperativo para consolidar las bases sobre las que se cierne la seguridad y activos de las empresas, especialmente durante la nueva Era de globalización informática que se ha ido introduciendo producto de la pandemia mundial por el virus del COVID-19. A partir de ello, se desglosan los objetivos que facilitarán los medios para proponer un manual de procedimientos para la implementación de un sistema de ciberseguridad basado en la confiabilidad de programas específicos para gestión y actualización de bases informáticas de uso privado. De acuerdo con lo anterior, se presentan, además, las bases teóricas que sustentarán las fuentes de información sobre el tema y, la importancia de este dentro del marco social y productivo. Para estos efectos, la investigación se justifica desde la perspectiva teórica, práctica y metodológica. En función de esto, se procederá a presentar el apartado con los resultados de la monografía, en la cual se espera cumplir con el objetivo general de la misma, en beneficio de la comunidad científica y los involucrados del tema.

Palabras claves: ciberseguridad, informática, sistema, teletrabajo.

ABSTRACT

The purpose of this proposal for a monograph is to identify the risks to the IT security of organizations in the form of teleworking, which are imperative for consolidating the foundations of corporate security and assets, especially during the new era of IT globalization that has been introduced because of the world pandemic by the COVID-19 virus. On this basis, the objectives that will provide the means to propose a manual of procedures for the implementation of a cybersecurity system based on the reliability of specific programs for the management and updating of computer bases for private use are broken down. In accordance with the above, the theoretical bases that will support the sources of information on the subject are also presented, as well as its importance within the social and productive framework. For these purposes, the research is justified from the theoretical, practical, and methodological perspective. Finally, the chronogram projected for the elaboration of the monograph during the period of seven months is established, complying with the minimum guidelines required to fully comply with the general objective proposed. Based on this, the section with the results of the monograph will be presented, in which it is expected to comply with the general objective of the monograph, for the benefit of the scientific community and those involved in the subject.

Keywords: cybersecurity, computing, system, telecommuting.

INTRODUCCIÓN

La ciberseguridad, se ha convertido en un verdadero desafío, teniendo en cuenta que, así como evoluciona la seguridad informática, aumentan los ataques por parte de la ciberdelincuencia, lo que torna complejo generar medidas de protección y la modalidad de teletrabajo no es la excepción. Es más, podría decirse que puede generar más vulnerabilidad en la protección de la información, debido a que si bien, las empresas tienen conocimiento sobre la modalidad del teletrabajo, en cierta forma desconocen su aplicación debido a que no han visto la necesidad de darle aplicación, por los aparentes costos que puedan generar y tornarse engorrosa su implementación, al migrar el trabajo y los procesos fuera de la empresa.

Lo anterior representa una de las mayores preocupaciones en el área de informática, por la complejidad de garantizar la confidencialidad de la información y sus procesos que las empresas ofrecen a sus clientes, inclusive si esa información no es confidencial, pero en algún orden es valiosa para la empresa.

Esto motiva la necesidad de llevar a cabo una evaluación de los riesgos que se pueden presentar en el área de informática, cuando los procesos y la información migran a la casa de los empleados de una organización, donde en la mayoría de las ocasiones se carece tan siquiera de medidas mínimas de seguridad.

Actualmente, debido a la pandemia del COVID-19, muchas compañías se ven en la necesidad de implementar la modalidad de teletrabajo, lo cual implica no solo la vulnerabilidad de la información sino también de los bienes de la empresa, ya que deben movilizar equipos informáticos como CPU y UPS. De otro lado, hay empresas que pretenden implementar la modalidad de teletrabajo, debido a la emergencia presentada, pero no cuentan con la capacidad de movilización y la logística necesaria para afrontar este tipo de eventos y por tanto sus trabajadores que en un gran colectivo no poseen conocimientos de seguridad informática deben hacer uso de sus propios equipos en casa, lo que afecta de manera importante la salvaguarda de la información, pues en la mayoría de casos, estos equipos no cuentan con la más mínima seguridad en cuanto a software, cortafuegos, etc., dejando la información expuesta a cualquier ataque.

Dando alcance a lo anteriormente dicho, este escrito tiene como base el análisis de aquellos riesgos que ponen en peligro la información de una empresa y así mismo, proponer medidas que puedan legitimar la información, integridad y salvaguarda de la misma, sin afectar la misión de las empresas en el mercado.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad, la ciberseguridad es un aspecto sumamente relevante para pequeñas y grandes empresas a nivel mundial[7], la ciberseguridad se basa en prevenir ataques o accidentes que causen filtración o alteración de la información confidencial o no, motivado a que de acuerdo con el nivel de encriptación y firewalls que ésta posea [8], se garantizará la confidencialidad de sus bases de datos y activos informáticos de carácter vulnerable[9]. Al respecto, Díaz *et al.*[10] mencionan que las tecnologías de la información y la comunicación (TIC) están presentes en todos los ámbitos de la vida diaria. Entre otras cosas, los precios cada vez más asequibles de los dispositivos de conexión a Internet han permitido su uso generalizado y se han convertido en un accesorio ineludible en la vida de las personas y las empresas[11].

Al igual que los múltiples beneficios que traen consigo las TIC, también han representado un peligro para las bases de datos en cuanto a seguridad para las

[7] Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario [Fecha de consulta: 17 septiembre 2020]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_ceseden_137.pdf

[8] Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [Fecha de consulta: 17 septiembre 2020]. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[9] CASTRO MARQUEZ, Deisy. Modelo de Integración de Estándares de Buenas Prácticas de Tecnologías de La Información En El Gobierno Coporativo de Las Empresas Colombianas En El Sector Asegurador [en línea]. Tesis de Maestría. Universidad Francisco de Paula Santander Ocaña, 2020 [consultado 10 mayo 2020]. Disponible en http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/2761?mode=full&submit_simple=Show+full+item+record

[10] Investigación En Ciberseguridad: Un Enfoque Integrado Para La Formación de Recursos de Alto Grado de Especialización [en línea]. La Plata: XX Workshop de Investigadores en Ciencias de la Computación, 2018. [Fecha de consulta: 10 mayo 2020]. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/68355/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

[11] VIERA, Rosa. Propuesta de Mejora Del Nivel de Gestión Del Proceso de Adquirir e Implementar Las Tecnologías de Información y Comunicaciones (TIC) En El Gobierno Regional de La Provincia de Piura [en línea]. Tesis de pregrado. Universidad Católica de los Ángeles de Chimbote, 2017 [consultado 10 mayo 2020]. Disponible en http://repositorio.uladech.edu.pe/handle/123456789/305

empresas, ocasionando millonarias pérdidas en el mundo[12]. Krutz y Vines[13] confirman que la seguridad de la información se da cuando se garantizan los principios fundamentales como confidencialidad, integridad y disponibilidad al igual que se garantice el no repudio, autenticidad y trazabilidad de la misma en cada proceso involucrado. Otros autores como Martínez[14] y Oltra e Ibáñez[15] destacan que estos principios son vulnerados cuando se produce un ciberataque, cuyo objeto es el ataque premeditado por un individuo o grupo hacia los sistemas informáticos para destruir medios electrónicos o para obtener un beneficio económico por extorsión.

En la actualidad, la confidencialidad del teletrabajo se está viendo afectada, ya que a pesar de que países como Tokio se estaban preparando para dicha modalidad con motivo de los Juegos Olímpicos 2020, para muchas otras empresas no era ni siquiera una opción. Debido a la pandemia por la que atraviesa actualmente el mundo, muchas empresas se han visto en la necesidad de cambiar su modalidad de trabajo bruscamente, afectando así la seguridad de la información.

En ese sentido, ha surgido la necesidad imperativa de las empresas por proveer una seguridad a sus activos informáticos a través de la implementación de sistemas de gestión informáticos dentro de sus instalaciones que incluyen protocolos ante los ciberataques[16], lo cual ha resultado beneficioso en cierto grado, dependiendo del nivel de seguridad que éste posea[17]. En el caso de Colombia, se data que, en el año 2017, el 30% de las empresas reportaron haber sido víctimas de ciberataques,

[12] Ciberseguridad y Ethical Hacking: La Importancia de Proteger Los Datos Del Usuario [en línea]. Cartagena de Indias: Revista de 2º congreso Latinoamericano de Ingeniería, 2019. [Fecha de consulta: 10 mayo 2020]. Disponible en: https://acofipapers.org/index.php/eiei2019/2019/paper/viewFile/3634/1221

[13] KRUTZ,R y VINES, R. The CISSP Prep Guide: Gold Edition, citado por SANTIAGO, Enrique y SÁNCHEZ ALLENDE, Jesús. Riesgos de Ciberseguridad En Las Empresas. *Revista de Tecnología y Ciencia*. 2017, vol. 15, no. 1, pp. 1-33. ISSN 1696-8085

[14] MARTÍNEZ LANDROVE, Noelia. Ciberseguridad y Riesgo Operacional En Las Organizaciones [en línea]. Tesis de maestría. ICADE School Business, 2019 [consultado 10 mayo 2020]. Disponible en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/42317/TFM001173.pdf?sequence=1&isAllowed=y

[15] OLTRA-GUTIÉRREZ, Juan e IBÁÑEZ-HERNÁNDEZ, Rafael. Ciberseguridad y Bibliotecas: Apuntes Para Una Propuesta de Formación Sobre Riesgo Tecnológico En Bibliotecas. *Revista de Métodos de Información*. 2019, vol. 10, no.19, pp. 75-126

[16] ANGARITA PINZÓN, Cristian y GUZMÁN FLÓREZ, Camilo. Protocolos de Mitigación de Ciberataques En El Hogar. Caso de Estudio: Estratos 3 y 4 de La Ciudad de Bogotá [en línea]. Proyecto de Trabajo de Grado. Universidad Católica de Colombia, 2017 [consultado 10 mayo 2020]. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf

[17] FREIRE FAJARDO, Franklin. Plan de Contingencia Ante Ciberataques [en línea]. Tesis de Maestría. Escuela Superior Politécnica del Litoral, 2017 [consultado 11 mayo 2020]. Disponible en https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf

mayormente por desactualizaciones en sus paquetes de información[18]. Lo que representa un porcentaje considerable que a la fecha se sigue intentando reducir a raíz de la evolución de las nuevas tecnologías y la incorporación de nuevos mecanismos[19]. La ley 1221 del año 2008, es la que gobierna el teletrabajo en Colombia y hace precisión en tres clases que son "autónomos" quienes trabajan en su casa, "dispositivos móviles" no tienen sitio fijo para su trabajo, sino que utilizan terminales inalámbricos y por último "suplementarios" que son quienes alternan su trabajo entre casa y lugar fijo de trabajo.

Con base en lo anterior, se puede afirmar que esta es una modalidad muy nueva en el mercado laboral colombiano pero que cuenta con respaldo del Gobierno Nacional, y Ministerio del Trabajo y de las TIC's, donde empresas del sector público y privado ya han dado pasos para entrar en ella desarrollando oportunidades para generar fuentes de empleo en el país.

Continuando con la seguridad cibernética, González[20], precisa que el ciberriesgo estará siempre presente cada vez el ser humano se sumerge más a un ecosistema cibernético, donde se almacenan datos sustancialmente atractivos para los ciberatacantes del mundo. En ese sentido, dada la situación actual vivida a nivel mundial con respecto a la pandemia denominada COVID-19, el proceso de inmersión tecnológica se ha acelerado de manera exponencial[21], obligando a todos los trabajadores a practicar el teletrabajo y vulnerar la seguridad de sus datos por medio de conexiones domésticas con protocolos de seguridad extremadamente bajos[22], lo cual representa un riesgo latente para las empresas que se mantienen en la vanguardia y buscan rescatar la economía de sus países[23].

A pesar de que muchas empresas siguen rigurosos protocolos de seguridad cibernética como uso de VPN, filtros o restricciones es importante tener en cuenta

---

[18] ORDUZ BARRERA, Diana. Análisis de Emergencias Cibernéticas Que Se Presentan En Las Ciudades de Tunja, Duitama y Sogamoso Con Respecto Al Respecto Del País En Los Últimos Dos Años [en línea]. Monografía de posgrado. Universidad Nacional Abierta y a Distancia, 2019 [consultado 11 mayo 2020]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31410/dmorduzb.pdf?sequence=1&isAllowed=y

[19] Ciberseguridad y Ethical Hacking: La Importancia de Proteger Los Datos Del Usuario [en línea]. Cartagena de Indias: Revista de 2º congreso Latinoamericano de Ingeniería, 2019. [Fecha de consulta: 11 mayo 2020]. Disponible en: https://acofipapers.org/index.php/eiei2019/2019/paper/viewFile/3634/1221

[20] GONZÁLEZ DÍAZ, Joshsua. Ciberriesgo Desde La Perspectiva de Riesgo Sistémico. *Revista de Sistemas*. 2019, no. 151, pp. 1-11. ISSN 0120-5919

[21] PINHEIRO BEZERRA, Italla. State of the Art of Nursing Education and the Challenges to Use Remote Technologies in the Time of Coronavirus Pandemic. *J Hum Growth Dev (JHGD)*. 2020, vol. 30, no.1, pp. 141-147

[22] BALLESTERO, Fernando. La Ciberseguridad En Tiempos Difíciles. *Boletín Económico de ICE*. 2020, no. 3122, pp. 39-48. ISSN 0214-8307

[23] AMRITA, M y AKHILESH, K Operations Management of Cyber-Physical Production Systems. En: Akhilesh K., Möller D. Singapur: Smart Technologies, 2020. p. 137-145.

que al final todo se puede ver vulnerado por las capacidades del empleado.

Es necesario mencionar que hay empresas que implementan esta modalidad como actividad principal y para la fecha en que inicio la pandemia ya estaban preparados con protocolos y procesos para evitar las vulnerabilidad de sus sistemas, sin embargo la seguridad de la información se puede ver afectada por la utilización que le dé el usuario, producto de la poca experiencia informática, y pueden compartir, divulgar y descargar información vulnerando los protocolos sin generar alarmas a los equipos de seguridad organizacionales.

Un estudio de la Federación Colombiana de Gestión Humana reveló que una de cada dos empresas en Colombia no contaba con políticas o esquemas de trabajo remoto antes de la pandemia. A pesar de que las características positivas, como ahorro económico y disminución de ausentismo laboral, este estudio se enfoca en cómo se ve afectado la seguridad cibernética por la falta de protocolos y la rapidez de la implementación del teletrabajo.

La problemática se concentra en que la modalidad del teletrabajo impuesta por las empresas a consecuencia de contingencia del COVID-19, lo cual coloca en riesgo y vulnerabilidad de la seguridad informática del sector empresarial en implementar la modalidad del trabajo a distancia con sus colaboradores con la finalidad de seguir operando sin ningún protocolo de seguridad al establecerse conexiones domesticas carentes de estándares de seguridad en prevenir ciberataques afectando el desempeño de las empresas y su permanencia.

Dado lo anterior expuesto, el presente estudio plantea como problemática actual, identificar los riesgos existentes en la seguridad de la información, relacionadas con las nuevas modalidades de trabajo remoto o teletrabajo, “los cuales no se encuentran sustentado bajo ningún protocolo de seguridad” [24]., dado que al establecer conexiones domésticas, estas conexiones se pueden encontrar en un estado vulnerable a ciberataques, generando una posible exposición de la información confidencial del usuario o de la empresa.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué riesgos existen en las conexiones de teletrabajo y cuál es el mejor plan para evitar que estos puedan comprometer los activos de las organizaciones?

[24] LOPEZ ZUÑIGA, Vicente Redes de transmision de datos. [en línea]. Tesis de pregrado, Universidad Autónoma del Estado de Hidalgo, 2005 [consultado 10 mayo 2020]. Disponible en https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/redes%20de%20transmision%20de%20datos.pdf

2 JUSTIFICACIÓN

Se conoce que la seguridad informática es un aspecto fundamental en el blindaje de datos y activos informáticos de cualquier organización, por lo que su protección se convierte de carácter imperativo y fundamental ante posibles ciberataques, al igual que el estudio de todos los riesgos actuales latentes que puedan generar una brecha en las barreras o «*firewalls*» de los protocolos de seguridad ya establecidos. Principalmente, el enfoque de este estudio se justifica en el reforzamiento de los sistemas de información existentes para brindar una guía práctica para aquellas pequeñas o medianas empresas que aún no posean la asesoría sobre cómo proteger sus datos personales y los de los involucrados en el proceso.

Asimismo, el investigador pondrá en función los conocimientos adquiridos a lo largo de la carrera y en pro de la investigación científica para brindar un aporte sustentable a la comunidad en materia de seguridad de la información con respecto a la nueva Era virtual que comprende el teletrabajo como un mecanismo de crecimiento profesional y económico durante el estado de emergencia actualmente en transcurso por la pandemia desencadenada por el virus del COVID-19. A través de la misma, se procura aplicar las prácticas para crear nuevas políticas de seguridad y uso de redes, así como asignar responsables de procesos y, posteriormente, concientizar y capacitar a los profesionales del área sobre la seguridad informática.

Como resultado de esta monografía, además, se pretende, describir las nuevas técnicas y/o herramientas disponibles en el mercado para uso y protección de la información de las organizaciones, por medio de un análisis de los beneficios ofrecidos por cada uno, así como destacar sus puntos débiles u oportunidades de mejora con respecto al rendimiento de estas. Finalmente, sugerir la más adecuada a emplear con base en una serie de criterios establecidos como costos, nivel de protección brindado e interfaz de usuario.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Determinar los riesgos y el plan estratégico en la seguridad de la información del teletrabajo en las organizaciones.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar los factores de riesgos informáticos en las organizaciones asociados al teletrabajo en la actualidad.

- Analizar las herramientas y técnicas disponibles para la seguridad de la información asociado al teletrabajo.

- Elaborar la matriz de responsabilidades de perfiles de seguridad de la información en las organizaciones asociadas al teletrabajo.

- Establecer el plan estratégico de seguridad de la información en las organizaciones asociada al teletrabajo.

4. MARCO CONCEPTUAL

4.1. ESTADO DEL ARTE

Tejena-Macías[25], en su artículo científico titulado “Análisis de riesgos en seguridad de la información”, aborda la generación de argumentos sustentables que permiten la identificación de la metodología adecuada para el análisis de riesgos y permite mejores tomas de decisiones gerenciales de la organización de estudio en materia de seguridad de la información. La metodología empleada incluyó OCTAVE, MEHARI, MARGERIT, CRAMM, EBIOS y NIST SP 800-30, las cuales comparten el mismo objetivo, pero representan características atractivas para las empresas de acuerdo con ciertos criterios. Por lo cual, se consideró que MARGERIT resulta efectiva en cuanto a integridad, confidencialidad, disponibilidad y otras características que garantizaban la seguridad de la información a nivel organizacional. En base al antecedente señalado anteriormente, se consideró y se evaluó como una referencia la metodología: OCTAVE, MEHARI, MARGERIT, CRAMM, EBIOS y NIST SP 800-30 para este proyecto, en cuanto al análisis de riesgos asociado al teletrabajo, sin embargo, para llevar a cabo el análisis de riesgos, se debían considera 2 factores importantes: la falta de administración del riesgo residual y el costo que implicaba la licencia del software

Alemán y Rodríguez [26], en la publicación señalada como “Metodología para el análisis de riesgos en los SGSi”, el cual, a través de la identificación, el análisis y el manejo de riesgos en toda la organización, la emisión de oportunidades y amenazas para lograr sus objetivos comerciales y oportunidades de administración, como el objetivo principal de mantener la seguridad del sistema informático en la actualidad. activo. Esta investigación describe las metodologías de análisis de riesgos más relevantes bajo las metodologías Octave, Magerit, Mehari, NIST SP 800: 30, Coras, Cramm y Ebios aplicadas en el campo de la seguridad informática, por lo cual llevará a que la empresa contrarreste la situación actual, mediante los riesgos y amenazas identificadas, mediante implementación del mecanismo de seguridad, y la integración del sistema de gestión de seguridad informática del SGSI, resultando de este estudio la minimización de los riesgos y definición de herramientas para llevar a cabo el análisis de los riesgos. Este estudio permitió tomar de referencia algunas de las herramientas necesarias para la protección de datos y la seguridad de la información

[25] TEJENA-MACÍAS, Mayra. Análisis de Riesgos En Seguridad de La Información. *Revista de ciencias de la computación*.2018, vol. 3, no. 4, pp. 230-244. ISSN: 2550-682X

[26] ALEMÁN NOVOA, Helena y RODRIGUEZ BARRERA, Claudia Metodologías para el análisis de riesgos en los SGSi. Publicación de investigación. 2015. Fundación universitarias Juan de Castellanos. Facultad de ingeniería. Boyacá, Colombia.

guilar [27], en el trabajo de grado denominado “Modelo de seguridad de la información para instituciones de educación superior”, el cual comprende el diseño de un modelo de seguridad de la información aplicable a las instituciones superiores mediante la caracterización de los procesos existentes, la comparación con las buenas prácticas de seguridad de la información existente, lo que permite estructurar los elementos que conforman el modelo de seguridad de la información teniendo como referentes Balance Sore Card, COBIT 5.9, ISO 27002:2015, con el propósito de permitir control efectivo en los procesos con el modelo de seguridad de la información, lo cual permitirá identificar las fortalezas y debilidades de los procesos de seguridad. Se concluyó que los objetivos empresariales, los 2 procesos de COBIT 5.0 se encuentran asociados con la seguridad de la información, pero resulta necesario incorporar las metas de TI y las métricas relacionadas, y se logró de determinar la viabilidad del modelo de seguridad de la información para la institución de Educación Superior teniendo como referente el método Delphi. El aporte de este estudio a la investigación se relacionada con la referencia en cuanto al análisis de riesgos considerando la evaluación del riesgo e impacto del riesgo.

Fonseca[28] en el trabajo de grado titulado: “Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS”, la intención es proponer un modelo de gestión de seguridad de la información adecuado para cualquier organización, que sea consistente con el estándar NTC-ISO-IEC 27001: 2013 y les permita comprender su estado actual relativo. Seguridad de la información e implementar los controles, procedimientos y estrategias necesarios de manera sistemática y efectiva para mantener la rectitud, privacidad y la integridad de los activos de información de la empresa Geoconsult CS. Obteniendo como resultado la importancia de la implementación del modelo a la organización Geoconsult CS, lo cual permitirá comprender y analizar el estado actual de la organización, en función de las normativas de la organización que se implementan para lograr operar correctamente, captar al RRHH especializado y obtener la estructura de seguridad, y. Por lo cual este estudio, tiene como aporte la información correspondiente a la autenticación del sistema de la seguridad de la información, en función de contrarrestar algunos de los factores relacionado a los actos maliciosos.

Parra [29], en el ensayo titulado: “Gestión del riesgo en la seguridad informática: “cultura de la auto-seguridad informática”, comprende la definición de forma genérica y sencilla la seguridad informática, y posteriormente comparar la definición

[27] AGUILAR QUINTERO, Norly Alejandra. Modelo de seguridad de la información para instituciones de educación superior. Proyecto de maestría 2019.Universidad Francisco de Paula Santander Ocaña. Facultad de ingeniería. Ocaña, Colombia.

[28] FONSECA HERRERA, Omar Andrés . Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS. Tesis de pregrado. 2019. EAN Universidad. Facultad de estudios ambientales. Bogotá, Colombia

[29] PARRA MORENO, Duver Augusto Gestión del riesgo en la seguridad informática: "cultura de la auto-seguridad informática". Ensayo de pregrado. 2012. Universidad militar de Nueva Granada. Bogotá

genérica con la definición de distintos autores, mediante la determinación de los orígenes de la sociedad de la información, gestión de riesgo en la seguridad informática, cultura de seguridad informática, auto-seguridad informática. La conclusión que se han efectuado varios cambios para lograr en la empresa las nuevas exigencias que requiere la gestión de riesgo de la seguridad informática y garantizar la confidencialidad, la integridad y la disponibilidad de la información para evitar la usurpación de identidad, uso inapropiado de datos o venta de información confidencial. Este ensayo se encuentra vinculada con las responsabilidades y roles que debe desarrollar el equipo de seguridad de información, desde la alta dirección, hasta el personal administrativo de los sistemas de control, dado que el personal en general debe cooperar para que la organización pueda proteger los datos de clientes, colaboradores y de la empresa.

Ríos [30], en el proyecto denominado "Técnicas herramientas de análisis de vulnerabilidad de una red", aborda el conjunto de herramientas disponibles para el análisis y explotación de vulnerabilidades en sistemas informáticos y redes de ordenadores, por lo cual se analizó el conjunto de herramientas de software libre actuales, de acuerdo al funcionamiento, opciones, motivación de uso de las herramientas: taxonomía de vulnerabilidades de un sistema informático, superficie de ataque, vectores de ataque, hacking ético, y metasploit framework, así mismo, se evaluó el comportamiento y se llevó a cabo el discernimiento los datos útiles para obtener información acerca de la vulnerabilidad existente en el sistema. Obteniendo como resultado, que el análisis y detención de vulnerabilidades por parte de un administrador de sistema competente que permite ofrecer a la organización un conjunto de técnicas para mejorar el sistema informático y evitar problemas futuros. El proyecto anteriormente descrito, proporciona técnicas para la estimación de los riesgos durante el análisis de los riesgos asociados al teletrabajo.

Rodríguez y Jiménez[31], en el estudio titulado "Mejoramiento de las buenas prácticas de seguridad informática en el teletrabajo a través de una herramienta web", acoge las mejores destrezas en la salvaguarda de los sistemas informáticos en las organizaciones dedicadas a la telecomunicación con la finalidad de implementar actividades laborales mediante una plataforma digital, en la que se desarrollan trabajos en forma remota y ofrecen información actual de las sistemas de protección de datos bancarios, lo que permite a las compañías un mayor nivel de exigencia en cuanto a los perfile laborales, dado que deben promover la integridad, la seguridad de la información y confidencialidad. Al administrar los datos digitales de BIBLORED y los métodos utilizados para procesar los datos a través de encuestas, la atención se centra en evaluar las estrategias de seguridad, la importancia de proteger la

[30] RÍOS YÁNEZ, Javier. Técnicas herramientas de análisis de vulnerabilidad de una red. Tesis de pregrado. 2014. Escuela técnica superior de ingeniería y sistemas de telecomunicaciones. Madrid, España.

[31] RODRÍQUEZ, Roger y JIMÉNEZ, Ingrid. Mejoramiento de las buenas prácticas de seguridad informática en el teletrabajo a través de una herramienta web. Tesis de postgrado. 2013. Universidad Piloto de Colombia. Bogotá

información, las buenas prácticas en el trabajo y la implementación de modelos de trabajo. Los resultados de la información se midieron en el diseño de la herramienta prototipo, que permite que los trabajadores remotos y las buenas prácticas se utilicen como herramientas para evaluar el conocimiento sobre el tema. El aporte de este estudio se encuentra vinculado con el desarrollo de la matriz de responsabilidades de perfiles de seguridad de la información en función del modelo de trabajo asociado al teletrabajo.

Abalco y Ruilova [32], en la publicación denominada: "Elaboración del plan de seguridad de la información para el fondo de cesantía y jubilación del MDMQ.", el cual contempla la caracterización de la empresa y describe las problemáticas del estado actual en cuanto a la seguridad de la información, así mismo, evalúa los riesgos mediante varias metodologías (OCTAVE, RISK, IT, NIST 800-30 y MAGERIT), en este caso la metodologías utilizada ha sido MAGERIT, mediante la validación del plan de seguridad de la información mediante la implementación de una política dentro del fondo de desempleo y jubilación para desarrollar un plan, mediante la comparación en cuanto al porcentaje de cumplimiento actual con la implementación del plan de seguridad de la información y también considera el porcentaje de cumplimiento para cada dominio de ISO 27001 dentro de la organización. La conclusión muestra que los fondos de desempleo y jubilación necesitan en la actualidad estrategias para salvaguardar las bases de datos, por ello se han detectado una sucesión de vacíos en cuanto a la lógica y la estructuración de técnicas protección de las bases de datos, dependiendo exclusivamente de las restricciones de tiempo. Con respecto a la información detallada anteriormente se contempló hacer uso de la metodología OCTAVE, MEHARI, MARGERIT, CRAMM, EBIOS y NIST SP 800-30 para la ejecución del análisis de riesgos, pero se debía considerar 2 factores importantes: nivel de salvaguardo y la estructuración de las bases de datos

Hernández y Naranjo[33], en su trabajo titulado "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial", abarca el procedimiento teórico – práctico a través del cual se debe gestionar la seguridad de la información en una empresa del sector comercial. Para estos efectos, la investigación se clasificó como descriptiva, en la cual se persiguió el objetivo de la implantación de normas, procedimientos y estándares informáticos para crear una cultura de seguridad óptima. El procesamiento de datos consistió en la evaluación de riesgos, las políticas de seguridad y el plan de seguridad informática. En las conclusiones se destaca la importancia de las herramientas tecnológicas bajo un asesoramiento adecuado para el alcance de los objetivos, así como el incremento

[32] HERNÁNDEZ, María y NARANJO, Bertha. Diseño de Un Plan Estratégico de Seguridad de Información En Una Empresa Del Sector Comercial [en línea]. 2016.Tesis de pregrado. [consultado 15 junio 2020]. *Disponible en* https://core.ac.uk/download/pdf/12401003.pdf

[33] HERNÁNDEZ, María y NARANJO, Bertha. Diseño de Un Plan Estratégico de Seguridad de Información En Una Empresa Del Sector Comercial [en línea]. 2016.Tesis de pregrado. [consultado 15 junio 2020]. *Disponible en* https://core.ac.uk/download/pdf/12401003.pdf

de la rentabilidad de la empresa a raíz de la implementación de estas políticas de seguridad. Este estudio proporciona aportes en cuanto al último objetivo de esta investigación, en referencia a la estructura que debe conservar el plan estratégico de seguridad de la información asociado al teletrabajo.

Cajusol [34], el trabajo de grado reconocido como: "Diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013 para la comercialización de productos de consumo masivo", busca definir la directiva de seguridad conforme a los procesos y requerimientos de la organización, mediante la realización de un análisis diferencial de acuerdo a los dominios y objetivos de control de la norma ISO/IEC 27001:2013, la declaración de aplicabilidad (SoA), para determinar los controles a la empresa de acuerdo a los recursos y procesos, y determinar si el personal posee conocimientos de la información y controles existentes. En las conclusiones se enfatiza que el 31% de los activos de información tienen un nivel de riesgo crítico, lo que induce que existe un alto déficit de implementación de directivas en aseguramiento en la empresa y de los 46 controles, 13 ya se están implementado en la empresa de acuerdo a la Declaración de Aplicabilidad (SoA). El principal aporte del estudio previamente señalado, se ubica en la detención de la norma ISO/IEC 27001:2013, la cual proporciona la referencia y requerimientos necesarios para el cumplir con el objetivo 1 relacionado al análisis de los riesgos y la evaluación total del índice de riesgos en la seguridad de la información asociado al teletrabajo y lo relaciona con la elaboración de la matriz de perfile de responsabilidades de la seguridad de la información.

Guzmán [35] en la investigación titulada "Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega" En este estudio, se analizaron diferentes métodos contra estos estándares para proponer un método para implementar, administrar y mejorar la seguridad de las tecnologías de información y comunicación en la clínica Ortega. También propone diferentes opciones estratégicas y discute su aplicabilidad o no, discute varios métodos conocidos de análisis y gestión de riesgos, y propone un método que se adapte a sus requisitos, tratando de aprovechar cada método de análisis Por la integración. Contiene recomendaciones en el organigrama de seguridad, que hace que la jerarquía estructural del grupo sea compatible con los requisitos de seguridad de la tecnología de la información y la comunicación. Las conclusiones extraídas se centran en la detección de amenazas a los activos de información y los requisitos de seguridad propuestos, que pueden definir el alcance del modelo, su estructura y la metodología de seguridad de la tecnología de información y comunicación involucrada en el modelo. Requiere la implementación de medidas de control de

[34] CAJUSOL TORRES, Lieth del Carmen, Diseño de un sistema de gestion de seguridad de información basado en la norma ISO/IEC 27001:2013 para la producción y comercialización de comsumo masivo. 2020 Tesis de pregrado. Lima. Perú.

[35] GUZMÁN PACHECO, Goyo Francisco . Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega. Tesis de postgrado 2015. Universidad Nacional del Centro de Perú

seguridad para monitorear, revisar y mantener el sistema y la información. El aporte de esta investigación se centra en el desarrollo del planteamiento del problema dado que el teletrabajo en la actualidad, dado la pandemia del COVID-19, resulta una de las estrategias más utilizadas para ejecutar actividades laborales, sin embargo, requiere de una identificación de riesgos previas y contar con las herramientas disponibles para desarrollar el teletrabajo de manera segura y disminuyendo las amenazas a los cuales se encuentra expuesto el sistema.

Narbona y Jiménez [36] en el estudio catalogado “El rol y la responsabilidad de la gestión de la tecnología de la información "enfatiza los servicios de gestión proporcionados a través de oficinas virtuales. Algunas personas tienen la infraestructura y los procesos para soportar estos servicios. Sin embargo, las personas no entienden sus roles, la infraestructura no está controlada y los procesos no están definidos. A partir del análisis del proceso, podemos encontrar cambios organizativos en la organización y los recursos humanos. Si queremos garantizar la seguridad y la calidad de los servicios de gestión electrónica, debemos resolverlos a través de recomendaciones basadas en la estructura organizativa de los recursos humanos de TI. El proceso de definir las funciones de TI es principalmente utilizar La definición de procesos, roles y responsabilidades propuestas por COBIT e ITIL. La conclusión determina la necesidad del marco de estructura organizacional del centro de TI del gobierno andaluz.” Este articulo proporcionó nociones e información acerca de algunos roles y responsabilidades (características), que se deben establecer para determinar la matriz de perfiles de responsabilidad de la seguridad de la información en las organizaciones asociadas al teletrabajo.

González, Gascó y Llopis[37], en el artículo científico denominado “Razones y riesgos del outsourcing de sistemas de información en las grandes empresas españolas” con el objetivo de identificar los principales riesgos a los cuales se encuentran expuestas las empresas y usuarios en el uso de los sistemas de información. La investigación propone una lista de razones y riesgos en función de datos, obtenido anteriormente de la aplicación de una encuesta replicada por 2da vez, y mediante el tratamiento de los datos por medio de un análisis longitudinal, el cual trazó la tendencia y evaluó la continuidad de las variables relacionadas con la seguridad de la información, obteniendo con resultado la clasificación de la empresa en 3 grupos empresas con outsourcing estratégico (preocupado por los proveedores), empresas con outsourcing económico-tecnológico (preocupado por sus capacidades) y las empresas indiferentes ante el outsourcing. El aporte de esta investigación se basa en suministrar una metodología para el desarrollo del análisis de los riesgos en la organización asociada al teletrabajo.

---

[36] NARBONA SARRIA, Manuel y JIMÉNEZ LOMA, Zenobia. Roles y responsabilidades para la gestión de las tecnologias de la información. Publicación. 2007 Dirección General de sistema de información económico-financiero. Consejería de economía y hacienda.

[37] GONZÁLEZ RAMIREZ, M. Reyes, GASCÓ GASCÓ, José Luis y LLOPIS TAVERNER, Juan. Razones y riesgos del outsourcing de sistemas de información en las grandes empresas españolas. Artículo. *Revista ELSERVIER*. 2015, vol. 1, no. 1, pp. 176-189. ISSN 1019-6838

Muñoz [38], en la investigación titulada “Diseño de un plan estratégico para la seguridad de la información de Cias & Profesionales S.A.S.”, este proyecto se realizó mediante la revisión de la infraestructura tecnológica, y evaluación del riesgo por medio de la metodología MAGERIT, mediante el análisis y políticas de seguridad, lo cual permitirá lograr garantizar la integridad, coherencia, confiabilidad y disponibilidad de la información de la investigación. Las conclusiones indican que el factor humano representa el mayor riesgo de seguridad dado que se detectó los riesgos de seguridad de información actuales de la empresa, entre lo cual se destaca que los funcionarios no hacen uso de las buenas prácticas, existe un incumplimiento de las políticas de seguridad de información de la empresa, no existen medidas correctivas para disminuir el riesgo y no se gestiona la implementación de normas relacionadas con la seguridad de la información y los recursos informáticos. El aporte principal del estudio mencionado, se basa en las políticas de seguridad de información y el desarrollo de las herramienta y técnicas disponibles para seguridad de la información en las organizaciones, dado que representa un factor que se puede representar una amenaza a los sistemas informáticos.

González[39], en su artículo científico titulado “Diseño de un plan estratégico de seguridad de la información, mediante la aplicación de análisis de riesgos con la norma ISO/IEC 27005. Caso de estudio INAMHI”, tuvo como objetivo el análisis de la gestión de la infraestructura, los sistemas de información y las medidas organizacionales adaptadas por la empresa desde una perspectiva tecnológica. La metodología fue de tipo inductivo-deductivo bajo un diseño experimental para poder manipular las variables de estudio. Se realizó una auditoría al EDSI para obtener la información inicial y se aplicaron los análisis de riesgos, teniendo como referencia la norma en mención para los controles, políticas y procedimientos de seguridad de la información. El resultado de la investigación resultó la obtención de un plan estratégico de seguridad de la información con las políticas de seguridad informáticas adecuadas y alineada con los objetivos de la empresa. De acuerdo al estudio anteriormente mencionado, se detectan que el principal aporte se relaciona con el plan estratégico de seguridad de la información de las organizaciones asociadas al teletrabajo, en función de proporcionar información para la definición de las políticas, parámetro, objetivos y normativas vinculadas con la seguridad de la información.

[38] MUÑOZ, Jorge Diseño de un plan estratégico de seguridad de la información de Cias & Profesionales S.A.S. Tesis de pregrado. 2017. Universidad Nacional Abierta y a Distancia. Mocoa, Colombia.

[39] GONZÁLEZ, Diego. Diseño de Un Plan Estratégico de Seguridad de La Información, Mediante La Aplicación de Análisis de Riesgos Con La Norma ISO/IEC 27005. Caso de Estudio INAMHI. *Revista INNOVA*. 2018, vol. 3, no. 2, pp. 84-91. ISSN 2477-9024

4.2. MARCO TEÓRICO

Las definiciones que se muestra a continuación, permitirán explicar los objetivos que corresponden a este proyecto:

4.2.1. Riesgos de la seguridad de la información

Según Fajardo, se define de la siguiente manera:

De acuerdo a la identificación de la vulnerabilidad y amenazas sobre activos, se debe entender que la información se ve comprometida cuando queda expuesta las bases de datos y los servidores donde se encuentra almacenada en asocio con un software, entre los cuales se identifican los siguientes [40].:

- "R1: Perdida parcial de información vinculada con nuevas características que resultan de la falta de actualizaciones de los desarrolladores a subversión y falta de actualización de las aplicaciones de gestión de documento.
- R2: Cambio y / o pérdida de información debido a la falta de controladores de acceso físicos y lógicos para organizar el repositorio de información
- R3: Debido a la falta de control de acceso lógico en el repositorio de información contenido en el software del documento, la información es confusa.
- R4: La divulgación no autorizada de defectos en las aplicaciones de gestión de documentos ha llevado el menoscabo del perfil corporativo de la organización.
- R5: Los datos en la aplicación de gestión de documentos es hurtada o perdida provocados por la no tenencia de protocolos que no garantizan la seguridad en la proyección de un software en un ambiente web.
- R6: Debido a la falta de nuevas pautas de seguridad en el software que requieren que los administradores cambien las contraseñas, se pierde reserva de los datos contenidos en la aplicación en la misión documental.
- R7: La información contenida en la aplicación de gestión de documentos se pierde, y esta información define la frecuencia y la complejidad de la actualización de la contraseña del usuario de la aplicación.
- R8: Se llegó a un acuerdo de servicio con el cliente debido a que el tercero aprovechó las debilidades existentes del software y dejó inutilizable la aplicación de gestión de documentos
- R9: Divulgación de terceros y detrimento de datos que no son autorizados, causado por la asignación excesiva en los roles de usuarios.
- R10: La falta de procedimientos para establecer pautas de información de respaldo y buenas prácticas de seguridad conduce a la pérdida de información en la organización

[40] FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el Mercado colombiano. Tesis de pregrado, 2017. Instituto Universitario Politécnico GranColombia.

- R11: Debido a una gestión de identidad insuficiente, la revisión de accesibilidad a los peculios de la organización y los bancos de datos, afectan la confidencialidad e integridad de estos.
- R12: Pérdida de información y daños en el servicio debido a un sistema operativo obsoleto y funciones antivirus en el servidor.
- R13: La degradación del rendimiento físico causada por la carencia de procedimientos preventivos de sostenimiento y apoyo en los diferentes dispositivos, hacen que la información alojadas en el servidor sean inutilizables.
- R14: Tiempo inútil debido a la falta de disponibilidad de información y servicios debido a la configuración de seguridad en el servidor
- R15: Debido a un control de acceso físico insuficiente al centro de cómputo, el daño o el robo de la infraestructura técnica ha afectado las operaciones de la organización.
- R16: Por la carencia de métodos de inspección en situaciones de orden ambiental, que son los niveles de humedad y los grados de temperatura, la información causada por la degradación de los equipos informáticos no está disponible
- R17: El sistema de apoyo de la red electica en el entorno estructural de la red en la organización está dañado o carece de electricidad, lo que resulta en un tiempo de inactividad en las operaciones de la empresa.
- R18: Detrimento integral o en parte en las instalaciones de índole técnico de la central de informática debido a un incendio en el circuito.
- R19: Debido a la carencia de gobernabilidad, lineamientos, políticas e inspecciones para establecer contraseñas en accesibilidad para dispositivos de tecnología física, se pierde la información confidencial de la organización.
- R20: Debido a fallas en su diseño e implementación, no es posible acceder a información o servicios a través de la red de la compañía.
- R21: El antivirus desactualizado causa que se pierda parte o toda la información
- R22: Las funciones antivirus obsoletas con el código malicioso causan daños en el hardware.
- R23: El impacto de la presencia de malware en el funcionamiento de la red de la compañía.
- R24: La fuga de información no autorizada debido a la falta de mecanismo de encriptación de la información en la unidad de almacenamiento electrónico conduce a la pérdida de clientes.
- R25: Por la carencia de pactos de orden confidencial y la salvaguardia de la posesión erudita con la organización y recurso humano directo, principiantes y alianzas estratégicas, la información confidencial de la organización se roba o se pierde.”

En relación con los riesgos anteriormente mencionados, se considera de suma importancia esta información, dado que permite definir los riesgos que se encuentran vinculadas a las actividades del teletrabajo y en función de las características propias de los riesgos, y las actividades que se desarrollan dentro

de la organización, se pueden definir los factores de riesgos informáticos en las organizaciones asociados al teletrabajo en la actualidad.

4.2.2. Herramientas y técnicas disponible para la seguridad de la información

4.2.2.1. Factores de riesgos informáticos

4.2.2.2. Actos maliciosos o malintencionados.

4.2.2.2.1. Virus informáticos o códigos maliciosos: alguna de las principales amenazas se ubica:

Según Fajardo, se define como:

- Spyware[41]: "Se conoce habitualmente como un programa espía, con el cual el delincuente aprovechando las puertas traseras de seguridad y haciendo uso del internet, instala en el equipo de la víctima un software malicioso, cuyo ataque es básicamente explorar la información que le interesa y hacer un compendio de ella. Dentro de esta arremetida, puede grabar registros de navegación, códigos de acceso de las páginas y servicios en línea, datos personales, etc. Con este tipo de programa espía, no solamente se ataca computadores, sino que también son susceptibles a estos ataques otros dispositivos como Tablet, equipos móviles entre otros."

De acuerdo con lo anteriormente descrito, se argumenta que los spyware, representan una amenaza importante para los sistemas operativos de ordenadores, por lo cual se deduce que los teletrabajo se exponen a ladrones de claves y troyanos bancarios.

Según López, se define los troyanos, virus, y gusanos, como se muestra a continuación:

- Troyanos, virus y gusanos[42]: "es coloquialmente un lobo disfrazado de oveja, ya que se presenta como un programa genuino y con lo que los atacantes hacen lo posible para acceder a los sistemas y generalmente

[41] FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el Mercado colombiano. Tesis de pregrado, 2017. Instituto Universitario Politécnico GranColombia.
[42] LÓPEZ PINO, José Luis. Contraseñas débiles, 2010 [consultado 30 junio 2020 Disponible en https://lopezpino.com/2010/07/20/contrasenas-debiles/

trasciende a través de unidades externas como son las USB, teniendo cabida en la contaminación de los equipos, sin que la víctima caiga en cuenta de ello y más aún porque no usan conexión a internet. Mientras que los virus se asocian al término programas nocivos, y estos se instalan en el computador por diferentes medios y su principal objetivo es la destrucción y el gusano es un malware que consume bastante recurso del sistema y su ataque es reproducirse a sí mismo, guardándose en diferentes lugares del dispositivo, cuyo objetivo es ralentizar los sistemas, llevándolos al colapso. Este ataque no arremete contra la información ni toca ningún archivo"

En función del uso de hardware incorrecto y en presencia de antivirus débiles, se presenta los gusanos, troyanos y virus, lo cuales representan la vulnerabilidad del sistema y pérdida de confianza para los usuarios.

Según lo que indica Palomo en la siguiente definición:

- Spam[43]: "Son correos electrónicos no autorizados, llamados también correos no deseados o correo basura, cuya finalidad es invadir el correo víctima con publicidad de forma intensiva y en la actualidad, su ataque se empieza a ver en los móviles Android o celulares".

  Mediante el uso de correos electrónicos, se reciben algunos spams, los cuales representan una potencial amenaza, por lo cual se debe pasar por algún tipo de antivirus antes de descargar el archivo, para bajar reducir el índice de amenaza.

  Según Grid solutions reason Rt clocks, se define a continuación como:

- Botnets[44]: "Conocido coloquialmente como red zombi, consistente en un software que el victimario instala en un equipo y este a su vez, de manera controlada por el delincuente infecta a otros dispositivos, tomando el control de ellos para lanzar registros fraudulentos, correos spam (Correos no deseados), y cuya finalidad es atacar otros sistemas."

  De acuerdo con lo anteriormente señalado, mediante los Botnets, se puede hacer uso de estos, para robar la información por medio de la

[43] PALOMO PASTOR, D. Francisco. Desarrollo de un Sistema de gestión de incidencias. Tesis de pregrado 2009. Universidad Politécnica de Madrid. España.

[44] GRID SOLUTIONS REASON RT CLOCKS. Falta de autenticación en función crítica en Grid Solution Reason RT clocks de GE. [en línea].2020 [consultado 01 de julio 2020]. Disponible en https://www. https://www.basquecybersecurity.eus/es/avisos/sistemas-control-industrial/falta-autenticacion-funcion-critica-grid-20200603.html

recepción de correos no deseados, y se puede detectar cuando se genera algún tipo de error en el ordenador.

Según el Instituto Nacional de Ciberseguridad, se argumenta a continuación que:

- Phishing[45]: “Es uno de los ataques que más de moda están hoy en día y desarrolla su ataque basado en la inocencia de su víctima. Esta arremetida es del orden social, ya que la víctima es engañada por medio de un link y/o mensaje de correo electrónico, que al abrirlo el ciberdelincuente tiene la facilidad de suplantar al usuario, robar códigos o claves y la información. Con este tipo de ataques, se comenten desfalcos financieros, robos de datos y cupos de tarjetas de créditos, seguridad social, etc.”

  Por lo cual, se deduce que la recepción de links, es una de las formas más fáciles para generar una amenaza al sistema, y obtener información importante de las bases de datos de las organizaciones, en caso de no contar con las herramientas de seguridad de la información.

  Según Vietis, como se define a continuación

- Trashing[46]: “Es un método cuyo ataque es mas de tipo externo, ya que el delincuente aprovecha todo lo que el usuario descarta o desecha en su trabajo común como son documentos (papel físico), diskette, cd. Este ataque consiste en verificar todo lo desechado en aras de obtener información que de alguna manera conduzca a información guardada en el equipo.”

  Lo anteriormente definido, indica que este tipo de amenaza consiste en lograr acceder a dispositivos u ordenadores que se encuentra en la papelera y resultan un ataque para los documentos o información importante de las organizaciones

4.2.2.3. Factores humanos

[45] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Glosario de términos de ciberseguridad: Guía de aproximación para los empresarios. 2017. Guía de investigación. España.

[46] GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

Según el Departamento administrativo de la función pública, se muestra a continuación:

"El factor humano debe ir de la mano de manera muy sincronizada con las políticas de seguridad que se requieran, los componentes de índole técnico, concatenado con la normatividad vigente (LEY 1273 DE ENERO 05 DE 2009), [47] esto, quiere decir que el factor humano es muy importante, ya que las organizaciones deben contar con personas idóneas, con ética y responsabilidad para el manejo de la información, la implementación de programas y/o aplicaciones a instalar, e materia de seguridad informática y la ejecución de procesos que cumplan los estándares de legalidad y seguridad, enmarcados dentro de la ley, como son los ministerios de las TICS y comunicaciones y las normas de la organización a las cuales prestan su servicio como es el de conservar la integridad, fidelidad y salvaguarda de la información.

Si la dirección general de una organización no vela por que se cumplan estas condiciones, es la organización como tal la que termina siendo la responsable por cualquier actuar errada o corrupta de sus empleados, lo que conlleva a ser merecedora de aquiescencias del peso de la ley, pérdidas económicas, hasta la quiebra y en el peor de los casos ser legitimados con procesos de índole penal. Algunos de los delitos más cometidos son: acceso a información ilegal, llámese páginas de contenido discriminatorio o racista, páginas con contenido sexual, etc, que no son acordes a las políticas y objetivos de una organización, Instalación de software no autorizado, uso indebido de los equipos de la organización, uso indebido de permisos, credenciales, claves, etc.

En los últimos años, los principales expertos en el campo de la seguridad informática nos han hecho darnos cuenta de que, al implementar un sistema de gestión de seguridad de la información, los factores humanos deben considerarse como uno de los factores más importantes, por lo que deben considerarse los factores humanos. Como uno de sus elementos clave, se deben considerar los siguientes aspectos: capacitación adecuada y conocimiento de los empleados, participación de gerentes y directores, y aprobación de regulaciones internas sobre el uso de computadoras e Internet en la organización [48]."

Por lo anterior se puede determinar que el recurso humano es factor esencial para la seguridad informática de una organización y es ahí donde los directivos deben tener especial cuidado en la contratación, capacitación y tener en cuenta el profesionalismo de su personal contratado y supervisar para que los valores éticos

[47] Departamento Administrativo de la Función Pública. Ley 1273 de 2009 (enero 05) "De la protección de la información y de los datos" Ley publicado por Función publica. 2009. Colombia.

[48] GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

primen en el entorno laboral y manejo de la información, haciendo énfasis por diferentes medios en concienciar a los empleados de cumplir las normas en el manejo de datos y sus procesos.

4.2.2.4. Fallas del sistema de procesamiento de información

4.2.2.4.1. Contraseñas débiles

Según López y Rosell, se definen a continuación las contraseñas débiles:

"Son aquellas no complicadas de averiguar, aquellas que se pueden deducir mediante poco esfuerzo para obtener un ataque de fuerza bruta [49], mientras que en la era internet y los dispositivos móviles, el número de contraseñas necesarias aumento significativamente, por lo cual, [50] asegura que el 42,7% de los usuarios utiliza la misma contraseña para todo, y el 56% de las personas aseguran no cambiar nunca sus contraseñas, por otro lado, el 77% reconocen utilizar contraseñas débiles conformadas por letras, número o la combinación de ambas y solo el 13% de los encuestados hacen uso de passwords considerados seguros, de los cuales el 42,1% utiliza la misma contraseña para todo y solo el 31% dispone de una diferente para cada entorno. Por lo cual usar este tipo de passwords significa quedar realmente expuestos a la posible acción de un hacker que podría acceder a nuestros dispositivos o cuentas inutilizando o robando información."

Los usuarios frecuentan el uso de contraseñas débiles y el uso de nombres relacionados con personas cercanas y comunes, fechas de nacimiento o fechas importantes, y se frecuenta muy poco el uso de caracteres especiales, por lo cual, resultan una posible amenaza a la información personal, organizacional o bancaria.

4.2.2.4.1.1. Claves endebles

Según Palomo, se define las claves endebles a continuación:

"Desde un empleado, hasta el usuario de a pie, por regla común, en la mayoría, no usan claves robustas, bien sea por temor a olvidarlas o por lo que pueda implicar complejidad al ingresarlas, con lo que dejan vulnerable desde un correo electrónico, temas financieros y las mismas informaciones que maneja una organización. [51]"

---

[49] LÓPEZ PINO, José Luis. Contraseñas débiles, 2010 [consultado 30 junio 2020 Disponible en https://lopezpino.com/2010/07/20/contrasenas-debiles/

[50] ROSELL, José. Sólo uno de cada diez usuarios utiliza una contraseña segura, 2017 [consultado 30 junio 2020]. Disponible en https://www.google.com/amp/s/amp.20minutos.es/noticia/2948625/0/estudio-usuarios-consenas-inseguras/

[51] PALOMO PASTOR, D. Francisco. Desarrollo de un Sistema de gestión de incidencias. Tesis de pregrado 2009. Universidad Politécnica de Madrid. España.

Por razones de olvido o extravió de claves, las personas hacen uso de claves que resultan poco desafiante para los hackers, y resulta información importante para acceder a la información importante de los ordenadores, correo electrónico, cuentas bancarias y redes sociales.

4.2.2.4.2. Bugs

Según Kanat, se define como se muestra a continuación:

“Es un término que suele aparecer en programas (Candy crush, SoundCloud o Facebook), el cual no actúa de acuerdo con la intención del programador, y la segunda intención del informático no cumple con las expectativas razonables del beneficiario. Cuando el funcionario genera nuevo contenido al usuario y causa problemas, eso significa que hay defectos inesperados en el código escrito por el programa. Aparecen en errores de software, también pueden existir en errores de hardware, generando un error en el software que causa el bloqueo del programa, o la mayoría de los errores son errores humanos[52]”

Estos se detectan cuando se genera un programa informático, y aparecen errores de software, por lo cual se debe hacer uso de software que adviertan y resuelvan los errores relacionados a los bugs.

4.2.2.4.3. Falta de cifrado de datos

Según Fajardo, se define como se muestra a continuación:

“La Falta de cifrado de datos, significa no alternarlos, mediante el uso de una clave de modo que sean legibles para quienes poseen dichas claves. Por lo cual resulta necesario el cifrado de datos, dado que implica que cada vez que se quiera acceder a datos, se deban descifrar, lo que agrega un nivel de complejidad al acceso simple, pero reduce la complejidad del proceso, por lo cual, la falta de protección de información confidencial de una organización conlleva a que, si la información sensible de la compañía cae en manos equivocadas, puede producirse perjuicios económicos, perdida de ventaja competitiva o cierre de la empresa, la falta de protección y prestigio de una organización, dado que existe cierta que si es robada puede dañar la imagen corporativa, la falta de protección en las comunicaciones de una organización, este factor es susceptible a intercesiones, dado que los mensajes enviados por las organizaciones difunden por medio de canales o infraestructura externa, y se genera la falta de protección para dispositivos móviles e inalámbricos,

[52] KANAT ALEXANDER, Max. Code simplicity: the science of software development., 2012. [en línea] Editorial O´reilly media Inc. Estados Unidos de América.

no hay garantía de que terceros no autorizados puedan ingresar información de la compañía por teléfono, teléfono móvil, tableta o computadora portátil[53]"

Mediante la información descrita anteriormente, resulta necesario el cifrado de datos, dada la importancia del generar un nivel de complejidad amplio para el sistema aun cuando el usuario hace un acceso de forma simple, por lo cual en las organizaciones resulta importante llevar a cabo esta estrategia dado que permite proteger el software y hardware de las mismas.

4.2.2.4.4. Redireccionamiento de URL a sitios no confiables

Según García, se define de la siguiente manera:

"Existe ocasiones en las que existe interés que una página web concreta apunte a otro dominio o a otra URL específica, por lo cual se utilizan los siguientes redireccionamientos.

- Redireccionamiento desde PHP, HTML o Javacript" PHP Header ("Location: http://www.example.com");" HTML: incluir, en la sección, la siguiente etiqueta:" Javascript window.location.href = 'http://www.example.com'; se puede redirigir de una página otra.

- Redirecciones 301: se incluye la actualización de una página web o al migrar a un nuevo dominio, con este tipo de redirección les estamos indicando a los buscadores que nuestra página ha transformado para que tengan en cuenta la nueva URL.

Otros aspectos. Cada página de un sitio debe incluir su URL completa ya que las páginas son encontradas, salvadas, recortadas, impresas y reenviadas en forma independiente; sin embargo, es importante que no pierdan el nexo con la estructura original. Un sitio cuidado evita cambiar las URLs, y si ese cambio se efectúa redirecciona al usuario de la antigua a la nueva dirección. [54]"

Una de las técnicas que se utilizan mucho para generar amenazas en los sistemas corresponde al redireccionamiento, ya que, a través de la navegación en internet, lo cual incurren en que los URL pierdan la estructura original.

4.2.2.4.5. Falta de autenticación para una autenticación crítica

[53] FREIRE FAJARDO, Franklin. Cifrados de información: la encriptación de datos en las empresas [en línea]. Guía corporativa. 2018 Enjoy Safer Technology.
[54] GARCÍA DE LEÓN, Alicia; GARRIDO DÍAZ, Adriana. Los sitios web como estructura de información: un primer abordaje en criterios de calidad [en línea]. 2002. Artículo de investigación. Universidad de la Republica de Monterrey, Uruaguay.

Según Grid Solutions Reason Rt clock, se define la falta de autenticación para una autenticación critica de la siguiente manera**.** [55]

- **“Problemas del modelo clásico**

El ataque al contenido cifrado, constituye una amenaza importante para el sistema de autenticación del sistema de información, por lo cual resulta importante descifrar la contraseña, pero el problema aparece cuando resulta fácil cifrar la palabra junto a una terminología determinada y comparar el resultado con la cadena almacenada en el archivo de clave. De esta manera, el atacante leerá el archivo / etc / password (si se quiere que el sistema funcione normalmente, este archivo debe tener permisos de lectura para todos los usuarios), y usará un *cracker* para cifrar todas las palabras del archivo llamado diccionario (archivo ASCII que contiene una gran cantidad de palabras de cualquier idioma o campo social: historia clásica, deportes, postres preferidos, canción favorita, color, países), y los resultados obtenidos en este proceso se comparan con la clave de cifrado del archivo de contraseña; en caso hacer la comparación y acceder al sistema no autorizado, se detecta de manera inmediata que ha fallado el sistema de autenticación por este medio.

- **Contraseñas inaceptables**

El método de ataque principal es usar contraseñas con palabras en archivos de diccionario típicos: no contenga caracteres como letras minúsculas y mayúsculas, y tampoco se incluya números con texto y combinaciones de símbolos, también se debe hacer uso de teclas simples (como web o security), nombres de familiares, nombres personales, combinaciones débiles (como alci21 o goals), nombres de lugares, actores de telenovelas o películas, libros preferidos, deportistas, pero es necesarios incluir todos los ítem de seguridad dentro de las contraseñas del sistema. Por lo que los administradores deben ejecutar un programa divisor regularmente, escriba crack para verificar que sus usuarios no hayan seleccionado una contraseña débil (aunque se usan Npasswd o Passwd +): estas pueden ser claves

Finalmente, debe recordarse que para que una contraseña sea aceptable, debe cumplir con el principio KISS.

- **Shadow Password**

El shadow password afecta directamente la protección del usuario y conduce a fallas de autenticación porque los usuarios sin privilegios pueden leer archivos que

[55] GRID SOLUTIONS REASON RT CLOCKS. Falta de autenticación en función crítica en Grid Solution Reason RT clocks de GE. [en línea].2020 [consultado 01 de julio 2020]. Disponible en https://www. https://www.basquecybersecurity.eus/es/avisos/sistemas-control-industrial/falta-autenticacion-funcion-critica-grid-20200603.html

almacenan claves de cifrado, por lo cual el archivo / etc / passwd debe tener permiso de lectura para todos si queremos que el sistema funcione correctamente. En una computadora con contraseña, todos los usuarios aún pueden leer el archivo, pero a diferencia de los mecanismos tradicionales, la clave cifrada no se guarda en él, sino en el archivo / root / shadow.

- **Envejecimiento de contraseñas**

Es importante destacar que afecta la falla de autenticación en el sistema es cuando la implementación actual de Password Password no se completa correctamente, porque generalmente incluye otra implementación de un conjunto de elementos de protección de claves (envejecimiento de claves o contraseñas), el cual consiste en proteger la contraseña del usuario para que tenga una vida útil determinada: la contraseña solo es válida durante un cierto período de tiempo, después del cual la contraseña caducará y el usuario debe cambiarla, concluyendo con que si la clave es válida perennemente, el usuario logró acceder de forma segura al servidor cuando sea necesario; sin embargo, si la clave tiene una vida útil corta, el atacante solo puede usarla antes de que el sistema nos obligue a cambiar la clave.

- **Otros métodos**

Un problema criticado de los esquemas de autenticación de usuarios, representan la amplitud de caracteres para fines de alta seguridad, y el otro problema radica en que las claves son demasiado cortas. Hace unos años era solo un método teórico ([DH77]), pero hoy es factible: ni siquiera implica problemas especiales de hardware, definitivamente es demasiado costoso para la mayoría de los atacantes, con una supercomputadora, Puedes descifrar la clave en menos tiempo. Dos días ([KI99]). Una forma de mejorar la seguridad de las claves para evitar ataques de intrusos es cifrar mediante una función llamada bigcrypt () o crypt16 (), que permite que las combinaciones sean más largas que cryp).

4.2.2.4.6. Cross-site scripting y falsificación

Esta es una vulnerabilidad existente en algunas páginas web generadas dinámicamente (basadas en datos de entrada). XSS proviene del acrónimo de scripting entre sitios. Debido a que el sitio web dinámico depende de la interacción del usuario, puede insertar un pequeño programa malicioso en el formulario, ocultarlo entre solicitudes legítimas y ejecutarlo para ejecutarlo. Los puntos de entrada comunes incluyen motores de búsqueda, foros, blogs y varios formularios alojados en páginas web.”

En cuanto a la falta de autenticación para autenticación crítica, se detecta mayor índice de vulnerabilidad, dado que permite que los hackers lleven a cabo comandos arbitrarios y enviar solicitudes a URL específicas, lo que puede hacer que el

dispositivo deje de responder, tomando en cuenta la necesidad de los sistemas en cambiar la contraseña de la cuenta de usuario de configuración, permitiendo que la nueva contraseña modifique la configuración del dispositivo a través de la interfaz web, o puede omitir la autenticación requerida para configurar el dispositivo y reiniciar el sistema

4.2.3. Desastres naturales

Según Díaz, define como se muestra a continuación:

"La gestión de la información implica la tecnología de la información y la comunicación en la gestión de la información sobre desastres porque implica: determinar con precisión la información, recopilar y analizar información, registrar, restaurar, usar y divulgar la información necesaria. Las TIC proveen la conexión necesaria entre los sensores y otros equipos utilizados para monitorear u observar el medio ambiente, y facilita la recopilación de información y los centros de análisis para abastecer a los usuarios análisis científicos o políticos a través de Internet y para uso privado para ejercer su conocimiento de las condiciones ambientales., dado que la mayoría de casos los .desastres naturales destruyeron la infraestructura de telecomunicaciones terrestres desde el principio e impidieron la comunicación en las áreas afectadas, la tecnología inalámbrica permitió garantizar la comunicación entre los servicios de emergencia y las operaciones de rescate.[56]

- **Protección contra código malicioso malware**

La protección contra código maliciosos es conocido como un software antivirus, este sistema lo deben tener todas las organizaciones independientemente el tamaño o actividad comercial, los cuales dentro de la estructura de la empresa deben considerar los sistemas informáticos, los servidores, labores, y los temas relacionado con la movilidad de la información como ocurren en la actualidad en el desarrollo del teletrabajo, el cual convierte esta actividad en una gran amenaza para la organización.

- **Protección contra ingeniería social y fraude**

Este tipo de protección representa una de las herramientas principales para que los grupos criminales en Internet para la obtención de información del usuario o infecten una gran cantidad de sistemas. Por lo cual en la actualidad existe una amplia gama de herramientas de seguridad en el mercado, la tecnología utilizada se está

[56] MENA DÍAZ, Nestor Las tecnologías de información y comunicación en el segumineto de los desastres naturales: estudio de un caso: La plataformainformática de la red UTEEDA para la gestión de la información sobre desastres. 2007. Artículo científico. ACIMED ISSN 1024-9435. Habana, Cuba.

volviendo cada vez más compleja y dirigida a grupos de usuarios específicos, por lo que, aunque las soluciones de seguridad pueden ayudarnos a resistir parcialmente estas amenazas a los sistemas en las empresas.

- **Contingencia y continuidad**

Estas herramientas están diseñadas para lograr la supervivencia de una empresa u organización de varias maneras después de un incidente de seguridad. En este tipo de solución, podemos encontrar copias de seguridad que incluyen copias de seguridad en la nube. Estas copias de seguridad nos permiten garantizar la seguridad de la información más importante de la organización. Sin esta información, la organización no podrá realizar actividades. También se contemplan otras herramientas de recuperación de sistemas completos, permitiendo recuperar no sólo información o virtualizaciones, sino también poder implementar una infraestructura de respuesta rápida, ante la presencia de un evento inesperado.

- **Protección de las comunicaciones**

La protección de las comunicaciones, permite proteger a las organizaciones ante una posible amenaza, como en el caso de accesos no autorizados o fallas la autenticación de datos, ataques de denegación de servicio y la interceptación de comunicaciones. Entre los principales instrumentos para lograr la protección se ubican: firewalls, VPN (redes privadas virtuales) o dispositivos electrónicos de red con funciones NAC (control de acceso a la red) en empresas y lugares de trabajo."

En cuanto a las definiciones anteriores, la identificación de los factores de riesgos asociados a la seguridad de la información, y las características que debe poseen las herramientas y técnicas disponible para la seguridad de la informática, entre las cuales destacan los actos maliciosos, humano, desastres naturales en las organizaciones; esta información resulta necesaria para definir las herramientas y técnicas disponibles para la seguridad de la información asociado al teletrabajo.

4.1.3. Responsabilidades de perfiles de seguridad en las organizaciones.

Según Rodríguez[57], se define a continuación las siguientes responsabilidades de perfiles de seguridad en las organizaciones:

- **Responsable de seguridad**

El gerente de seguridad es la persona más importante en el desarrollo de la seguridad de la información. La persona a cargo del campo de TI asumirá esta función y delegará sus responsabilidades actuales a los empleados que están

[57] RODRÍGUEZ CONDE, Luis. Elaboración de una plan de implementación ISO/IEC 270001:2013. 2017. Plan Director de Seguridad de Ícaro S.A. Universidad Rovira I Virgili

debajo de él para asumir la nueva función. Además, también recibirá capacitación relevante sobre este rol. Sus responsabilidades en seguridad de la información son las siguientes:

-Preparar, promover y mantener estrategias de seguridad de la información.
-Preparar planes de riesgo y posibles soluciones para mitigar amenazas.
-Proponer nuevas metas con respecto a la seguridad de la información.
-Desarrollar y mantener marcos regulatorios de seguridad y monitorear el cumplimiento.
-Verificar la implementación de los requisitos de seguridad necesarios.
-Liderar la implementación del SGSI.
-Establecer medidas de control y medidas técnicas y organizativas para garantizar los sistemas de información.
-Gestionar globalmente la seguridad de la información organizacional.
-Gestión y análisis de incidentes de seguridad en la organización.
-Verifique periódicamente el estado de seguridad de la información.
-Seguir los incidentes de seguridad.
-Inspeccionar y verificar los indicadores definidos.
-Definir y verificar la aplicación del proceso de notificación y gestión de eventos.
-Informe al Comité de Seguridad sobre cuestiones relacionadas con la seguridad de la información.

- **Comité de seguridad**

El comité de seguridad es el siguiente: director de seguridad, gerente general, director de operaciones y director técnico. Las funciones y responsabilidades del comité de seguridad son:

-Llevar a cabo las directrices de la Administración general.
-Establecer los diferentes roles y funciones en términos de seguridad.
-Proponer políticas, normas y responsabilidades de seguridad. Información para aprobarlo. -Verifique el mapa de riesgos y las medidas de mitigación recomendadas.
-Verifique el plan de seguridad y envíelo a la gerencia para su aprobación.
-Inspeccionar el desarrollo y mantenimiento de planes de continuidad de negocio.
-Asegurar el cumplimiento de la normativa vigente.
-Mejorar la capacitación del personal y la seguridad de la información.
-Certificar y analizar regularmente el tablero para garantizar la seguridad de la información y el desarrollo del SGSI

- **Personal con perfil de usuario**

Una persona con datos personales del usuario se refiere a una persona que utiliza el sistema de información de la empresa para realizar sus actividades profesionales, pero no realiza ninguna gestión o gestión administrativa o tiene privilegios. Este personal tiene las siguientes reglas y responsabilidades:

-Observar y seguir las reglas y procedimientos definidos en la política de seguridad de la compañía.
-Mantener la confidencialidad de la información.
-Hacer uso completo de los activos de la organización.
-Cumplir con la normativa vigente.
-Notificar al personal de seguridad sobre condiciones anormales o incidentes de seguridad y condiciones sospechosas.

- **Personal con acceso privilegiado**

En las empresas, lo máximo de miembros del departamento de TI que deben tener acceso a los sistemas de información son una cantidad de 5 personas, de los cuales 2 personas se especializan en gestión de servidores y virtualización del sistema de información, 2 se especializan en estaciones de trabajo y sistemas de la compañía, y el último es el jefe del departamento de TI y el director de seguridad. Estos archivos de configuración tienen acceso de administrador a los sistemas de información (equipos de usuario y sistemas de centros de datos), así como acceso físico a áreas restringidas relacionadas con los sistemas de información (CPD). Las funciones y obligaciones de cada archivo de configuración se describen en detalle a continuación:

Administrador de puesto de trabajo y sistemas corporativos

Responsabilidades:
-Software y hardware de mantenimiento para equipos de usuario (PC, teléfono, teléfono inteligente, impresora, red, etc.).
-Administrar el directorio activo de la organización, mediante el registro de usuarios, cancelación y modificación, y gestión de roles.
-Gestión del sistema de correo electrónico empresarial, a través de tareas de gestión de buzones, registro de usuarios, cancelación y modificación, etc.
-Gestionar el sistema del sitio web empresarial, con los archivos de usuarios internos y externos.
-Gestión de la base de datos de la empresa.
-Gestión del sistema CAS -Gestión ERP.
-Gestión y gestión de todos los servidores que admiten sistemas de la empresa, con la colaboración de los administradores del servidor y la virtualización del sistema.

Administradores de servidores y virtualización del sistema.
Responsabilidades:

-Gestión de salas de almacenamiento que recolectan datos del sistema de información y la red electrónica utilizada para acceder al sistema.
-Gestión de entorno virtualizado.
-Gestión de los servidores físicos que soportan el sistema.

-Gestión de elementos electrónicos de red y elementos de seguridad en todo el CPD.
-Apoyo al equipo administrador del sistema de software.
-Asistir a los administradores de estaciones de trabajo y sistemas de la empresa en momentos específicos [58]"

Con respecto a la información señalada en los párrafos antes descritos, se destacan las características necesarias para el comité de seguridad, personal con acceso privilegiada, personal con perfil de usuario, y responsables de seguridad, y las responsabilidades que deben poseer dentro de cada equipo de seguridad de información, esta información es de gran importancia para el desarrollo de la matriz de responsabilidades de perfiles de seguridad en las organizaciones.

4.2. MARCO LEGAL

Estas bases legales sustentan al objeto de estudio, por lo cual se hace referencia a las siguientes leyes:

- Ley 1150 (2007). Seguridad de la información electrónica en contratación en línea, mediante la aplicación de esta ley se detecta la importancia de la seguridad de la información en ámbitos como la contratación, en la cual mediante el Art.8 "se establece como obligatorio publicar los proyectos de pliegos de condiciones junto con los estudios previos", y por lo cual resulta necesaria la identificación y posteriormente el análisis de los riesgos a los cuales se encuentra expuesto el sistema de contrataciones y mediante esta norma se puede tomar de referencia para establecer políticas del plan estratégico.
- Ley 1273 (2009) Delitos informáticos protección de la información Art.269 C Interceptación de datos informáticos, el que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático o las emisiones electromagnéticas, provenientes de un sistema informáticos que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses"
  Art.269E Uso de software malicioso "el que sin estar facultado para ello destruye, dañe, borre, deteriore, altere, o suprima datos informáticos, o un sistema de tratamiento de información o por partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes"
  Art. 269J Transferencia no consentida de activos "El que, con ánimo de lucro y validándose de alguna manipulación informática o artificio semejante, consiga una transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya un delito sancionado con pena más grave,

[58] RODRÍGUEZ CONDE, Luis. Elaboración de una plan de implementación ISO/IEC 270001:2013. 2017. Plan Director de Seguridad de Ícaro S.A. Universidad Rovira I Virgili

incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 y 1500 salarios mínimos mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, o posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará a la mitad."

Estos artículos resultan importantes para la investigación dado que indican características y normativas que debe existir para definir la elaboración de la matriz de responsabilidades de perfiles de seguridad de la información asociada al teletrabajo, y se vinculan a los factores vinculados a los actos maliciosos y factor humano que generan vulnerabilidad en los sistemas, dado que la ley permite dar a conocer las multas que aplicarían ante infracción.

- CONPRES 3701 (2011) Lineamientos de política para ciberseguridad y ciber-defensa, "fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciber-defensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio", lo cual resulta necesario en esta investigación, ya que permite tomar de referencias para el desarrollo de políticas dentro del plan de estrategia para la seguridad de la información y considerar la importancia de detectar vulnerabilidades en el sistema.

- Norma técnica colombiana NTC/ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información, mediante la norma técnica se puede generar el análisis de los riesgos, determinar características asociadas a las responsabilidades, y roles en la empresa necesarios para el desarrollo de este proyecto.

- Norma técnica colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información, se encuentra relaciona con la definición de las políticas de seguridad de la información dentro del plan estratégicos.

- ISO/IEC 27005 Information technology systems-security techniques- information security risk management, esta norma resulta necesaria para el análisis de los riesgos, dado que indica la metodología para la entrada de las actividades a las que se encuentra expuesto el teletrabajo, entre los cuales se destaca: identificación de los riesgos, estimación del riesgo, valoración de la probabilidad, valoración del impacto, y la matriz de probabilidad-impacto de los riesgos de la seguridad de la información asociado al teletrabajo.

- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: control de gestión, componente: actividades de control, elemento: monitoreo y revisión e información" mediante este modelo se posiciona este estudio en un sistema

de control interno que deben desarrollar las organizaciones, en la cual este estudio se ubica en un subsistema de control estratégico (administración de riesgos), lo cual resulta información necesario para el desarrollo del análisis de los riesgos de seguridad de la información asociada al teletrabajo.

- Ley 1221 (2008) “Reconocimiento del teletrabajo en Colombia como modalidad laboral y como instrumento de generación de autoempleo mediante la utilización de las TIC”
  Art. 30. Políticas públicas de fomento al teletrabajo: “para el cumplimiento del objetivo de la presente Ley el Gobierno Nacional, a través del Ministerio de la Protección Social, formulara, previo estudio Conpres, una Política Pública de Fomento al trabajo. Para efectos , el Ministerio de la protección Social contara con el acompañamiento del Ministerio de Comunicaciones, el ministerio de Comercio, Industrial y Turismo y el departamento Nacional de Planeación El Departamento Administrativo de la Función Pública, el SENA y la dirección de impuestos y aduanas nacionales- DIAN, esta política tendrá en cuenta los siguientes componentes: infraestructura de telecomunicaciones, acceso a equipos de computación, aplicaciones y contenido, divulgación y mercadeo, capacitación, incentivos y evaluación permanente y formulación de correctivo cuando su desarrollo lo requiera”, este articulo corresponde al desarrollo de referencias necesarias para la realización del plan estratégico de seguridad de la información asociada al teletrabajo.

4.3. MARCO CONCEPTUAL

- **Ciberriesgo**[59]**:** posibilidad de que una amenaza atraviese las vulnerabilidades de los equipos informáticos de una organización.
- **Ciberseguridad**[60]**:** es la acción de las entidades, bien sea privadas o públicas constituidas por la agrupación de actividades dirigidas a resguardar la infraestructura tecnológica contra los ciberataques producidos en pro de perjudicar el bienestar social y económico del ciberespacio. El concepto de

[59] ORDUZ BARRERA, Diana. Análisis de Emergencias Cibernéticas Que Se Presentan En Las Ciudades de Tunja, Duitama y Sogamoso Con Respecto Al País En Los Últimos Dos Años [en línea]. Monografía de posgrado. Universidad Nacional Abierta y a Distancia, 2019 [consultado 11 mayo 2020]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31410/dmorduzb.pdf?sequence=1&isAllowed=y

[60] ABAD PARRALES, Wagner, *et al*. La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. México: 3 ciencias, 2019, p. 65. ISBN 978-84-121167-6-2

ciberseguridad es estudiado ampliamente por autores como Freire[61], Gago[62] y Cubajante *et al.*[63] concuerdan con la definición de que "es el cuidado de la confidencialidad, la integridad y la disponibilidad de la información".

- **Ciberespacio**[64]**:** hace mención a la interconexión electrónica dispuestas en red que representan un espacio de relación integrado por componentes de la naturaleza material de base tecnológica.
- **Ciberataque**[65]**:** ofensiva o acciones deliberadas contra los valores, las personas, los bienes, los sistemas o los servicios transmitidos por el ciberespacio y la tecnología que los conecta.
- **Carding**[66]: es el proceso a través del cual se emplean tarjetas de créditos o números de terceros, haciendo uso de la ingeniería social para obtener información. En la actualidad es un mecanismo que se da desde buscar un extracto en la basura o hurgar en el buzón de otras personas para conseguir números de tarjetas de crédito y proceder a realizar los fraudes.
- **Ciberatacante**[67]**:** persona o grupo de personas dedicadas al ciberataque que emplean diversos mecanismos para obtener información de personas de manera fraudulenta con el propósito de obtener beneficios económicos.

---

[61] FREIRE FAJARDO, Franklin. Plan de Contingencia Ante Ciberataques [en línea]. Tesis de Maestría. Escuela Superior Politécnica del Litoral, 2017 [consultado 11 mayo 2020]. Disponible en https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf

[62] GAGO, Edgardo. El Enfoque Argentino Sobre Ciberseguridad y Ciberdefensa [en línea] Tesis Doctoral. Escuela Superior de Guerra Ttl Grl Luis María Campos [consultado 17 mayo 2020]. Disponible en https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&as_ylo=2016&q=DEFINICION+DE+CIBERSEGURIDAD&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3AnR6gf2qgQBwJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D1%26hl%3Des

[63] CUJABANTE VILLAMIL, Ximena *et. al*. Ciberseguridad y Ciberdefensa En Colombia: Un Posible Modelo a Seguir En Las Relaciones Cívico-Militares [en línea]. Bogotá: Seguridad y Defensa, 2020 [consultado 17 mayo 2020]. Disponible en https://revistacientificaesmic.com/index.php/esmic/article/view/588

[64] ASENCIO-GUILLÉN, Antonio y NAVÍO-MARCO, Julio. El Ciberespacio Como Sistema y Entorno Social: Una Propuesta Teórica a Partir de Niklas Luhmann [en línea]. Pamplona: Commnication & Society, 2018. [Fecha de consulta 11 de mayo 2020]. Disponible en https://search.proquest.com/openview/2a80c2a19a2f9ac9b341136efd1a54bc/1?pq-origsite=gscholar&cbl=1216381

[65] LAZAR, Elena y NICOLAE COSTESCU, Dragos. Los Ciberataques: Una Noción Sin Tipificación, Pero Con Un Futuro [en línea]. Coruña: Anuario da Facultade de Dereito da Universidade da Coruña, 2018. [Fecha de consulta 11 de mayo 2020]. Disponible en https://ruc.udc.es/dspace/bitstream/handle/2183/22352/AD_2018_22_art_7.pdf?sequence=3&isAllowed=y

[66] KIGERL, Alex. Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories [en línea]. Washington: Social Science Computer Review, 2017. [Fecha de consulta 16 mayo 2020]. Disponible en https://journals.sagepub.com/doi/10.1177/0894439317730296

[67] MARTÍN RODRÍGUEZ, Guillermo. La Gestión de Los Riesgos Tecnológicos [en línea]. Tesis de Maestría. Universidad Pontificia Comillas, 2018 [consultado 15 mayo 2020]. Disponible en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/33058/TFM001074.pdf?sequence=1&isAllowed=y

- **Phishing**[68]**:** es el mecanismo por el cual se puede acceder de manera fraudulenta a información confidencial, como contraseñas y datos bancarios reservados. Por ejemplo, un phisher puede utilizar un correo electrónico o un sitio web para suplantar la identidad de una empresa y obtener información fingiendo que actualiza la información del cliente, tal como el envío de correos electrónicos pidiendo los detalles de la tarjeta de crédito y las contraseñas; se debe tener presente que un trabajador de este tipo de entidades nunca pide esta clase de información. También se puede ejecutar la operación a través de correos electrónicos con archivos adjuntos de códigos maliciosos que permiten acceder a los computadores.
- **Vishing**[69]**:** es un mecanismo empleado para robar información, tal como el phishing, pero éste se realiza por medio de llamadas telefónicas. Para ello, la persona dedicada a este tipo de estafas posee poder de convencimiento al igual de buena oratoria para recabar información sensible de la víctima como contraseñas y números de tarjetas de créditos bajo falsos supuestos.
- **Baiting**[70]**:** Las personas que se especializan en trabajos de cebo operarán dejando un dispositivo extraíble (como un CD o almacenamiento USB) cuyo contenido es malware, que se ejecutará solo y robará información de la computadora cuando se abra.
- **Teletrabajo**[71]**:** Nueva forma de organización del trabajo cuya novedad radica en que la prestación se realiza online desde diferentes lugares fuera del entorno físico de la empresa, con la ayuda de las nuevas tecnologías de la comunicación

4.4. MARCO HISTÓRICO

Los sistemas de información se caracterizan por presentar una fuente de

[68] BALBOA ROMERO, José. Ransomware, Hacking y Phising: Conducta Típica Del Delito de Daños Informáticos [en línea]. Tesis de pregrado. Universidad Internacional de la Rioja, 2018 [consultado 15 de mayo 2020]. Disponible en https://reunir.unir.net/bitstream/handle/123456789/6929/BALBOA%20ROMERO%2c%20FRANCISCO%20JOS%c3%89.pdf?sequence=1&isAllowed=y

[69] DÍAZ JIMÉNEZ, Sebastian *et al.* Análisis Del Delito de Fraude Electrónico: Modalidad Tarjeta de Crédito [en línea]. Tesis de pregrado. Universidad Cooperativa de Colombia Sede Montería, 2018 [consultado 16 mayo 2020]. Disponible en https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

[70] CRISTIAN LUGA, Jason y EROLA, Arnau. Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks [en línea]. Oxford: Human-Centric Computing and Information Sciences, 2016. [Fecha de consulta 16 mayo 2020]. Disponible en https://link.springer.com/content/pdf/10.1186/s13673-016-0065-2.pdf

[71] MORENO AYALA, Enyi y PEÑA VELANDIA, Wilson. El Teletrabajo, Impacto En La Calidad de Vida de Los Colaboradores Del Área de Soporte Técnico de La Compañía Colvatel S.A [en línea]. Tesis de posgrado. Universidad de Bogotá Jorge Tadeo Lozano, 2018 [consultado 17 mayo 2020]. Disponible en https://expeditiorepositorio.utadeo.edu.co/bitstream/handle/20.500.12010/8345/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

vulnerabilidades que pueden ser objetivo de ciberataques que buscan perpetrar un siniestro contra de una empresa u organización, de ese modo se ha evidenciado un auge en la importancia de respaldar la seguridad en contra de los riesgos informáticos que existen en la actualidad.

Motivado a esto, autores como Freire[72] y Martín[73] desarrollaron protocolos seguridad, basados en las tecnologías de información y comunicación (TIC) para resguardar los activos de sus sistemas de información.

Asimismo, se ha abordado esta problemática por autores como Durango y Quimiz[74] y Huayllani[75], cuyo propósito consistió en la ejecución de estudios de sensibilidad a los sistemas de información para detectar brechas en la seguridad que pudiesen ser subsanadas por medio de la implementación de políticas de seguridad informática e implementación de softwares avalados para contrarrestar el impacto que generan los ciberataques en la red, llegando a la conclusión de que es imperativo contar con una gestión de riesgos informáticos fundamentados en las teorías de información de seguridad y respaldo de los datos de los usuarios.

En este sentido, también responde al tema de una nueva era de globalización causada por las nuevas tecnologías disponibles en el mercado. Esta es la razón por la cual, bajo las pautas de implementación de sistemas de seguridad de la información en modelos empresariales u organizativos, estos conceptos son adecuados para ser reconocidos y puestos en práctica en trabajos remotos o en nuevos modos de trabajo remoto.

Para ello, se evalúan aspectos como el empleo de técnicas de seguridad en las bases de datos como corta juegos, programas de seguridad, firewalls, bloqueo de puertos, entre otros. Análogamente, estos resultados fueron también validados con otros estudios, como el de Osio[76], que explican la efectividad de las TIC en la

[72] FREIRE FAJARDO, Franklin. Plan de Contingencia Ante Ciberataques [en línea]. Tesis de Maestría. Escuela Superior Politécnica del Litoral, 2017 [consultado 11 mayo 2020]. Disponible en https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf FREIRE FAJARDO.FREIRE FAJARDO.FREIRE FAJARDO, “Plan de Contingencia Ante Ciberataques.”

[73] MARTÍN RODRÍGUEZ, Guillermo. La Gestión de Los Riesgos Tecnológicos [en línea]. Tesis de Maestría. Universidad Pontificia Comillas, 2018 [consultado 15 mayo 2020]. Disponible en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/33058/TFM001074.pdf?sequence=1&isAllowed=y MARTÍN RODRÍGUEZ.MARTÍN RODRÍGUEZ.MARTÍN RODRÍGUEZ, “La Gestiónd de Los Riesgos Tecnológicos.”

[74] DURANGO ESPINOZA, Rayner y QUIMIZ MOREIRA, Mauricio. Estudio de La Seguridad de La Información de Los Pacients En Los Hospitales Públicos Tipo II de Ecuador [en línea]. Tesis de pregrado [consultado 9 junio 2020]. Disponible en http://201.159.223.2/handle/123456789/3060

[75] HUAYLLANI MUÑÓZ, Oscar. Sistema de Gestión de Seguridad de La Información y La Gestión Del Riesgo En El Ministerio de Salud [en línea]. Tesis de maestría [consultado 9 junio 2020]. Disponible en http://repositorio.ucv.edu.pe/handle/20.500.12692/42775

[76] OSIO HAVRILUK, Lubiza. Salud y Seguridad En El Teletrabajo. *Revista de visión general*. 2016, no. 2, pp. 410-426. ISSN 1317-8822

seguridad de la información en el teletrabajo y el buen uso que puede dársele a estas para permitir la versatilidad del usuario de estar cubierto desde cualquier lugar donde se encuentre sin comprometer la confidencialidad de los datos de la empresa.

5. DISEÑO METODOLÓGICO

5.1. Tipo de investigación: El tipo de investigación según Colciencias[77], el cual consiste en trabajo experimentales que se emprenden principalmente para obtener nuevos conocimientos de los fenómenos y hechos observables, sin pensar en dales ninguna aplicación o utilización determinada, por lo cual esta monografía se clasifica desde un enfoque semi cuantitativo al observar que los análisis de los riesgos de la seguridad de la información se abordan desde el análisis de los criterios cualitativos y se cuantifican en factores cuantitativos para su posterior definición de estrategias correspondientes a la seguridad de la información asociado al teletrabajo, y este estudio se limitará al estudio de los perfiles de seguridad en las organizaciones y el establecimiento de estrategias.

5.2. Alcance de la investigación: Según Hernández, Fernández y Baptista [78],en cuanto alcance de la investigación, representa el resultado que se pretende alcanzar con la investigación que se relaciona con la explicación de la variable en estudio, por lo cual, mediante el plan estratégico de la seguridad de la información se pretende disminuir las amenazas a los sistemas informáticos, ante los riesgos a los cuales se encuentra expuestos los usuarios, clientes y colaboradores que hagan uso del teletrabajo en la actualidad.

[77] Departamento Administrativo de Ciencias, Tecnología e Innovación- Colciencias. Tipo de Investigación [en línea]. Publicación Gestión de conocimiento. Colombia. 2020. [Fecha de consulta 16 mayo 2020]. Disponible en: https://www.funcionpublica.gov.co/web/eva/tipos-de-investigacion

[78] HERNÁNDEZ, R; FERNÁNDEZ, C y BAPTISTA, L. Metodología de la investigación. México: McGraw-Hill, 2016. p .252

6. FASES DEL PROYECTO

Las fases de este proyecto se muestran a continuación:

6.1. Fase 1. Análisis de los factores de riesgos informáticos en las organizaciones asociados al teletrabajo en la actualidad: en esta fase se procede al análisis de los riesgos, mediante las siguientes actividades:

6.1.3. Identificación de los riesgos existentes en el teletrabajo: en este ítem se detallan los 11 riesgos, entre los cuales se hará énfasis en la perdida de información, las pautas de seguridad para el software, sistemas operativos obsoletos, antivirus desactualizado, impacto de malware, falta de confidencialidad y gestión de seguridad de información deficiente

6.1.4. Estimación del riesgo informáticos en las organizaciones asociados al teletrabajo en la actualidad: se llevará a cabo la escala de probabilidades en los niveles: raro, improbable, posible, probable y casi seguro

6.1.5. Determinación del riesgo informáticos en una organización asociados al teletrabajo en la actualidad: en esta actividad se establecerá una escala de impacto del 1 al 20, en los niveles: insignificantes (≥1 y ≤4), menor (≥5 y ≤8), moderado (≥9 y ≤12), mayor (≥13 y ≤16) y catastrófico (≥17 y ≤20).

6.1.6. Determinación de la matriz de probabilidad-impacto de los riesgos informáticos de la organización asociados al teletrabajo en la actualidad: se hará una valoración de los riesgos de la seguridad de información de manera cualitativa, en la cual se comparará la probabilidad de ocurrencia y el impacto, y con esta información realizar una matriz de probabilidad-impacto, y se evaluarán el total de índice de riesgos de sistemas de información en las organizaciones asociadas al teletrabajo

6.2. Fase 2. Definición de las herramientas y técnicas disponibles para la seguridad de la información asociado al teletrabajo: en esta etapa del proyecto se debe considerar el análisis de los riesgos, a continuación, se muestran las actividades para la segunda fase:

6.2.3. Determinación de las herramientas necesarias para la seguridad de la información: se llevará a cabo una tabla en la que se ubicará las herramientas vs los riesgos, en lo cual se deberá interceptar los riesgos en el teletrabajo y la herramienta para contrarrestar: la vulnerabilidad y falta de confianza del sistema.

6.3. Fase 3. Elaborar la matriz de responsabilidades de perfiles de seguridad de la información en las organizaciones asociadas al

teletrabajo: se llevará a cabo una matriz que contemplará perfiles asociados al teletrabajo en la cual se caracterizará en función del: rol, conformación, responsabilidades, educación, formación, habilidad y experiencia.

6.3.3. Determinación de los roles necesarios para definir los perfiles asociados a la matriz de responsabilidad: se deberá evaluar los roles necesarios para: la alta dirección, director de seguridad de la información, comité de seguridad, personal con perfil de usuario, personal con acceso privilegiado: administradores de servidores y virtualización del sistema y Personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos

6.3.4. Determinación de la conformación para definir los perfiles asociados a la matriz de responsabilidad: se deberá evaluar características de la alta dirección, director de seguridad de la información, comité de seguridad, personal con perfil de usuario, personal con acceso privilegiado: administradores de servidores y virtualización del sistema y personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos para lograr la formación de los grupos informáticos que permitan contrarrestar las amenazas del sistema

6.3.5. Determinación de las responsabilidades para definir los perfiles asociados a la matriz de responsabilidad: se deberá evaluar las responsabilidades que deben poseer la alta dirección, director de seguridad de la información, comité de seguridad, personal con perfil de usuario, personal con acceso privilegiado: administradores de servidores y virtualización del sistema y personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos

6.3.6. Analizar los perfiles de los cargos: se definirán las características que deben poseer los cargos necesarios para: la alta dirección, director de seguridad de la información, comité de seguridad, personal con perfil de usuario, personal con acceso privilegiado: administradores de servidores y virtualización del sistema y Personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos, en función de la educación, formación, habilidad y experiencia.

6.4. Fase 4. Establecer el plan estratégico de seguridad de la información en las organizaciones asociada al teletrabajo: en esta fase se llevará a cabo un plan estratégico de seguridad como se muestra continuación:

6.4.3. Elaboración de plan estratégico de seguridad de la información: se realizará un plan que contempla la siguiente información: introducción, objetivo general, objetivos específicos, definiciones, normas, elementos de las políticas de la seguridad de la información en el teletrabajo, parámetros

para establecer políticas de seguridad de la información para teletrabajos y políticas del plan estratégico de seguridad en la información del teletrabajo

7. ANÁLISIS Y RESULTADOS

7.1. CAPITULO 1. Análisis de los factores de riesgos informáticos en las organizaciones asociados al teletrabajo en la actualidad.

7.1.1. Identificación del riesgo

Tabla 1 Identificación de los riesgos informáticos en la organización asociada actualmente al teletrabajo

ID	COD	RIESGO
1	R2	Cambio o pérdida de información debido a la falta de controladores de acceso físicos y lógicos para organizar el repositorio de información.
2	R3	Debido a la falta de control de acceso lógico en el repositorio de información contenido en el software del documento, la información es confusa.
3	R6	La falta de pautas de seguridad en el software ha provocado que los administradores pierdan la confidencialidad de la información contenida en las aplicaciones de gestión de documentos, que requieren que los administradores cambien sus contraseñas.
4	R11	Debido a una gestión de identidad insuficiente, los repositorios de información de seguridad, y el registro de acceso de los recursos de la organización se encuentran afectando la confidencialidad e integridad de la información de seguridad de la organización.
5	R12	Pérdida de información y daños en el servicio debido a un sistema operativo obsoleto y funciones antivirus en el servidor.
6	R13	La degradación del rendimiento físico causada por la inexistencia de un plan de mantenimiento preventivo destinado hacia la protección del hardware hace que la información alojada en el servidor sea inutilizable
7	R14	Tiempo inútil debido a la falta de disponibilidad de información y servicios debido a la configuración de seguridad en el servidor
8	R21	El antivirus desactualizado causa que se pierda parte o toda la información
9	R22	Las funciones antivirus obsoletas con el código malicioso causan daños en el hardware.
10	R23	El impacto de la presencia de malware en el funcionamiento de la red de la compañía.

11	R25	La falta de convenios confidenciales y resguardo de la propiedad intelectual, entre la empresa y los empleados directos, aprendices, profesionales y alianzas estratégicas, lo cual genera que la información confidencial de la organización sea robada o se pierda.

Fuente: Elaboración propia.

7.1.2. Estimación del riesgo informáticos en la organización asociados al teletrabajo en la actualidad.

En el análisis de los factores de riesgo informáticos, se considera la estimación del riesgo informático en la organización, en la que se evalúa la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias para obtener información para establecer el nivel de riesgo. Riesgos, prioridades de riesgo y estrategias de tratamiento, al evaluar los riesgos y prioridades, se debe considerar lo siguiente

Tabla 2 Escala de probabilidad de riesgos informáticos en una organización actualmente asociados al teletrabajo

Escala de probabilidad		
Nivel		Descripción
1	Raro	Acontecimiento que puede ocurrir sólo en situaciones excepcionales, entre 0 y 1 vez en un semestre
2	Improbable	Acontecimiento que puede ocurrir en pocos escenarios, entre 2 y 5 veces en un semestre.
3	Posible	Acontecimiento que puede ocurrir entre 6 y 10 veces en un semestre.
4	Probable	Evento que puede ocurrir entre 15 veces en un semestre.
5	Casi seguro	Acontecimiento que puede ocurrir en algunos contextos más de 15 veces en un semestre.

Fuente: Elaboración propia.

7.1.3. Determinación del riesgo informáticos en una organización asociados al teletrabajo en la actualidad

Para el análisis de los factores de riesgos informático, se considera la escala de impacto, se la cual se posicionan los riesgos en los diferentes niveles desde el insignificante hasta el catastrófico en las escalas del 1 al 20, con la finalidad de obtener información acerca de las consecuencias a las que puede incurrir el riesgo y los efectos que puede contraer, como se muestra a continuación:

Tabla 3 Escala de impacto de riesgos informáticos en una organización en la actualidad asociaos al teletrabajo

Valor de impacto			
Nivel		Descripción	Escala
1	Insignificante	R2	≥1 y ≤4
2	Menor	R3, R13	≥5 y ≤8
3	Moderado	R12, R22; R23	≥9 y ≤12
4	Mayor	R11; R14; R21	≥13 y ≤16
5	Catastrófico	R6; R25	≥17 y ≤20

Fuente: Elaboración propia.

Entre las consecuencias que se pueden tener en cuenta se encuentran: pérdidas financieras, costes de reparación, interrupción del servicio, disminución de rendimiento, infracciones legales, perdidas de ventajas competitivas, daños personales, por lo cual resulta importante medir y controlar estas variables, dado el gran impacto al que puede incurrir el negocio.

7.1.4. Determinación de la matriz de probabilidad-impacto de los riesgos informáticos de la organización asociados al teletrabajo en la actualidad

La valoración de los riesgos de información se hace de manera cualitativa, en la cual se compara la probabilidad de ocurrencia y el impacto, lo cual conlleva a la obtención de una matriz de probabilidad-impacto, en la cual se califican los riesgos con los niveles de impacto y probabilidad establecidos como zonas de riesgo, lo cual permitirá generar posibles soluciones:

Tabla 4 Matriz probabilidad-impacto de los riesgos informáticos en una organización en la actualidad asociados al teletrabajo

Impacto	Valor	Evaluación				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	Probabilidad	Raro	Improbable	Posible	Probable	Casi seguro

Fuente: Elaboración propia.

Con respecto al análisis de los datos obtenidos anteriormente, se determina que mediante una matriz de impacto probabilístico se puede evaluar el riesgo y detectar el grado de riesgo que pueden soportar las organizaciones dedicadas al teletrabajo, en función de la probabilidad de ocurrencia: raro, improbable, posible, probable, y

casi seguro y el impacto que puede generar: catastrófico, mayor, moderado, menor, e insignificante. La matriz de riesgo es una herramienta que muestra áreas de riesgo y facilita el análisis gráfico. Puede realizar un análisis global del riesgo y de acuerdo con el área de riesgo (área de bajo riesgo, Medio, alto o extremo) para promover el enfoque de las decisiones de tratamiento organizacional y la implementación de planes de acción. Las áreas de riesgo se distinguen por colores y números de área, de la siguiente manera:

-Zonas de riesgos.
B: Zona de riesgo baja (color verde) 5 zonas siendo la Z-5 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 4 zonas siendo la Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 8 zonas siendo la Z-17 la de mayor riesgo
E: Zona de riesgo extrema (color vino tinto) 8 zonas siendo la Z-25 la de más alto riesgo

Por lo cual, se ubica los riesgos según la zona:

- Zona de riesgo baja: Caos causado por la falta de control de acceso lógico al repositorio lógico de información contenida en el software del documento (2,3), pérdida de información y servicios afectados por sistemas operativos obsoletos y software antivirus (3,1) en el servidor
- Zona de riesgo moderado: Cambios o pérdida de información debido a la falta de controladores de acceso físicos y lógicos para organizar el repositorio de información (1,5), padecimiento de la información alojada en los servidores por deterioro físico causado por la ausencia de planes de mantenimiento preventivo sobre el hardware
- 2.4) y daños a la operación de la red de la compañía debido a la presencia de malware. (3,3)
- Zona de riesgo alta: debido a la falta de pautas de seguridad requeridas por el administrador para cambiar la contraseña de los nuevos usuarios en el software, la información contenida en la aplicación de gestión de documentos ha perdido la confidencialidad (5,3). Debido a la gestión de identidad insuficiente, los recursos de la organización y el repositorio de información Control de acceso (4,3), pérdida parcial o completa de información debido a información desactualizada y / o faltante, lo que resulta en la confidencialidad e integridad de la información (4,3) y daños en el hardware antivirus (3,5) desactualizados causados por código malicioso
- Zona de riesgo extrema: tiempo inútil debido a información y servicios no disponibles debido a la configuración de seguridad en el servidor. (4,4) y el robo y / o pérdida de información confidencial de la organización debido a la falta de acuerdos confidenciales y protección de la propiedad intelectual entre la empresa y sus empleados directos, aprendices, profesionales y alianzas estratégicas (5,4)

Tabla 5 Evaluación total del índice de riesgos del sistema de información en las organizaciones asociadas al teletrabajo

	Evaluación				
Descripción	Zona de riesgo baja	Zona de riesgo moderada	Zona de riesgo alta	Zona de riesgo extremo	Total
R3	6	0	0	0	6
R12	3	0	0	0	3
R2	0	5	0	0	5
R13	0	8	0	0	8
R23	0	9	0	0	9
R6	0	0	15	0	15
R11	0	0	12	0	12
R21	0	0	12	0	12
R22	0	0	15	0	15
R14	0	0	0	16	16
R25	0	0	0	16	16

Fuente: Elaboración propia.

Figura 1 Riesgos de las organizaciones asociadas al teletrabajo

Como resultado, en la evaluación, en términos de otros factores, R3, R13, R6, R22, R14 y R15 tienen una mayor probabilidad de ocurrencia, por lo que se deben tomar medidas para atacar, y esto no significa pérdida o pérdida económica. Fiabilidad de organizaciones con entidades de oficinas remotas. Sin embargo, el resto de los

factores son muy riesgosos y representan acciones correctivas que pueden evitar problemas con los propietarios, clientes y organizaciones del sistema.

7.2. CAPITULO 2. Definición de las herramientas y técnicas disponibles para la seguridad de la información asociado al teletrabajo.

Las herramientas y tecnologías de seguridad están diseñadas para controlar el acceso a la red, proteger los flujos de información confidencial y prevenir ataques maliciosos contra los sistemas de telecomunicaciones. Algunas de estas herramientas son software antivirus, capacitación especializada en capital humano, diseminar buenas prácticas de seguridad, aumentar la conciencia del capital humano y observar buenas Modelo de prácticas de seguridad de la información, pruebas de penetración (pentest), sistema de correlación de eventos, filtración de contenido web, IPS, movile device managment, autenticación con sistemas biométricos, cifrado de archivos, control de acceso (password), políticas, lineamientos de seguridad, buenas prácticas de desarrollo de software, HTTPS par sitios web, firmas electrónicas/PKI. Monitoreo de redes, respaldo de información, seguridad perimetral, análisis de vulnerabilidad, Gateway anti-spam, software antimalware y redes privadas virtuales. De las cuales se contemplan en las organizaciones asociadas al teletrabajo, de acuerdo a los riesgos a los que se encuentra expuesta este tipo de empresa.

Tabla 6 Herramientas y/o técnicas disponibles para la seguridad de la información asociado al teletrabajo

Herramientas y/o técnicas disponibles para la seguridad de la información asociado al teletrabajo											
	R3	R12	R2	R13	R23	R6	R11	R21	R22	R14	R25
Antivirus/ antimalware		X		X	X	X	X	X	X		
Firewall/ equipo perimetral			X			X			X		
Control de acceso	X		X			X	X				X
Cifrado de datos		X	X					X			X
Respaldo Información		X	X		X			X			X
Redes privadas virtuales						X	X		X		

Filtrado de contenido						X				X	X
IPS						X	X		X		

Fuente: Elaboración propia.

Los riesgos que requieren controles de acceso, son los R3, R2, R6, R11 y R25 estos controles pueden implementarse en el sistema operativo sobre la base de dato de aplicaciones especializadas, Microsoft Office, LibreOffice, GoogleDocs, Gmail, Yahoo, Hotmail, Disco duro, Google Drive o Dropbox, Yahoo Messenger, Skype, WhatsApp, Line, telegram, scanner, webcam. Mientras que los riesgos de tipo R12, R13, R23, R6, R11, R21 y R22, lo más recomendable se puede hacer uso de antivirus/antimalware, sin embargo, en cuanto al firewall/equipo perimetral en los teletrabajos, permite inspeccionar el acceso a la red del ordenador, lo cual resulta importante para contrarrestar los riesgos R2, R6 y R22, por medio de la protección de la información que guardan los ordenadores bloqueando los ataque ante posibles intrusos.

Otras de las herramientas disponibles para la seguridad de la información disponible para llevar a cabo los teletrabajos, es el cifrado de datos, mediante el acceso a la información si se utiliza la contraseña o código que establezca la empresa, lo cual permitirá reducir o eliminar R12, R2, R21, y 25. Y en cuanto al respaldo de la información, las organizaciones de teletrabajo en busca de ahorrar tiempo, dinero y requerir mayor cantidad de almacenamiento, han incurrido a respaldos en nube que no representan el 100% de la confiabilidad del sistema, lo cual conllevo al desencadenamiento de los siguientes riesgos R12, R2, R23, R21 y R25, por lo cual, resulta imprescindible al momento de adaptar esta herramienta al teletrabajo, para disponer de una gran capacidad de almacenamiento y hacer respaldos seguros de la información, para lograr una sincronización efectiva.

Así mismo, usar redes privadas virtuales para llevar a cabo el teletrabajo, resulta una tecnología para conectar varias computadoras a una red privada por internet, pero también incurre a la generación de riesgos como el R6, R11, y R22, por lo cual, representa un medio, que utiliza las organizaciones para dar acceso a sus empleados a la información y archivos por vías remotas. Por lo tanto, para corregir los errores mencionados anteriormente, y utilizar a los VPN como herramienta, se debe agregar una nueva red con los datos de la organización, y al proporcionar los datos de inicio de sesión, se genere una alerta a la organización para detectar cualquier situación irregular, en cuanto a la respuesta de la información.

Con respecto, a los errores R6, R14, y R25, por lo cual, se hace uso de la herramienta mediante filtrado de contenido, en la que en un directorio se ubican dispositivos que pueden acceder y controlar el uso de la red corporativa, por lo cual lo recomendable se ubica en la asignación de un código para identificar en la red sólo a los que cumplan con estos lineamientos. Y en cuanto a los riesgos R6, R11

y R22, se recomienda los IPS, lo cual permitirá monitorear acciones a nivel de capa 3 (red) y nivel de capa 7 (aplicaciones), con el propósito de conocer el comportamiento de archivos sospechosos e indebidos, y generar una respuesta oportuna antes de generar un daño mayor al sistema o alguna pérdida de información importante.

Por lo cual, se obtuvo como resultado de este objetivo, que los riesgos que cuentan con más herramientas para disminuir el riesgo a los cuales se encuentra la información, como en el caso de R6, el cual se puede contrarrestar con el uso de antivirus, firewall, control de acceso, VPN, IPS, y filtro de contenido, Los riesgos R2, R11, R22, y R25, cuentan con 4 herramientas, los riesgos R12 y R21 cuenta con respaldo de la información, antivirus y cifrado de datos, el R23 cuenta con el antivirus y respaldo de información como la herramienta de seguridad, y R3, R13, R14 solo cuenta con una herramienta cada uno entre los cuales se encuentran: control de acceso, antivirus y filtrado de información. Por lo cual, los R23, R3, R13 y R14 son los más expuestos, dado que cuenta con la menor cantidad de herramientas para generar confiabilidad a los datos de los usuarios y de las empresas.

7.3. CAPITULO 3. Elaboración de la matriz de responsabilidades de perfiles de seguridad de información en las organizaciones asociadas al teletrabajo.

Tabla 7 Matriz de responsabilidades de perfiles de seguridad en las organizaciones

				Perfil de cargo			
Ítem	Rol	Conformación	Responsabilidades	Educación	Formación	Habilidad	Experiencia
1	Alta dirección	Equipo de inversionistas	-Especificar políticas de la seguridad de la información	N/A	N/A	N/A	N/A
2	Director de seguridad de la información	Ejercido por un profesional en ingeniería de sistemas especializado en seguridad de la información	-Establecer normativas de seguridad y garantizar el fiel cumplimiento. -Propuestas en materia del mejoramiento de la seguridad de información a la alta dirección. -Conseguir resultados de la gestión de segur	Educación universitaria	-Capacitación en prevención y recuperación ante posibles amenazas a los sistemas de información en el desarrollo del teletrabajo -Conocimiento en los sistemas de información y telecomunicaciones de las empresas asociadas al teletrabajo.	-Habilidades de relaciones interpersonales -Liderazgo ante los equipos de trabajo -Capacidad de solventar problemas ante amenazas de perdida de información o extracción de información de las bases de datos de la empresa. -Estratega ante la presentación de información a la alta dirección de proyectos enfocados	4 años de experiencia

						en la seguridad de la información	

Fuente: Elaboración propia.

Tabla 8 Matriz de responsabilidades de perfiles de seguridad de información en las organizaciones asociadas al teletrabajo (continuación)

				Perfil de cargo			
Ítem	Rol	Conformación	Responsabilidades	Educación	Formación	Habilidad	Experiencia
3	Comité de seguridad	Equipo de comité de seguridad de la información (4 integrantes)	-Asegurar el cumplimiento de la normativa vigente de todos los colaboradores del teletrabajo -Establecer objetivos claros dentro del plan de seguridad de la información en donde se requiere que los colaboradores adquieran un compromiso en función de la misión y visión de la empresa en la que prevalezca la confiabilidad y resguardo de la información -Exige el fiel cumplimiento de las políticas y normas establecidas en función	Educación universitaria	-Resolución de conflictos en ambientes laborales -Capacidad para manejar y capacitar al personal ubicado en distintas entidades geográficas -Conocimiento en auditoria internas y externas de los sistemas de información asociados al teletrabajo.	-Capacidad para resolver fallas en el sistema e interfiere en el correcto desarrollo del teletrabajo -Generar la documentación pertinente mediante procedimientos y diagramas para accionar en caso de algún incidente de seguridad -Resolver diferencias que se puedan generar entre los diferentes departamentos en cuanto a la	5 años o más de experiencia

			de la seguridad de la información en el teletrabajo			seguridad de la información	

Fuente: Elaboración propia.

Tabla 9 Matriz de responsabilidades de perfiles de seguridad de información en las organizaciones asociadas al teletrabajo (continuación)

				Perfil de cargo			
Ítem	Rol	Conformación	Responsabilidades	Educación	Formación	Habilidad	Experiencia
4	Personal con perfil de usuario	Personal de seguridad de confianza (2 integrantes)	-Encargado de la visualización y el seguimiento de las políticas de seguridad correspondiente al teletrabajo- -Garantizar la seguridad de la información bajo un acto de confidencialidad hacia la organización. -Verificar que los sistemas de información, mediante los sistemas operativos, la transferencia de información se haga de manera correcto y en caso de observar alguna situación irregular, el deber del personal con perfil de usuario es	Educación Universitaria/técnica	-Detención de anomalías en los sistemas de información -Políticas de seguridad de las organizaciones asociadas al teletrabajo -Habilidades comunicación a nivel gerencia y operativa.	-Capacidad de resguardo de información -Demostración de capacidades de concentración ante largas jornadas laborales en observación dado que el descuido de algunos minutos puede representar un gran problema. -	3 años de experiencia

			notificar al comité de seguridad o directamente al gerente de seguridad para tomar las medidas necesarias.				

Fuente: Elaboración propia.

Tabla 10 Matriz de responsabilidades de perfiles de seguridad de la información en las organizaciones asociadas al teletrabajo (continuación)

				Perfil de cargo			
Ítem	Rol	Conformación	Responsabilidades	Educación	Formación	Habilidad	Experiencia
5	Personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos	Personal administrativo de seguridad de la información (1 integrante)	-Representa la persona encargada del análisis de riesgo de la situación actual de los sistemas de información del teletrabajo -Presentar cada 3 meses informes al gerente de seguridad de la información acerca de los inconvenientes que se han presentado en ese periodo, los sistemas que se encontraron más expuestos, las medidas efectivas que se aplicaron, el porcentaje de confiabilidad que ofrecieron al usuario y a	Educación universitaria /técnico	-Excelente manejo e interpretación de documentación de sistemas de seguridad de la información en función de las actividades desarrolladas en el teletrabajo -Capacidad en auditorias técnicas necesarias en los sistemas de información para el teletrabajo -Experticia en hardware y software, considerando que	-Garantizar la confiabilidad de los sistemas de información que influyen directamente en la imagen corporativa de la empresa. -Detectar los inconvenientes por medio de auditorías para la implementación de mejoras, y certificaciones para desarrollar sistemas más seguros tanto para la empresa (en función de	5 años de experiencia.

			la organización, la transferencia de información de forma correcta y sin intrusos en las actividades asociadas al teletrabajo.		el uso de este elemento no considere un riesgo a la seguridad de la información	pérdida de información) como el usuario (en función de perdida de datos importantes)	

Fuente: Elaboración propia.

Tabla 11 Matriz de responsabilidades de perfiles de seguridad de la información en las organizaciones asociada al teletrabajo (continuación)

				Perfil de cargo			
Ítem	Rol	Conformación	Responsabilidades	Educación	Formación	Habilidad	Experiencia
6	Personal con acceso privilegiado: Administradores de servidores y virtualización del sistema.	Personal administrativo de seguridad de la información (2 integrantes)	-Implementar medidas de seguridad a los sistemas de seguridad asociados con el teletrabajo -Inspeccionar el uso correcto de las herramientas disponibles para la seguridad de la información en función del análisis de los riesgos a los cuales se encuentra expuesto los sistemas asociados a teletrabajo -	Educación universitaria/ técnico	-Servidores actuales utilizados en el teletrabajo -Detectar la incompatibilidad de hardware con equipos de sistema de información. -Manejo de cuentas de los funcionarios y usuarios en general -Manejo de políticas de seguridad en función de la detención de	-Planificación, generar soporte y mantenimiento del sistema de información asociadas al teletrabajo -Generara una respuesta oportuna al usuario cuando lo requiera -Inspección y seguimiento del sistema de información de los usuarios y funcionario del teletrabajo	4 años de experiencia

					claves débiles o claves aceptables para acceder al sistema de información del teletrabajo.		

Fuente: Elaboración propia.

7.4. CAPITULO 4. Establecimiento del plan estratégico de seguridad de la información del teletrabajo en las organizaciones.

	Rev.0
	PLAN001

Plan estratégico de seguridad de la información de la organización asociada al teletrabajo

Octubre 2020

Índice

Plan estratégico de seguridad de la información del teletrabajo en las organizaciones

1. Introducción

En la actualidad, la tecnología genera una cantidad de avance importante a grandes velocidades, por lo cual muchas veces se escapa de las manos de los funcionarios o colaboradores de detectar los cambios, lo cual conlleva a la generación de fallas informáticas, y sistemas en los cuales se pierde la confianza, dado que los usuarios presentan renuencia en ingresar datos ya consideran que el sistema no respaldará de forma segura la información. Por lo cual la sociedad actual, no solo pide mayores índices de seguridad en cuanto a los datos personales y la información confidencial que implica finanzas, sino los profesionales están generando en muchas partes del mundo nuevas modalidades de trabajos, los cuales se pueden llevar mediante los sistemas tecnológicos de información avanzados, por lo cual, hoy en el día, se puede migrar de la modalidad del trabajo convencional al trabajo remoto mediante la modalidad del teletrabajo y las empresas han logrado adaptarse a estas, sin embargo, se debe evaluar que las empresas se encuentran en el desarrollo de estrategias para garantizar que las conexiones se realicen de forma segura, que la transferencia de datos pase por un antivirus eficiente que pueda evitar los ataques hardware, y así evitar la extracción de información confidencial de la organización mediante la generación de firewall, cifrado de información, respaldo de información y otra herramientas que permitan garantizar la seguridad de la información. Este proyecto se trata de una cooperación entre los responsables de la seguridad de la información mediante la auditoria, detecciones inmediatas de situaciones sospechosas y monitoreo del sistema, las inversiones en tecnología que puede llevar a cabo directiva de la organización, y el usuario.

2. Objetivo

- Implementar políticas de seguridad necesarias para el desarrollo del teletrabajo

3. Objetivos específicos

- Identificación de los elementos de una política de seguridad informática del teletrabajo
- Determinación de parámetro para establecer políticas de seguridad en el teletrabajo.

Plan estratégico de seguridad de la información del teletrabajo en las organizaciones

4. Definiciones:

- Riesgos: son todas las contingencias, incertidumbre o probabilidad de que ocurra algún percance o daño inminente.
- Teletrabajo: es el trabajo realizado fuera de la empresa o entidad laboral utilizando las redes de telecomunicación cumpliendo con las responsabilidades a su cargo
- Parámetros: son los datos variable o factores que al estar asociados a un grupo de elementos permiten ser identificados a través de su valor numérico
- Elementos: son todos los componentes que constituyen un conjunto
- Políticas de seguridad de sistemas de información: son todas las reglas que deben de ser cumplidas y respetadas antes de poder tener acceso a la información en un sistema, las cuales deben ser continuamente actualizadas velando por la mejoría de las mismas y son desarrolladas con la finalidad de proteger la integridad, confidencialidad e información de una empresa.
- Plan estratégico: es el trazado cuantitativo, descriptivo y temporal, de los objetivos principales, acciones a tomar para conseguirlos y proyección temporal del cumplimiento de los mismos en una empresa
- Política: directrices que definen el modo de actuar de una persona en un asunto o área específica.
- Confidencialidad: acuerdo entre dos o más partes de que se mantendrá reservado todo lo dicho, escuchado y hecho.

5. Normas

Norma ISO 27001:2013 “Gestión de la seguridad de la información”
Norma ISO 27002:2013 “Information technology. Security techniques. Code of practice for information security management”

6. Tiempo de implementación propuesta:

6 meses

7. Características que deben desarrollar las organizaciones asociadas al teletrabajo

A continuación, se presentan las características necesarias requeridas para el plan estratégico, con la finalidad de reducir las amenazas en los sistemas de seguridad relacionado al teletrabajo:

- La organización deberá exigir a los responsables de la seguridad de la información, establecer contraseñas seguras, que incluya caracteres y condiciones especiales, por un tiempo definido (cada 2 meses), permitiendo

generar mayor confiabilidad en el acceso a los sistemas de seguridad de la empresa.

- Dentro de la normativa legal de la empresa se deberá indicar las multas ante posibles infracciones, vinculadas a la transferencia de información sin previa autorización o acceso a los portales con información confidencial de la organización asociada al teletrabajo sin autorización.
- La empresa debe instaurar un plan de mantenimiento y actualización a los ordenadores y hardware que permiten el desarrollo del trabajo, para garantizar la inexistencia de virus, troyanos o gusanos, donde se detecte las condiciones del antivirus para la descarga de correo no deseados, y la recepción de links, lo cuales pudieran resultar el medio de amenaza para el desarrollo del teletrabajo. Por consiguiente, deberá proporcionar equipos en buenas condiciones y la capacidad requerida para el desarrollo de las labores que permita las actualizaciones correspondientes del software y algunos programas.
- Las organizaciones asociadas al teletrabajo deberán desarrollar programas basados en contrarrestar las amenazas a los sistemas considerando los factores asociados a los actos maliciosos (fase 1), factor humano (fase 2) y desastres naturales (fase 3), dado que se debe contar con procedimientos de acción hacia la presencia de alguno de los 3 factores mencionados anteriormente.
- La empresa asociada al teletrabajo, deberán poseer un sistema de gestión de seguridad de la información que contenga: definir la política, alcance, análisis de los riesgos, gestión de riesgos, selección de los controles a implementar, declaración de la aplicabilidad y revisión del sistema.
- La organización deberá implementar la ISO 27001:2013 en el apartado “las políticas y medidas de seguridad para proteger la información accesible, procesada o almacenada en los sitios de teletrabajo, con el uso de estándar de seguridad de los dispositivos móviles dado que genera la garantía de continuidad del negocio”

8. Elementos de las políticas de la seguridad de la información en el teletrabajo

- Objetivos

Establecer elementos que permitan la protección de la información para los usuarios y colaboradores en la modalidad de teletrabajo, mediante la generación de garantía de respaldo de información y confiabilidad del sistema.

- Requerimientos mínimos:

-Inspección de la documentación y procedimientos para el desarrollo del plan estratégico mediante las políticas de seguridad.

-Garantizar la confiabilidad de la información de los interesados

-Garantizar la propuesta de nuevas tecnologías en función de las políticas de seguridad y la proyección de la organización asociada al teletrabajo.

- Definición de reglamentos por incumplir políticas de seguridad de la información:

9. Parámetros para establecer políticas de seguridad de la información para teletrabajos

- Realizar un análisis de riesgos en donde se evalué la probabilidad de ocurrencia y el impacto que puede generar, y en función de las variables anteriormente señaladas definir la matriz de impacto-probabilidad lo cual permitirá atacar de una forma eficiente la vulnerabilidad del teletrabajo
- Establecer encuentros mensuales de los encargados del departamento, en el cual el comité lidere y genere una visualización de los temas críticos de la organización
- Informar al personal general acerca de las políticas de seguridad de la organización, así mismo, de la detención de vulnerabilidades, lanzamiento de nuevos softwares, problemáticas con algunos hardware y la lluvia de ideas acerca de prácticas de mejoras para la garantía de la seguridad de la información
- Establecer al profesional responsable de cada departamento de seguridad el cual debe garantizar el respaldo y cifrado de la información que corresponde a la organización
- Involucrar las ideas del personal en general para el desarrollo de los procedimientos y genere actualizaciones paulatinas de las políticas de seguridad de la información en el teletrabajo.

10. Políticas del plan estratégico de seguridad en la información del teletrabajo

P1: Elaboración del plan estratégico de seguridad de la información
P2: Implementar capacitación del personal mensual, en cuanto a la seguridad de la información para los funcionarios, responsables de seguridad en la empresa, asignados en diferentes entidades geográficas y al usuario.
P3: Establecer un análisis de riesgos por puestos de trabajos, en la que cada usuario y operador consideren los posibles riesgos a los cuales se encuentra expuesto
P4: Exigir a los encargados de la auditoria de la seguridad de la información, el desarrollo de un software que permita que entes externos puedan hacer un sistema de auditoria y garantizar la confiabilidad de la organización
P5: Garantizar las buenas prácticas en el desarrollo de los sistemas de información de seguridad en el teletrabajo
P6: Instaurar unidades que permitan generar una gestión de auditoria de las redes que utilizan los usuarios del teletrabajo.
P7: Denegado el acceso a redes sociales de los colaboradores dado que representa un medio para el intercambio de información de seguridad de los interesados

P8: Las organizaciones asociadas al teletrabajo generará usuarios y claves no débiles lo cual permitirá controlar la conexión mediante una decodificación, de lo contrario, el sistema no permitirá el acceso a la información

P9: Las conexiones por teletrabajo, deben realizarse fuera de la infraestructura tecnológica y bajo el uso de las herramientas disponibles de seguridad, para evitar vulnerabilidades.

P10: Informar a los responsables de la seguridad de la actualización de software y de hardware en malas condiciones o infectados, dado que representan una amenaza para el sistema del teletrabajo.

8. CONCLUSIONES

- En cuanto al análisis de los factores de riesgos informáticos en las organizaciones, se obtuvo que un 36,36% de los factores se ubican zona riego alta, y posteriormente la zona de riesgo moderado que representa un 27,27%, mientras que en la zona de riesgo baja y la zona de riesgo extremo se ubica el 18, 18% cada zona, lo cual incurre directamente en el robo de información debido a la falta de acuerdos confidenciales y protección de la información de seguridad del personal que labora en la modalidad del teletrabajo, por lo cual se considera importante la capacitación del personal y el valor de la confiabilidad, dada la vulnerabilidad que representa el mal uso de la información, ya que afecta la imagen corporativa organizacional, datos del usuarios e información de colaboradores.
- De acuerdo a las herramientas disponibles para la seguridad de la información, resulta recomendado el control de acceso, herramienta que se usa para contrarrestar amenazas como lo son R3, R2, R6, R11y R25, sin embargo, para uso de redes, interacciones digitales y transferencia de archivos se hace uso de antivirus/antimalware para riesgos de tipo R13, R23, R6, R11, R21 y R22, para los riesgos R2, R6 y R22,el firewall representa una excelente herramienta, en cuanto a los riesgos R12, R2, R21, y R25, se debe hacer uso del cifrado de información para contrapesar la vulnerabilidad del sistema, el respaldo de información representa la herramienta más utilizada para R12, R2, R23, R21 y R25 eliminar amenazas, y generar mayor confiabilidad de los usuarios, en cuanto a los riesgos R6, R14, y R25, mediante el filtrado de contenido se permite identificar en la red sólo a los que cumplan con estos lineamientos, aunque en lo que respecta al VPN resulta una instrumento que genera una alerta de los riegos R6, R11, y R22, e IPS mediante el uso de esta, se pude monitorear acciones a nivel de capa para conocer el comportamiento de intrusos.
- La matriz de responsabilidades cuenta con 6 directrices: alta dirección, gerente de seguridad de la información, personal con acceso privilegiado: Administradores de servidores y virtualización del sistema, personal con acceso privilegiado: administrador de puesto de trabajo y sistemas corporativos, comité de seguridad y personal con perfil de usuario, los cuales se encuentran enfocados en el cumplimiento de las políticas de seguridad de la información, mediante la capacitación de personal especializado, establecimiento de capacidades en función del departamento, roles y responsabilidad, desarrollo de valores de integridad, confiablidad y resguardo de la información dentro de la organización asociada a teletrabajo, detectando que se requiere de lazos de comunicación en todos los estratos organizacionales y de suma importancia la formación profesional y técnica de los encargados, para solventar algún tipo de irregularidad en los sistemas.
- El plan de estrategias se basó en el desarrollo de políticas de seguridad de información para el teletrabajo, en donde se definen los objetivos que se

pretenden alcanzar con el plan estratégico, mediante la identificación de los elementos y el establecimiento de parámetros de seguridad, lo cual permitirá obtener mejores resultados en el desarrollo de los teletrabajo, así mismo, se propone la implementación en un lapso de 6 meses, mediante el cual se logrará minimizar amenazas, la vulnerabilidad del sistema y generar mayor índice de confiabilidad hacia el usuarios y mantener una imagen organización aceptable.

9. RECOMENDACIONES

1. La empresa debe contar con el conocimiento de la totalidad de sus activos, con lo cual se facilita la labor para la creación de planes estratégicos para tener respuestas eficientes a los incidentes de seguridad informáticos.
2. La empresa debe contar con una correcta clasificación de la información en orden de importancia y entro de esa clasificación poder determinar que datos se pueden migrar, transmitir y así para determinar su nivel de criticidad.
3. Las empresas deben contar con un perfil profesional y especializado en seguridad informática y su personal técnico debe tener conocimientos en esa área, de no ser así, la comprensión y manejo de las amenazas y vulnerabilidades de la información llevará a la toma de malas decisiones pues no será posible medir el riesgo.
4. El personal responsable del área de seguridad de la información debe tener la perseverancia necesaria para el monitoreo y/o seguimiento a las posibles anomalías y así mismo, deberá estar actualizando sus conocimientos, los cuales, se estarán aplicando casi que, de manera permanente, pues las amenazas y riesgos viven en un continuo cambio y por ende también evolucionan los ataques. De no ser así, por más que la empresa cuente con los mejores equipos, software, cortafuegos y/o antivirus, sino cuenta con el personal especializado para manejar todos estos elementos, se puede concluir que la inversión que haga la empresa en este sentido, no va a ser eficiente lo que generaría que los activos y procesos queden en alto riesgo.
5. Es imprescindible que dentro del personal idóneo se cuente con un especialista en seguridad informática, ya que este ROL se confunde con el administrador de sistema que por regla general en muchas empresas es un ingeniero de sistemas. Así mismo, es importante que contando con el profesional de eventos de seguridad “Especialista en seguridad informática” también la empresa cuente con el hardware y software actualizados y de calidad, pues si bien la empresa puede contar con el personal idóneo y no tiene la estructura necesaria y actualizada en el tiempo, el trabajo que se llegase a realizar y el tiempo de respuesta ante vulnerabilidades y ataques, no será eficaz.
6. Realizar auditorías esporádicas con la finalidad de verificar activos, procesos y personal idóneo y no cuando sea requerido por una entidad foránea y/o para una certificación.
7. Implementar herramientas SaaS con el fin de disminuir la carga en los puntos finales de VPN.

10. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de riesgos y estrategias de seguridad de la información del teletrabajo en las organización, puedan acceder al documento.

11. BIBLIOGRAFÍA

ABAD PARRALES, Wagner, *et al*. La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. México: 3 ciencias, 2019, p. 65. ISBN 978-84-121167-6-2

AGUILAR QUINTERO, Norly Alejandra. Modelo de seguridad de la información para instituciones de educación superior. Proyecto de maestría 2019.Universidad Francisco de Paula Santander Ocaña. Facultad de ingeniería. Ocaña, Colombia.

ALEMÁN NOVOA, Helena y RODRIGUEZ BARRERA, Claudia Metodologías para el análisis de riesgos en los SGSi. Publicación de investigación. 2015. Fundación universitarias Juan de Castellanos. Facultad de ingeniería. Boyacá, Colombia.

AMRITA, M y AKHILESH, K Operations Management of Cyber-Physical Production Systems. En: Akhilesh K., Möller D. Singapur: Smart Technologies, 2020. p. 137-145.

ANGARITA PINZÓN, Cristian y GUZMÁN FLÓREZ, Camilo. Protocolos de Mitigación de Ciberataques En El Hogar. Caso de Estudio: Estratos 3 y 4 de La Ciudad de Bogotá [en línea]. Proyecto de Trabajo de Grado. Universidad Católica de Colombia, 2017 [consultado 10 mayo 2020]. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf

ASENCIO-GUILLÉN, Antonio y NAVÍO-MARCO, Julio. El Ciberespacio Como Sistema y Entorno Social: Una Propuesta Teórica a Partir de Niklas Luhmann [en línea]. Pamplona: Commnication & Society, 2018. [Fecha de consulta 11 de mayo 2020]. Disponible en https://search.proquest.com/openview/2a80c2a19a2f9ac9b341136efd1a54bc/1?pq-origsite=gscholar&cbl=1216381

BALBOA ROMERO, José. Ransomware, Hacking y Phising: Conducta Típica Del Delito de Daños Informáticos [en línea]. Tesis de pregrado. Universidad Internacional de la Rioja, 2018 [consultado 15 de mayo 2020]. Disponible en https://reunir.unir.net/bitstream/handle/123456789/6929/BALBOA%20ROMERO%2c%20FRANCISCO%20JOS%c3%89.pdf?sequence=1&isAllowed=y

BALLESTERO, Fernando. La Ciberseguridad En Tiempos Difíciles. *Boletín Económico de ICE*. 2020, no. 3122, pp. 39-48. ISSN 0214-8307

CAJUSOL TORRES, Lieth del Carmen, Diseño de un sistema de gestion de seguridad de información basado en la norma ISO/IEC 27001:2013 para la

producción y comercialización de comsumo masivo. 2020 Tesis de pregrado. Lima. Perú.

CASTRAÑON DELGADO, Ernesto. Sistemas de control de acceso alternativo a passwords.[en línea]. Trabajo especial de grado 2012 [consultado 10 mayo 2020]. Disponible en http:// oa.upm.es>PFC_ERNESTO…PDF Sistemas de control de acceso alternativos a passwords-Archivo DIGITAL UPM-Universidad…

CASTRO MARQUEZ, Deisy. Modelo de Integración de Estándares de Buenas Prácticas de Tecnologías de La Información En El Gobierno Coporativo de Las Empresas Colombianas En El Sector Asegurador [en línea]. Tesis de Maestría. Universidad Francisco de Paula Santander Ocaña, 2020 [consultado 10 mayo 2020]. Disponible en http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/2761?mode=full&submit_simple=Show+full+item+record

CHINEA, Jorge. Tipos de herramientas básicas para garantizar la ciberseguridad en la empresa. 2014 artículo de investigación. INSTITUTO NACIONAL DE CIBERSEGURIDAD. España.

Ciberseguridad y Ethical Hacking: La Importancia de Proteger Los Datos Del Usuario [en línea]. Cartagena de Indias: Revista de 2º congreso Latinoamericano de Ingeniería, 2019. [Fecha de consulta: 10 mayo 2020]. Disponible en: https://acofipapers.org/index.php/eiei2019/2019/paper/viewFile/3634/1221

CRISTIAN LUGA, Jason y EROLA, Arnau. Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks [en línea]. Oxford: Human-Centric Computing and Information Sciences, 2016. [Fecha de consulta 16 mayo 2020]. Disponible en https://link.springer.com/content/pdf/10.1186/s13673-016-0065-2.pdf

CUJABANTE VILLAMIL, Ximena *et. al*. Ciberseguridad y Ciberdefensa En Colombia: Un Posible Modelo a Seguir En Las Relaciones Cívico-Militares [en línea]. Bogotá: Seguridad y Defensa, 2020 [consultado 17 mayo 2020]. Disponible en https://revistacientificaesmic.com/index.php/esmic/article/view/588

Departamento Administrativo de la Función Pública. Ley 1273 de 2009 (enero 05) “De la protección de la información y de los datos” Ley publicado por Función publica. 2009. Colombia.

DÍAZ JIMÉNEZ, Sebastian *et al.* Análisis Del Delito de Fraude Electrónico: Modalidad Tarjeta de Crédito [en línea]. Tesis de pregrado. Universidad Cooperativa de Colombia Sede Montería, 2018 [consultado 16 mayo 2020]. Disponible en https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

DURANGO ESPINOZA, Rayner y QUIMIZ MOREIRA, Mauricio. Estudio de La Seguridad de La Información de Los Pacients En Los Hospitales Públicos Tipo II de Ecuador [en línea]. Tesis de pregrado [consultado 9 junio 2020]. Disponible en http://201.159.223.2/handle/123456789/3060

EGUILUZ PEREZ, Javier Introduccion a JavaScript [en línea]. Publicación de investigación 2008 [consultado 10 mayo 2020]. Disponible en http:// www.google.com/url?sa=t&source=web&rct=j&url=http://www.librosweb.es/javascript

ESCOBAR, Frank Sistema de Prevención de intrusos [en línea]. Publicación de articulo en blog del informatico. 2015 [consultado 10 mayo 2020]. Disponible en http://franyagami28.wixsite.com/blog-del-informatico/single-post/2015/09/13/Sistema-de-Prevenci%C3%B3n-de-Intrusos-IPS

FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el Mercado colombiano. Tesis de pregrado, 2017. Instituto Universitario Politécnico GranColombia.

FERNANDEZ HERNANDEZ, Jesús; ALONSO, BERROCAL, Jose, FIGUEROLA PANIAGUA, Carlos, ZAZO RODRIGUEZ, Angel, Redes ptivadas virtuales [en línea]. Informe técnico 2006 [consultado 10 mayo 2020]. Disponible en http:// www.google.com/url?sa=t&source=web&rct=j&url=http://eprintd.rclis.org/13992/1/fernandez2006redes.pdf&ved=2ahKEwiDt7KS4tnqAhXqguAKHaZzDoQQFjACegQIBRAB&usg=AOvVaw1rGSF7hFLCan6IBMbrWkon

FONSECA HERRERA, Omar Andrés . Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS. Tesis de pregrado. 2019. EAN Universidad. Facultad de estudios ambientales. Bogotá, Colombia

FREIRE FAJARDO, Franklin. Cifrados de información: la encriptación de datos en las empresas [en línea]. Guía corporativa. 2018 Enjoy Safer Technology.

GAGO, Edgardo. El Enfoque Argentino Sobre Ciberseguridad y Ciberdefensa [en línea] Tesis Doctoral. Escuela Superior de Guerra Ttl Grl Luis María Campos [consultado 17 mayo 2020]. Disponible en https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&as_ylo=2016&q=DEFINICION+DE+CIBERSEGURIDAD&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3AnR6gf2qgQBwJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D1%26hl%3Des

GARCÍA DE LEÓN, Alicia; GARRIDO DÍAZ, Adriana. Los sitios web como estructura de información: un primer abordaje en criterios de calidad [en línea]. 2002. Artículo de investigación. Universidad de la Republica de Monterrey, Uruguay.

GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

GONZÁLEZ DÍAZ, Joshsua. Ciberriesgo Desde La Perspectiva de Riesgo Sistémico. *Revista de Sistemas*. 2019, no. 151, pp. 1-11. ISSN 0120-5919

GONZÁLEZ RAMIREZ, M. Reyes, GASCÓ GASCÓ, José Luis y LLOPIS TAVERNER, Juan. Razones y riesgos del outsourcing de sistemas de información en las grandes empresas españolas. Artículo. *Revista ELSERVIER*. 2015, vol. 1, no. 1, pp. 176-189. ISSN 1019-6838

GONZÁLEZ, Diego. Diseño de Un Plan Estratégico de Seguridad de La Información, Mediante La Aplicación de Análisis de Riesgos Con La Norma ISO/IEC 27005. Caso de Estudio INAMHI. *Revista INNOVA*. 2018, vol. 3, no. 2, pp. 84-91. ISSN 2477-9024

GRID SOLUTIONS REASON RT CLOCKS. Falta de autenticación en función crítica en Grid Solution Reason RT clocks de GE. [en línea].2020 [consultado 01 de julio 2020]. Disponible en https://www. https://www.basquecybersecurity.eus/es/avisos/sistemas-control-industrial/falta-autenticacion-funcion-critica-grid-20200603.html

GUZMÁN PACHECO, Goyo Francisco . Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega. Tesis de postgrado 2015. Universidad Nacional del Centro de Perú

HURTADO de BARRERA, J. Metodología de la investigación holística. Venezuela: Sypal, 2000. p. 666.

HERNÁNDEZ, R; FERNÁNDEZ, C y BAPTISTA, L. Metodología de la investigación. México: McGraw-Hill, 2016. p .252

HERNÁNDEZ, María y NARANJO, Bertha. Diseño de Un Plan Estratégico de Seguridad de Información En Una Empresa Del Sector Comercial [en línea]. 2016.Tesis de pregrado. [consultado 15 junio 2020]. *Disponible en* https://core.ac.uk/download/pdf/12401003.pdf

HUAYLLANI MUÑÓZ, Oscar. Sistema de Gestión de Seguridad de La Información y La Gestión Del Riesgo En El Ministerio de Salud [en línea]. Tesis de maestría [consultado 9 junio 2020]. Disponible en http://repositorio.ucv.edu.pe/handle/20.500.12692/42775

INSTITUTO NACIONAL DE CIBERSEGURIDAD, Glosario de términos de ciberseguridad: Guía de aproximación para los empresarios. 2017. Guía de investigación. España.

Investigación En Ciberseguridad: Un Enfoque Integrado Para La Formación de Recursos de Alto Grado de Especialización [en línea]. La Plata: XX Workshop de Investigadores en Ciencias de la Computación, 2018. [Fecha de consulta: 10 mayo 2020]. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/68355/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

JAIMES, Alonso. Web site as a basic device for information and communication. Theoretic approach: definition and essential elements [en línea]. Revista científica de información y comunicación Tesis de Maestría. 2008 [consultado 10 mayo 2020]. Disponible en http://institucional.us.es/revistas/comunicacion/5/07alonso.pdf

KANAT ALEXANDER, Max. Code simplicity: the science of software development., 2012. [en línea] Editorial O´reilly media Inc. Estados Unidos de América.

KIGERL, Alex. Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories [en línea]. Washington: Social Science Computer Review, 2017. [Fecha de consulta 16 mayo 2020]. Disponible en https://journals.sagepub.com/doi/10.1177/0894439317730296

KRUTZ,R y VINES, R. The CISSP Prep Guide: Gold Edition, citado por SANTIAGO, Enrique y SÁNCHEZ ALLENDE, Jesús. Riesgos de Ciberseguridad En Las Empresas. *Revista de Tecnología y Ciencia*. 2017, vol. 15, no. 1, pp. 1-33. ISSN 1696-8085

LAZAR, Elena y NICOLAE COSTESCU, Dragos. Los Ciberataques: Una Noción Sin Tipificación, Pero Con Un Futuro [en línea]. Coruña: Anuario da Facultade de Dereito da Universidade da Coruña, 2018. [Fecha de consulta 11 de mayo 2020]. Disponible en https://ruc.udc.es/dspace/bitstream/handle/2183/22352/AD_2018_22_art_7.pdf?sequence=3&isAllowed=y

LÓPEZ PINO, José Luis. Contraseñas débiles, 2010 [consultado 30 junio 2020 Disponible en https://lopezpino.com/2010/07/20/contrasenas-debiles/

MARTÍN RODRÍGUEZ, Guillermo. La Gestión de Los Riesgos Tecnológicos [en línea]. Tesis de Maestría. Universidad Pontificia Comillas, 2018 [consultado 15 mayo 2020]. Disponible en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/33058/TFM001074.pdf?sequence=1&isAllowed=y

MARTÍNEZ LANDROVE, Noelia. Ciberseguridad y Riesgo Operacional En Las Organizaciones [en línea]. Tesis de maestría. ICADE School Business, 2019 [consultado 10 mayo 2020]. Disponible en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/42317/TFM001173.pdf?sequence=1&isAllowed=y

MENA DÍAZ, Nestor Las tecnologías de información y comunicación en el segumineto de los desastres naturales: estudio de un caso: La plataformainformática de la red UTEEDA para la gestión de la información sobre desastres. 2007. Artículo científico. ACIMED ISSN 1024-9435. Habana, Cuba.

MORENO AYALA, Enyi y PEÑA VELANDIA, Wilson. El Teletrabajo, Impacto En La Calidad de Vida de Los Colaboradores Del Área de Soporte Técnico de La Compañía Colvatel S.A [en línea]. Tesis de posgrado. Universidad de Bogotá Jorge Tadeo Lozano, 2018 [consultado 17 mayo 2020]. Disponible en https://expeditiorepositorio.utadeo.edu.co/bitstream/handle/20.500.12010/8345/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

MUÑOZ, Jorge Diseño de un plan estratégico de seguridad de la información de Cias & Profesionales S.A.S. Tesis de pregrado. 2017. Universidad Nacional Abierta y a Distancia. Mocoa, Colombia.

NARBONA SARRIA, Manuel y JIMÉNEZ LOMA, Zenobia. Roles y responsabilidades para la gestión de las tecnologias de la información. Publicación. 2007 Dirección General de sistema de información económico-financiero. Consejería de economía y hacienda.

OLTRA-GUTIÉRREZ, Juan e IBÁÑEZ-HERNÁNDEZ, Rafael. Ciberseguridad y Bibliotecas: Apuntes Para Una Propuesta de Formación Sobre Riesgo Tecnológico En Bibliotecas. *Revista de Métodos de Información*. 2019, vol. 10, no.19, pp. 75-126

ORDUZ BARRERA, Diana. Análisis de Emergencias Cibernéticas Que Se Presentan En Las Ciudades de Tunja, Duitama y Sogamoso Con Respecto Al Respecto Del País En Los Últimos Dos Años [en línea]. Monografía de posgrado. Universidad Nacional Abierta y a Distancia, 2019 [consultado 11 mayo 2020]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31410/dmorduzb.pdf?sequence=1&isAllowed=y

OSIO HAVRILUK, Lubiza. Salud y Seguridad En El Teletrabajo. *Revista de visión general*. 2016, no. 2, pp. 410-426. ISSN 1317-8822

PALOMO PASTOR, D. Francisco. Desarrollo de un Sistema de gestión de incidencias. Tesis de pregrado 2009. Universidad Politécnica de Madrid. España.

PARRA MORENO, Duver Augusto Gestión del riesgo en la seguridad informática: "cultura de la auto-seguridad informática". Ensayo de pregrado. 2012. Universidad militar de Nueva Granada. Bogotá

PINHEIRO BEZERRA, Italla. State of the Art of Nursing Education and the Challenges to Use Remote Technologies in the Time of Coronavirus Pandemic. *J Hum Growth Dev (JHGD)*. 2020, vol. 30, no.1, pp. 141-147

RÍOS YÁNEZ, Javier. Técnicas herramientas de análisis de vulnerabilidad de una red. Tesis de pregrado. 2014. Escuela técnica superior de ingeniería y sistemas de telecomunicaciones. Madrid, España.

RIVAS RECALDE, Carlos. Formulación de Un Marco de Referencia Para Implementaciones Ágiles de BI Sobre CLOUD Para Apoyar La Toma de Decisiones Estratégicas En La Industria de Servicios [en línea]. Tesis de Maestría. Universidad de las Américas, 2018 [consultado 17 mayo 2020]. Disponible en http://dspace.udla.edu.ec/handle/33000/9765

RODRÍGUEZ CONDE, Luis. Elaboración de una plan de implementación ISO/IEC 270001:2013. 2017. Plan Director de Seguridad de Ícaro S.A. Universidad Rovira I Virgili

RODRÍQUEZ, Roger y JIMÉNEZ, Ingrid. Mejoramiento de las buenas prácticas de seguridad informática en el teletrabajo a través de una herramienta web. Tesis de postgrado. 2013. Universidad Piloto de Colombia. Bogotá

ROSELL, José. Sólo uno de cada diez usuarios utiliza una contraseña segura, 2017 [consultado 30 junio 2020]. Disponible en https://www.google.com/amp/s/amp.20minutos.es/noticia/2948625/0/estudio-usuarios-consenas-inseguras/

Tarazona T, Cesar H. Amenazas informáticas y seguridad de la información. Consultor en seguridad de la Información, Etek International.

TEJENA-MACÍAS, Mayra. Análisis de Riesgos En Seguridad de La Información. *Revista de ciencias de la computación*.2018, vol. 3, no. 4, pp. 230-244. ISSN: 2550-682X

VIERA, Rosa. Propuesta de Mejora Del Nivel de Gestión Del Proceso de Adquirir e Implementar Las Tecnologías de Información y Comunicaciones (TIC) En El Gobierno Regional de La Provincia de Piura [en línea]. Tesis de pregrado. Universidad Católica de los Ángeles de Chimbote, 2017 [consultado 10 mayo 2020]. Disponible en http://repositorio.uladech.edu.pe/handle/123456789/305

VILLALÓN HUERTA, Antonio, Según en unix y redes [en línea]. 2002. Documento de licencia. España.

ZAMORA LUCIO, Marco Antonio. Internet [en línea]. Publicación técnica 2014 [consultado 10 mayo 2020]. Disponible en http://www.google.com/url?sa=t&source=web&rct=j&url=http://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/Presentaciones_Enero_Junio_2014/Definiciones%2520de%2520Internet.pdf&ved=2ahUKEwiG0ufc5NnqAhUgMUakhtr6c0iqfJaJegQICRA&usg=A0vVaw1pVGTHeu8s1CJjl8A-eo