ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA LA IMPLEMENTACIÓN DEL TELETRABAJO

ALVARO ISIDRO TOVAR SALAZAR

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

BOGOTA
2022

ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA LA IMPLEMENTACIÓN DEL TELETRABAJO

ALVARO ISIDRO TOVAR SALAZAR

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

Director
Edgar Dulce Villareal
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, 25 de julio del 2022

DEDICATORIA

Con amor dedico este trabajo a mi hija, esposa, hermana, papá y mamá que con su carisma y comprensión me han acompañado en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones; para todos mis seres queridos, muchas gracias por su apoyo, consagración y paciencia, para lograr este gran triunfo en mi vida personal y profesional.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso, les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTADO DE TABLAS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: "Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones".[1]

AMENAZA INFORMÁTICA: "Es la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad".[2]

ANTIVIRUS: "Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware"*.[3]

BACKUP: "Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados".[4]

---

[1] INSTITUTO NACIONAL DE CIBERSEGURIDAD,Glosario de Términos de Ciberseguridad, Una guia de aproximación para el empresario.2017, 82 p.

[2] AGUILERA LOPEZ, Purificación, Seguridad Informatica - Ciclos Formativos. 1ª edición. Pozuelo de Alarcon - Madird: Editex,2010. 243 p. ISBN 9788497717618.

[3] INSITUTO NACIONAL DE CIBERSEGURIDAD. Op.Cit., p.8.

[4] Ibíd., p.12.

CONFIDENCIALIDAD: “Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información”.[5]

CRIPTOGRAFÍA: “Técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado”.[6]

DISPONIBILIDAD: “Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran”.[7]

FUGA DE INFORMACIÓN: “Es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros”.[8]

INCIDENTE INFORMÁTICO: “Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información”.[9]

INTEGRIDAD: “Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha

---

[5] Ibíd.,p.17.

[6] Ibíd.,p.19.

[7] Ibíd.,p.21.

[8] Ibíd.,p.22.

[9] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información. NTC-ISO/IEC 27035. Bogota D.C.:El instituto, 2012. 103 p.

producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales".[10]

MALWARE: "Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información".[11]

RED PRIVADA VIRTUAL: "También conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet".[12]

VIRUS: "Programa diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos".[13]

VULNERABILIDAD INFORMÁTICA: "También puede referirse a cualquier tipo de debilidad en el propio sistema de información, o a un conjunto de procedimientos o a cualquier cosa que deje la seguridad de la información expuesta a una amenaza".[14]

---

[10] INSTITUTO NACIONAL DE CIBERSEGURIDAD,Glosario de Términos de Ciberseguridad, Una guia de aproximación para el empresario.2017, 25 p.

[11] Ibíd., p.26.

[12] Ibíd., p.31.

[13] Ibíd., p.37.

[14] INGERTEC. NORMAISO27001. [Sitio WEB]. Cordoba - España. La entidad. [17, junio, 2022]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def377/.

RESUMEN

En la actualidad el riesgo informático al que se exponen las organizaciones es una de las principales preocupaciones de los empresarios. A medida que surgen cambios y nuevas tecnologías, surgen nuevos ataques informáticos que pueden desestabilizar y poner en riesgo la economía de la organización.

El activo más importante en una entidad es la información, por ello es relevante que las empresas garanticen la seguridad de la información en todos sus niveles. Por ello se deben tener protocolos mínimos de seguridad en sus estaciones de trabajo, en los equipos de los empleados que, por las necesidades actuales del servicio, deben conectarse a la red institucional, desde dispositivos electrónicos personales para el desarrollo y cumplimiento de sus funciones, generando riesgos en la seguridad de la información, que deben ser mitigados con protocolos apropiados y ajustados a las necesidades del teletrabajo.

Todo el esfuerzo de las empresas debe estar direccionado a la política de seguridad de la información y a fortalecer los planes de acción para mitigar y prevenir los riesgos originados con la implementación del teletrabajo.

ABSTRACT

Currently, the computer risk of exposing organizations is one of the main concerns of entrepreneurs. As changes and new technologies emerge, new cyber attacks emerge that can destabilize and endanger the organization's economy.

The most important asset in an entity is information, so it is relevant for companies to guarantee the security of information at all levels. For this reason, there must be minimum security protocols in their workstations, in the team of employees who, due to the current needs of the service, must have the institutional network, from personal electronic devices for the development and fulfillment of their functions, generate information security risks, which must be mitigated with the affected protocols and adjusted to the needs of teleworking.

All the efforts of the companies should be directed towards the information security policy and strengthen the action plans to mitigate and prevent the risks originated by the implementation of telework.

INTRODUCCIÓN

En el nuevo marco económico y social las organizaciones se han visto en la necesidad de migrar hacia nuevas maneras de optimizar la productividad de sus empresas con actividades que están siendo subutilizadas como el teletrabajo. Según Thibault[15], el teletrabajo es una forma de ejecución del trabajo realizada en gran parte a distancia y mediante el uso intensivo de herramientas informáticas.

Pero al implementar el teletrabajo, la empresa está exponiendo su activo más importante, la información. Es por ello por lo que se hace de suma importancia tener un marco de gestión de seguridad de la información con unos parámetros específicos tanto para los directivos de la organización como para el personal operativo de la misma, a fin de que el activo más valioso siempre este protegido.

A fin de lograr esto, se plantean los objetivos buscando analizar todos los aspectos a tener en cuenta en la seguridad de la información a la hora de implementar el teletrabajo para luego, teniendo como referencia el modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar un modelo de gestión de seguridad de la información aplicable a cualquier organización ya se pública o privada que implemente el teletrabajo como una opción productiva para su empresa.

[15] THIBAULT ARANDA, Javier. El teletrabajo, análisis jurídico-laboral. 2 ed. Madrid-España.: Consejo Económico y Social, 2000. 320 p. ISBN: 84-8188-113-9.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El teletrabajo se convirtió en un fenómeno muy concurrido a nivel mundial por la facilidad que ofrece a los empleados para laborar desde sus lugares de residencia y mejorar la productividad de la empresa; como lo indico Gabriela Morales y Katy Romanik,[16] esta modalidad de trabajo que surgió en los Estados Unidos en la década de 1970 cuando estalló la crisis petrolera, en el cual el físico norteamericano Jack Nilles, analizó el impacto ambiental en relación al desplazamiento que realizaban los trabajadores desde su hogar al lugar de trabajo, dado que eran extensos los recorridos y más preocupante aún el alto consumo de combustible, que para aquella época empezaba a escasear. Por ello, dada la connotación del momento, pensaron en la idea de que "el trabajo fuera al trabajador", y de esta manera se resolvería el problema de escasez de petróleo, congestión vehicular y contaminación ambiental. Aunque es 20 años después, en los años 90 cuando esta figura de empleo se implementa mayormente en los Estados Unidos, debido al amplio desarrollo tecnológico con los objetivos de reducir costos y aprovechar mejor el tiempo. Uno de los ejemplos más relevantes fue el de la empresa IBM, permitió a los directivos que ejercieran sus funciones laborales a distancia desde cualquier locación que tuviera acceso a internet, a fin de reducir costos y aprovechar el tiempo libre de sus empleados.

En Europa, en los años 1996 a 1998, la Comisión Europea financió el proyecto MIRTI1, con el cual buscaban presentar recomendaciones para realizar y reglamentar el Teletrabajo, ya para el año 2002, la Confederación Europea de

[16] MORALES, Gabriela y ROMANIK, Katy, Una mirada a la figura del teletrabajo. Chile: Direccion del Trabajo, 2011. 60 p. ISBN: 978-956-7978-07-6.

Sindicatos - CES, la Unión de Confederaciones de la Industria y de Empresarios de Europa -UNICE, la Unión Europea del Artesanado y de la Pequeña y Mediana Empresa - UNICE y el Centro Europeo de la Empresa Pública -CEEP, firmaron el Acuerdo Marco Europeo sobre el Teletrabajo, que "busca modernizar la organización del trabajo con el objetivo de mejorar la productividad y la competitividad de las empresas y lograr el equilibrio necesario entre flexibilidad y seguridad"[17].

En el caso de América Latina, puntualmente en la República de Argentina, entre los años 1998 y 2002, se vivió la fuerte crisis económica que ocasiono una tasa de desempleo superior al 20%, lo que permitió que implementaran nuevas formas de organización laboral, que disminuyeran costos a las compañías. Creando así el Programa de Promoción del Empleo en Teletrabajo - PROPET, con el fin de difundir esta modalidad laboral y ya para el año 2013 reglamenta el teletrabajo bajo la Resolución No. 595 del 2013 del Ministerio de Trabajo, Empleo y Seguridad Social del Gobierno de Argentina.

Durante su puesta en marcha a nivel mundial, este trajo consigo un sinfín de inconvenientes en temas de seguridad informática, puesto al implementar un sistema de teletrabajo sin tomar las medidas adecuadas de seguridad, se enfrentaban a ataques contra la infraestructura tecnológica y al riesgo inminente de perder información vital para el normal funcionamiento de la organización. Adicional, algunas empresas no cuentan con los medios económicos y tecnológicos necesarios para garantizar conexiones seguras y en su afán de implementar mencionada iniciativa incurrieron en errores elementales a la hora de planificar los

[17] QUINTANILLA NAVARRO, Raquel Yolanda. El teletrabajo de la dispersión normativa presente a la necesaria regulación normativa europea y estatal futura. [en línea]. Madrid-España.: 2017.[Consultado 13,noviembre,2020]. Disponible en :https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-madrid/documents/article/wcms_548615.pdf.

permisos de conexión remota, al no tener presente la evaluación de los posibles riesgos a los que estaría expuesta la infraestructura tecnológica de la entidad.

Por otra parte, al otorgar privilegios de acceso de conexión remota a los funcionarios, sin delimitar los permisos concedidos y en la diligencia de garantizar el normal funcionamiento de la operación de la empresa, terminaron por afectar la misma al no contar con mecanismos para hacerle frente a los posibles ataques informáticos; al materializarse estas vulnerabilidades se incrementaron los incidentes de seguridad y las infecciones por malware, virus, suplantación de identidad (phishing), ataques del hombre en el medio, ataque de denegación de servicio, inyecciones SQL, secuencias de comandos entre sitios, *rootkits*, entre otros etc., afectando los equipos de cómputo institucionales, la red de datos de comunicaciones y en algunos casos, perdidas de información y dinero.

En la actualidad las causas de pérdida y fuga de información en las empresas, han estado relacionadas con el teletrabajo, puesto que los ciberdelincuentes se han aprovechado de las malas prácticas de implementación de controles de ciberseguridad; existen muchas formas con las que un computador puede infectarse, desde recibir mensajes vía email de un destinario desconocido hasta la infección mediante una memoria USB, esto se facilita aún más si no se tienen herramientas básicas como antivirus, anti *malware*, anti *rootkits* para contrarrestar mencionados métodos de infección, de ahí la importancia de contar con *software* que gestione mencionadas vulnerabilidades.

Por lo anterior, es importante contar con una guía de buenas prácticas para la implementación del teletrabajo que permita proteger a la entidad de incidentes informáticos, minimizar el impacto, garantizar la recuperación de la información que sea comprometida y sobre todo garantizar la continuidad del negocio.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo activar una estrategia de seguridad de la información en las organizaciones al implementar la modalidad de teletrabajo?

2. JUSTIFICACIÓN

En el escenario planteado de Ciberseguridad para el teletrabajo, las empresas están expuestas constantemente a diferentes ataques tales como: *malware*, suplantación de identidad (*phishing*), ataques del hombre en el medio, ataque de denegación de servicio, inyecciones SQL, secuencias de comandos entre sitios, *rootkits*, entre otros, los cuales se han incrementado desmedidamente, aprovechando la coyuntura del momento. Las organizaciones pese a tener planes de mitigación de riesgos e implementación de controles robustos, que buscan cerrar brechas en la seguridad para evitar que los ciberdelincuentes accedan a la infraestructura tecnológica ya que de lograrlo generarían grandes pérdidas económicas, pérdida de imagen institucional, clientes, información y llevarla a la banca rota, no tienen contemplado un procedimiento claro frente a las implicaciones que trae el acceso a la información desde conexiones remotas.

Por ello, al optar por esta medida de flexibilidad para trabajar, deben generar cultura organizacional para con los empleados que están bajo esta modalidad de trabajo y explicarles los riesgos a los que se pueden exponer y de paso a la organización, si no se toman las medidas correspondientes al momento de realizar una conexión remota desde sus hogares a la red corporativa mediante el uso de internet; dado la cantidad de amenazas y los riesgos en seguridad informática que abundan en la red y que afectaría negativamente la infraestructura tecnológica y la información de la empresa por malas prácticas y desconocimiento mínimo de medidas de autoprotección en seguridad de la información.

Por lo anterior, es fundamental realizar una diagnóstico del estado para la toma de decisiones relevantes en el manejo de la Ciberseguridad para el modelo organizacional de teletrabajo, todo de la mano de herramientas de *software* gratuito muy robustos para realizar auditoria a sus sistemas informáticos y tener un análisis

detallado, frente a posibles vulnerabilidades y ataques a los que estaría expuesta la infraestructura tecnológica de la organización con ocasión de la implementación del teletrabajo.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Elaborar una guía que sirva de referencia de Seguridad informática para la gestión de la información en el proceso de implementación del teletrabajo en una organización.

3.2 OBJETIVOS ESPECIFICOS

- Identificar y analizar los riesgos probables en seguridad de la información, que pueden estar presentes al momento de la implementación del teletrabajo en la organización.

- Establecer un modelo de un sistema de gestión de seguridad de la información en la implementación del teletrabajo orientado en los riesgos identificados.

- Diseñar un documento detallado con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información, de acuerdo a los riesgos encontrados en la implementación del teletrabajo.

- Orientar a las organizaciones para la adopción de mejores prácticas en seguridad y privacidad de la información con la inclusión del teletrabajo.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

El presente trabajo de grado se centra en la importancia de la seguridad de la información para la implementación del teletrabajo, convirtiéndose en una herramienta que permite a las empresas fortalecer los controles de seguridad de la información, mitigando la pérdida y fuga de información, de la mano de la adopción de mencionada modalidad de trabajo, optimización del tiempo de sus empleados, mejorando su calidad de vida y los servicios que prestan a la entidad. Una vez realizada la búsqueda de bibliografía relacionada con el tema a fin, se encontraron tesis de grado, artículos científicos, artículos de revistas, entre otros, que mencionan esta modalidad de trabajo y que se enumeran a continuación:

Como lo señala Domingo Verano Tacoronte, Heriberto Suárez Falcón y Silvia Sosa Cabrera[18] en el artículo “El teletrabajo y la mejora de la movilidad en las ciudades”, donde el objetivo es incentivar el compromiso de las organizaciones para aumentar la implementación del teletrabajo; teniendo presente las bondades y beneficios que conllevaría a las entidades la puesta en marcha de mencionada modalidad, a la sociedad en general y los trabajadores, puesto que mejoraría notablemente la movilidad en las ciudades. Mencionada investigación, se llevó a cabo con el fin de elegir el teletrabajo como una opción laboral mediante el uso de las Tecnologías de la Información y las Comunicaciones – TIC, demostrando los efectos directos e

[18] VERANO TACORONTE Domingo, SUÁREZ FALCÓN,Heriberto, y SOSA CABRERA, Silvia. El teletrabajo y la mejora de la movilidad en las ciudades.Investigaciones Europeas de Direccion y Economia de la Empresa. [en línea].Pontevedra - España:. 2014.0. [Consultado 10,octubre,2020]. Disponible en: https://redalyc.org/pdf/2741/274129585006.pdf .

indirectos; directos como reducción de los desplazamientos de los trabajadores y del espacio de la oficina e indirectos como la contaminación.

Según Gallego Eva[19] en el artículo El teletrabajo como una nueva forma de empleo, en su definición clásica del teletrabajo: como un modo de empleo en el que el trabajador está localizado remotamente de una oficina central o de un centro de producción, con o sin contacto cara a cara con co-trabajadores, pero que permite la comunicación vía el uso de la tecnología de sistemas de comunicación (Conner, Fletcher, Firth-Conzens y Colling, 1994). Padilla[20] en 1997 indica que "teletrabajo es una estrategia funcional de una organización, basada en trabajar cuando quiera y en cualquier parte, haciendo los Recursos Humanos, por tanto, más flexibles.

En síntesis, el teletrabajo es un término global que abarca un sinfín de modalidades de trabajo, de modo de organización o de tareas propiamente dichas. Según Gontier[21], lo que crea el vínculo entre dichas labores es la transmisión de la información en tiempos reales, en general medios telemáticos.

Por otra parte, para Jane Tate[22], redactora del informe sobre teletrabajo de la Comisión Europea, el significado teletrabajo indica aquellas actividades ejercidas lejos de la sede de la empresa (se les denomina también, en ocasiones, trabajo a

---

[19] CIFRE GALLEGO, Eva, 'Estrategias de Mejora de La Salud Psicosocial Del Teletrabajador. El Arte de Conjugar Teoría y Práctica', Estudios Financieros. Revista de Trabajo y Seguridad Social. Comentarios, Casos Prácticos. Recursos Humanos, 300, 2008, 181–200.

[20] CHAPARRO NIÑO, Wilson Alexander. Tecnología: Hacia un nuevo concepto de la subordinación laboral.[en línea]. Monografia. Universidad Nacional de Colombia. Bogota, D.C.: 2018. [Consultado 17,junio,2022].Disponible en:https://repositorio.unal.edu.co/bitstream/handle/unal/69780/80195584.2018.pdf

[21] Ibíd., p.49.

[22] Ibíd., p.49.

distancia), mediante la comunicación directa o diferida y con la ayuda de las nuevas tecnologías.

Adicional Gray, Hodson y Gordon[23], indican que el teletrabajo es una forma flexible de organización del trabajo, que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador en la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y pueden realizarse en tiempo completo o parcial. La actividad profesional en el teletrabajo implica el uso permanente de algún medio de telecomunicación para el contacto entre el teletrabajador y la empresa.

D. Xavier Thinault[24] lo define como una forma de organización y/o ejecución del trabajo realizado a distancia, en gran parte o principalmente, mediante el uso intensivo de las técnicas informáticas y/o de telecomunicación.

4.1.1 Teletrabajo. Como afirma el Portal del Teletrabajo[25], en su definición: Aunque existen diversas definiciones derivadas especialmente de las legislaciones de los distintos países, para Colombia son válidas estas dos referencias:

La Organización Internacional de Trabajo -OIT- define teletrabajo como:

"Una forma de trabajo en la cual: a) el mismo se realiza en una ubicación alejada de una oficina central o instalaciones de producción, separando así al trabajador del contacto personal con colegas de trabajo que estén en esa oficina y, b) la nueva

[23] Ibíd., p. 49.

[24] Ibíd., p. 49.

[25] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Teletrabajo. [Sitio WEB]. Bogotá, D.C. La entidad. [28, mayo, 2020]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8228.html.

tecnología hace posible esta separación facilitando la comunicación". Citado en Vittorio Di Martino, 2004.[26]

En Colombia, el teletrabajo se encuentra definido en la Ley 1221 de 2008, en el Artículo 2, el cual indica:

“Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo”.[27]

4.1.1.1 Características del teletrabajo. Como se indica en el libro Blanco, el ABC del Teletrabajo en Colombia[28], se evidencia que: más allá de la definición, el teletrabajo se entiende a partir de sus características:

- Una actividad laboral que se lleva a cabo fuera de la organización en la cual se encuentran centralizados todos los procesos.
- La utilización de tecnologías para facilitar la comunicación entre las partes sin necesidad de estar en un lugar físico determinado para cumplir sus funciones.
- Un modelo organizacional diferente al tradicional que replantea las formas de comunicación interna de la organización y en consecuencia genera nuevos mecanismos de control y seguimiento a las tareas.

---

[26] CHAPARRO NIÑO.Op.Cit., p.50.

[27] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1221(16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. En: Diario Oficial. Julio, 47.Nro. 052. p. 1-6.

[28] COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y MINISTERIO DEL TRABAJO, Libro Blanco. ABC del Teletrabajo en Colombia.2014, nro. 01 . p. 1-97. ISSN 1098-6596, p. 12.

4.1.1.2 Modalidades del teletrabajo. En Colombia, la Ley 1221 de 2008 en el Artículo 2,[29] establece tres modalidades de teletrabajo o tipo de teletrabajador, que responden a los espacios de ejecución del trabajo, las tareas a ejecutar y el perfil del trabajador:

4.1.1.3 Teletrabajo Autónomo. "Trabajadores independientes o empleados que se valen de las TIC para el desarrollo de sus tareas, ejecutándolas desde cualquier lugar elegido por ellos".[30]

4.1.1.4 Teletrabajo Suplementario. "Trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la empresa y un lugar fuera de ella usando las TIC para dar cumplimiento. Se entiende que teletrabajan al menos dos días a la semana".[31]

4.1.1.5 Teletrabajo Móvil. "Trabajadores que utilizan dispositivos móviles para ejecutar sus tareas. Su actividad laboral les permite ausentarse con frecuencia de la oficina. No tienen un lugar definido para ejecutar sus tareas".[32]

4.1.2 Beneficios. En el libro, Libro Blanco el ABC del Teletrabajo en Colombia33 se evidencian, las ventajas y beneficios derivados de la implementación de un modelo de teletrabajo en las organizaciones pueden entenderse desde distintos ámbitos:

[29] Ibíd., p.12.

[30] Ibíd., p.12.

[31] Ibíd., p.12.

[32] Ibíd., p.12.

[33] Ibíd., p.14.

4.1.2.1 Beneficios para las organizaciones

Para el negocio.

- "Mayor productividad equivale a mayores ingresos y mayor crecimiento del negocio".[34]
- "Costos predecibles asociados a la flexibilidad de la inversión en planta física, tecnología y recursos humanos que responderán a la demanda. A mayor demanda, crecimiento de la organización con inclusión de teletrabajadores; a menor demanda, escasos costos fijos".[35]
- "Reducción de costos fijos en planta física, mantenimiento, servicios públicos, entre otros".[36]

Para las operaciones.

- "Control y seguimiento permanente al desarrollo de las tareas programadas a través de las herramientas tecnológicas".[37]
- "Procesos descentralizados pero interconectados".[38]

Para el área de recursos humanos.

- "Mejoramiento de las condiciones del reclutamiento al poder contratar al personal más calificado sin importar su ubicación o disponibilidad de desplazamiento hacia la sede de la organización".[39]

---

[34] Ibíd., p.15.

[35] Ibíd., p.15.

[36] Ibíd., p.15.

[37] Ibíd., p.15.

[38] Ibíd., p.15.

[39] Ibíd., p.15.

- “Mayor índice de retención del personal capacitado”.[40]
- “Equilibrio entre los espacios laborales y personales de los empleados que generan mayor calidad de vida que se traduce en mayor productividad”.[41]

Para el área de tecnología.

- “Reducción del costo en adquisición de *hardware* y *software”*.
- “Política "*Bring Your Own Device* -BYOD-"[42] que aprovecha los dispositivos de propiedad del trabajador y no aumenta costos para la organización”.[43]
- “Control total sobre los escritorios virtuales y el flujo de la información”.[44]
- “Reducción del esfuerzo en mantenimiento de equipos y optimización de la capacidad de respuesta frente al crecimiento de la compañía”.[45]

Para los programas de Responsabilidad Social.

- “Reducción de la huella de carbono al evitar el desplazamiento de los trabajadores hacia la empresa”.[46]

---

[40] Ibíd., p.15.

[41] Ibíd., p.15.

[42] ESET. Welivesecurity. Guía de Bring Your Own Device.[Sitio WEB]. Canada. La entidid. [6, noviembre,2013]. Disponible en:https://www.welivesecurity.com/la-es/post_paper/guia-de-bring-device.

[43] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES and MINISTERIO DEL TRABAJO, Libro Blanco el ABC del Teletrabajo en Colombia.1 edición. Bogota, D.C.: 2014, nro. 01 . p. 197. ISSN 1098-6596, p. 15.

[44] Ibíd., p.15.

[45] Ibíd., p.15.

[46] Ibíd., p.15.

- “Inclusión sociolaboral de población vulnerable gracias a las TIC: situación de discapacidad, aislamiento geográfico, cabezas de familia”.[47]
- “Aporte al mejoramiento de la movilidad de las ciudades y reducción del tráfico asociado a las jornadas de trabajo”.[48]
- “Aplicación de buenas prácticas laborales que contribuyen al mejoramiento de la calidad de vida de los trabajadores y a su desarrollo, con la integración de los últimos avances de la tecnología y nuevas formas de trabajar”.[49]

4.1.3 Beneficios para los trabajadores. “Los empleados de las organizaciones reciben la posibilidad de trabajar en lugares distintos a su oficina como una oportunidad para mejorar su calidad de vida y aumentar su rendimiento. Entre los beneficios específicos para ellos se encuentran”[50]:

- “Ahorros en tiempos por desplazamientos entre hogar y oficina[51]”.
- “Ahorros en dinero derivados de la disminución de desplazamientos, tangibles en la reducción de costos de combustible o pagos de transporte público”.[52]
- “Ahorros y mejoras significativas en la alimentación y la salud de los trabajadores, al consumir alimentos preparados en sus hogares”.[53]
- “Mejoras en la salud al reducir el estrés derivado de los desplazamientos y los gastos asociados, además de oportunidades de incluir en la rutina diaria tiempo para el cuidado físico”.[54]

---

[47] Ibíd., p.15.

[48] Ibíd., p.15.

[49] Ibíd,. p.15.

[50] Ibíd., p.15.

[51] Ibíd., p.15.

[52] Ibíd., p.15.

[53] Ibíd., p.15.

[54] Ibíd., p.15.

- “Reducción de la huella de carbono y el impacto ambiental producido por cada trabajador durante los desplazamientos y el consumo de energía en las oficinas”.[55]
- “Mejora en los lazos familiares y vecinales al tener mayor presencia física en el hogar y otros espacios de socialización”.[56]
- “Optimización de las actividades personales gracias al desarrollo de habilidades para la gestión del tiempo y las tareas”.[57]

4.1.4 Retos para la implementación. “El teletrabajo es sinónimo de innovación organizacional, en consecuencia, supone un cambio interno y nuevas formas de relacionamiento entre jefes y empleados, por eso es necesario considerar algunos factores”.[58]

4.1.4.1 Control. “Es posible hacer seguimiento a los colaboradores por cumplimiento de tareas y no de horarios”.[59]

4.1.4.2 Productividad. ” Un trabajador concentrado en el logro de metas definidas y disfrutando de mayor balance entre su vida laboral y personal es más productivo”.[60]

4.1.4.3 Costos. “Realizar inversiones iniciales en tecnología que retornen en el mediano plazo como reducciones en costos fijos”.[61]

---

[55] Ibíd., p.15.

[56] Ibíd., p.15.

[57] Ibíd., p.15.

[58] Ibíd., p.16.

[59] Ibíd., p.16.

[60] Ibíd., p.16.

[61] Ibíd., p.16.

4.1.4.4 Cultura Organizacional. "Realizar inversiones iniciales en tecnología que retornen en el mediano plazo como reducciones en costos fijos".[62]

4.1.4.5 Políticas. "La legislación colombiana ya reguló el teletrabajo. Ajustar las políticas corporativas requiere una revisión en materia de horarios y cumplimiento".[63]

4.1.4.6 Tecnológico. "Las necesidades tecnológicas dependen de la proyección de cada organización, y aunque se requieren algunas inversiones y cambios en plataformas, estas se revierten en productividad y optimización de los recursos tecnológicos de las organizaciones".[64]

4.1.5 Requerimientos. "¿Qué debe tener en cuenta una organización al momento de adoptar teletrabajo? Cultura organizacional, tecnología y legislación."[65]

4.1.5.1 Requerimientos Organizacionales. "Gestión del cambio organizacional, compromiso y sensibilización de la organización, y seguimiento al modelo de implementación del teletrabajo".[66]

4.1.5.2 Requerimientos tecnológicos. "Definición de la infraestructura y plataformas tecnológicas que soportarán el teletrabajo".[67]

---

[62] Ibíd., p.16.

[63] Ibíd., p.16.

[64] Ibíd., p.16.

[65] Ibíd., p.18.

[66] Ibíd., p.18.

[67] Ibid., p.19.

- **Requerimientos jurídicos**. "Atención a la legislación vigente en materia jurídica, de riesgos laborales y relaciones con los sindicatos".[68]

- **La vulnerabilidad de la información en el teletrabajo**. Purificación Aguilera López69 define la vulnerabilidad como la probabilidad que existe de que una amenaza se materialice contra un activo. En informática las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad de este. "Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido, causando que se ejecute código malicioso sin el conocimiento del usuario"70.

  "En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones"[71]. "Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas,

---

[68] Ibíd., p.19.

[69] AGUILERA LÓPEZ, Purificación. Seguridad Informática - Ciclos Formativos, 1 edición. Pozuelo de Alarcon - Madrid: Editex, 2010.243 p. ISBN 9788497717618.

[70] MICROSOFT, CORPORTION. Microsoft Security Intelligence Report. [En línea]. 2013, 16 edición. 120 p. [Consultado 13, mayo, 2020]. Disponible en: http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_English.pdf.

[71] GUZMAN, Anggie. Vulnerabilidad, Riesgo y Amenaza. Seguridad Informatica. [sitio WEB]. [Consultado el 11, octubre, 2020]. Disponible en: http://seguridadanggie.blogspot.com/2011/11/vulnerabilidad.html.

porque, en principio, no existe sistema 100% seguro"[72]. Por lo tanto, existen vulnerabilidades teóricas y vulnerabilidades reales.

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, *hotfixs* o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático. "Las vulnerabilidades se descubren muy seguido en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas"[73].

La vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. "Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: ambiental, física, económica, social, educativo, institucional y política".[74]

---

[72] POSTECH IT SOLUTION PROVIDER S.A. Tecnicas y Herramientas para la evaluación de vulnerabilidades de la red. Postech IT Solution Provider [sitio WEB]. [Consultado el 10, octubre,2020]. Disponible en: https://postech.com.mx/Postech/ES/tecnicas.php.

[73] ALEGSA. Definición de Vulnerabilidad - Portal de informática, internet, tecnologias y web.Diccionario de Informática y Tecnología. [Sitio WEB]. Santa fe - Argentina. La entidad. [11, octubre, 2020]. Disponible en: https://www.alegsa.com.ar/Dic/vulnerabilidad.php.

[74] Instituto de Investigación de Recursos Biológicos Alexander von Humboldt, «El ABC de la Gestión de Riesgos», *Fundamentos conceptuales de la Gestión de Riesgos*, 2004.

Para toda empresa es importante la información que maneja, sus clientes y los negocios que se desarrollan, todo esto siempre está vulnerable a ser afectado por factores internos o externos puesto que ya sea para las instalaciones físicas, la información que viaja en la red, los empleados que trabajan en la compañía entre otras, siempre existirán amenazas que se pueden aprovechar de debilidades de los sistemas, es importante fortalecer la infraestructura de la entidad y evaluar continuamente el sistema en búsqueda de falencias o fallas que pueden ser explotadas por los cibercriminales para al negocio.

En el momento en el que una empresa decide implementar la modalidad de teletrabajo debe planear muy bien desde el perfil del empleado hasta las políticas de seguridad que va a aplicar para proteger el activo de la empresa, ya que no tendrá el total control del trabajador y de las actividades y horarios en las que realiza las tareas asignadas, por esta razón, se debe enfocar más que crear políticas, es sensibilizar a los empleados de la importancia de utilizar las buenas prácticas y valorar el activo de la compañía, porque al no poder controlar totalmente al empleado y las herramientas que utiliza, las vulnerabilidades tienden a ser más notorias, que en ambientes controlados y cerrados.

- **Amenazas y riesgos en la seguridad informática.** García Alfonso y Alegre María del Pilar75 definen una amenaza como todo aquello ya sea físico o

[75] ALEGRE RAMOS,Maria del Pilar y GARCÍA-CERVIGÓN HURTADO,Alfonso. Seguridad Informática. [En Línea]. Madrid-España.:2011. 1era edición. 169 p. [Consultado 11,octubre,2020]. ISSN 99788497328128. Disponible en: https://books.google.com.mx/books?id=c8kni5g2Yv8C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

lógico que puede provocar una pérdida de información o de su privacidad, o bien un fallo en los equipos físicos. Royal P. Fisher76 define una amenaza como la intención de infligir un daño; algo que pudiese o fuese a ocurrir causando una pérdida de activos, o reducción en el valor de los activos. En sistemas informáticos se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndoles daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información. En función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

- **De interrupción:** El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

- **De interceptación:** Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

[76] ROYAL P. Fisher, Seguridad en Los Sistemas Informáticos. [En Línea]. Madrid-España:.1988. 1era edición. 278 p. [Consultado 11,octubre,2020]. ISSN 8486251958. Disponible en: https://books.google.co.ve/books?id=_Hu6Zu6VLP4C&printsec=copyright#v=onepage&q&f=false.

- **De modificación:** Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información, sino que además los modificarían.

- **De fabricación:** Agregarían información falsa en el conjunto de información del sistema.

Según su origen las amenazas se clasifican en:

Accidentales: Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos, o en el *software*, errores humanos.

Intencionadas: Son debidas siempre a la acción humana, como la introducción de *software* malicioso, -*malware*- (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano) intrusión informática (con frecuencia se produce previa la intrusión de *malware* en los equipos), robos o hurtos. "Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma"[77].

El riesgo se define como la "combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Se han propuesto diversas definiciones del riesgo: Situación que puede conducir a una consecuencia negativa no deseada en un acontecimiento o bien probabilidad de que suceda un determinado peligro potencial o aun consecuencias no deseadas de una actividad dada, en relación con la probabilidad de que ocurra"[78].

---

[77] AGUILERA LÓPEZ, Purificación.Op.Cit., p.14.

[78] NACIONES UNIDAS. Estrategia Internacional para la Reducción de Desastres.[En Línea]. Nueva York.: 2009.[Consultado 15,octubre,2020]. Disponible en: https://reliefweb.int/report/world/2009-

Joaquim Casal y otros[79] indica que el tratamiento riguroso del riesgo requiere una definición más precisa que permita su cuantificación. Una definición que cumple estos requisitos y que es utilizada por muchos profesionales es la basada en el producto de la frecuencia prevista para un determinado suceso por la magnitud de las consecuencias probables.

Riesgo = Frecuencia * magnitud consecuencias

Josep M. Rovira[80] define el riesgo como un suceso susceptible de ocurrir que pueda alterar el desarrollo normal de un acontecimiento previsto por la conjunción de unas acciones conscientemente programadas, produciendo un daño. Julio Téllez Valdés[81] define el riesgo como la incertidumbre o probabilidad de que ocurra o se realice una eventualidad, la cual puede estar prevista. Por tanto, se afirma que el riesgo es la contingencia de un daño.

- **La seguridad de la información en el teletrabajo**. La Seguridad de la Información es un "conjunto de métodos y herramientas destinados a

unisdr-terminolog%C3%ADa-sobre-reducci%C3%B3n-del-riesgo-de-desastres. Citado por RODRIGUEZ MENJUREN, Roger Edson, mejoramiento de las buenas prácticas de seguridad informatica en el teletrabajo a través de una herramienta web. Bogota, Universidad Piloto De Colombia,2013. p.32 .

[79] CASAL FÀBREGA. Joaquim and others. Análisis del Riesgo en Instalaciones Industriales. [En Línea]. Cataluña-España.:2009. 1era edición. 364 p. [Consultado 11, octubre,2020]. ISSN 978-8483012277. Disponible en: https://upcommons.upc.edu/handle/2099.3/36154.

[80] SERER FIGUEROA,Marcos. Gestión integrada de proyectos. [En Línea]. Madrid-España.:2010. 3era edición. 484 p. [Consultado 11,octubre,2020]. ISSN 978-8498804300. Disponible en: https://www.abebooks.com/9788483018873/Gesti%C3%B3n-integrada-proyectos-96-Politext-848301887X/plp.

[81] TELLEZ VALDEZ, Julio. Teletrabajo. [En Línea]. Mexico, D.C.: 2007.[Consultado 10,octubre,2020]. Disponible en:https://archivos.juridicas.unam.mx/www/bjv/libros/5/2458/43.pdf.

proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan considerando la seguridad como algo secundario”82 y generalmente no se invierte el capital humano ni económico necesario para prevenir principalmente el daño o pérdida de la información, ya que hoy en día las amenazas que afectan las características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información pueden ser internas o externas, originadas accidentalmente o con un fin perverso dejando a la organización con problemas como por ejemplo la paralización de sus actividades que deja como resultado una perdida cuantiosa de tiempo de producción y dinero, factores importantes para el desarrollo de una organización.

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y de telecomunicaciones, sino también aspectos físicos, medioambientales, humanos, etc. La seguridad de la información no es una “propiedad funcional de un sistema de información, sino más bien una propiedad emergente. A lo largo de los años la percepción de la seguridad de la información ha ido cambiando hasta llegar a la realidad de hoy en día. Nació ligada a los entornos militares, diplomáticos y gubernamentales”[83].

---

[82] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES and MINISTERIO DEL TRABAJO. Op.Cit., p.15.

[83] AREITIO, Javier, Seguridad de La Información. Redes, Informática y Sistemas de Información. [En Línea]. Madrid -España: 2008. 1era edición. 592 p. [Consultado 11,octubre,2020] . ISSN 9788497325028. Disponible en:

A nivel empresarial empezó siendo un lujo, algo que estaba bien pero que no era necesario; seguidamente paso a estar de moda, e incluso, a ser una recomendación útil y deseable, percibiéndose como un gasto necesario para poder llevar a cabo los negocios. Posteriormente, se consideró como una obligación para que las empresas no queden desprotegidas, desde el punto de vista legal frente a leyes y reglamentos tales como la Ley de la propiedad intelectual e industrial. En la actualidad la seguridad de la información se ha convertido en un elemento integral de la capacidad de una organización para que esta sea competitiva. Es, por ello, un activo estratégico que no puede estar separado del núcleo de todo negocio u organización, percibiéndose como una de las mejores inversiones para el futuro de la empresa.

Finalmente, se hacen recomendaciones de Ciberseguridad establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, para las empresas, personal y dispositivos móviles, que desarrollarían sus funciones administrativas desde sus lugares de residencia, aplicando el teletrabajo; dado la relevancia y exposición a las que estarías inmersas las organizaciones en el ámbito del seguridad informática, razón esencial de investigación del presente trabajo de monografía para determinar las amenazas, vulnerabilidades y recomendaciones que se puedan emitir con ocasión del mismo.

---

https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&hl=es#v=onepage&q&f=false.

4.2 MARCO CONCEPTUAL

Se puede definir el teletrabajo como la actividad laboral que se desarrolla desde otros lugares que no sean las propias instalaciones de la organización. Los teletrabajadores pueden utilizar varios terminales también conocidos como *endpoints*, como ordenadores de sobremesa, portátiles, teléfonos inteligentes o tabletas, para leer y enviar correo electrónico, acceder a sitios web, crear y editar documentos, así como otras muchas tareas propias de su labor diaria.

Estos dispositivos pueden ser controlados por la organización, por terceros (contratistas/ prestadores de servicios, interlocutores comerciales o proveedores de la organización) o por los propios usuarios cuando utilizan sus dispositivos para trabajar, lo que se conoce como BYOD. La seguridad del teletrabajo también se ve afectada por el uso de estos dispositivos y de otros medios de almacenamiento extraíbles (memorias USB, discos duros, etc.), así como por el uso de aplicaciones en la nube y mecanismos de acceso remoto a la red y servidores de la empresa.

La mayoría de los teletrabajadores utilizan el acceso remoto (a través de VPN, escritorio remoto, etc.), lo que permite que los usuarios de una organización puedan acceder a los recursos informáticos de la empresa desde ubicaciones externas distintas de las instalaciones de la empresa. A lo largo de este documento se explicarán las distintas medidas necesarias para garantizar conexiones remotas seguras, proteger los dispositivos de teletrabajo, el uso seguro de la nube y las herramientas colaborativas y la seguridad en movilidad.

Activo de información: “Es cualquier información o sistema relacionado con el tratamiento de esta y que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de

información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización".[84]

Amenaza: "Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad".[85]

Análisis de riesgos: "Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo".[86]

Causa: "Se conoce como causa al fundamento, motivo, origen y principio de algo".[87]

Ciclo de Deming: "consiste en un sistema de cuatro pasos cuyo objetivo es mejorar la competitividad de la empresa. Su característica principal es que es cíclico, de modo que cada uno de los pasos alimenta al siguiente, éste al siguiente y así de manera sucesiva".[88]

---

[84] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Op.Cit., p.7.

[85] Ibíd., p.8.

[86] Ibíd., p.9.

[87] 7Graus. Significado de Causa. Significados. [Sitio WEB]. Madrid - España. La entidad. [30, octubre, 2020]. Disponible en: https://www.significados.com/causa.

[88] INFOEMPLEO. Hrtrends.Círculo de Deming: Qué Es y En Qué Beneficia a Tu Empresa. [Sitio WEB]. Madrid-España. La entidad. [7,noviembre,2020]. Disponible en: https://empresas.infoempleo.com/hrtrends/circulo-de-deming.

Confidencialidad: “Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información”.[89]

Controles: “Medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad”.[90]

Disponibilidad: “Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran”.[91]

Impacto: “Es el conjunto de consecuencias que origina un riesgo si llegará a presentarse”.[92]

Integridad: “Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales”.[93]

---

[89] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Op.Cit., p.17.

[90] INGERTEC. NORMAISO27001. [Sitio WEB]. Cordoba - España. La entidad. [17, junio, 2022]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def377/.

[91] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Op.Cit., p.21.

[92] GRUPO ALBE. Grupo Albe Consutloria. Los tres conceptos más importantes para evaluar los riesgos empresariales. [Sitio WEB]. Mexico. D.C. La entidad. [11,noviembre,2021]. Disponible en: https://www.grupoalbe.com/consultoria-empresarial-3-conceptos-sobre-como-evaluar-los-riesgos-empresariales.

[93] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Op.Cit., p.25.

MINTIC: "Siglas del Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia".[94]

MSPI: "Es la sigla del Modelo de Seguridad y Privacidad de la Información".[95]

Oficial de Seguridad: "es el profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos".[96]

Probabilidad de ocurrencia: "es utilizado para hacer referencia a la oportunidad de que algo suceda, esté definido o no, medido o determinado de forma objetiva o subjetiva, de modo cuantitativo o cualitativo".[97]

Riesgo: "es utilizado para hacer referencia a la oportunidad de que algo suceda, esté definido o no, medido o determinado de forma objetiva o subjetiva, de modo cuantitativo o cualitativo".[98]

---

[94] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio WEB]. Bogotá, D.C. La entidad. [13, septiembre,2020]. Disponible en: https://www.mintic.gov.co/portal/inicio

[95] FUNCIÓN PÚBLICA. Red de los servidores públicos. Documento Técnico - Instrumento de Evaluación MSPI. [Sitio WEB]. Bogotá D.C. La entidad. [15,septiembre,2020]. Disponible en: https://www.funcionpublica.gov.co/eva/red/publicaciones/documento-técnico---instrumento-de-evaluación-mspi.

[96] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Sistema de Gestion de Seguridad de la Informacion. Bogota D.C.: Superintendencia de Industria y Comercio, 2016. 15 p. ISBN 1098-6596.

[97] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Riesgo. Principios y Directrices. NTC-ISO/IEC 31000. Bogota D.C.:El instituto, 2011. 34 p .

[98] Ibíd., p. 4.

Seguridad de la Información: “es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable”.[99]

SI: “Un sistema de información está conformado por una serie de datos vinculados entre sí para conseguir un objetivo común”.[100]

SGSI: “Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001”.[101]

Vulnerabilidad: “Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota”.[102]

[99] AGUILERA LÓPEZ, Purificación.Op.Cit., p.9.

[100] ECONOPEDIA. Sistema de Información. [Sitio WEB]. Madrid - España. La entidad. [16, agosto, 2021]. Disponible en: https://economipedia.com/definiciones/sistema-de-informacion.html.

[101] INSTITUTO NACIONAL DE CIBERSEGURIDAD.Op.Cit., p.34.

[102] Ibíd., p.38.

4.3 MARCO LEGAL

4.3.1 Ley 1221 de 2008. Marco normativo donde se reconoce “el Teletrabajo en Colombia como modalidad laboral y como instrumento de generación de empleo y autoempleo mediante la utilización de las TIC. Por otra parte, se establece las bases para la creación de una política pública de fomento al teletrabajo y la política para su implementación. Se crea la Red Nacional de Fomento al Teletrabajo, con el propósito de promover y difundir esta práctica en el territorio colombiano”[103].

4.3.2 Ley 1273 de 2009. Se precisaron los “delitos y las conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales”[104].

4.3.3 Ley 1581 de 2012. Por medio de la cual se busca “proteger la información de las personas que esté en poder de empresas públicas o entidades privadas, las cuales tienen la responsabilidad de adaptar sus procesos con el fin de realizar un manejo adecuado de sus bases de datos”[105.].

---

[103] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1221(16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. En: Diario Oficial. Julio, 47.Nro. 052. p. 1-6.

[104] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial, Enero, 47. Nro. 223. p. 1-5.

[105] COLOMBIA COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial, Octubre, 48. Nro. 587. p. 1-15.

4.3.4 Decreto 0884 de 2012. Por el cual se reglamenta la ley 1221 de 2008 con la cual se busca promover el "teletrabajo como actividad laboral en el país. Esta norma, plantea las condiciones de contrato en cuanto a vinculación de teletrabajo a través de medios tecnológicos. También establece el tipo de responsabilidades en cuanto a seguridad social, medidas de seguridad informática y riesgos profesionales. Tal como lo señala el documento generado desde el Ministerio de Trabajo, titulado "Guía Jurídica Para la Implementación del Teletrabajo", se resume dicho decreto cinco aspectos jurídicos mediante los cuales las empresas deben usar para su implementación[106]."":

- Voluntariedad del teletrabajo.
- Acuerdo de teletrabajo.
- Modificación del reglamento interno de trabajo.
- Reporte ante la administradora de riesgos laborales.
- Reversibilidad del Teletrabajo.
- Ahora bien, para el caso de ser una entidad pública, se requiere.
- Adopción de manual de funciones y competencias laborales a la modalidad de teletrabajo.
- La resolución, decreto, o proyecto de acuerdo con que haya lugar, el cual implemente el teletrabajo al interior de la organización.

Es necesario indicar que, para la implementación de esta práctica del teletrabajo, en las entidades públicas, se sugiere recurrir al documento como hoja ruta a fin de llegar a una buena implementación de esta práctica, en aras de brindar una seguridad jurídica a las partes implicadas, y de realizar los ajustes de fondo y forma,

[106] COLOMBIA.MINISTERIO DE TRABAJO. Decreto 0884 (30, abril, 2012). Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones. Bogotá D.C.: El Ministerio, p. 1-6.

tal como lo indica el mismo documento generado desde el Ministerio de Trabajo, titulado “Guía Jurídica para la Implementación del Teletrabajo[107].

Según Mintic[108], La Voluntariedad es un elemento indispensable y un principio básico para que el teletrabajo funcione. El empleador puede proponer esta modalidad al trabajador, y este último puede aceptar o rechazar tal solicitud. El empleado puede proponer esta modalidad al empleador y a su vez, él puede aceptar o no. En ambos casos, no se estará vulnerando ningún derecho, o por lo contrario no se estará incumpliendo ninguna obligación. Así mismo en cuanto a la adopción de un manual de funciones, conforme lo menciona la guía, debe analizarse: El artículo 6 del Decreto 884 de 2012, establece que para los servidores públicos las entidades deberán adaptar los manuales de funciones y competencias laborales, con el fin de permitir y facilitar la implementación del teletrabajo como una forma de organización laboral.

4.3.5 Ley 1429 de 2010. En el Artículo 03[109] indica, la focalización de los programas de desarrollo empresarial. Dentro de los seis (6) meses siguientes a la entrada en vigor de la presente ley, el Gobierno Nacional, bajo la coordinación del Ministerio de Comercio, Industria y Turismo, deberá:

---

[107] COLOMBIA.CONCEJO DE BOGOTÁ, ‘Proyecto de Acuerdo 249 (2013). Por medio del cual se estable en el Distrito Capital, la estrategia para la implementación del Teletrabajo en Bogota. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53426.

[108] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y MINISTERIO DEL TRABAJO.Op.Cit., p.115.

[109] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1429 (29, diciembre, 2010). Por la cual se expide la Ley de Formalización y Generación de Empleo. En: Diario Oficial. Diciembre, 47. Nro. 937. p. 1-15. p 3.

- Diseñar y promover programas de formación, capacitación, asistencia técnica y asesoría especializada, que conduzcan a la formalización y generación empresarial, del empleo y el teletrabajo".

4.3.6 Ley 1562 de 2012. Por la cual se "reglamenta las obligaciones del empleador de un teletrabajador en riesgos profesionales y sistema general de seguridad y salud en el trabajo.

- Artículo 26: Modifíquese el literal g) y adiciónese el parágrafo 2 al artículo 21 del Decreto número 1295 de 1994 así:

- Parágrafo 2: Referente al teletrabajo, las obligaciones del empleador en Riesgos laborales y en el Sistema de Gestión de la Seguridad y Salud en el Trabajo SGSST son las definidas por la normatividad vigente" [110].

4.3.7 Proyecto de acuerdo 128 de 2013. Por el cual se establece en el distrito capital la estrategia para la implementación del teletrabajo.

- Contexto: El presente Proyecto de Acuerdo tiene como objetivo mejorar las condiciones laborales del trabajador, empleado o colaborador, su calidad de vida, la de su familia y en general la relación con el entorno, además de causar un impacto positivo en la movilidad y en el medio ambiente para Bogotá.

Bajo esta premisa, es pertinente señalar la sentencia C-337 de 2011 de la Corte Constitucional, ya que se constituye en el primer pronunciamiento jurídico, en el cual este Alto Tribunal plantea directamente la figura del teletrabajo, ratificando que se

[110] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1562 (11, julio, 2012). Por la cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materias de salud ocupacional. En: Diario Oficial. Julio, 47. Nro 937. p. 1-22.

deben garantizar a los teletrabajadores distintos beneficios, entre ellos el subsidio familiar y todas las prerrogativas propias consagradas en la legislación laboral vigente.

Con este normativo, no se intenta promover o permitir formas de explotación o flexibilidad laboral, en perjuicio del trabajador, que deriven en la promoción de algún tipo de informalidad laboral; la práctica del Teletrabajo debe constituirse en apoyo al trabajador y a la promoción del empleo digno en el Distrito Capital.

5. DESARROLLO DE LOS OBJETIVOS

5.1 RIESGOS INFORMÁTICOS EN LA IMPLEMENTACIÓN DEL TELETRABAJO

Uno de los principales cambios que nos dejó la pandemia en términos laborales fue la modalidad del teletrabajo o trabajo en remoto, que si bien existía desde antes, solo hasta hace un poco más de dos años (marzo de 2020) fue implementada masivamente por empresas de todo el mundo, que vieron en esta una rápida solución para continuar con sus operaciones y la prestación de sus servicios (las que no requerían de la presencialidad). Y aunque esta modalidad de trabajo, que actualmente sigue siendo implementada por organizaciones de diferentes sectores y tamaños, representa grandes ventajas tanto para los directivos como para los empleados, es importante tener en cuenta que sin las medidas preventivas y de protección adecuadas puede poner en riesgo y generar impactos negativos en la seguridad de la información.

La pandemia desafió la continuidad del negocio de las empresas a nivel mundial, puesto que muchas entidades no estaban preparadas para asumir los retos de la implementación del teletrabajo en sus organizaciones, en una encuesta de seguridad realizada por la empresa Cisco[111] denominada: Una visión 20/20 para la Ciberseguridad, desarrollada a finales del año 2019 y publicada en el *Benchmark Report* en el mes de febrero del año 2020, se evidenció que las empresas constantemente están expuestas a ataques, donde se destacó que el 17% informaron haber recibido más de 100.000 o incluso más alertas de seguridad por

[111] CISCO. Cisco Cybersecurity Report Series 2020. [Sitio WEB]. San José - California. La entidad. [Consultado 25, junio, 2021]. Disponible en: https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf.

día, generando caos en los departamentos de TI de las entidades. A pesar de los esfuerzos empresariales para mitigar la perdida y o fuga de información, eran evidente los fallos de seguridad con la adopción de esta nueva modalidad de trabajo en casa. Como lo indica Mike Spaulding[112] experto en seguridad de la información y director de operaciones de la empresa Vertiv, hay varios riesgos de fraudes electrónicos que debe tener en cuenta, entre ellos se destacan la usurpación de marca, la suplantación de figuras de autoridad -donde los atacantes envían correos electrónicos directos y se hacen pasar por áreas como TI, Recursos Humanos o Finanzas, de ahí la importancia de fortalecer los controles al personal de empleados que se encontraban en trabajo en casa, pues son el reto continuo de las empresas y suelen ser fáciles de explotar por los cibercriminales aprovechando el miedo y confusión de los empleados frente a los diferentes eventos mundiales y las nuevas prácticas laborales.

El instituto Ponemon[113], en su tercer informe anual de Riesgos de Datos en el Ecosistemas de Terceros, publicado en el mes de noviembre del año 2018, descubrió que el 59% de las empresas había sufrido una filtración de datos debido a un tercero. Por ello al tener en cuenta las recomendaciones y lista de riesgos que se exponen en los documentos y encuestas de seguridad anteriormente citadas, se realizó la identificación y análisis de los riesgos probables que se pueden evidenciar con mayor frecuencia así:

- Alteración y destrucción de datos en bases de datos.

---

[112] SPAULDING Mike and FULKERT Kate. Las Cambiantes Amenazas a las Redes de TI Exigen una Mayor Vigilancia. [En Línea]. Latinoamerica.: 2020. [Consultado 3,noviembre, 2020]. Disponible en: https://www.vertiv.com/es-emea/about/news-and-insights/articles/blog-posts/threats-to-it-networks-are-changing-requiring-greater-vigilance.

[113] PONEMON INSTITUTE. Data Risk in the Third-Party Ecosystem. [Sitio WEB]. Traverse - Michigan. La entidad. [Consultado 7, noviembre, 2020]. Disponible en: https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/.

La inadecuada administración y la inexistencia de políticas de seguridad pueden ocasionar perdidas de información esencial para el normal funcionamiento de la empresa, igualmente afectaría la reputación e imagen empresarial.

- Acceso por usuarios no autorizados a la base de datos.
  Todo tipo de ingreso y operación no autorizada a los sistemas de información puede comprometer la operación de la entidad e inclusive evidenciarse fuga de información crítica de la empresa.

- Robo de información.
  Este tipo de evento se produce por la ausencia de controles encaminados a la seguridad de la información, conllevando a la violación de secretos empresariales sin la autorización del dueño titular de esta.

- Acceso a datos sensibles o privados de los documentos del proceso. El inapropiado uso de contraseñas y políticas de seguridad de la información a nivel interno en la empresa, brindan la oportunidad al ciberdelincuente de acceder a información privilegiada de la empresa, aprovechando el desconocimiento en materia de seguridad para cometer su propósito de sustraer información.

- Modificación a información privada.
  Se debe realizar la asignación de permisos y roles para el acceso de la información catalogada sensible para la empresa, según el perfil y el cargo del funcionario, debido a que al ser expuesta generaría traumatismos administrativos y altos costos.

- Destrucción de copias de respaldos.
  Si no se tiene establecido un procedimiento de Backup y un plan de recuperación ante incidentes informáticos, sería catastrófico para la empresa no contar con los medios para el restablecimiento de la información y reiniciar sus operaciones,

afectando a clientes, proveedores y funcionarios para el normal funcionamiento de la empresa.

- Riesgo en la integridad del *Software* y la información, por la instalación de *software* sin autorización del área de sistemas o el coordinador de IT.
  La falta de controles en los perfiles y roles en los equipos de cómputo, generan grandes vacíos de seguridad, dando oportunidad para la instalación de *software* no autorizado por el área encargada en la empresa.

- Pérdida de información por error de *Hardware*.
  Es importante contar con un cronograma de mantenimiento preventivo, a fin de realizar verificaciones al *hardware* de la empresa, para mitigar la pérdida o daño en la infraestructura tecnológica.

- Descarga y Propagación de virus por navegación en la web.
  Configurar de forma granular en los equipos de seguridad perimétrica, los permisos de navegación para los usuarios de la empresa, esto de la mano con antivirus y antispam para fortalecer los controles establecidos y evitar la transmisión de *malware* al interior de la empresa.

- Una conexión a una red inalámbrica desconocida o una conexión habilitada sin seguridad, es decir, no se solicita una clave de inicio de sesión.
  Es importante tener presente que las redes inalámbricas están expuestas a ataques de seguridad y son aprovechadas por los ciberdelincuentes para sustraer información esencial para la empresa mediante un tercero, que este caso sería el empleado, aprovechando vulnerabilidades existentes en mencionada red de conexión.

- Divulgación indebida o accidental de credenciales para el establecimiento de la VPN.

La inadecuada administración en seguridad de la información en las credenciales de acceso y contraseñas no seguras, son un factor determinante al momento de realizar la asignación de roles y permisos para el acceso mediante el uso de VPN, por ello la entrega de mencionadas claves de acceso al usuario final se deben notificar mediante el correo electrónico institucional, una vez notificado el usuario será responsable de su uso.

- Almacenamiento indebido de información, ya sea en dispositivos no autorizados o sin la seguridad necesaria.
  Es importante concientizar a los funcionarios de la empresa, en cuanto a malas prácticas al momento de almacenar o guardar información de la entidad en dispositivos móviles y equipos de cómputo personales, puesto que, en caso de materializarse fuga o pérdida de información, estarán inmersos en investigaciones jurídicas y disciplinarias.

- Archivos de respaldo.
  Es esencial contar con un procedimiento de Backup ante una contingencia que se pueda presentar en caso de materializarse un riesgo asociado a la pérdida de información.

- Robo de equipos por necesidad de traslado.
  Los equipos de cómputo que por necesidades de la implementación del teletrabajo requieran de su uso por fuera de la empresa, deben contar con los controles pertinentes de seguridad para asegurar la información institucional que reposa en ellos.

- Manejo en los equipos de información no empresarial (música, videos, juegos, etc.).
  Se deben establecer controles, revistas y monitoreo constante en relación con la información personal que los funcionarios contengan en los equipos de

cómputo, puesto que, por política de seguridad, está restringido el almacenamiento de información que no sea de uso institucional.

- Fuga de información por otro medio electrónico.
  Es importante generar cultura de seguridad de la información a todo nivel en la empresa, visto que todos los funcionarios deben velar por el buen uso de los activos de información, fortaleciendo las medidas de autocuidado de la mano de los equipos de seguridad perimétrica que están blindando el activo más valioso de la empresa, por ello se deben fortalecer controles asociados a la fuga de información.

En síntesis, el teletrabajo se convierte es un modelo eficaz, en el cual muchas organizaciones recurren a esta práctica para que sus empleados y directivos cumplan con las tareas propias de sus cargos; es indispensable velar por salvaguardar la información e implementar diferentes acciones y medidas confiables, con el fin de evaluar en todos los niveles de la organización, la importancia de establecer y determinar los riesgos asociados a la puesta en marcha de citada modalidad de trabajo, evitando la materialización de riesgos asociados a esta, siendo el análisis de riesgos la clave para garantizar la seguridad de la información en la entidad.

5.2 MODELO DE SEGURIDAD INFORMÁTICA PARA TELETRABAJO

Dado que la información se ha convertido en un recurso estratégico que debe ser utilizado de manera segura, generar transacciones de alta calidad, contar con controles de acceso a la información, es necesario implementar un modelo de gestión de seguridad de la información que ayude a las organizaciones a manejar los datos de manera responsable, proteger la información, las buenas prácticas y obtener evidencia durante la auditoría y desarrollar acciones preventivas y correctivas.

La aplicación de este modelo es necesaria en una organización ya que asegura la integridad, confidencialidad, disponibilidad y exactitud de la información, reduciendo así la vulnerabilidad ante ataques, brindando en algunos casos una ruta a seguir, generando planes de acción y mejorando y haciendo cumplir los controles a través de auditorías.

El modelo de seguridad de la información que se adaptaría con bastante facilidad a las entidades con la implementación del teletrabajo, es el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea – (MSPI)[114], este contempla un ciclo de operación que consta de cinco (05) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información, enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad alineados al teletrabajo.

[114] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

5.2.1 Fase Diagnóstico. En esta fase se identifica el estado actual de la empresa.

5.2.2 Fase Planificación (Planear). Se establecen los objetivos a alcanzar y las tareas que se deben mejorar, así mismos indicadores que sean medibles para controlar y cuantificar los objetivos.

5.2.3 Fase Implementación (Hacer). En esta fase se efectúa el plan establecido para la ejecutar acciones de las mejoras establecidas.

5.2.4 Fase Evaluación de desempeño (Verificar). Una vez determinada las acciones de mejora, se establece el tiempo para su implementación.

5.2.5 Fase Mejora Continua (Actuar). Se examinan los resultados de las acciones de mejora determinadas, con el fin de analizar su efectividad y eficacia.

5.2.6 Marco de Referencia de Seguridad Informática. Para el desarrollo de la presente guía se tiene como marco normativo la norma ISO 27001:2013, que sirve como guía para evaluar y determinar posibles riesgos, brindando estrategias y controles eficaces para mitigar la pérdida o fuga de información, alineado al modelo MSPI.

Tabla 1. MSPI vs ISO 27001

Fase	Anexo “A” ISO 27001:2013
Diagnóstico	4. Contexto de la Organización
Planificación	5. Liderazgo
	6. Planificación
	7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño

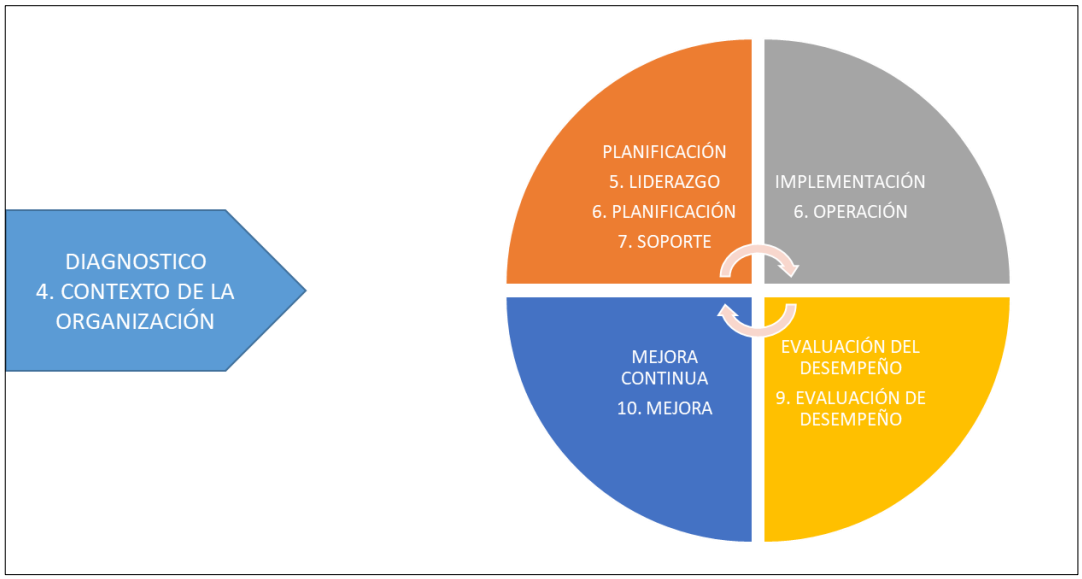
Mejora Continua	10. Mejora

Fuente: Elaboración propia del autor

5.3 DESARROLLO DEL MODELO MSPI POR FASES

El funcionamiento del ciclo de ejecución del modelo MSPI se establece de manera detallada en cinco (5) fases como se describe en la “Ilustración 1 – Modelo MSPI Ciclo PHVA”. Citado ciclo contiene metas, objetivos y herramientas (orientación) para hacer de la seguridad y privacidad de la información un sistema de gestión sostenible dentro de una entidad de la mano del ciclo PHVA con el fin de establecer una hoja de ruta para cumplir las tareas inmersas en la implementación del modelo descrito.

Ilustración 1 Modelo MSPI – Ciclo PHVA



Fuente: Modelo de Seguridad y Privacidad de la Información[115].

[115] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf>.

5.3.1 Fase de diagnóstico.

5.3.1.1 Capítulo 4 - Contexto de la organización: “En la norma ISO 27001:2013, se trata del punto de partida para desarrollar el SGSI y consiste en determinar o identificar los “problemas” internos y externos a los que se enfrenta la organización”.[116]

5.3.2 Fase planeación.

5.3.2.1 Capítulo 5 – Liderazgo. En la norma ISO 27001:2013, se requiere de una “participación y compromiso de la alta dirección de la organización evitando situaciones de indiferencia frente a la mejora continua de los procesos de la entidad”.[117]

5.3.3 Capítulo 6 – Planeación. En la norma ISO 27001:2013, la “identificación de los riesgos y oportunidades que afectan al contexto de la organización se evidencian en el apartado correspondiente de la norma Sección 4 el contexto de la organización donde se determinan en base a las necesidades y expectativas de las partes interesadas en relación con la seguridad de la información”.[118]

5.3.4 Capítulo 7 – Soporte. En la norma ISO 27001:2013, la “implementación de un SGSI es necesariamente disponer de los recursos necesarios para que el sistema de gestión pueda llevarse a cabo según lo planeado”.[119]

---

[116] INGERTEC. NORMAISO27001. [Sitio WEB]. Cordoba - España. La entidad. [25, mayo, 2020]. Disponible en: https://normaiso27001.es/fase-2-analisis-del-contexto-de-la-organizacion-y-determinacion-del-alcance/.

[117] Ibíd.

[118] Ibíd.

[119] Ibíd.

5.3.5 Fase implementación.

5.3.5.1 Capítulo 8 – Operación. En la norma ISO 27001:2013, se presentan una serie de requisitos y medidas adecuadas para lograr los objetivos de la Seguridad de la Información.[120]

5.3.6 Fase evaluación del desempeño.

5.3.6.1 Capítulo 9 - Evaluación del desempeño. En la norma ISO 27001:2013, se requiere "evaluar para medir el rendimiento del SGSI. Se trata de determinar los cursos de acción para medir, controlar, cuándo, quién y cómo".[121]

5.3.7 Fase mejora continua.

5.3.7.1 Capítulo 10 – Mejora. En la norma ISO 27001:2013, enfoque "basado en el riesgo, el papel de las acciones preventivas como tal deja su lugar a las conclusiones del análisis de riesgos".[122]

5.3.8 Lineamientos para el teletrabajo. En todas las organizaciones se deben establecer lineamientos claros de seguridad para el teletrabajo. Estos comprenden:

---

[120] Ibíd.

[121] Ibíd.

[122] Ibíd.

5.3.8.1 Descripción del servicio y conexión remota a la red de datos.

Para desarrollar las actividades es probable que se necesite un enlace directo a la red de la organización mediante una red privada virtual que cumpla con los criterios mínimos de conexión para garantizar la confidencialidad e integridad en la transferencia de la información. En caso de que el colaborador no requiera hacer uso de los servicios descritos, no se hace necesario la asignación de una Red Privada Virtual, pero deberá apoyarse en las herramientas colaborativas dispuestas por la organización.

Para tales efectos se deberá instalar en el equipo de cómputo asignado al trabajador el *software* y las credenciales de acceso requeridas para el establecimiento de la Red Privada Virtual. En ninguna situación especial se autorizará la instalación de *software* institucional en los equipos de cómputo de propiedad del Teletrabajador. Al momento de establecer la conexión remota se deberá tener en cuenta:

- No se deben realizar conexiones a redes inalámbricas que no cuenten con la seguridad mínima, en otras palabras, que no solicite credenciales de acceso. El riesgo es que una persona no autorizada pueda obtener información de forma indebida.

- Se deben cambiar periódicamente las credenciales y claves de acceso a la Red Privada Virtual. Dichas solicitudes de cambio se registran por el servicio de soporte técnico de la organización.

- Las claves y credenciales asignadas son personales y su uso indebido es responsabilidad solo del teletrabajador.

5.3.8.2 Repositorio de información. Usar el almacenamiento establecido por la organización para alojar la información. Si se utilizan los discos duros de los equipos asignados se debe propender por el uso de una partición protegida y descargar periódicamente la información en los repositorios de la organización para evitar que, en la eventualidad de hurto, perdida o daño del equipo, la información de la organización quede expuesta.

- El área de soporte técnico de la organización debe instalar una herramienta que permita el cifrado de disco para salvaguardar la información almacenada.

- La organización puede limitar o restringir el uso de USB, Unidades CD/DVD, Discos externos, con el fin de evitar pérdida o fuga de información sensible para la organización y garantizar la protección de los datos.

- Si por alguna razón se hace necesario el uso de información física o almacenada en dispositivos extraíbles para el ejercicio de la labor del teletrabajador, este debe hacerse responsable por salvaguardar la data. Se recomienda tener medidas preventivas para proteger los bienes preferiblemente bajo llave y en un lugar seguro.

5.3.8.3 Acceso a servidores de archivos. De acuerdo con el perfil y al cargo se debe asignar el acceso a los servidores de archivos de la organización teniendo en cuenta los siguientes aspectos:

- Se debe velar por la seguridad y confidencialidad de la información contenida en los servidores de archivo.

- El teletrabajador debe evitar compartir el equipo de cómputo con personas no autorizadas, para evitar accesos no permitidos a la información de la organización.

5.3.8.4 Acceso a los sistemas de información. Las credenciales de acceso a los sistemas de información de la organización se asignan de acuerdo con los perfiles y cargos autorizados por la gerencia. Se debe tener en cuenta:

- El Teletrabajador, para acceder a los sistemas de información, debe hacerlo con las credenciales asignadas.

- Dichas credenciales son de uso personal e intransferible. No deben divulgarse ni compartirse.

- El teletrabajador se compromete a salvaguardar la información contenida en los diferentes sistemas de información a los que se tenga acceso autorizado, evitando compartir el equipo de cómputo con personas ajenas.

5.3.8.5 Uso de *software* y *hardware*. El *software* y el *hardware* asignado por la entidad, para el cumplimiento de la modalidad de Teletrabajo se debe utilizar exclusivamente para ejecutar actividades laborales establecidas. Por esta razón, se deben tener en cuenta los siguientes aspectos:

- Evitar la apertura de correos electrónicos, descargar o ejecutar archivos adjuntos de los cuales no se conozca su emisario. Este tipo de práctica es una de las principales fuentes de propagación de *malware*, que pueden afectar de manera irreversible las estaciones de trabajo y la confidencialidad de la información de las organizaciones.

- Es importante no abrir y/o ejecutar ventanas emergentes en los diferentes navegadores, instalar barras de herramientas adicionales, programas, enlaces desconocidos de los cuales no se cuente con la seguridad de su uso y estos pueden conducir a sitios de suplantación web para capturar datos que pueden afectar la disponibilidad, integridad y confidencialidad de la información de la organización.

- Se debe restringir la instalación de *software* no autorizados por la organización y que no estén alineados al desarrollo de las funciones de las tareas asignadas. Solo el personal de TI de la organización es el autorizado para realizar la instalación *software* en los equipos de cómputo institucionales.

- El área de soporte técnico deberá realizar el alistamiento correspondiente en los equipos de cómputo institucionales, en los cuales deberá contar con antivirus para proteger el equipo de posibles amenazas de virus, así mismo el Teletrabajador deberá comprobar el correcto funcionamiento de este, y si se presenta alguna falla técnica deberá ser reportada a la mesa de servicio de soporte. Es de tener presente que una vez sea asignado el equipo de cómputo el Teletrabajador es directamente responsable por los daños ocasionados y por el mal uso de estos, por lo tanto, se tienen en cuenta las siguientes recomendaciones:

    - El equipo de cómputo es para uso exclusivo en el lugar de residencia por lo tanto no debe estar expuesto a sitios públicos.

    - Hacer uso del equipo de cómputo asignado únicamente en el lugar de teletrabajo aprobado por la organización. Este espacio debe contar con las

condiciones de seguridad física para proteger los recursos de la organización.

- Evitar exponer el equipo de cómputo a zonas donde exista un alto grado de humedad, puesto que puede dañar el *hardware*.

- Evitar golpes y consumir líquidos mientras se desarrollan actividades de Teletrabajo ya que existe el riesgo de avería parcial o total del equipo de cómputo.

- Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento, esto generaría daño en la fuente y a nivel general.

- En caso de robo o pérdida del equipo de cómputo, el funcionario que se encuentre bajo la modalidad de Teletrabajo debe informar inmediatamente al área de soporte técnico y realizar el respectivo denuncio ante la entidad competente.

- Cualquier *software* adicional que sea instalado al momento de la entrega del equipo de cómputo, deberá ser notificado al personal del área de soporte técnico para efectos de inventario.

- No está autorizado ningún tipo de modificación en el *hardware*.

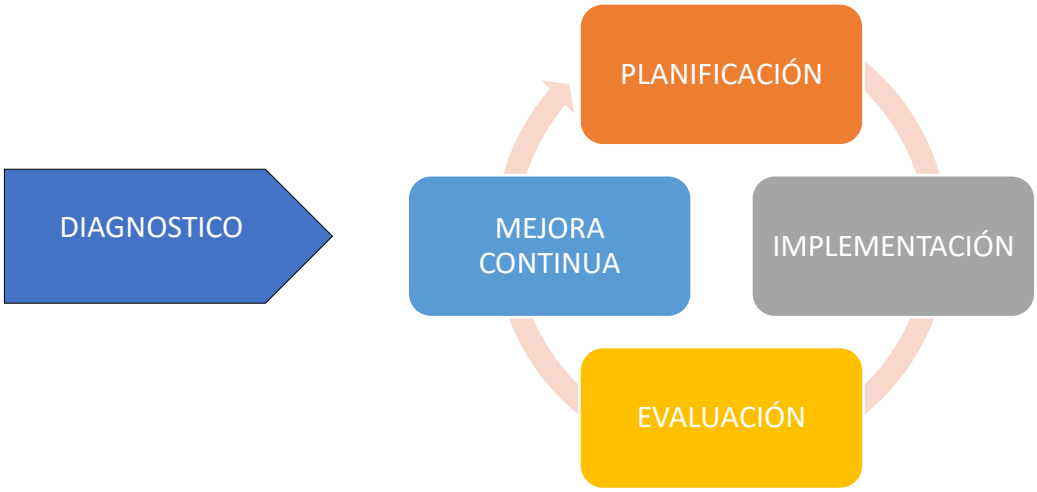
- El Teletrabajador debe verificar el estado en el cual es entregado el equipo en el momento de su recepción. Para ello se genera un formato de entrega que debe ser firmado indicando conformidad en la entrega y recepción por parte del Teletrabajador y el área de soporte técnico.

Por tanto, el modelo de seguridad informática se convierte en una herramienta esencial en las organizaciones, porque ayudan a identificar riesgos y proponen controles para ayudar a minimizarlos, y permiten la confidencialidad e integridad de los datos y la información, esto de acuerdo con la gran cantidad de datos que procesan las entidades, lo que requiere generar controles de acceso definidos por roles y permisos de usuarios para acceder a la información, evitar amenazas y garantizar el normal funcionamiento del sistema. El modelo propuesto en este documento tendrá el potencial de superar las debilidades de seguridad y privacidad de la información en las entidades y que puede ser utilizado por entes públicos como privados.

5.4 MODELO DE GESTIÓN DE SEGURIDAD

La seguridad y la privacidad de la información es un componente de apoyo horizontal de la política de seguridad de la información de la entidad, por ello es importante el desarrollo y la implementación de un modelo de seguridad que se centre en proteger la confidencialidad, la integridad y la disponibilidad de la información, ayudando al cumplimiento de la misión y los objetivos estratégicos de la entidad. Por ello, es indispensable tener presente la “Ilustración 2 -Diagrama Modelo MSPI” en la cual se establece la manera adecuada para implementar el modelo que se propone en el marco del desarrollo de la presente guía, por ello se plasma el siguiente diagrama donde se resume el paso a paso para cumplir con lo establecido en el modelo planteado.

Ilustración 2 Diagrama Modelo MSPI



Fuente: Modelo de Seguridad y Privacidad de la Información[123].

[123] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

5.4.1 Fase I Diagnóstico - Etapas previas a la implementación. Se realiza un análisis minucioso del estado actual de la entidad en relación con el modelo de seguridad y privacidad de la información, para ello es importante tener presente lo que se indica en la "Ilustración 3 – Etapa previa a la implementación", donde se debe realizar una serie de actividades que anteceden a la implementación del modelo:

Ilustración 3 Etapa previa a la Implementación MSPI

Fuente: Modelo de Seguridad y Privacidad de la Información[124].

Para tener claridad las tareas a desarrollar en la fase de diagnóstico, el Modelo de Seguridad y Privacidad de la Información – MSPI, establece mediante la "Tabla 2 – Metas y Actividades Fase Implementación", en donde se determina la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se cuente con el resultado inicial y se determine el nivel de madurez la entidad puede proceder con la siguiente etapa que es la de planificación.

[124] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Tabla 2. Metas y Actividades Fase Implementación

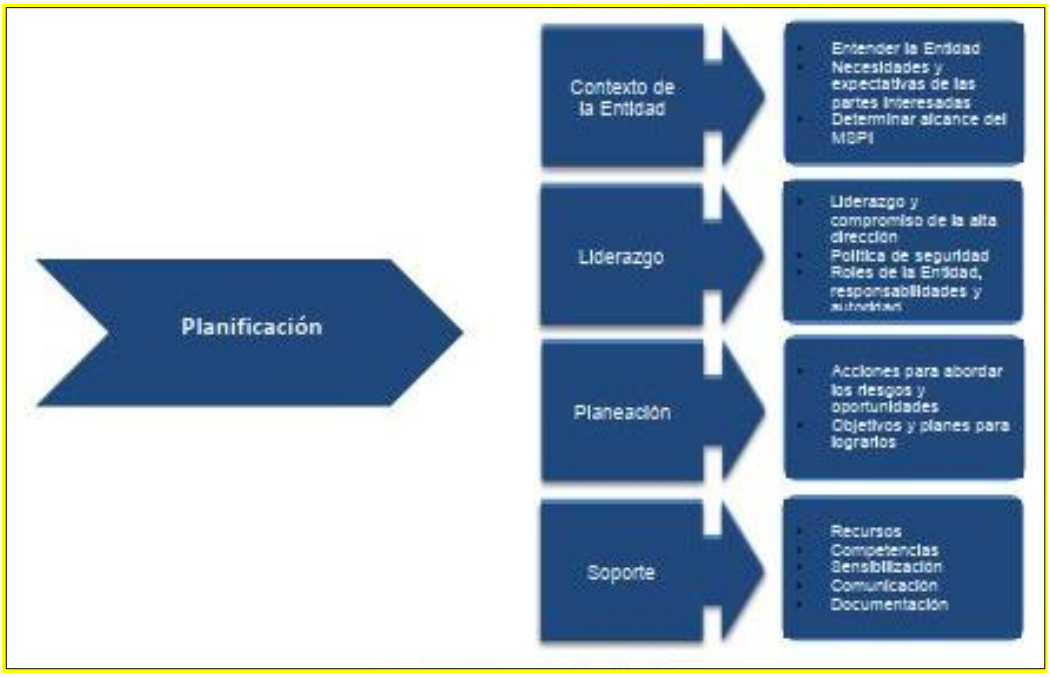
Metas	Actividades
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Diagnóstico de la situación actual de la entidad con relación a la Gestión de seguridad de la información. Diagnóstico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la Norma ISO 27001:2013. Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.

Fuente: Modelo de Seguridad y Privacidad de la Información[125].

5.4.2 Fase II Planificación. Es vital el desarrollo de la etapa anterior, puesto que es el insumo para proceder a elaborar el plan de seguridad y privacidad de la información, se estudian de manera acertada y alineado a los objetivos misionales de la entidad, con el firme propósito de implementar las acciones a nivel de seguridad y privacidad de la información, mediante una metodología de gestión del riesgo, por ello en la "Ilustración 4 – Fase de Planificación MSPI", se determinan una serie de actividades en la cual la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

[125] Ibíd .

Ilustración 4 Fase de Planificación – MSPI



Fuente: Modelo de Seguridad y Privacidad de la Información[126].

En la "Tabla 3 – Metas y Actividades Fase de Planificación", se explica de manera general la fase de planificación del Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en esta fase.

Tabla 3. Metas y Actividades Fase de Planificación

Metas	Actividades
Realizar un análisis interno y externo de la entidad, roles, responsables, funciones, metodología de riesgos, políticas de seguridad y privacidad de la información	Análisis del contexto de la entidad con relación al capítulo 4,5,6 y 7 de la norma ISO 27001:2013

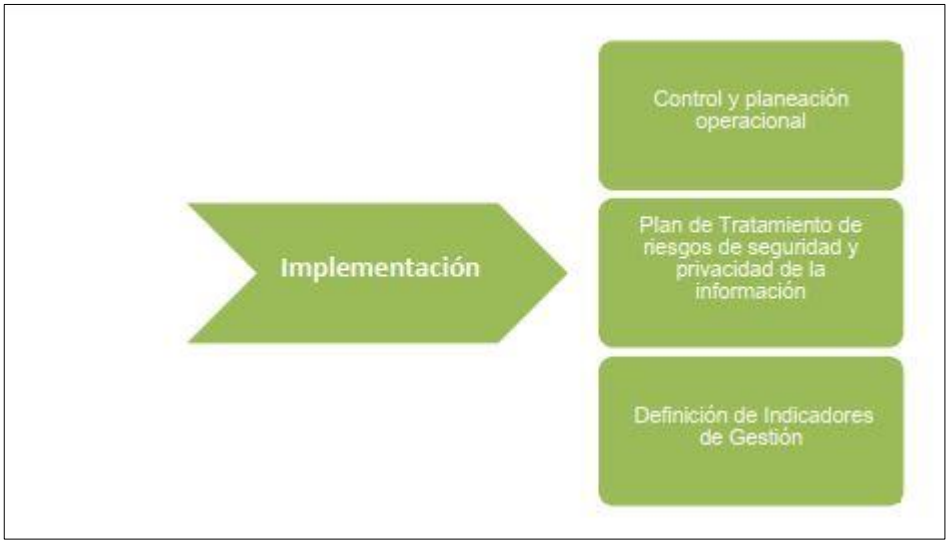
Fuente: Modelo de Seguridad y Privacidad de la Información[127].

[126] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

[127] Ibíd .

5.4.3 Fase III Implementación. Esta etapa se determinará la "planificación realizada en la fase anterior del MSPI", por tal manera es importante ejecutar lo estipulado en la "Ilustración 5 – Fase de Implementación MSPI".[128]

Ilustración 5 Fase de Implementación - MSPI



Fuente: Modelo de Seguridad y Privacidad de la Información[129].

Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades como corresponde en la "Tabla 4 – Metas y Actividades Fase de Implementación".

Tabla 4. Metas y Actividades Fase de Implementación

Metas	Actividades
Establecer el plan de seguridad informática, plan de tratamiento de riesgos, indicadores de gestión de	Plan de implementación del modelo de seguridad y privacidad de la información, así mismo ejecutar todos

[128] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad.[En Línea]. Bogota, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

[129] Ibíd.

seguridad, procedimiento de gestión de incidentes, gestión de vulnerabilidades, plan de capacitación de seguridad informática, pruebas de vulnerabilidad.	los planes establecidos para el modelo de seguridad de la información, establecido en el capitulo 8 de la norma ISO 27001:2013.

Fuente: Modelo de Seguridad y Privacidad de la Información[130].

5.4.4 Fase IV Evaluación de desempeño. El proceso de "seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas",[131] se debe tener en cuenta la "Ilustración 6 – Fase de Evaluación de Desempeño MSPI", que permite orientar como se desarrolla la evaluación de desempeño.

Ilustración 6 Fase de Evaluación de Desempeño - MSPI

Fuente: Modelo de Seguridad y Privacidad de la Información[132].

En esta parte del proceso la entidad debe crear un plan que contemple actividades tales como las fijadas en la "Tabla 5 – Metas y Actividades Fase de Evaluación de Desempeño", en donde el plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles

[130] Ibíd.

[131] Ibíd.

[132] Ibíd .

permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

Tabla 5. Metas y Actividades Fase de Evaluación de Desempeño

Metas	Actividades
Ejecución de auditorías, plan de seguimiento de evaluación y análisis del SGSI	Ejecución de auditorías la modelo de seguridad, en relación con temas normativos y de estricto cumplimiento previa aprobación por la alta dirección, así mimos documento con el plan de seguimiento, evaluación y análisis del modelo, establecido en el capítulo 9 de la norma ISO 27001:2013.

Fuente: Modelo de Seguridad y Privacidad de la Información[133].

[133] Ibíd .

5.4.5 Fase de mejora continua. Se consolida los "resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información",[134] como se determinan en la "Ilustración 7 – Fase de Mejoramiento Continuo MSPI", donde se deben consolidar los resultados obtenidos, tomando las acciones oportunas para mitigar las debilidades identificadas.

Ilustración 7 Fase de Mejoramiento Continuo – MSPI

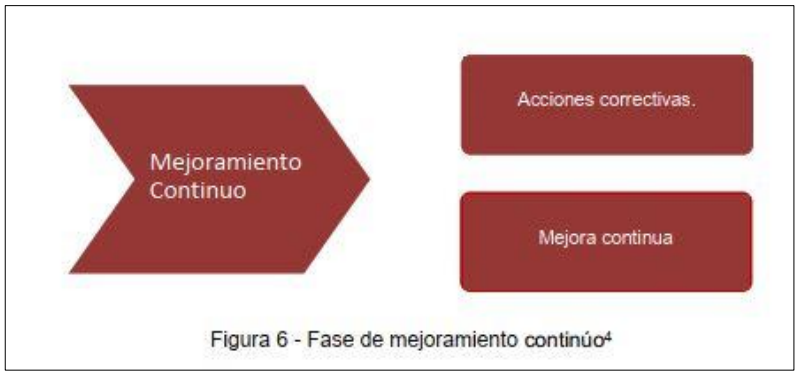


Figura 6 - Fase de mejoramiento continúo[4]

Fuente: Modelo de Seguridad y Privacidad de la Información[135].

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua como se establece en la "Tabla 6 – Metas y Actividades Fase de Mejoramiento Continuo", con base en los resultados de la fase de evaluación del desempeño.

Tabla 6. Metas y Actividades Fase de Mejoramiento Continuo

Metas	Actividades
Diseñar el plan de mejoramiento	Establecer el plan de mejoramiento de seguridad y privacidad de la información que permita corregir las acciones identificadas para el sistema de gestión de seguridad de la

[134] Ibíd.

[135] Ibíd .

	información, establecido en el capítulo 10 de la norma ISO 27001:2013

Fuente: Modelo de Seguridad y Privacidad de la Información[136].

Es importante al momento de realizar la implementación del modelo de seguridad, el cumplimiento de las diferentes fases establecidas para fortalecer los procesos de seguridad de la información a nivel interno y externo de la empresa, así mismo se definen buenas prácticas a nivel de seguridad de la información que complementan el modelo sugerido en la presente guía, con el fin de aunar esfuerzos, blindando a las entidades con la implementación del teletrabajo ante posibles amenazas que se puedan presentar en la infraestructura tecnológica de la empresa.

5.4.6 Buenas prácticas para el teletrabajo. Esta guía de buenas prácticas para la protección de la información, está dirigida a los posibles riesgos que pueden surgir durante la implementación del teletrabajo y que deben ser considerados relevantes al momento de la implementación de esta modalidad de trabajo, en especial atención, a la tendencia creciente de utilizar ocasionalmente equipos de cómputo personales para realizar actividades laborales desde el lugar de residencia, durante un tiempo determinado, para mantenerse en contacto con el entorno de trabajo, realizar seguimiento de las tareas o proyectos, o para resolver problemas urgentes en los cuales no pueden trasladarse físicamente al lugar de trabajo.

Aunque la lista de recomendaciones que se mencionan a continuación para salvaguardar la información no es exhaustiva, si se consideran críticas. Se debe tener presente que cualquier forma de teletrabajo, debe ser aprobada formalmente por la gerencia y así mismo tener un control exhaustivo en relación con los usuarios que utilizan este método. Por lo anterior, se listan recomendaciones respecto a situaciones críticas que pueden presentarse en la entidad con la adopción de esta modalidad de trabajo:

[136] Ibíd .

5.4.6.1 Acceso por usuarios no autorizados a la base de datos.

- Instaurar y ejecutar el procedimiento de administración de usuarios y contraseñas a través del cual se formalizan las solicitudes de acceso y los privilegios correspondientes.

- Implantar los controles de acceso lógico correspondientes de acuerdo con los servicios de red, los componentes de la plataforma tecnológica o los sistemas de información, considerando los riesgos a los que se encuentra expuesta la información contenida en ellos y las políticas de seguridad de la información.

- Establecer los perfiles y roles de acceso lógico de usuarios o grupos de usuarios, considerando segregación de funciones y limitación de accesos según necesidad de uso, de acuerdo con sus funciones y las políticas de seguridad de la información.

- Monitorear la efectividad de los controles de acceso lógico implantados, con el objetivo de generar propuestas de mejora de acuerdo con las políticas de seguridad de la información.

5.4.6.2 Robo de información.

- Establecer canales para el reporte de eventos de seguridad de la información.

- Clasificar los eventos que corresponden y no corresponden a incidentes de seguridad de la información.

- Definir y establecer procedimientos para asegurar una adecuada gestión de los incidentes de seguridad de la información, considerando aspectos como el

tratamiento del incidente y la recolección de evidencia cuando así se requiera. De ser necesario, poner denuncia ante las autoridades competentes.

- Capacitar al personal sobre que es un incidente de seguridad de la información y cuál es el procedimiento que se debe seguir en caso de presentarse uno.

- Establecer los mecanismos que se usaran para la recolección de evidencias.
- Instaurar mecanismos para cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

5.4.6.3 Acceso a datos sensibles o privados de los documentos del proceso.

- Revisar los perfiles y roles de acceso lógico de usuarios o grupos de usuarios, de acuerdo con las funciones de cargo y las políticas de seguridad de la información en cada uno de los sistemas de información existentes, servicios de red y recursos tecnológicos, con fin de ratificar o de ser necesario ajustar, los perfiles y roles de acuerdo con los cambios detectados durante la revisión.

- Llevar a cabo cuando resulte necesario, el ajuste de los perfiles y roles, siguiendo el procedimiento de administración de usuarios y contraseñas por el cual se deben realizar este tipo de cambios, generando registros de control.

5.4.6.4 Modificación a información privada.

- Implementar un servidor de logs para el monitoreo periódico de los eventos de seguridad.

- Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema.

- Realizar la configuración de protocolos, puertos y servicios necesarios para el desarrollo de las labores en las estaciones de usuario de la empresa.

- Establecer políticas de dominio y listas de acceso que rijan las configuraciones de las estaciones de usuario.

- Renombrar las cuentas de administrador y proteger o deshabilitar las cuentas de invitado en las estaciones de usuario, con el fin mitigar los riesgos relacionados con los nombres de usuario y cuentas por defecto.

- Verificar y optimizar los procesos y servicios de arranque de los sistemas operativos de las estaciones de usuario.

- Actualizar los componentes de *software* y los parches de seguridad de las estaciones de usuario siguiendo los lineamientos para la gestión del cambio.

- Habilitar y personalizar los mecanismos de auditoría y monitoreo de las estaciones de usuario, considerando aspectos como la generación de registros sobre las acciones de los administradores, eliminación de registros de auditoría y acceso a diferentes elementos del sistema.

- Seguir buenas prácticas y guías de aseguramiento de acuerdo con el sistema operativo con el que cuenten las estaciones de usuario.

5.4.6.5 Archivos de respaldo.

- Elaborar el procedimiento de copias de respaldo junto a un formato asociado en el cual se deben consignar los registros de dichas copias.

- Divulgar y establecer el procedimiento de copias de respaldo junto con el formato asociado.

- Definir la frecuencia de generación de copias de respaldo considerando aspectos como los requisitos de seguridad de la información involucrada y la importancia de la continuidad en la operación.
- Definir el sitio de custodia externa y, de ser necesario, suscribir los contratos o convenios para dicha custodia.

- Establecer períodos para realizar pruebas de restauración de información aleatorias a partir de las copias de respaldo.

- Determinar el tiempo de retención de las copias de respaldo teniendo en cuenta la importancia de la información respaldada y los requisitos legales que rigen a la entidad.

- Evaluar la necesidad de instaurar controles criptográficos a las copias de respaldo, considerando los requisitos legales aplicables a la entidad.

5.4.6.6 Robo de equipos por necesidad de traslado.

- Realizar, difusión al personal de la entidad mediante campañas de concienciación y educación, la divulgación correspondiente de los riesgos a los que se ven expuestos los equipos de cómputo, dispositivos móviles y cualquier otro medio que contenga información, cuando son retirados de la entidad.

- Establecer los mecanismos adecuados con el fin de evitar la fuga de información en los equipos de cómputo, dispositivos móviles y cualquier otro medio que contenga información, a través del uso de controles como los criptográficos.

5.4.6.7 Fuga de información por otro medio electrónico.

- Revisar los perfiles y roles de acceso lógico de usuarios o grupos de usuarios, de acuerdo con las funciones de cargo y las políticas de seguridad de la información en cada uno de los sistemas de información existentes, servicios de red y recursos tecnológicos, con fin de ratificar o de ser necesario ajustar, los perfiles y roles de acuerdo con los cambios detectados durante la revisión.

- Llevar a cabo cuando resulte necesario, el ajuste de los perfiles y roles, siguiendo el procedimiento de administración de usuarios y contraseñas por el cual se deben realizar este tipo de cambios, generando registros de control.

- Monitorear periódicamente los Logs de eventos de seguridad.

- Revisar periódicamente el estado de los usuarios, roles y permisos los sistemas.

- Implementar mecanismo de cifrado de disco duro de los dispositivos móviles y portátiles de la entidad.

- Garantizar la implementación del bloqueo de dispositivos externos en los computadores de la entidad.

- Clasificar la información de la entidad, conforme si es pública, privada o confidencial.

5.4.6.8 Riesgo en la integridad del *Software* y la información, por la instalación de *software* sin autorización del área de sistemas o el coordinador de TI. Es fundamental tener el control del *software* que se instala y utilizan los equipos de cómputo del personal de la empresa, las implicaciones legales, económicas y penales a las cuales se ven inmersas las empresas que no cumplan con *software* licenciado. Por ello es importante establecer controles de instalación y monitoreo de aplicaciones instaladas en las terminales.

- Solo el personal de TI de la entidad puede instalar, actualizar y eliminar *software*, estos a su vez deberán tener el control del *software* que se instala en las maquinas e inventario de este.

- Los usuarios y empresas tienen una mayor probabilidad de infectarse con algún tipo de virus informático al adquirir *software* no legal.

- El *software* ilegal puede robar contraseñas, imitar sitios web, registrar todo lo que se digita en el teclado, redirigir búsquedas en internet, recopilar información y enviar información falsa.

- Utilizar el equipo de cómputo para realizar ataques de denegación de servicios e identificar y robar información confidencial.

- La instalación de *software* pirata puede conllevar a permitir libre acceso a personas no autorizadas al equipo de cómputo remotamente e inclusive tomar el control total del equipo de cómputo.

- Al instalar *software* pirata se corre el riesgo de ser objetivo de ciberdelincuentes y se pueden presentar perdidas de información vital para la empresa.

5.4.6.9 Pérdida de información por error de *Hardware*. La pérdida de datos se puede presentar por cualquier causa, avería o inclusive por error humano, borrado accidental o provocado y en algunos casos por desastres naturales. Es indispensable tener un plan de respaldo de la información crucial para la entidad, con el fin de mitigar la perdida de datos valiosos para el normal funcionamiento de la empresa.

- Establecer la política de copias de seguridad de la información relevante para la continuidad del negocio, en caso de presentarse alguna falla en el *hardware*.

- Verificar picos de tensión que puedan presentarse en los equipos electrónicos de la empresa y/o de la residencia del empleado, dado que una sobrecarga en la red eléctrica puede generar daños en el *hardware*. Se recomienda la instalación de UPS o reguladores de voltaje para mitigar el impacto que surta con las variaciones eléctricas.

- Uno de los daños más comunes que se presentan, es la avería mecánica en los discos duros, por continuas dilataciones y contracciones debidas al proceso sucesivo de calentamiento y enfriamiento de los dispositivos, una vez sucede el evento, el procedimiento para la recuperación de la data es tediosa y costosa, puesto que se requiere de personal calificado para realizar el arreglo y posterior recuperación de la información.

- Otro daño frecuente y que puede ser producido por errores del usuario, son los daños lógicos en los discos duros, esto ocurre por bloqueos del sistema, acción de virus o un posible sabotaje interno. Comúnmente sucede cuando se genera un bloqueo en el equipo de cómputo y se reinicia el mismo, se suele producir una descarga de memoria caché o RAM, al disco y sí el equipo lleva bloqueado un rato, las cabezas del disco se colocan en la zona de comienzo del disco realizando esta descarga de datos en una zona inadecuada, rescribiendo las

tablas de partición y el sector de arranque, siendo luego imposible arrancar el sistema de manera normal.

- Descarga y propagación de virus por navegación en la web. Navegar en internet trae consigo muchos riesgos de seguridad para las entidades, así como insertar una memoria USB, CD o DVD en el equipo de cómputo, exponiéndolo a virus, afectando el normal funcionamiento del ordenador, robo de información, eliminación y ocultamiento de datos importantes para el usuario. Existen métodos para evitar la propagación de *malware* y daños irreparables para las empresas que se mencionan a continuación.

- El equipo de cómputo debe tener instalado un *software* de antivirus, que es una de las formas apropiadas para proteger el ordenador, puesto que la función que ejerce es alertar de archivos maliciosos que se quieran instalar o copiar, es de resaltar que esta herramienta debe estar actualizándose constantemente para ejecutarse de forma correcta.

- Configuración del firewall o cortafuegos de manera correcta, para prevenir los posibles ataques a los que pueda ser sometido el equipo de cómputo o sistema de información, impidiendo que usuarios no autorizados accedan al PC.

- No descargar información innecesaria en los equipos de cómputo, evitando aplicaciones desconocidas o archivos que pueden presentarse llamativos para el usuario, donde mediante el uso de publicidad engañosa incitan a acceder a las mismas, dañando el equipo de cómputo, Por otra parte, al descargar cualquier información, es indispensable escanearlas con el antivirus que se tenga establecido para ello.

- Evitar ingresar en anuncios publicitarios en internet, dado que pueden estar contagiados con algún virus y al acceder a estos, se pueden instalar en el ordenador causando daños catastróficos.

- El equipo de cómputo debe escanearse constantemente, para detectar posibles virus que pueda estar oculto en el PC, este proceso debe realizarse de forma regular, mínimo una vez en la semana.

- Destrucción de copias de seguridad. Los medios de almacenamiento físico, donde reposa la información de la empresa, siendo este el activo más importante, pueden verse involucrados en situaciones ocasionadas por fallos eléctricos, fallo del dispositivo, virus, borrado accidental, robos, inundaciones, sabotaje, entre otros, donde sería imposible acceder a la información, poniendo en peligro la continuidad del negocio. Por lo anterior es importante tener en cuenta las siguientes consideraciones.

- Realizar un inventario de activos de información y clasificación de los mismos, en relación a la criticidad para el negocio, cuya finalidad es tener al detalle todo el *software* y datos esenciales para que la empresa de tal manera determine la periodicidad de los backup y el contenido y en caso de presentarse un incidente de seguridad se pueda fácilmente a reiniciar la operación.

- Asignar los responsables de realizar mencionadas copias de seguridad y definir un procedimiento, tanto para ejecutarlas como para realizar el proceso de restauración.

- Una vez establecida la criticidad de la información al interior de la empresa, se determinará los tipos de copia de seguridad, es decir si se realizaran backup de forma completa, incremental, diferencial, espejo, sintética completa o protección de datos continua (CDP).

- Determinar los tipos de copia de seguridad según su destino, es decir se realizarán de manera local, externa, remota o en línea.

- Establecer el tipo de copia de seguridad que más se adecuada a las necesidades de la empresa, dado que la inversión puede ser elevada dependiendo de los factores mencionados anteriormente.

- Una conexión a una red inalámbrica desconocida o una conexión habilitada sin seguridad, es decir, no se solicita una clave de inicio de sesión. Mencionadas redes inalámbricas que permiten una conexión gratuita no son seguras puesto que no cifran la información y no se tiene la certeza de los usuarios que acceden a ella, se debe evitar la conexión a redes desconocidas, visto que se expone a un sinfín de riesgos asociados a la conexión.

- Al acceder a este tipo de conexión, se está expuesto al robo de datos transmitidos, es decir la información que se envía, puede ser fácilmente expuesta a cualquier usuario que sepa como leerla y para ello no se requiere conocimientos avanzados.

- Al formar parte de una red pública, en la cual están conectados varios usuarios, los equipos de cómputo están expuestos y por tanto propensos a recibir cualquier ataque desde un dispositivo que esté conectado a la red.

- Fácilmente se puede ser víctimas de una infección de *malware*, por esta razón es importante contar con antivirus y actualizaciones de seguridad del sistema operativo.

- Almacenamiento indebido de información, ya sea en dispositivos no autorizados o sin la seguridad necesaria. Existen diversas maneras y formas para el

almacenamiento de la información de la entidad, por ello es importante establecer directrices para el almacenamiento y disposición final de la data, definiendo la ruta a tomar en caso de que se materialice la pérdida o fuga de la información y que tipo de información se debe alojar en los equipos de cómputo.

- Establecer una política para almacenamiento local en los equipos de trabajo, almacenamiento en la red corporativa, dispositivos externos, almacenamiento en *cloud*, reglas, criterios y procedimientos a seguir para el almacenamiento de la información, dispositivos autorizados para su alojamiento, plan de recuperación en caso de pérdida y conservación de la misma.

- Establecer el plan de mitigación de riesgos asociados con las repercusiones importantes para la empresa en caso de que se produzca una pérdida de datos temporal o definitiva, donde se ocasionarían múltiples perjuicios al normal funcionamiento de la empresa.

- Pérdidas económicas, tiempo y dinero por las actividades que se requieran ejecutar para restaurar o recuperar la información que con ocasión de la mala administración de la data se pierda o caiga en las manos equivocadas.

- Indisponibilidad de la información y retrasos en los procesos asociados a la materialización de la perdida de la data.

- Daño en la imagen corporativa de la empresa y pérdida de credibilidad por parte de sus clientes y proveedores.

- Demandas por parte de los clientes por el mal uso de la información.

5.5 BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL TELETRABAJO

Los ataques informáticos, la pérdida y fuga de información son situaciones que muchas empresas deben afrontar constantemente en sus procesos e infraestructura tecnológica y más importante aún, si no han adoptado las medidas necesarias para afrontar este tipo de eventualidades. La información se convierte en el activo más importante para cualquier entidad, así mismo el más apetecido por los cibercriminales, que están al acecho de las vulnerabilidades que se pueden generar de manera interna y externa en la entidad. Ante el constante riesgo y en algunos casos no se cuentan con las medidas básicas para salvaguardar la data, surten grandes retos para los departamentos de TI de las empresas; con el avance tecnológico también se incrementa la complejidad de los ataques cibernéticos, así pues, surte la necesidad de generar conciencia al interior de la organización siendo este un factor importante para mitigar posibles ataques y garantizar la operación de las empresas.

Durante el desarrollo de la presente guía, se han dejado plasmadas recomendaciones muy generalizadas y que se pueden presentar en las entidades de manera muy simple, por lo cual se sugiere tener presente al momento de realizar la implementación del teletrabajo. Mencionar que las buenas prácticas deben ser articulas con la alta gerencia de las empresas de la mano del personal técnico experto de los departamentos de TI o quien haga sus veces, dimensionando los riesgos a los cuales está expuesta la infraestructura de TI de las empresas con la adopción del teletrabajo.

Un principio básico es la importancia de recalcar las responsabilidades a nivel jurídico, tecnológico y logístico por parte de todos los funcionarios que acceden a la red de datos de la empresa, no solo mediante el teletrabajo, sino también los que

de una u otra forma por la naturaleza de su cargo, deben asistir de manera presencial a la empresa para cumplir con sus funciones y obligaciones labores.

Antes de implementar la modalidad de teletrabajo o trabajo en casa, se debe definir claramente todo el contenido relacionado con el equipo de trabajo, responsabilidades y costos, y lo que es más importante, se deben tomar las medidas adecuadas para evitar ataques, pérdidas o fugas de información para garantizar un trabajo remoto seguro.

Por lo anterior y con el ánimo de fortalecer las salvaguardas con la implementación del teletrabajo, se enumeran algunas sugerencias establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia para las empresas y personas que realizan su trabajo desde casa:

5.5.1 Recomendaciones para Empresas

- Activar configuraciones de doble autenticación de autenticación en cuentas de correo electrónico personales y corporativas para confirmar la identidad de las personas que acceden al correo electrónico y otras herramientas.
- Implementar canales de comunicación seguros desde Internet en las organizaciones y/o entidades, como SSL-VPN, para colaboradores y funcionarios en oficinas remotas y conexiones de trabajo remotas.
- Si se requiriere habilitar los servicios de Internet, se debe evaluar los riesgos antes de iniciar actividades; es decir que las medidas de emergencia no afecten la seguridad de la información.
- Actualice su sistema operativo con los últimos parches de seguridad emitidos por el fabricante, así mismo instalar y mantener actualizado el antivirus de fabricantes de renombre para evitar infecciones como virus o *malware*.

- Establecer y/o considerar la elaboración de la política de privacidad de la información, con el propósito de salvaguardar la información sensible y privada de la organización o entidad.
- Implementar soluciones de almacenamiento corporativas para almacenar y alojar información del personal que labora en teletrabajo mediante la infraestructura establecida en el servidor de archivos establecida.
- Activar perfiles de navegación para usuarios autorizados de SSL / VPN. Monitoreo permanente de la infraestructura de servicios que utilizan los trabajadores remotos para analizar posibles operaciones no autorizadas.
- Implementar verificaciones de seguridad mínima para los dispositivos BYO (*Bring Your Own Device*), cuando se conecte a la red de la entidad utilizando conexión a través de SSL-VPN, adicional, protección contra virus, *malware*, gusanos, *spyware*, troyanos, *ransomware*, entre otros y contar con las actualizaciones de parches de seguridad vigentes.
- Evitar el almacenamiento automático de las credenciales de usuario, relacionadas con las herramientas, aplicaciones y acceso a bases de datos de la empresa. Es importante crear una estrategia de respaldo para evitar la pérdida de información.
- Implementar estrategias de cifrado en los computadores, portátiles, servidores y herramientas comerciales para garantizar la protección de la información de la empresa. Ejecutar la segmentación en los privilegios mínimos a los recursos que accederá de forma remota el usuario, para garantizar que no tenga acceso a medios innecesarios y/o usuarios que contengan información sensible, con el fin de impedir el acceso inadecuado a la infraestructura tecnológica de la entidad mediante el uso de la red.
- Llevar a la practica el uso de herramientas de protección de equipos como EDR (*Endpoint Detection and Response*) para permitir una gestión integral y centralizada de las políticas de seguridad de la empresa a nivel local en los dispositivos de los empleados.

- Si los empleados utilizan dispositivos móviles para acceder a los servicios proporcionados por la organización y/o Entidad, es esencial prohibir el uso de dispositivos Rooteados o realizado *Jailbreak*.
- En caso de pérdida del dispositivo móvil, se deben realizar las configuraciones de seguridad previa, para proteger la información de la empresa (ubicación, bloqueo de pantalla, borrado remoto de información y monitoreo de aplicaciones en ejecución).
- La empresa debe implementar un plan de capacitación en temas relacionados con seguridad de la información a todo nivel en la entidad, donde sus empleados estén concientizados en el correcto uso de los medios tecnológicos asignados para el teletrabajo.

5.5.2 Recomendaciones para personas

- Utilizar verificación de doble o triple factor de autenticación al momento de efectuar transacciones de comercio electrónico.
- Periódicamente cambiar las claves el acceso a WiFi, para evitar el uso de redes inalámbricas abiertas, ya que pueden ser utilizadas para sustraer información privilegiada.
- Utilizar los medios de almacenamiento proporcionados por la organización y/o entidad para efectuar copias de seguridad de la información de manera periódica.
- No enviar archivos o información que contenga datos sensibles mediante aplicaciones de terceros como: *WhatsApp, Dropbox, WeTransfer*, correos de dominio gratuito, etc. En los cuales se pueden presentarse perdida o fuga de información.
- Cierre la sesión cuando no utilice el dispositivo en casa o en lugares públicos.
- Mantener actualizado el equipo de cómputo con los últimos parches de seguridad liberados por el fabricante para el sistema operativo, en el caso que realice las actividades laborales desde su propio dispositivo.

- Disponer de un antivirus actualizado periódicamente, para mitigar virus, *malware*, gusanos, *spyware*, troyanos, *ransomware*, entre otros, con la finalidad de evitar la pérdida o fuga de información.
- Contar con un espacio adecuado para realizar las tareas asignadas por la empresa con ocasión del teletrabajo, evitando la perdida de información por daños en el equipo de cómputo, por mala manipulación de alimentos, por ejemplo.
- No instalar *software* o extensiones en los navegadores WEB de fuentes anónimas puesto que generalmente pueden traer *malware*, afectando los equipos de cómputo y extraer la información confidencial.
- Minimizar el uso de aplicaciones para conexión de acceso remoto que no estén plenamente validadas por el área de TI de la organización y/o entidad, dado que dichas herramientas pueden crear puertas traseras en las cuales pueden comprometer el servicio o las credenciales de acceso de los usuarios y por lo tanto permitir el acceso a los equipos corporativos.
- Optimizar el uso de Internet, porque todas las conexiones se establecerán a través del mismo canal, priorizando las actividades laborales en un momento determinado, para que no sufra interrupciones en el servicio.
- Recuerde que, aunque se esté trabajando desde casa, siempre debe garantizar la seguridad de los datos y cumplir con las exigencias de seguridad impuestas por la organización y/o Entidad y la Ley de protección de datos personales.

5.5.3 Recomendaciones en dispositivos móviles

- No enviar mensajes de texto con datos confidenciales, información privada e información financiera.
- Encriptar los dispositivos móviles, adicional de la autenticación de usuarios, también implementaremos mecanismos de encriptación de documentos en los dispositivos.

- No conecte su teléfono a un puerto USB desconocido y no acepte ninguna relación de confianza a través de USB sin garantizar una conexión confiable.
- No se conecte a redes *Wifi*-públicas abiertas (o puntos de acceso *Wifi*).
- No instale aplicaciones que no sean de fuentes confiables, como la tienda oficial de aplicaciones.
- No instale aplicaciones que requieran permisos (acceso al calendario, ubicación geográfica, etc.) que pongan en riesgo información confidencial.
- Realizar copias de seguridad periódicas sincronizadas con los servicios de nube. Mantener actualizado el sistema operativo del celular.

El teletrabajo significa una nueva forma de gestión de la información a través de las TIC en un espacio externo a la oficina. Sin embargo, trae nuevos riesgos asociados a la gestión inadecuada de la información, como la pérdida, fuga o alteración de datos, todo lo cual plantea nuevos retos de seguridad de la información. Por esta razón, es importante que las entidades formulen una política para definir claramente los métodos de seguridad de la información en el teletrabajo, incluidas las pautas de integridad, autenticidad, legalidad y confidencialidad. Siempre que la estrategia de seguridad de la información sea clara y se verifique permanentemente, los riesgos de seguridad de la información también se pueden identificar a tiempo y se diseñan soluciones para mitigar estos riesgos.

6. CONCLUSIONES

Es de gran relevancia tener presente las recomendaciones que se plantean en la presente guía, aunque no se enumeran todos los eventos a los que se exponen las organizaciones y pueden quedarse cortas, pero es un referente con el fin de mitigar la perdida y/o fuga de información al interior de las organizaciones, garantizando la continuidad del negocio e imagen institucional.

- Los principales riesgos identificados se relacionan con la fuga de información debido a la dificultad en el control de acceso a la misma. De ahí la importancia de tener protocolos bien establecidos y una óptima socialización de estos, con el personal que se va a dedicar a la labor por teletrabajo, para lograr el cumplimiento de estos y así evitar los riesgos por mala utilización de las herramientas de teletrabajo.

- Es importante definir un Modelo de Seguridad y Privacidad de la Información acorde a las necesidades institucionales, donde se debe definir los lineamientos para la implementación de la estrategia de seguridad digital, alineados de un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contemple el ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

- En el protocolo se debe tener un apartado para la selección del personal que ejercerá el teletrabajo y un protocolo anexo de contratación en el que se especifiquen los compromisos adquiridos al asumir la labor por teletrabajo.

- Las organizaciones deben contar con políticas de seguridad de la información claras, precisas y bien estructuradas, ya que estas guiaran la conducta personal

y profesional de todos los funcionarios logrando el cumplimiento de los requisitos legales a los cuales está obligada.

- La elección acertada de un modelo de Seguridad de la Información para la implementación del teletrabajo, requiere el compromiso y el trabajo en equipo de toda la organización, involucrando a la alta dirección en la importancia de mantener la seguridad de la información de la organización, de manera que el modelo a implementar ayude a minimizar los riesgos asociados a la fuga de información; de la mano con el compromiso, la eficiencia y gestión para garantizar el cumplimiento de las funciones misionales de la organización con el apoyo del uso adecuado de las TIC.

- Entendiendo la importancia de una adecuada gestión de la información con la implementación del teletrabajo, las áreas de TI de las organizaciones deben fortalecer su compromiso en la implementación de un modelo de gestión de la seguridad de la información, tendiente a establecer un marco de confianza para el cumplimiento de las tareas de sus usuarios sin descuidar la seguridad de la infraestructura que soporta mencionada labor, todo ello en estricto cumplimiento de la ley y buenas prácticas para proteger la información de la entidad.

7. RECOMENDACIONES

- Es indispensable en cualquier entidad pública o privada, establecer el análisis de riesgos para el desarrollo y operación de un SGSI, es decir los riesgos asociados al manejo de la información de la empresa, principales vulnerabilidades a las cuales están expuestos sus activos de información y cuáles de estas pueden ser explotadas por piratas informáticos con la implementación del teletrabajo, planteando las medidas preventivas que garanticen los niveles de seguridad en su información.

- Es fundamental disponer de un modelo de seguridad de la información que más se ajuste a las necesidades de la empresa para la implementación de buenas prácticas en materia de seguridad informática. Llevarlo a la práctica permite proteger el activo más importante de la organización, la información, adicional generar confianza entre clientes, empleados y proveedores.

- La implementación de un Sistema de Gestión de Seguridad de la Información es una acción estratégica, donde debe trascender a toda la organización, incluyendo el respaldo y conducción de la dirección, por ello la participación genera confianza entre sus empleados y directivos y a la vez se refleja en la confianza de sus clientes en la continuidad del negocio.

- Encaminar el uso de buenas prácticas en materia de seguridad informática, conlleva a mitigar la pérdida o fuga de información con la implementación del teletrabajo, de esta manera se blindaría la seguridad física, el acceso a los sistemas de información y aplicar recomendaciones en materia de ciberseguridad establecidas para tal fin.

BIBLIOGRAFIA

7Graus. Significado de Causa. Significados. [Sitio WEB]. Madrid - España. La entidad. [30, octubre, 2020]. Disponible en: https://www.significados.com/causa.

AGUILERA LOPEZ, Purificación, Seguridad Informática - Ciclos Formativos. 1ª edición. Pozuelo de Alarcón - Madrid: Editex,2010. 243 p. ISBN 9788497717618.

ALEGRE RAMOS, María del Pilar y GARCÍA-CERVIGÓN HURTADO, Alfonso. Seguridad Informática. [En Línea]. Madrid-España.:2011. 1era edición. 169 p. [Consultado 11, octubre,2020]. ISSN 99788497328128. Disponible en: https://books.google.com.mx/books?id=c8kni5g2Yv8C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

ALEGSA. Definición de Vulnerabilidad - Portal de informática, internet, tecnologías y web. Diccionario de Informática y Tecnología. [Sitio WEB]. Santa fe - Argentina. La entidad. [11, octubre, 2020]. Disponible en: https://www.alegsa.com.ar/Dic/vulnerabilidad.php.

AREITIO, Javier, Seguridad de La Información. Redes, Informática y Sistemas de Información. [En Línea]. Madrid -España: 2008. 1era edición. 592 p. [Consultado 11, octubre,2020]. ISSN 9788497325028. Disponible en: https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&hl=es#v=onepage&q&f=false.

CASAL FÀBREGA. Joaquim and others. Análisis del Riesgo en Instalaciones Industriales. [En Línea]. Cataluña-España.:2009. 1era edición. 364 p. [Consultado 11, octubre,2020]. ISSN 978-8483012277. Disponible en: https://upcommons.upc.edu/handle/2099.3/36154.

CHAPARRO NIÑO, Wilson Alexander. Tecnología: Hacia un nuevo concepto de la subordinación laboral. [en línea]. Monografía. Universidad Nacional de Colombia. Bogotá, D.C.: 2018. [Consultado 17, junio,2022]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/69780/80195584.2018.pdf

CIFRE GALLEGO, Eva, 'Estrategias de Mejora de La Salud Psicosocial Del Teletrabajador. El Arte de Conjugar Teoría y Práctica', Estudios Financieros. Revista de Trabajo y Seguridad Social. Comentarios, Casos Prácticos. Recursos Humanos, 300, 2008, 181–200.

CISCO. Cisco Cybersecurity Report Series 2020. [Sitio WEB]. San José - California. La entidad. [Consultado 25, junio, 2021]. Disponible en: https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial, Octubre, 48. Nro. 587. p. 1-15.

COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y MINISTERIO DEL TRABAJO, Libro Blanco. ABC del Teletrabajo en Colombia.2014, nro. 01. p. 1-97. ISSN 1098-6596, p. 12.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1221(16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. En: Diario Oficial. Julio, 47.Nro. 052. p. 1-6.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1221(16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. En: Diario Oficial. Julio, 47.Nro. 052. p. 1-6.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial, Enero, 47. Nro. 223. p. 1-5.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1429 (29, diciembre, 2010). Por la cual se expide la Ley de Formalización y Generación de Empleo. En: Diario Oficial. Diciembre, 47. Nro. 937. p. 1-15. p 3.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1562 (11, julio, 2012). Por la cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materias de salud ocupacional. En: Diario Oficial. Julio, 47. Nro 937. p. 1-22.

COLOMBIA.CONCEJO DE BOGOTÁ, 'Proyecto de Acuerdo 249 (2013). Por medio del cual se estable en el Distrito Capital, la estrategia para la implementación del Teletrabajo en Bogotá. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53426.

COLOMBIA.MINISTERIO DE TRABAJO. Decreto 0884 (30, abril, 2012). Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones. Bogotá D.C.: El Ministerio, p. 1-6.

ECONOPEDIA. Sistema de Información. [Sitio WEB]. Madrid - España. La entidad. [16, agosto, 2021]. Disponible en: https://economipedia.com/definiciones/sistema-de-informacion.html.

ESET. Welivesecurity. Guía de Bring Your Own Device. [Sitio WEB]. Canada. La entidad. [6, noviembre,2013]. Disponible en: https://www.welivesecurity.com/la-es/post_paper/guia-de-bring-device.

FUNCIÓN PÚBLICA. Red de los servidores públicos. Documento Técnico - Instrumento de Evaluación MSPI. [Sitio WEB]. Bogotá D.C. La entidad. [15, septiembre,2020]. Disponible en: https://www.funcionpublica.gov.co/eva/red/publicaciones/documento-técnico---instrumento-de-evaluación-mspi.

GRUPO ALBE. Grupo Albe Consultoría. Los tres conceptos más importantes para evaluar los riesgos empresariales. [Sitio WEB]. México. D.C. La entidad. [11, noviembre,2021]. Disponible en: https://www.grupoalbe.com/consultoria-empresarial-3-conceptos-sobre-como-evaluar-los-riesgos-empresariales.

GUZMAN, Anggie. Vulnerabilidad, Riesgo y Amenaza. Seguridad Informática. [sitio WEB]. [Consultado el 11, octubre, 2020]. Disponible en: http://seguridadanggie.blogspot.com/2011/11/vulnerabilidad.html.

INFOEMPLEO. Hrtrends. Círculo de Deming: Qué Es y En Qué Beneficia a Tu Empresa. [Sitio WEB]. Madrid-España. La entidad. [7, noviembre,2020]. Disponible en: https://empresas.infoempleo.com/hrtrends/circulo-de-deming.

Informática en el teletrabajo a través de una herramienta web. Bogotá, Universidad Piloto De Colombia,2013. p.32.

INGERTEC. NORMAISO27001. [Sitio WEB]. Córdoba - España. La entidad. [17, junio, 2022]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def377/.

INGERTEC. NORMAISO27001. [Sitio WEB]. Córdoba - España. La entidad. [25, mayo, 2020]. Disponible en: https://normaiso27001.es/fase-2-analisis-del-contexto-de-la-organizacion-y-determinacion-del-alcance/.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información. NTC-ISO/IEC 27035. Bogotá D.C.: El instituto, 2012. 103 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Riesgo. Principios y Directrices. NTC-ISO/IEC 31000. Bogotá D.C.: El instituto, 2011. 34 p.

Instituto de Investigación de Recursos Biológicos Alexander von Humboldt, «El ABC de la Gestión de Riesgos», Fundamentos conceptuales de la Gestión de Riesgos, 2004.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, Glosario de Términos de Ciberseguridad, Una guía de aproximación para el empresario.2017, 82 p.

MICROSOFT, CORPORTION. Microsoft Security Intelligence Report. [En línea]. 2013, 16 edición. 120 p. [Consultado 13, mayo, 2020]. Disponible en: http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_English.pdf.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES and MINISTERIO DEL TRABAJO, Libro Blanco el ABC del

Teletrabajo en Colombia.1 edición. Bogotá, D.C.: 2014, nro. 01. p. 197. ISSN 1098-6596, p. 15.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Teletrabajo. [Sitio WEB]. Bogotá, D.C. La entidad. [28, mayo, 2020]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8228.html.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio WEB]. Bogotá, D.C. La entidad. [13, septiembre,2020]. Disponible en: https://www.mintic.gov.co/portal/inicio

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad. [En Línea]. Bogotá, D.C.: 2015. [Consultado 9, junio, 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

MORALES, Gabriela y ROMANIK, Katy, Una mirada a la figura del teletrabajo. Chile: Dirección del Trabajo, 2011. 60 p. ISBN: 978-956-7978-07-6.

NACIONES UNIDAS. Estrategia Internacional para la Reducción de Desastres. [En Línea]. Nueva York.: 2009. [Consultado 15, octubre,2020]. Disponible en: https://reliefweb.int/report/world/2009-unisdr-terminolog%C3%ADa-sobre-reducci%C3%B3n-del-riesgo-de-desastres. Citado por RODRIGUEZ MENJUREN, Roger Edson, mejoramiento de las buenas prácticas de seguridad

PONEMON INSTITUTE. Data Risk in the Third-Party Ecosystem. [Sitio WEB]. Traverse - Michigan. La entidad. [Consultado 7, noviembre, 2020]. Disponible en: https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/.

POSTECH IT SOLUTION PROVIDER S.A. Técnicas y Herramientas para la evaluación de vulnerabilidades de la red. Postech IT Solution Provider [sitio WEB]. [Consultado el 10, octubre,2020]. Disponible en: https://postech.com.mx/Postech/ES/tecnicas.php.

QUINTANILLA NAVARRO, Raquel Yolanda. El teletrabajo de la dispersión normativa presente a la necesaria regulación normativa europea y estatal futura. [en línea]. Madrid-España.: 2017. [Consultado 13, noviembre,2020]. Disponible en: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-madrid/documents/article/wcms_548615.pdf.

ROYAL P. Fisher, Seguridad en Los Sistemas Informáticos. [En Línea]. Madrid-España:.1988. 1era edición. 278 p. [Consultado 11, octubre,2020]. ISSN 8486251958. Disponible en: https://books.google.co.ve/books?id=_Hu6Zu6VLP4C&printsec=copyright#v=onepage&q&f=false.

SERER FIGUEROA, Marcos. Gestión integrada de proyectos. [En Línea]. Madrid-España.:2010. 3era edición. 484 p. [Consultado 11, octubre,2020]. ISSN 978-8498804300. Disponible en: https://www.abebooks.com/9788483018873/Gesti%C3%B3n-integrada-proyectos-96-Politext-848301887X/plp.

SPAULDING Mike and FULKERT Kate. Las Cambiantes Amenazas a las Redes de TI Exigen una Mayor Vigilancia. [En Línea]. Latinoamérica.: 2020. [Consultado 3, noviembre, 2020]. Disponible en: https://www.vertiv.com/es-emea/about/news-and-insights/articles/blog-posts/threats-to-it-networks-are-changing-requiring-greater-vigilance.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Sistema de Gestión de Seguridad de la Información. Bogotá D.C.: Superintendencia de Industria y Comercio, 2016. 15 p. ISBN 1098-6596.

TELLEZ VALDEZ, Julio. Teletrabajo. [En Línea]. México, D.C.: 2007. [Consultado 10, octubre,2020]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2458/43.pdf.

THIBAULT ARANDA, Javier. El teletrabajo, análisis jurídico-laboral. 2 ed. Madrid-España.: Consejo Económico y Social, 2000. 320 p. ISBN: 84-8188-113-9.

VERANO TACORONTE Domingo, SUÁREZ FALCÓN, Heriberto, y SOSA CABRERA, Silvia. El teletrabajo y la mejora de la movilidad en las ciudades. Investigaciones Europeas de Dirección y Economía de la Empresa. [en línea]. Pontevedra - España: 2014.0. [Consultado 10, octubre,2020]. Disponible en: https://redalyc.org/pdf/2741/274129585006.pdf.