RESUMEN – TRABAJO DE GRADO

AUTORES	Nelson Fernando Gaona Díaz		
FACULTAD	**Facultad de Ingenierías**		
PLAN DE ESTUDIOS	**Maestría en Gobierno de TI**		
DIRECTOR	Torcoroma Velásquez Pérez.		
TÍTULO DE LA TESIS	**Modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo**		
TITULO EN INGLES	Information security governance model for the business sector in the framework of teleworking		
RESUMEN (70 palabras)			
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, el teletrabajo tomo auge en la pandemia. El objetivo del presente proyecto se centró en proponer un modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo.			
RESUMEN EN INGLES			
Teleworking is a flexible form of work organization that consists of carrying out professional activity without the worker's physical presence in the company during a significant part of their working hours. Teleworking took off during the pandemic. The objective of this project focused on proposing an information security governance model for the business sector within the framework of teleworking.			
PALABRAS CLAVES	Modelo de gobierno, seguridad de la información, gobierno de TI, sector empresarial.		
PALABRAS CLAVES EN INGLES	Government model, information security, IT governance, business sector.		
CARACTERÍSTICAS			
PÁGINAS:94	PLANOS:	ILUSTRACIONES:	CD-ROM:

Modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo

Nelson Fernando Gaona Díaz

Facultad de Ingenierías, Universidad Francisco de Paula Santander Ocaña

Maestría en Gobierno de TI

Dr. Torcoroma Velásquez Pérez.

Co-director Mg. Andrés Mauricio Puentes Velásquez

9 de noviembre de 2023

Índice

1. Modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo 8

1.1 Descripción del problema 8

1.2 Formulación del problema 10

1.3 Objetivos 10

1.3.1 Objetivo General 10

1.3.2 Objetivos Específicos 11

1.4 Justificación. 12

1.5 Delimitaciones 13

2. Marco referencial 14

2.1 Antecedentes investigativos 14

2.2 Antecedentes legales 16

2.2.1 Administración de las políticas de seguridad de la información 16

2.3 Marco Conceptual 17

2.3.1 Teletrabajo 17

2.3.2 Sector Empresarial 17

2.3.3 Seguridad de la información 18

2.3.4 Seguridad de recursos humanos 19

2.3.5 Cobit 5 19

2.3.6 Cobit 2019 19

2.4 Marco Teórico 21

2.4.1 Teoría de la sociedad de la información 21

2.4.2 Seguridad de la información 23

2.4.3 Teletrabajo 24

2.5 Marco Contextual 26

3. Diseño metodológico 27

3.1 Población 28

3.2 Muestra 28

3.3 Técnicas de recolección de la información 29

3.3.1 Análisis de la información. 29

4. Modelo de gobierno de seguridad de la información en el sector empresarial en el marco del teletrabajo 30

4.1 Caracterización de los fundamentos teóricos y prácticos del teletrabajo y los componentes de seguridad de la información requeridos 30

4.2 Estructuración de los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo. 39

4.2.1 Diagnóstico del nivel de madurez de los procesos de seguridad de la información en el marco del teletrabajo 39

4.2.2 Métodos de análisis cualitativo en el cumplimiento de la norma de teletrabajo y trabajo en casa. 47

4.2.3 Estructuración del modelo de gestión de seguridad en el marco del teletrabajo y trabajo en casa. 53

4.3 Validación el modelo de gobierno de ti orientado a la seguridad de la información mediante el juicio de expertos 63

Conclusiones 70

Recomendaciones 72

Referencias 73

Apéndices 79

Lista de Tablas

Tabla 1. Matriz de objetivos.....11

Tabla 2. Evaluación de prácticas de gestión aplicables.....40

Tabla 3. Categorías principales y subcategorías.....49

Tabla 4. Caracterización de los expertos.....63

Tabla 5. Consolidado de respuestas de expertos.....65

Tabla 6. Respuesta de los expertos 66

Lista de Figuras

Figura 1. Fundamentos teóricos de Teletrabajo 31

Figura 2. Fundamentos prácticos de Teletrabajo 37

Figura 3. Niveles de Capacidad de las empresas tecnológicas.....44

Figura 4. Niveles de Capacidad del sector público 45

Figura 5. Niveles de Capacidad de Instituciones de Educación Superior 46

Figura 6. Niveles de Capacidad de Instituciones Técnicas y Tecnológicas 47

Figura 7. Red de categoría Salud Mental 50

Figura 8. Red de categoría Recursos.....50

Figura 9. Red de categoría Productividad 51

Figura 10. Red de categoría Clima Laboral 52

Figura 11. Red de categoría Seguridad de la Información.....53

Figura 12. Modelo de seguridad de información para las empresas en el marco del teletrabajo 56

Figura 13. Formula del Alpha 67

Figura 14. Valoración de la fiabilidad.....68

Lista de Apéndices

Apéndice 1. Matriz de operacionalización de variables.....80

Apéndice 2. Cuestionario.....82

Apéndice 3. Guion de preguntas.....88

Apéndice 4. Categorías previas.....95

1. Modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo

1.1 Descripción del problema.

La sociedad en la actualidad se enfrenta a un cúmulo de cambios, innovaciones y/o transformaciones, algunas favorables para impulsar el progreso y desarrollo de la población en general; otras con menos intensidad de incidencia en el desenvolvimiento laboral dentro de una sociedad que en la actualidad se enfrenta a una situación atípica originada por lo que ha sido la pandemia del COVID – 19; donde los entes gubernamentales han intervenido y han creado estrategias que recaen en la cuarentena, en el confinamiento entre otros, lo cual ha impactado en la fuerza laboral de la Nación.

Por otra parte, en el marco de la emergencia sanitaria provocada por el covid19, la situación que han tenido que enfrentar las empresas al implementar estrategias de mitigación contra el virus han sido radicales; tal es el caso de enviar a sus trabajadores a sus hogares, iniciando de esta manera nuevas modalidades de trabajo que hoy por hoy han entrado en auge. En ese sentido el trabajo desde casa o teletrabajo tomo fuerza como una estrategia al buscar disminuir los índices de contagios. De acuerdo a lo expuesto por Rodríguez (2007) dentro de su conceptualización de hace 14 años, el autor afirma 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 puede realizarse a 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 (p.2)

Aunado a lo anterior y con la llegada de la emergencia sanitaria el concepto sobre el teletrabajo de acuerdo a Viancha y Sarmiento (2021), se conceptualiza de la siguiente manera:

> El teletrabajo se ha desarrollado de forma vertiginosa en los últimos meses como consecuencia del COVID-19. Para muchas empresas se ha convertido en una modalidad esencial para la continuidad de su negocio. Su uso debe hacerse respetando una serie de medidas de seguridad si no se quiere ser víctima de un incidente de seguridad que ponga en riesgo la continuidad de la empresa (p.1).

Tal y como se logra evidenciar desde las perspectivas de los autores, se encuentran diversas opiniones al respecto y esto se debe claramente al cambio del contexto y las circunstancias; Sin embargo, en estas dos conceptualizaciones surgen dos temas fundamentales, por un lado, el que expresa Rodríguez (2007), “la actividad profesional en el teletrabajo implica el uso permanente de algún medio de telecomunicación para el contacto entre el teletrabajador y la empresa” (p.2). y por el otro según Viacha y Sarmiento (2021), “su uso debe hacerse respetando una serie de medidas de seguridad si no se quiere ser víctima de un incidente de seguridad que ponga en riesgo la continuidad de la empresa” (p.1). En ese sentido la seguridad de la información en el ámbito del teletrabajo ha comenzado a tener un rol fundamental ya que, en el marco de la pandemia, la disposición del teletrabajo, ha generado el surgimiento de ciberataques, aprovechándose del contexto donde se labora, situación que produce inseguridades cibernéticas, que ponen en duda las capacidades de protección de información.

En tal sentido, con la situación que se ha presentado en los últimos meses se ha logrado observar que es pertinente profundizar sobre este caso atípico dentro de la cotidianidad; sin duda alguna el activo más importante dentro de las organizaciones es la información, por lo que las empresas deben prestar especial cuidado si de tratar de no ser víctimas de ataques informáticos se trata.

Por otra parte, es conveniente señalar que las empresas en su mayoría no habían previsto un plan de contingencia para situaciones como la que se ha vivido en los últimos tiempos y para lo cual se requiere que se busquen opciones de parte de las organizaciones para diseñar estrategias que converjan en modelos que permitan mitigas los ataques informáticos.

Así mismo tal y como lo expone Medina y Ocampo (2021), la seguridad de la información es una necesidad creciente en las empresas a nivel mundial. Aunque su auge ha aumentado, todavía no hay normativa que exija su cumplimiento y hasta el momento, no hay un estándar que lo gobierne.

1.2 Formulación del problema.

¿Cuál es la estructura de un modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo

1.3 Objetivos.

1.3.1 Objetivo General

Proponer un modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo

1.3.2 Objetivos Específicos

Caracterizar los fundamentos teóricos y prácticos del teletrabajo y los componentes de seguridad de la información requeridos

Estructurar los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo.

Validar el modelo de gobierno de TI orientado a la seguridad de la información mediante el juicio de expertos.

Para el desarrollo de los objetivos se plantea la siguiente matriz de objetivos

Tabla 1. *Matriz de objetivos*

Objetivo	Actividades	Indicadores
1. Caracterizar los fundamentos teóricos y prácticos del teletrabajo y los componentes de seguridad de la información requeridos	1. Identificación de fundamentos teóricos y prácticos de teletrabajo y trabajo en casa 2. Caracterizar los conceptos identificados	Fundamentos identificados Caracterización de los fundamentos teóricos y prácticos de teletrabajo y trabajo en casa
• Estructurar los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo.	1. Diseño del instrumento 2. Aplicó el instrumento 3. Tabuló el instrumento 4. Identificación de componentes 5. Diseño del Modelo	Instrumento diseñado Instrumento aplicado Tabulación de resultados Identificación de componentes Modelo diseñado

• Validar el modelo de gobierno de TI orientado a la seguridad de la información mediante el juicio de expertos.	1. Seleccionar la técnica de validación 2. Identificaron los expertos 3. Calificaron los expertos 4. Realizar la validación	Técnica seleccionada Expertos identificados Expertos calificados Validación del modelo

1.4 Justificación.

Los beneficios de la innovación digital orientada a optimizar el desarrollo de las actividades cotidianas que impregnan con mayor fuerza a la sociedad moderna, carecen de inmunidad tanto a nivel personal como organizacional, provocando la permanente exposición a fuertes amenazas (Prince, 2018).

En la actualidad las empresas se han enfrentado a cambios e innovaciones, algunas favorables y otros mejorables, razón que conlleva a repensar el modo cotidiano de planeación, organización, ejecución, control y producción, de las empresas y que en tiempos de crisis e incertidumbre se deben repensar para poder mantener la producción y la calidad; por lo tanto, la presente investigación se justifica desde el plano teórico por ser una necesidad que fortalezca los procesos que confluyen sobre la seguridad de la información de tal forma que se logre el apoyo hacia la mitigación sobre la materialización de cualquier amenaza.

Así mismo, es conveniente señalar que la justificación metodológica se enmarca en una metodología mixta que converge en el enfoque anidado; es decir, que se pretende emplear la lo cuantitativo y en él se anida lo cualitativo; puesto que, de los aspectos cuantitativos se van a desprender las categorías y es allí donde se seleccionan los informantes y se concretan acciones reforzadas y bien complementadas, debido a que se logra que lo que se deje pasar en la parte en

lo cuantitativo, lo cualitativo lo puede tocar; de esa manera se garantiza que existan una rigurosidad investigativa, bastante alta.

En fin, la justificación del presente trabajo, se perfila en proponer un modelo de gobierno de seguridad de la información para el sector empresarial en el marco del teletrabajo. La presente investigación estará fundamentada en recientes análisis de diversos autores, entre los cuales citaremos estudios como el desarrollado por (Lee & Yen, 2018), quienes abordan la seguridad de la información desde el ámbito de las empresas Fintech, (término compuesto que viene del inglés y que resulta de unir la primera sílaba de las palabras Finance y Technology); como concepto acuñado a las organizaciones de servicios que usan tecnología de punta para ofrecer productos y servicios, en donde se expone las falencias de las políticas de seguridad existentes.

1.5 Delimitaciones

Geográficas. La investigación se desarrollará en las empresas de Norte de Santander

Temporales. El tiempo definido para la ejecución de la presente investigación corresponde a dos semestres académicos o 12 meses contemplado desde la aprobación de la propuesta.

Conceptuales. La conceptualización utilizada para el desarrollo de la investigación es la asociada con Seguridad de la información, teletrabajo, Gobierno de TI, Gestión de TI

Operativa. Para el desarrollo del proyecto se consideran las limitaciones de acceso a la información en algunas empresas, adicionalmente se pueden presentar problemas de orden público.

2. Marco referencial

2.1 Antecedentes investigativos.

En ecuador realizaron una investigación acerca de Mecanismos de ciberseguridad en dispositivos de teletrabajo para una institución financiera. El autor menciona que en la actualidad, debido a la gran cantidad de ataques y estafas cibernéticas que se realizan, las instituciones tendrían en cuenta que la aplicación de ciberseguridad es una prioridad, sobre todo en este caso que se trata de una institución financiera, la cual aplicaría mecanismos de ciberseguridad para el control de los dispositivos que realizan teletrabajo, existen varios riesgos que serían mitigados con la aplicación de estos mecanismos, como se analizó en la Tabla 30, teniendo un impacto positivo como protección tanto a los dispositivos, como al bien más importante que es la información, permitiendo contrarrestar posibles ataques a futuro (Silva, 2020).

En España Reinoso y Gómez (2021), hicieron un trabajo sobre una propuesta de políticas de Ciberseguridad para el Teletrabajo. Caso de estudio Rectorado ESPOCH, el objetivo del proyecto fue proponer políticas de ciberseguridad orientadas a personas que realizan teletrabajo. Como resultado, se evidencio que en el análisis realizado se demostro una diferencia significativa del antes y después en reflejado en el P Valor, donde, este es menor al valor de significancia demostrando la propuesta de políticas de ciberseguridad para el teletrabajo permite el uso adecuado de la información del Rectorado de la ESPOCH. Como conclusión, las prácticas de políticas orientadas a ciberseguridad para el teletrabajo han hecho que los funcionarios del Rectorado de la ESPOCH conozcan de los riegos que conlleva el teletrabajo y las formas que se pueden evitar posibles ataques y la pérdida de la información de esta dependencia. Si bien las políticas de ciberseguridad para el teletrabajo están bajo la norma ISO/IEC 27001, estás no están

complementadas con las buenas prácticas o controles establecidos en la norma ISO/IEC 27002 siendo una limitante en este estudio

Por otro lado, Bustos (2015), realizo un trabajo de investigación sobre la seguridad informática para el teletrabajo en empresas privadas en Colombia, en el documento se sugiere como tratar temas en la seguridad de equipos de cómputo y sistema operativo la seguridad de las comunicaciones, la seguridad de la información y la seguridad del recurso humano.
En conclusión, los autores proponen implementar políticas de ciberseguridad en organizaciones en modo de trabajo remoto como una solución completa no solo para proteger, mantener y administrar de manera efectiva todo tipo de recursos con los que cuenta la organización, sino que también busca brindar soluciones para prevenirlos y evitarlos. Controlar y minimizar el daño de los incidentes que afectan a la organización, por lo que preparar y capacitar a los empleados en temas relacionados con la ciberseguridad y cómo enfrentar los incidentes para responder adecuadamente es uno de los principales objetivos de esta estrategia.

A nivel nacional, Molina y Quintero (2021), hicieron una investigación sobre el diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Bonos y Descuentos SAS, a partir de la norma ISO 27001: 2013. El objetivo del proyecto fue diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para Bono y Descuento SAS, basado en los lineamientos de la norma ISO 27001:2013, para asegurar los activos de información. En conclusión, el seguro de propiedad ha demostrado ser muy importante, ya que es posible identificar debilidades y amenazas, estructurar y planificar medidas orientadas al riesgo, utilizar los recursos de manera eficaz y eficiente, invertir en el lugar correcto y reducir costos a largo plazo.

2.2 Antecedentes legales.

2.2.1 Administración de las políticas de seguridad de la información

Las políticas de seguridad de la información se revisan y actualizan anualmente para garantizar su validez y relevancia para lograr los objetivos de la organización. Asimismo, se revisa cuando se presentan condiciones tales como: cambios organizacionales, culturales o ambientales internos o externos, o cambios operativos u organizacionales que afecten a la organización. , cuando ocurren incidentes de seguridad de la información que requieren controles o directivas mejorados, o como resultado de la gestión de riesgos institucionales. A continuación, se relacionan de decretos asociados al objeto de estudio del presente trabajo.

Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Decreto No. 2106 del 22 de noviembre de 2019. “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.”

Documento CONPES 3854, Política Nacional de Seguridad Digital.

Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES)

Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado. Versión 04 Si este documento se encuentra impreso no se garantiza su vigencia. Fecha: 2020-02-20 La versión vigente reposa en el Sistema Integrado de Planeación y Gestión (Intranet).

Circular Externa Conjunta No. 04 del 5 de septiembre de 2019. Tratamiento de datos personales en sistemas de información interoperables.

Norma Técnica Colombiana NTC- ISO/IEC colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos

2.3 Marco Conceptual.

2.3.1 Teletrabajo

El trabajo remoto o teletrabajo es una de las alternativas que permite alcanzar mejores tasas de crecimiento, aprovechando los beneficios que trae para el desarrollo económico, cultural y social, el progreso tecnológico, rendimiento laboral etc. (Parraga y Mora, 2022).

El teletrabajo es una forma de trabajo que se realiza en un lugar alejado de las oficinas centrales o de las instalaciones de producción, mediante la utilización de las nuevas tecnologías de la comunicación (Medina et al., 2022)

2.3.2 Sector Empresarial

El sector empresarial es el pilar fundamental de las economías de mercado, al sostener las decisiones de políticas relacionadas con el empleo e implementación de funciones sustantivas en la estructura comercial. Asimismo, la gestión empresarial se relaciona directamente con la innovación, al aplicar nuevas actividades productivas en el empleo, formulaciones de comercio y servicios (Pozos and Acosta, 2016). El sector empresarial es el segmento en los que se dividen las actividades económicas y productivas de la sociedad. Es también conocido como el sector de la economía, consta de tres sectores: primario que involucra la agricultura, la ganadería y el extractivismo; secundario, referido a la industria y la construcción civil; y terciario, que comprende el comercio y la prestación de servicios" (Pinos et al., 2022).

Por otro lado, "el sector empresarial puede definirse como grandes áreas o segmentos en los que se dividen las actividades económicas desarrolladas por la sociedad. Esta categorización se realiza mediante tres sectores, que agregan empresas, negocios y puestos de trabajo similares en su forma de ejecución y / o en su finalidad final" (Pinos et al., 2022).

2.3.3 Seguridad de la información

La seguridad de la información surge como una medida de asegurar que la información tenga los niveles adecuados de protección en cuanto a Confidencialidad, Integridad y Disponibilidad (Nieves, 2017).

Como lo expresa Suárez y Fontalvo (2015):

> La seguridad de la información es un tema de nunca acabar y que por tal motivo la actualización de los distintos recursos y procesos que se identifiquen día a día es sumamente importante para minimizar los riesgos en el ámbito de seguridad de las organizaciones (p.6).

2.3.4 Seguridad de recursos humanos

Las características de los recursos humanos son probablemente el elemento más importante para garantizar las tres características de la seguridad de la información que son: integridad, confidencialidad y disponibilidad, y de ahí la necesidad de establecer controles y medidas de gestión, razones que pueden lograrse para ayudar a mitigar el impacto de los riesgos. derivados de esto (Postos, 2015). En este sentido, la capacitación de los empleados es un factor muy importante porque lamentablemente el recurso humano es el más vulnerable de todos los activos de la empresa, ya que la capacitación permite que los empleados desempeñen un papel activo dentro de la organización de manera de aplicar el conocimiento para proteger completamente la información confiada.

2.3.5 Cobit 5

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. Por lo tanto, COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público (Mora et al., 2017).

2.3.6 Cobit 2019

COBIT® 2019 es la evolución de la versión anterior COBIT 5, construida sobre sus fundamentos sólidos añadiendo las últimas actualizaciones en materia de información y tecnología empresariales. Además de la versión actualizada del framework, COBIT ofrece más recurso de implementación, guías prácticas y profundizaciones, así como oportunidades de formación completa (Monfort, 2016).

COBIT 2019 ayuda en la gestión empresarial a través de información y tecnologías independientemente del lugar de origen.

- Introducción de nuevos conceptos como esferas de interés y factores proyectuales que proporcionan una guía adicional para crear un sistema de gobierno a medida para las necesidades de la empresa
- El alineamiento actualizado a los estándares, marcos y mejores prácticas globales mejora la relevancia del COBIT
- Un modelo “open-source” permitirá a la comunidad de gobierno global obtener la habilidad de ser informados sobre las actualizaciones futuras proporcionando feedback, compartiendo aplicaciones y proponiendo mejorías al marco y a los productos en tiempo real, con ulteriores evoluciones COBIT lanzadas gradualmente
- Una nueva guía y nuevas herramientas soportan el desarrollo de un sistema de gobierno más adecuado, haciendo COBIT® 2019 más perspectivas.

2.4 Marco Teórico

2.4.1 Teoría de la sociedad de la información

Durante la última década, la expresión o frase "sociedad de la información" ciertamente se ha establecido como un término poderoso, no necesariamente porque ofrece claridad teórica, sino por el bautismo que representa. recibido en las políticas oficiales de los países más avanzados, así como la coronación que se supone honrará con una cumbre mundial (Burch, 2005).

En 1973, el sociólogo estadounidense Daniel Bell introdujo el concepto de "sociedad de la información" en su libro The Birth of a Post-Industrial Society (Bell), declarando que su enfoque principal sería el conocimiento teórico y advirtiendo que los servicios basados en el conocimiento tendrían convertirse en la estructura básica de la nueva economía y sociedad Información basada donde las ideologías serían superfluas.

Esta expresión reaparece con fuerza en los años 90, en el contexto del desarrollo de Internet y de las TIC. A partir de 1995, fue incluida en la agenda de las reuniones del G7 (luego G8, donde se juntan los jefes de Estado o gobierno de las naciones más poderosas del planeta). Se ha abordado en foros de la Comunidad Europea y de la OCDE (los treinta países más desarrollados del mundo) y ha sido adoptada por el gobierno de los Estados Unidos, así como por varias agencias de las Naciones Unidas y por el Grupo Banco Mundial. Todo ello con gran eco mediático. A partir de 1998, fue elegida, primero en la Unión Internacional de Telecomunicaciones y luego en la ONU, como el nombre de la Cumbre Mundial a realizarse en 2003 y 2005 (Burch, 2005).

En cuanto a la sociedad del conocimiento, en una publicación posterior señala: “se trata de una sociedad en la que las condiciones de generación de conocimiento y procesamiento de información han sido sustancialmente alteradas por una revolución tecnológica centrada en el procesamiento de información, en la generación del conocimiento y en las tecnologías de la información” (Castells, 2002).

La sociedad de la información facilita las actividades de millones de individuos en todo el mundo, pues ofrece soluciones a problemas de distinta naturaleza (cotidianos, académicos, culturales, sociales, económicos, etc.) a través de la creación, acceso, manejo e intercambio de contenido electrónico.

Tubella (2012) considera que:

> En la sociedad de la información, la acción comunicativa y el conjunto de los medios de comunicación de masas (*los media*) adquieren un renovado papel decisivo en el proceso de construcción del poder. Puesto que los discursos se generan, difunden, debaten, internalizan e incorporan a la acción humana, en el ámbito de la comunicación socializada en torno a las redes locales-globales de comunicación, las redes de comunicación y nuestra actuación en y a partir de ellas, resultará clave en la definición de las relaciones de poder en nuestros días (p. 99).

Los principales factores para el desarrollo y avance de la sociedad del conocimiento son la innovación y la creatividad, lo que ha llevado al cambio en todos los niveles estructurales y operativos a través de la transformación de procesos, género, introducción de nuevas tecnologías, provisión de nuevos servicios, etc. Sin estas variables, la sociedad actual no habría existido o decaería por completo, ya que la sociedad del conocimiento

se construye a través del intercambio, la acumulación, la gestión y la producción de conocimiento. Por lo tanto, si hay acuerdo en el supuesto de que el hombre está integrado en la comunidad de la verdad -cuyas principales características son el conocimiento, sus efectos, su compatibilidad y su relación con los diversos campos de la investigación y las ciencias, entonces podemos hablar de una comunidad innovadora, empresa tecnológica y creativa (Pérez et al., 2018).

2.4.2 Seguridad de la información

La seguridad de la información es un tema de negocios y cómo las instituciones financieras deben ser conscientes de ello para hacer frente a un entorno altamente regulado y competitivo; Por ello, la perspectiva adecuada para lograr un cumplimiento normativo satisfactorio es abordarlo desde un enfoque gubernamental, transversal a toda la organización, no solo desde un enfoque gubernamental. En este contexto, la adopción de las mejores prácticas como Cobit 5 e ISO 27000 nos brinda una guía clara para definir el alcance, los objetivos de mejora, las soluciones y la planificación de proyectos, que definen las métricas de sostenibilidad y los catalizadores de desempeño que permiten la gestión empresarial y la gestión de la seguridad de la información (Arévalo, 205).

La seguridad de la información es un principio transversal en la protección de los derechos de los ciudadanos, la integridad del estado y la industria, es por ello que el estado colombiano desarrollo la estrategia gobierno en línea (GE) que tiene como objetivo tener un estado más eficiente, transparente y participativo, reglamentado de forma unificada a través del decreto 1078 de 2015 - *Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones*- de obligatorio cumplimiento para las entidades que conforman la

administración pública colombiana y en donde se establece su ámbito de aplicación, definiciones, principios y propósitos fundamentales (Carvajal et al., 2019).

La seguridad de la información es un sistema tradicionalmente asociado a la gestión de las tecnologías de la información y las comunicaciones, cuyo fin es mantener un nivel aceptable de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten recolectar la información. Recopilación, procesamiento, acceso, intercambio, El almacenamiento y la transferencia están totalmente presentes. Está definido por ISO/IEC 27000 como el mantenimiento de la confidencialidad, integridad y disponibilidad de la información (Valencia y Orozco, 2017).

La adopción temprana de la ISO 27001 en todo el mundo en comparación con otros estándares de gestión (Freixo & Rocha, 2014), pone de manifiesto la importancia que ha tomado la seguridad de la información, lo cual se ratifica a partir del número de certificaciones otorgadas por la Organización Internacional para la Estandarización (ISO) en los últimos años, presentando un crecimiento exponencial, al pasar de un total de 5797 certificaciones en el año 2006, a 27536 en 2015, siendo Japón y el Reino Unido los países con mayor número de empresas certificadas, de acuerdo al último informe de la entidad (ISO, 2017). No obstante, las normas establecen el deber ser, y no la forma como se logra, de allí la importancia de establecer metodologías que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para tal fin.

2.4.3 Teletrabajo

La sociedad de la información ha flexibilizado y matizado la rígida relación laboral formada en el siglo XX, expandiendo así su alcance a lugares

antes inimaginables. El trabajo remoto es producto de esta flexibilidad y constituye una forma de trabajo que disfrutan empresarios y trabajadores de todo el mundo, debido a sus enormes beneficios económicos, sociales y ambientales. La práctica social es el motor de las relaciones jurídicas, que deben ser reguladas por la ley. El teletrabajo como realidad social merece atención legal, regulación e institucionalización, como ya ha comenzado en la Unión Europea. Los campos académicos de los países deben estar vinculados a este trabajo normativo, ya que el trabajo a distancia es aún un campo en construcción que merece el aporte de todos (Rodríguez, 2007).

El teletrabajo es una forma de organización del trabajo, que implica la prestación del servicio en un lugar distinto a la empresa y utiliza como herramienta fundamental las tecnologías de la información.

Tomando los anteriores elementos pero agregándole otros, nos aventuramos a presentar una definición de teletrabajo: Es aquel trabajo, que pudiendo ejecutarse en las oficinas de la empresa, se caracteriza precisamente porque es realizado por un trabajador en su casa a través de un computador siguiendo las órdenes de su jefe recibidas por Internet, trabajo que luego enviará por esta misma vía a su jefe y por el cual recibirá una remuneración; o en otras palabras, es un trabajo cuya ejecución se realiza en el computador y cuyos resultados llegan al jefe por vía del Internet, es decir, no hay desplazamiento del trabajador hacia el sitio de trabajo porque éste trabaja en su hogar. (Rodríguez, 2007)

El teletrabajo es una forma organizada de trabajo realizado en el marco de un contrato de trabajo o una relación laboral, incluido el desempeño de funciones y responsabilidades, utilizando tecnologías de la información y la comunicación. Sin embargo, el logro de metas y resultados es esencial. Esta es una relación comercial legal y como tal está sujeta a la legislación

laboral y demás leyes laborales aplicables en cada país. Los días ordinarios no podrán reservarse y los extraordinarios registrarse económicamente. Cabe recalcar que los trabajadores que trabajan a distancia por condiciones de trabajo están sujetos a jornada laboral y, en su caso, pago de horas extras por día, y estas condiciones siempre deben ser determinadas de acuerdo con el acuerdo de las partes con el empleador (Santillan, 2020).

El teletrabajo es una derivación del trabajo previamente establecido, que se ha diseñado con la finalidad de que el recurso humano de una institución labore desde su hogar con beneficios para ambas partes, convirtiéndose hoy en la mejor oportunidad para hacer compatible la protección frente a la pandemia de la COVID-19 con el mantenimiento de las actividades productivas. Para muchos teletrabajadores con experiencia previa, la novedad ha sido la amplitud con la que han utilizado esta modalidad, que en estos días se ha convertido en exclusiva (Peiró y Soler, 2020).

2.5 Marco Contextual

El trabajo será desarrollado en Norte de Santander Nor oriente Colombiano zona que limita con la república Bolivariana de Venezuela. Se abordarán empresas tanto públicas como privadas, tomando diferentes sectores con el educativo, el financiero, el sector transporte y empresas del estado como alcaldías.

3. Diseño metodológico

En este capítulo se describe el tipo de estudio y los diferentes factores que permiten diseñar una intervención para lograr el objetivo de la investigación.

Esta investigación tiene una connotación de multimétodos, se define a partir del estudio de una situación que permiten definir procesos aplicables fundamentados con un enfoque cuantitativo que permite la recolección de información con el objetivo de demostrar hipótesis y dar validez a las teorías. La Metodología Cuantitativa es aquella que permite examinar los datos de manera numérica, especialmente en el campo de la Estadística. Para que exista Metodología Cuantitativa se requiere que entre los elementos del problema de investigación exista una relación cuya Naturaleza sea lineal. Es decir, que haya claridad entre los elementos del problema de investigación que conforman el problema, que sea posible definirlo, limitarlos y saber exactamente donde se inicia el problema, en cual dirección va y que tipo de incidencia existe entre sus elementos (Palacios, 2016)**.**

El alcance de la investigación cuantitativa es poder establecer las relaciones de causa-efecto que se pueden presentar también cuando abordamos problemas sociales. Este tipo de investigación también se fundamenta en hallazgos comunes que permitan relacionar las variables en diversas realidades en la sociedad mediante el uso de la estadística, donde otros investigadores sociales pueden fundamentarse para continuar con otros estudios (Babativa, 2017).

Así mismo para el logro del modelo se opta por utilizar una metodología descriptiva, en las investigaciones de tipo descriptiva, llamadas también investigaciones diagnósticas, buena

parte de lo que se escribe y estudia sobre lo social no va mucho más allá de este nivel. Consiste, fundamentalmente, en caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciadores (Morales, 2012).

De igual manera se contempla el enfoque cualitativo porque quiere entenderse el fenómeno objeto de estudio, abordando desde la perspectiva de diferentes actores involucrados en el proceso.

3.1 Población

Se contará con empresas tanto públicas como privadas de Norte de Santander. De igual manera, se estratificará por tipo de empresas de orden educativo, financiero, transporte y alcaldías.

Para la investigación cualitativa se contará con Informantes claves: Empresarios, Trabajadores y líderes de seguridad

3.2 Muestra

Como empresas se tomarán en el sector educativo de orden oficial y privada, financiero bancos y cooperativas de ahorro, empresas de transporte creadas en el departamento y la alcaldía de la provincia de Ocaña.

Para la investigación cualitativa se contará con Informantes claves: (3) Empresarios,

(5)Trabajadores y (2) líderes de seguridad

3.3 Técnicas de recolección de la información

Al utilizar multimétodos se contará con diferentes técnicas de recolección de la información, se parte de una matriz de operacionalización de variables de donde se estructura una encuesta (Ver Anexo 1), se diseña un instrumento cuestionario aplicable a trabajadores en teletrabajo y trabajo en casa (Ver Anexo 2) y se trabaja guion de preguntas para las entrevistas para empresarios, trabajadores y líderes de seguridad (Ver Anexo 3) para esto se tiene establecido unas categorías previas (Ver Anexo 4)

3.3.1 Análisis de la información.

Para el análisis de la información recopilada se tomarán herramientas como SPSS para el análisis cuantitativo y ATLAS TI para el análisis cualitativo que genera diferentes redes de información.

4. Modelo de gobierno de seguridad de la información en el sector empresarial en el marco del teletrabajo

En este capítulo se muestran los resultados obtenidos siguiendo el diseño metodológico

4.1 Caracterización de los fundamentos teóricos y prácticos del teletrabajo y los componentes de seguridad de la información requeridos

El teletrabajo, también conocido como trabajo remoto o trabajo a distancia, es una modalidad laboral en la que los empleados realizan sus tareas desde ubicaciones fuera de la oficina principal de la empresa, generalmente desde sus hogares o lugares de su elección (Beltran et al., 2020). Los fundamentos teóricos y prácticos del teletrabajo implican una combinación de aspectos organizativos, tecnológicos y de seguridad de la información. Aquí tienes una caracterización de estos fundamentos (Prieto et al., 2022):

Fundamentos Teóricos del Teletrabajo

Figura 1. *Fundamentos teóricos de Teletrabajo*

Flexibilidad Laboral: El teletrabajo se basa en la idea de proporcionar a los empleados la flexibilidad para realizar sus tareas en un horario y lugar que les resulte conveniente, lo que puede mejorar su equilibrio entre el trabajo y la vida personal.

La flexibilidad laboral, un componente fundamental del teletrabajo, trae consigo una transformación significativa en la forma en que concebimos y llevamos a cabo nuestras responsabilidades laborales. En este nuevo paradigma, los trabajadores tienen la capacidad de adaptar su horario y entorno de trabajo de acuerdo con sus necesidades personales y profesionales, marcando un hito en la evolución del mundo laboral (Jiménez y Serrano, 2023).

La joya de la corona de esta flexibilidad es la posibilidad de establecer un horario laboral flexible. Los empleados ya no están atados a las restricciones tradicionales de 9 a 5, sino que pueden diseñar su día laboral de acuerdo con sus ritmos y preferencias individuales. Esta libertad no solo aumenta la satisfacción laboral, sino que también puede impulsar la productividad, ya

que las personas tienden a rendir mejor cuando trabajan en sus momentos de mayor energía y concentración.

El teletrabajo, al eliminar el desplazamiento diario, libera un valioso recurso: el tiempo. Ese tiempo antes utilizado en el tráfico o el transporte público ahora se puede invertir en actividades que enriquecen la vida personal. La capacidad de conciliar el trabajo con compromisos familiares, ejercicio, desarrollo personal o simplemente tiempo de calidad con seres queridos se convierte en una realidad alcanzable (Arriola Y Chavez, 2023).

La flexibilidad geográfica añade un toque de aventura a esta nueva forma de trabajar. Algunos empleados tienen la libertad de elegir su lugar de trabajo, lo que les permite explorar nuevos destinos mientras cumplen con sus tareas laborales. Esta flexibilidad geográfica también puede beneficiar a las empresas al permitirles acceder a un talento diverso y global.

Sin embargo, esta libertad no viene sin responsabilidad. Los trabajadores remotos deben gestionar su tiempo de manera efectiva y cumplir con las expectativas laborales acordadas con sus empleadores. La comunicación abierta y la transparencia son esenciales para establecer y mantener una relación laboral exitosa en el teletrabajo.

En resumen, la flexibilidad laboral en el teletrabajo representa una revolución en la forma en que vivimos y experimentamos el trabajo. Al liberarnos de las restricciones de tiempo y lugar, esta modalidad no solo mejora el equilibrio entre trabajo y vida personal, sino que también potencia el bienestar de los trabajadores y la eficiencia laboral. El teletrabajo no solo es un cambio en la ubicación de la oficina, sino un cambio de paradigma que redefine cómo conciliamos nuestras vidas profesionales y personales en la era digital.

Tecnología de la Información: La disponibilidad de tecnología de la información avanzada, como computadoras portátiles, acceso a Internet de alta velocidad y software de colaboración en línea, ha hecho posible el teletrabajo.

Las tecnologías de la información desempeñan un papel central en la viabilidad y eficacia del teletrabajo. Desde las computadoras portátiles y dispositivos móviles que actúan como nuestras puertas de entrada al mundo laboral digital, hasta las aplicaciones de colaboración en línea que nos permiten interactuar con colegas y supervisores en tiempo real, estas herramientas tecnológicas son la columna vertebral del teletrabajo. La conectividad a Internet de alta velocidad se convierte en el puente que nos une a nuestras tareas y responsabilidades, mientras que el software de gestión de proyectos y las plataformas de comunicación en línea hacen posible la coordinación de equipos y proyectos, sin importar la ubicación geográfica de los miembros. La seguridad informática también es esencial, ya que las VPN y las herramientas de protección garantizan que los datos y sistemas empresariales estén a salvo de amenazas cibernéticas. En última instancia, estas tecnologías hacen que la flexibilidad y la eficiencia del teletrabajo sean posibles, brindando una solución valiosa para las empresas y trabajadores que buscan un enfoque más flexible y adaptativo hacia la labor (Botero, 2023).

Productividad y Eficiencia: Los defensores del teletrabajo argumentan que puede aumentar la productividad al reducir las distracciones de la oficina y minimizar el tiempo de desplazamiento.

La productividad y la eficiencia en el teletrabajo se basan en la capacidad de los empleados para gestionar su tiempo de manera efectiva, mantener un entorno de trabajo propicio y aprovechar al máximo las herramientas tecnológicas disponibles. La autodisciplina y la motivación son pilares clave, ya que los trabajadores deben establecer rutinas sólidas y

mantenerse enfocados en sus tareas. La comunicación constante con el equipo y la claridad en los objetivos también desempeñan un papel crucial, asegurando que todos estén alineados en sus esfuerzos. Además, la evaluación continua y la adaptación a medida que se identifican oportunidades de mejora permiten optimizar aún más la productividad y la eficiencia en este entorno de trabajo en evolución constante. En última instancia, la combinación de autogestión, herramientas tecnológicas y apoyo organizacional adecuado contribuye a un teletrabajo exitoso y altamente productivo.

La productividad y la eficiencia en el teletrabajo son cuestiones críticas tanto para los empleados como para las organizaciones, y su importancia se ha vuelto aún más evidente en el contexto actual de trabajo a distancia generalizado. Un elemento esencial en este contexto es la autogestión del tiempo. Los empleados deben aprender a administrar su jornada laboral de manera efectiva, estableciendo horarios regulares y garantizando que sus tareas se completen en los plazos establecidos. La ausencia de supervisión directa implica que los trabajadores deben ser responsables de sus propias actividades y asegurarse de no caer en la procrastinación o la dispersión (Rosales et al., 2023).

Además, la eficiencia en el teletrabajo está vinculada a la organización del espacio de trabajo. Un entorno de trabajo adecuado, libre de distracciones y ergonómico, puede contribuir en gran medida a mantener la concentración y el rendimiento. La configuración de un espacio de trabajo cómodo y profesional crea un ambiente propicio para el trabajo productivo, evitando que las interrupciones familiares o domésticas afecten negativamente la concentración.

El uso efectivo de herramientas tecnológicas es otro pilar fundamental de la productividad en el teletrabajo. Las aplicaciones de colaboración en

compañeros de trabajo. La gestión de proyectos y el seguimiento de tareas a través de software especializado, como Trello o Asana, aseguran que los proyectos avancen de manera ordenada y que los plazos se cumplan sin problemas (Díaz et al., 2023).

La motivación también juega un papel esencial. Los trabajadores deben encontrar formas de mantenerse motivados y enfocados en sus tareas, a menudo sin la presencia física de colegas o supervisores. Establecer metas claras y autoevaluarse regularmente puede ser útil en este sentido.

En última instancia, la productividad y la eficiencia en el teletrabajo son el resultado de una combinación de factores, que incluyen la autodisciplina, la organización del espacio de trabajo, el uso efectivo de herramientas tecnológicas y la motivación personal. Las organizaciones pueden apoyar estos esfuerzos proporcionando capacitación en teletrabajo, estableciendo políticas claras y ofreciendo un entorno de apoyo que permita a los empleados prosperar en esta modalidad laboral (Díaz et al., 2023).

Acceso al Talento Global: El teletrabajo permite a las empresas reclutar y retener talento de todo el mundo, ya que no están limitadas por la ubicación geográfica de sus empleados.

El teletrabajo ha revolucionado la forma en que las organizaciones acceden al talento global. Antes, las restricciones geográficas limitaban la búsqueda de candidatos y el alcance de una empresa. Ahora, con el teletrabajo en auge, es posible reclutar a profesionales altamente calificados sin importar su ubicación. Esto abre un mundo de posibilidades para las empresas.

Imagínate poder reclutar a un desarrollador de software en la India, un diseñador gráfico en Brasil o un experto en marketing en Australia, todo en el mismo equipo. Esto no solo diversifica tu fuerza laboral, sino que también te da acceso a una riqueza de perspectivas culturales y experiencia internacional.

Además, el acceso al talento global puede ser crucial para la obtención de habilidades específicas. Si necesitas un especialista en un campo particular y no puedes encontrarlo en tu área local, el teletrabajo te permite buscar en todo el mundo y encontrar al candidato adecuado.

La flexibilidad en las zonas horarias es otro beneficio clave. Imagina un equipo que pueda atender a clientes o proyectos en diferentes partes del mundo las 24 horas del día. Esto no solo mejora la satisfacción del cliente, sino que también aumenta la eficiencia operativa (Escobar et al., 2023).

El acceso a trabajadores independientes o contratistas de todo el mundo también se ha vuelto más sencillo. Puedes contratar temporalmente para proyectos específicos sin preocuparte por reubicaciones costosas o compromisos a largo plazo.

El teletrabajo también contribuye a la retención de empleados. Al ofrecer esta modalidad, las organizaciones pueden mantener a empleados talentosos que, de lo contrario, podrían buscar oportunidades en otras partes debido a restricciones de ubicación.

En última instancia, el acceso al talento global no solo enriquece la fuerza laboral sino que también puede impulsar la capacidad competitiva, permitiéndote expandirte a nuevos mercados y fomentar la innovación a través de la diversidad de perspectivas y habilidades. El teletrabajo ha roto las barreras geográficas, abriendo un mundo de posibilidades para las organizaciones que buscan el mejor talento, sin importar dónde se encuentre.

Fundamentos Prácticos del Teletrabajo

De acuerdo a Villalón (2021), los fundamentos prácticos del teletrabajo son los siguientes:

Figura 2. *Fundamentos prácticos de Teletrabajo*

Políticas y Procedimientos: Las empresas deben establecer políticas claras de teletrabajo que definan quiénes son elegibles, cómo se solicita y se aprueba el teletrabajo, y las expectativas de desempeño y comunicación.

Tecnología y Herramientas: Proporcionar a los empleados acceso a la tecnología y las herramientas necesarias, como computadoras portátiles seguras, conexiones VPN (Red Privada Virtual) y software de colaboración en línea.

Comunicación Efectiva: Establecer canales de comunicación efectivos para que los teletrabajadores se mantengan conectados con sus equipos y supervisores, como reuniones en línea, chats y correo electrónico.

Gestión del Desempeño: Implementar sistemas de seguimiento y evaluación del desempeño que permitan a los empleadores medir el rendimiento de los teletrabajadores de manera objetiva.

Componentes de Seguridad de la Información Requeridos:

De acuerdo a Reinoso y Gómez (2021), los componentes de seguridad para el teletrabajo son los siguientes:

Protección de Datos: Garantizar que los datos sensibles o confidenciales estén protegidos mediante cifrado y medidas de acceso restrictivas.

Acceso Seguro: Establecer autenticación de dos factores (2FA) y utilizar conexiones VPN para asegurarse de que solo los usuarios autorizados puedan acceder a los sistemas y datos de la empresa.

Actualizaciones de Seguridad: Mantener el software y los sistemas actualizados con parches de seguridad para protegerse contra vulnerabilidades conocidas.

Políticas de Uso Adecuado: Establecer pautas claras sobre cómo los empleados deben usar los recursos de la empresa, incluyendo el uso de dispositivos personales para el trabajo.

Formación en Seguridad: Proporcionar capacitación a los empleados sobre prácticas seguras de teletrabajo y cómo identificar posibles amenazas de seguridad.

Respuesta a Incidentes: Desarrollar un plan de respuesta a incidentes para abordar posibles brechas de seguridad de manera efectiva y minimizar el impacto.

Cumplimiento Legal y Regulatorio: Asegurarse de que el teletrabajo cumpla con todas las regulaciones y leyes de privacidad de datos aplicables en la jurisdicción en la que opera la empresa.

4.2 Estructuración de los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo.

4.2.1 Diagnóstico del nivel de madurez de los procesos de seguridad de la información en el marco del teletrabajo

Para el desarrollo de este objetivo se parte de la matriz de operacionalización de variables (Ver Apéndice 1) donde se definen como dimensiones Normatividad y los objetivos de gobierno y gestión priorizados para el modelo considerando las metas empresariales, metas de alineamiento. Dichos objetivos priorizados son APO07 gestionar los recursos humanos y apo13 gestionar la seguridad.

Con esta matriz identificada se diseña el cuestionario (Ver Apéndice 2) aplicado a 20 trabajadores que desarrollan sus actividades en el marco del teletrabajo y trabajo en casa. A continuación, se evidencian los resultados de los instrumentos aplicados, en estos resultados se observan los valores promedios obtenidos para cada proceso tomado, del total de procesos 3 de ellos tuvieron un valor por debajo de los 3 puntos, lo indican fuertes deficiencia en APO07.01, APO07.03, APO13.03, por otro lado hubieron 4 procesos que obtuvieron un valor sobre 3 puntos, de entre los cuales se destaca APO07.02, APO07.04, APO07.06, APO13.01 y APO13.02, por otra parte, el proceso APO07.05 logro obtener 4 puntos, estos resultados dejan evidenciar las falencias en variables fundamentales que podrían tener un impacto a mediano y largo plazo, por lo que se hace necesario a generar estrategias encaminadas en contrarrestar los bajos índices encontrados.

De cierta manera hay elementos en los cuales se debe mejorar más aun cuando del teletrabajo se trata.

Tabla 2. *Evaluación de prácticas de gestión aplicables*

PROCESO	ACTIVIDAD	PROMEDIO
APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada.	1. Evaluar los requisitos de personal de forma periódica o ante cambios mayores Asegurar que tanto la empresa como la función de TI tengan los suficientes recursos para apoyar las metas y los objetivos empresariales, procesos y controles empresariales y las iniciativas habilitadas por I&T de forma adecuada y apropiada. 2. Mantener los procesos de contratación y retención de personal empresarial y de TI en línea con todas las políticas y procedimientos de personal de la empresa. 3. Establecer una estructura de recursos flexible, como el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, para apoyar el cambio en las necesidades empresariales. 4. Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad y/o criticidad de la función.	**2,7**
APO07.02 Identificar al personal clave de TI.	1. Como precaución de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que tomarán las personas clave 2. Tomar las acciones pertinentes relativas a cambios laborales, en especial terminación de contratos. 3. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico. 4. Comprobar regularmente los planes de respaldo de personal	**3,5**
APO07.03 Mantener las habilidades y competencias del personal.	1. Identificar las habilidades y competencias disponibles actuales, tanto de recursos internos como externos. 2. Identificar las brechas entre las habilidades requeridas y las disponibles Desarrollar planes de acción, como capacitación (habilidades técnicas y de conducta), contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.	**2,8**

	3. Revisar los materiales y programas de capacitación de forma regular. Garantizar su idoneidad con respecto a los requisitos en constante evolución de la empresa y su impacto sobre el conocimiento, capacidades y habilidades necesarias. 4. Proporcionar acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias 5. Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad. 6. Realizar evaluaciones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Evaluar la planificación de los reemplazos.	
APO07.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados.	1. Considerar las metas empresariales/funcionales como el contexto para establecer metas individuales 2. Establecer metas individuales alineadas con las metas empresariales y de I&T relevantes. Basar las metas en objetivos específicos, medibles, alcanzables, relevantes y en tiempo (SMART) que reflejen las competencias principales, los valores empresariales y las habilidades requeridas para los roles. 3. Proporcionar retroalimentación oportuna acerca del rendimiento comparado con las metas individuales 4. Proporcionar instrucciones específicas para el uso y el almacenamiento de la información personal en el proceso de evaluación, en cumplimiento de la legislación vigente sobre datos personales y laboral vigente. 5. Recopilar resultados de evaluación de rendimiento de 360 grados. 6. Proporcionar planes formales de planificación y de desarrollo profesional conforme a los resultados del proceso de evaluación para fomentar el desarrollo de competencias y las oportunidades para el avance personal y para reducir la dependencia de individuos clave. Proporcionar coaching a los empleados sobre el rendimiento y la conducta cuando sea apropiado. 7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, desarrollo de competencias y logro de las metas de desempeño. Asegurar que el proceso se aplique de forma consistente y en línea con las políticas organizativas. 8. Implementar y comunicar un proceso disciplinario.	**3,8**
APO07.05 Planificar y	1. Crear y mantener un inventario de recursos humanos empresariales y de TI.	**4**

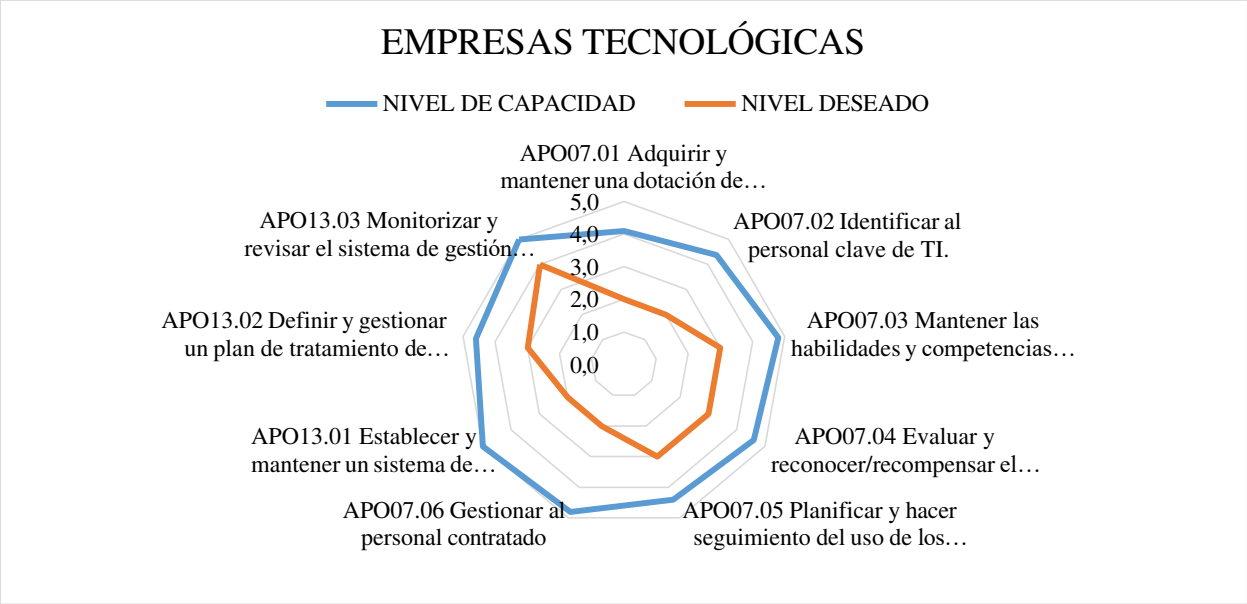
hacer seguimiento del uso de los recursos humanos del negocio y de TI.	2. Entender la demanda actual y futura de recursos humanos para contribuir a lograr los objetivos de I&T y ofrecer servicios y soluciones conforme al portafolio de iniciativas relacionadas con I&T, al portafolio de inversión futura y necesidades operativas diarias. 3. Identificar las carencias y proporcionar recomendaciones sobre los planes de abastecimiento, así como de los procesos de contratación de personal empresarial y de TI. Crear y revisar la planificación de personal, mediante un seguimiento de su uso real. 4. Mantener una información adecuada sobre el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos.	
APO07.06 Gestionar al personal contratado	1. Implementar las políticas y procedimientos del personal contratado 2. Al inicio del contrato, obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de I&T empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación 3. Avisar a los contratistas de que los directivos se reservan el derecho a supervisar e inspeccionar todo el uso de los recursos de TI, incluido el correo electrónico, comunicaciones de voz y todos los programas y archivos de datos. 4. Como parte de sus contratos, proporcionar a los contratistas una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados. 5. Revisar el trabajo de contratistas y basar la aprobación de los pagos en los resultados 6. En contratos formales y no ambiguos, definir todo el trabajo realizado por personal externo 7. Realizar revisiones periódicas para garantizar que el personal contratado haya firmado y aceptado todos los acuerdos necesarios. 8. Realizar revisiones periódicas para garantizar que los roles de los contratistas y los derechos de acceso sean adecuados y conforme a los contratos	**3,2**
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa	**3,4**

información (SGSI).	Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información. Comunicar la estrategia de SGSI. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	
APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.	Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades. Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información. Implementar programas de formación y concienciación sobre seguridad de la información y privacidad. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	**3**
APO13.03 Monitorizar y revisar el sistema de gestión de	Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad. Realizar auditorías de SGSI a intervalos planificados.	**2,8**

seguridad de la información (SGSI).	Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI. Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI. Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	

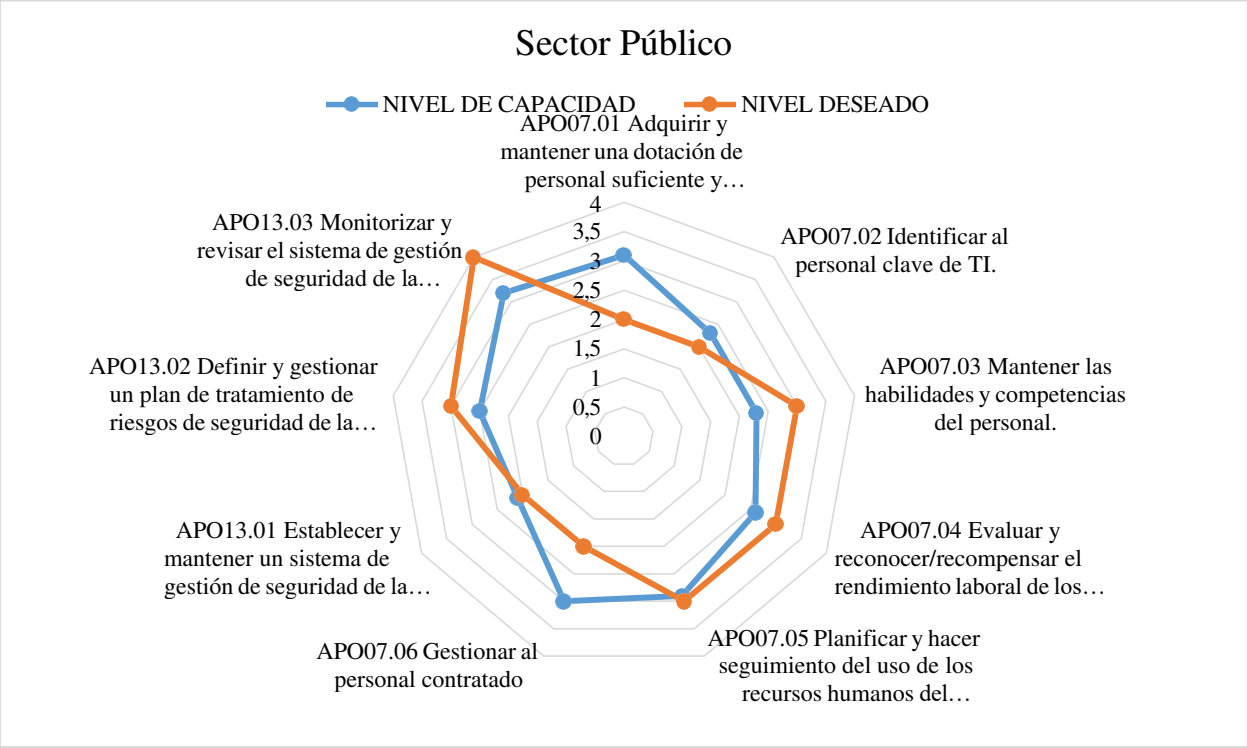
El análisis se realizó en sectores como empresas tecnológicas, sector público, instituciones de educación superior, instituciones técnicas y tecnológicas presentando los siguientes resultados

Figura 3. *Niveles de Capacidad de las empresas tecnológicas*



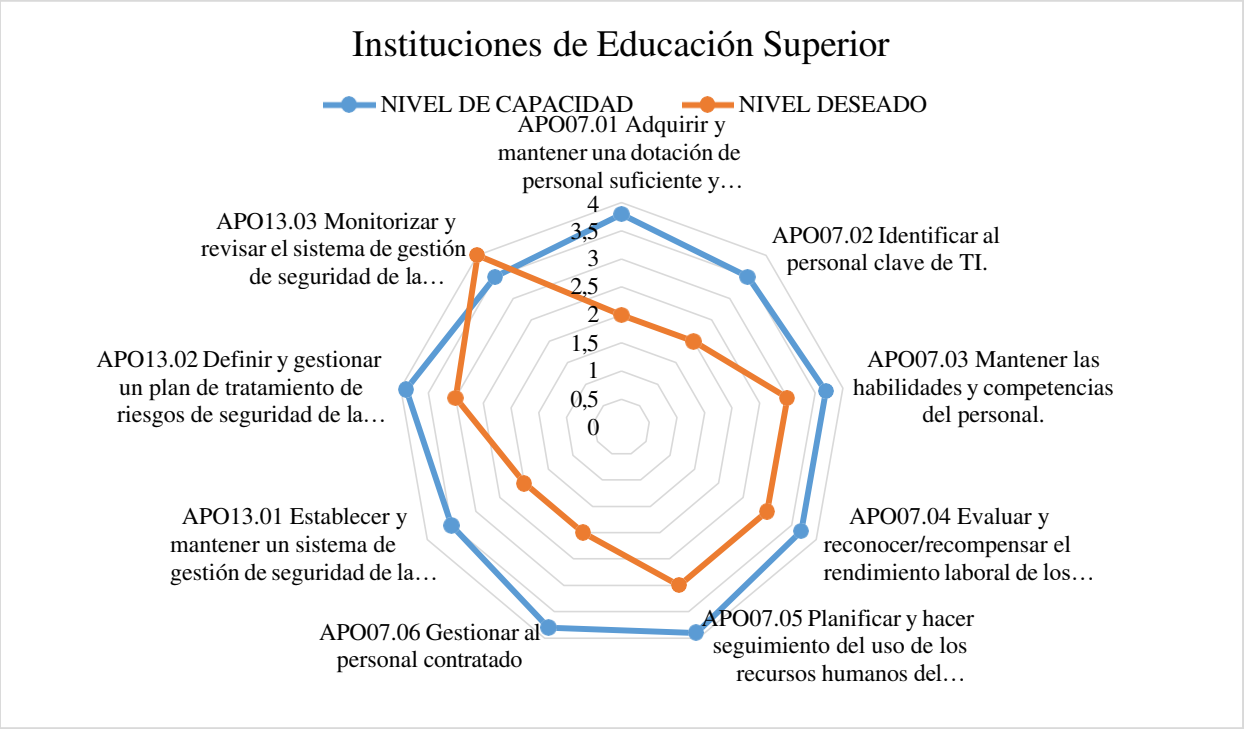
Este fue el sector mejor evaluado su nivel de capacidad está por encima del nivel deseado en los dos objetivos de gestión analizados.

Figura 4. *Niveles de Capacidad del sector público*



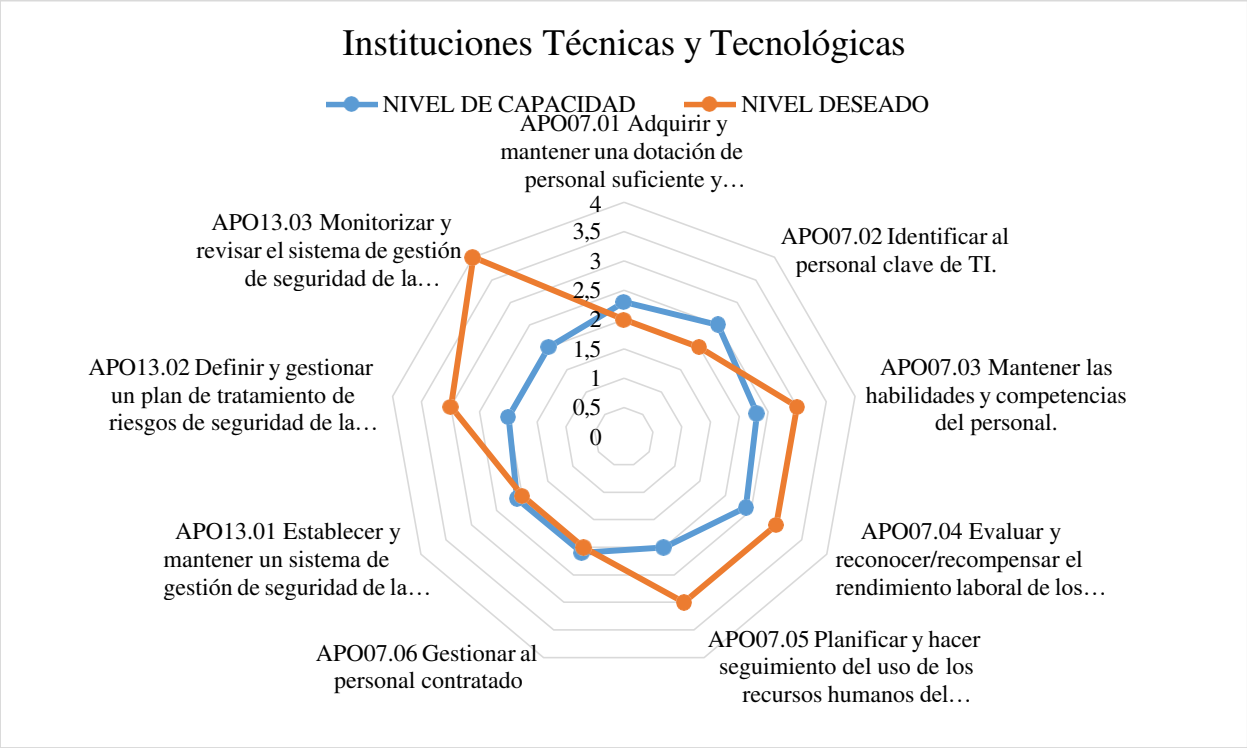
En el sector público se encuentran tres que no cumplen el nivel de capacidad deseado el APO0701 Adquirir y mantener una dotación de personal suficiente y el APO0702 correspondiente a la identificación del persona clave de TI, otra práctica no alcanzada fue PO07.06 Gestionar al personal contratado.

Figura 5. *Niveles de Capacidad de Instituciones de Educación Superior*



En las instituciones de educación superior sólo no se cumple en el apo13.03 correspondiente al monitoreo y revisión del sistemas de gestión de la seguridad de la información los demás practicas dieron resultado mayor que el nivel deseado.

Figura 6. *Niveles de Capacidad de Instituciones Técnicas y Tecnológicas*



La evaluación de los niveles de capacidad en las Instituciones técnicas y tecnológicas mostro que este sector es el que presenta mayor incumpliendo de las prácticas de gestión propuestas por COBIT 2.019 sólo están por encima el AO0701 y el APO0702.

4.2.2 Métodos de análisis cualitativo en el cumplimiento de la norma de teletrabajo y trabajo en casa.

Considerando métodos cualitativos se trabajó con grupos focales (Ver Anexo 3) se presentaron los siguientes resultados:

A nivel general los elementos que no se cumplen: ley 1221

En los casos en los que el empleador utilice solamente tele trabajadores, para fijar el **importe del salario** deberá tomarse en consideración la naturaleza del trabajo y la remuneración que se paga para labores similares en la localidad.

Los Elementos que no se cumplen: ley 2088 de 2021

- **Desconexión laboral.** Es la garantía y el derecho que tiene todo trabajador y servidor público a disfrutar de su tiempo de descanso, permisos, vacaciones, feriados, licencias con el fin de conciliar su vida personal, familiar y laboral. Por su parte el empleador se abstendrá de formular órdenes u otros requerimientos al trabajador por fuera de la jornada laboral.

- **Procedimientos necesarios para la implementación del Trabajo en Casa.** Previo a la implementación del trabajo en casa, toda empresa y entidad pública o privada deberá contar con un procedimiento tendiente a proteger este derecho y garantizar a través de las capacitaciones a que haya lugar el uso adecuado de las tecnologías de la información y la comunicación - TIC o cualquier otro tipo de elemento utilizado que pueda generar alguna limitación al mismo. Para dar inicio a esta habilitación, el empleador deberá notificar por escrito a sus trabajadores acerca de la habilitación de trabajo en casa, y en dicha comunicación, se indicará el periodo de tiempo que el trabajador estará laborando bajo esta habilitación.

- **Para los servidores públicos, el auxilio de conectividad se reconocerá en los términos y condiciones establecidos para el auxilio de transporte.**

- **Programas de bienestar y capacitación.** Para la implementación de la habilitación de trabajo en casa, el empleador deberá promover la formación, capacitación y el desarrollo de competencias digitales, en los servidores públicos y trabajadores del sector privado cuando la actividad a desarrollar así lo requiera.

Se realizaron los análisis correspondientes con las categorías principales y sus subcategorías

Tabla 3. *Categorías principales y subcategorías*

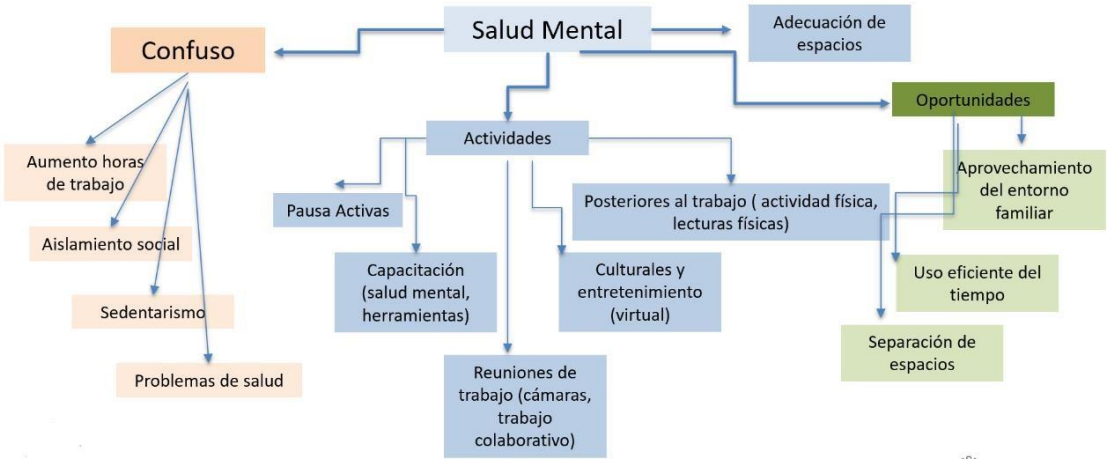
Categorías Principales	Subcategorías
Salud Mental	Derecho a la intimidad
	Privacidad
Recursos	Financieros
	Temporales
	Físicos
	Tecnológicos
Productividad	
Clima laboral	Trabajo en equipo
	Aislamiento
Seguridad de la información	

Para salud mental se obtuvo el siguiente resultado:

En la red generada se veía que al principio de la pandemia fue muy confuso porque se presentó aumento de horas de trabajo produjo aislamiento social que los afecto mucho, el sedentarismo provocó varios problemas de salud. Fue clave la incorporación de actividades como las pausas activas, las capacitaciones sobre salud mental, las reuniones con cámaras y el trabajo colaborativo para no sentirse solos y las recomendaciones después del trabajo desarrollar otro tipo de actividades como físicas o lúdicas.

También fue importante adecuar espacios adecuados para el desarrollo del trabajo y al final lo vieron como una oportunidad para mejorando el espacio los horarios aprovechar el entorno familiar y poder compartir más con sus familias.

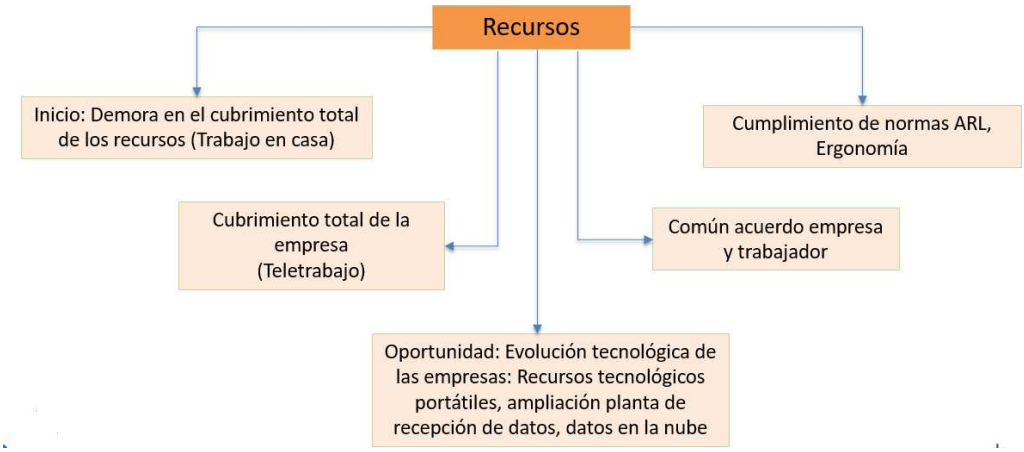
Figura 7. *Red de categoría Salud Mental*



Categoría Recursos:

Esta categoría mostro en sus inicios mucha demora en el cubrimiento total de los recursos para un trabajo en casa adecuado, en el caso de teletrabajo con las personas entrevistadas posteriormente se cubrió totalmente por la empresa en cuanto al ARL y ergonomía y se establecieron acuerdos entre los empleados y sus empleadores.

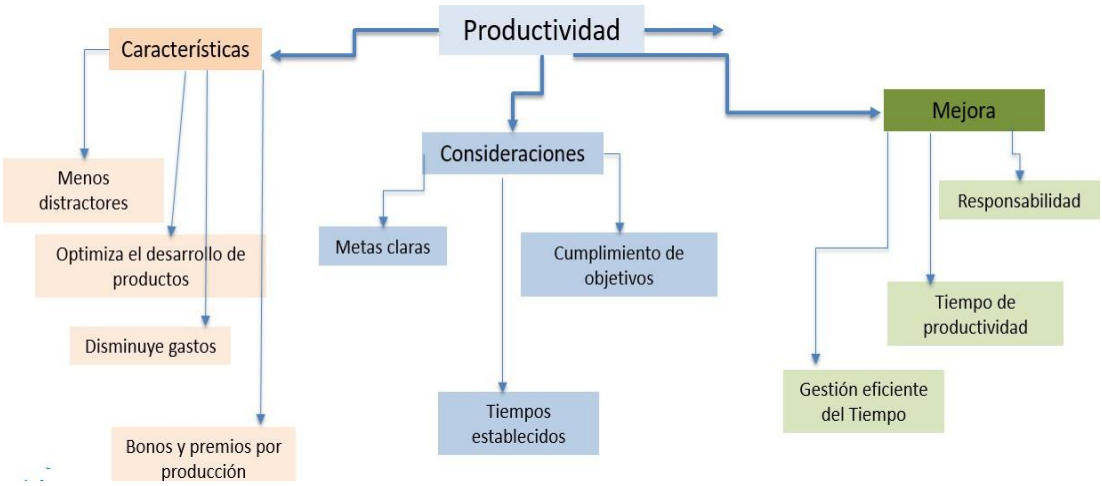
Figura 8*. Red de categoría Recursos*



En la Categoría productividad:

Los participantes encontraron unas características interesantes de menos distractores, disminución de gastos de ellos y de la empresa, se incentivaron los bonos y premios por producción logrando optimizar el desarrollo de productos esto fue más notorio en empresas del sector tecnológico. Esto se logra con la mejora en la responsabilidad, tiempo productivo y la una gestión eficientes del tiempo considerando metas claras, cumplimiento de objetivos y tiempos establecidos.

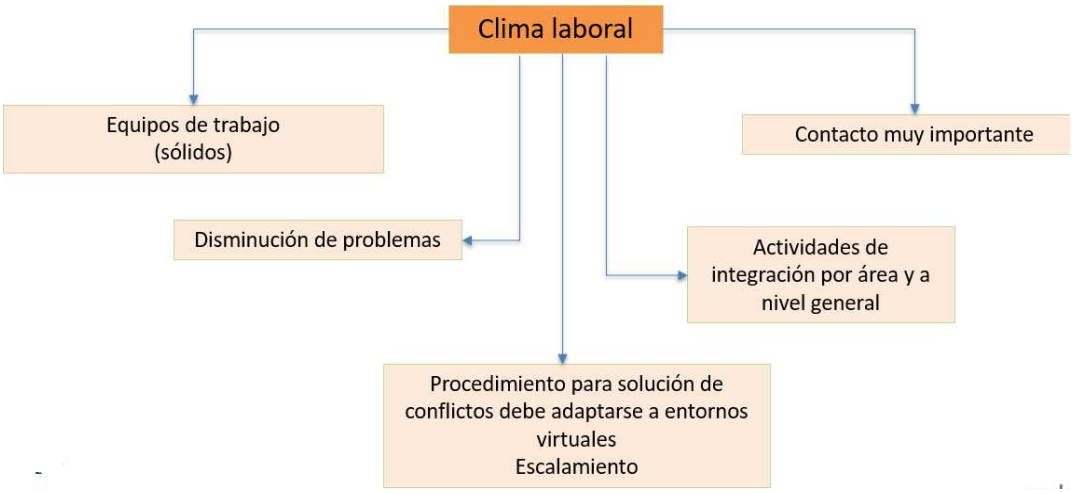
Figura 9. *Red de categoría Productividad*



Categoría Clima laboral

En cuanto al clima laboral al principio se generaron algunos problemas mientas se ajustaban pero posteriormente se logró la consolidación de equipos sólidos, la disminución de problemas una vez se establecieran procedimientos para la solución de conflictos adaptado a entornos virtuales logrando un mejora escalamiento de los problemas. Se hizo mucho énfasis que era importante mantener un contacto, programar actividades de integración virtuales por áreas.

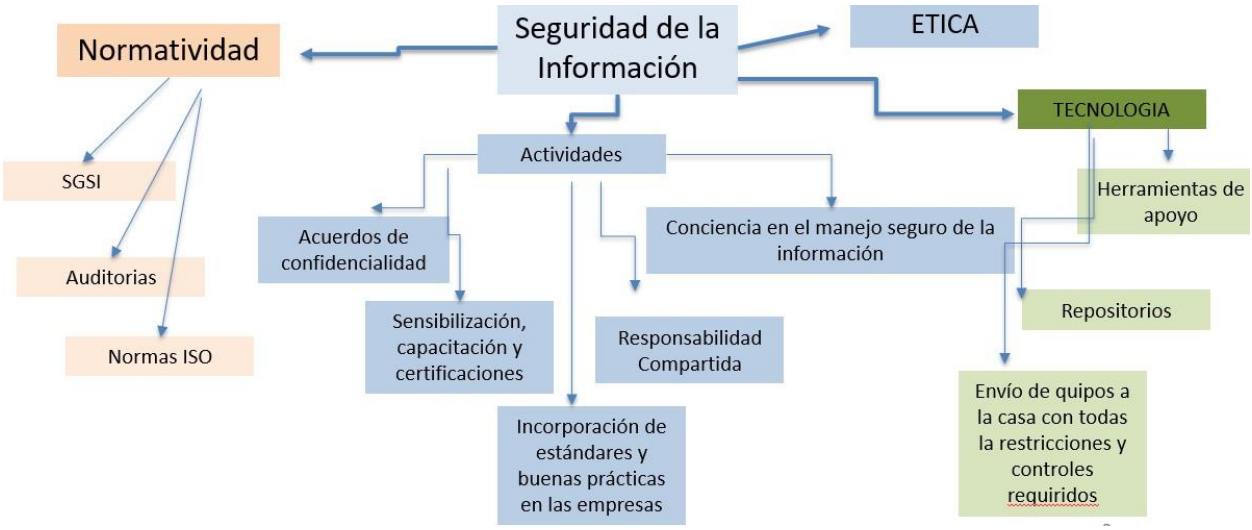
Figura 10. *Red de categoría Clima Laboral*



Categoría seguridad de la información

Para esto las empresas debían adaptar sino las tenían normatividad acorde con los sistemas de gestión de seguridad de la información, con normas ISO y el desarrollo de auditorías que también se desarrollaron de forma virtual, se tenía que hacer mucho énfasis en la ética en los procesos, buscando promover actividades que incluyeran sensibilidad y capacitación y certificaciones en el tema de seguridad de la información y gestión de riesgos, la incorporación de estándares y buenas practicas fue fundamental, teniendo claro las funciones y que responsabilidades serían compartidas, establecer acuerdos de confidencialidad y conciencia en el manejo seguro de la información. Se consolido la tecnología como elemento fundamental para los procesos de negocio consideran los adecuados controles y restricciones de los equipos en casa, herramientas de apoyo y repositorios para gestionar mejor el conocimiento.

Figura 11. *Red de categoría Seguridad de la Información*



4.2.3 Estructuración del modelo de gestión de seguridad en el marco del teletrabajo y trabajo en casa.

Para la estructuración de los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo el modelo inicia reconociendo a la ISO 27002 y NIST, la ISO 27002 y el NIST (Instituto Nacional de Estándares y Tecnología) son dos marcos de referencia ampliamente reconocidos en el ámbito de la seguridad de la información y la gestión de riesgos, y ambos desempeñan un papel esencial en el contexto del teletrabajo. La ISO 27002 proporciona pautas y mejores prácticas específicas para gestionar la seguridad de la información, destacando áreas clave como políticas de seguridad, autenticación, gestión de dispositivos y comunicaciones seguras, todo ello crucial cuando los empleados trabajan de forma remota. Por su parte, el NIST, a través de su Marco de Ciberseguridad, se centra en la identificación de activos, la gestión de accesos, la detección y respuesta a incidentes, así como la educación en seguridad, elementos esenciales para mantener

la ciberseguridad en un entorno de teletrabajo. Ambos marcos ofrecen un enfoque integral y sólido para abordar los desafíos de seguridad en el trabajo a distancia, y la elección entre uno u otro dependerá de las necesidades específicas de cada organización y de la normativa aplicable.

La importancia de la ISO 27002 y el Marco de Ciberseguridad del NIST en el contexto del teletrabajo radica en varios factores cruciales para la seguridad de la información y la gestión de riesgos en un entorno remoto.

En primer lugar, el teletrabajo implica que los empleados accedan a los sistemas y datos de la empresa desde ubicaciones fuera de las instalaciones físicas de la organización. Esto crea desafíos significativos en términos de seguridad, ya que se amplían las superficies de ataque. La ISO 27002 y el NIST proporcionan directrices específicas para la gestión de accesos y autenticación, lo que garantiza que solo personal autorizado tenga acceso a los sistemas, reduciendo así el riesgo de brechas de seguridad.

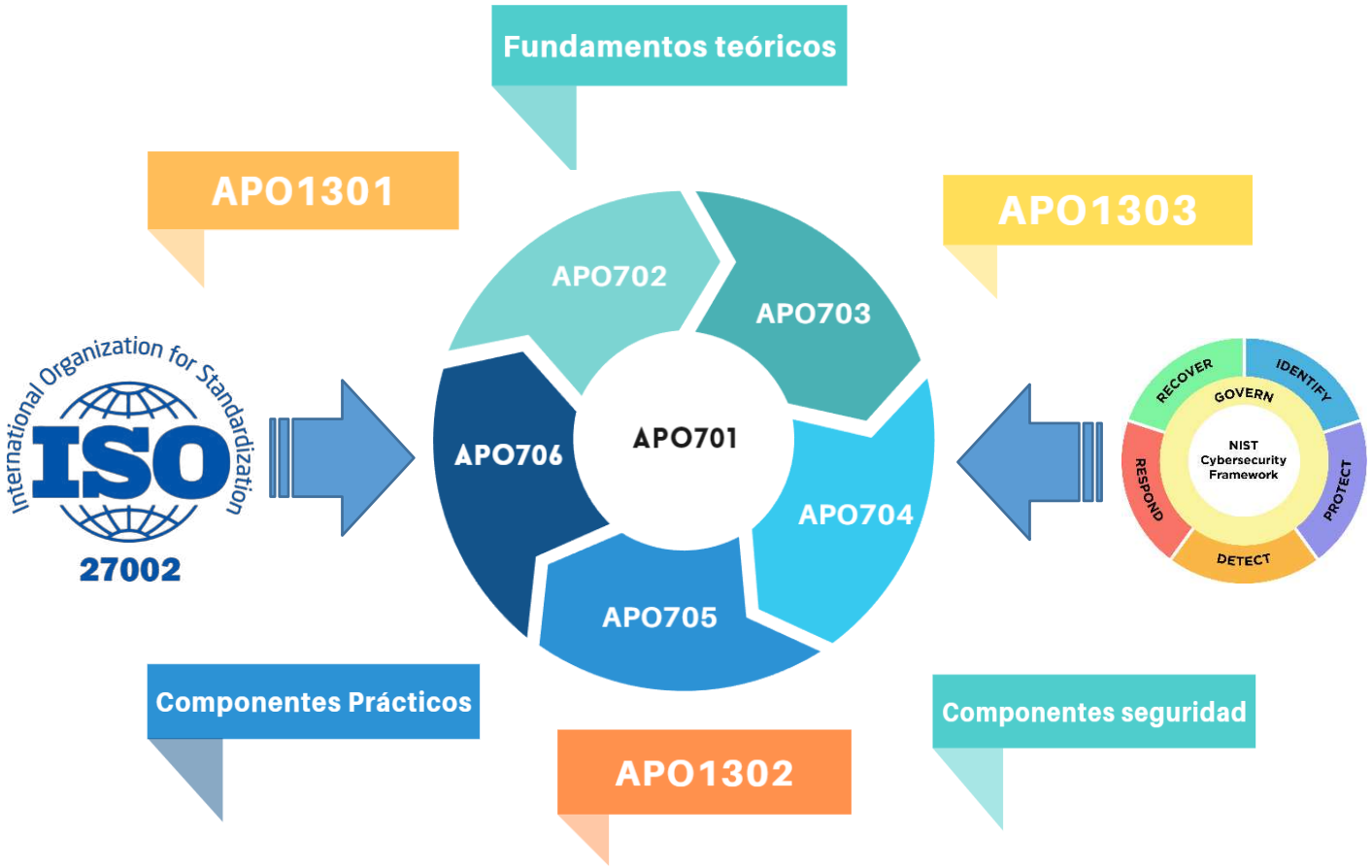
En segundo lugar, la gestión de activos y la identificación de activos críticos de información son fundamentales en el teletrabajo. Las organizaciones deben saber qué datos y sistemas son esenciales para sus operaciones y protegerlos de manera efectiva. Ambos marcos ofrecen enfoques estructurados para esta identificación y protección, ayudando a las organizaciones a priorizar sus recursos de seguridad de manera eficiente.

En tercer lugar, el teletrabajo puede aumentar la probabilidad de incidentes de seguridad, como intentos de intrusión o phishing. La detección y respuesta a incidentes son áreas clave abordadas por la ISO 27002 y el NIST, lo que permite a las organizaciones estar preparadas para identificar y responder a amenazas de manera oportuna, minimizando así el impacto potencial de los ataques.

Por último, la educación y la concienciación en seguridad son especialmente relevantes en el teletrabajo. Los empleados que trabajan de forma remota deben estar informados sobre las prácticas de seguridad adecuadas, como el manejo de contraseñas, la identificación de correos electrónicos de phishing y la protección de datos confidenciales. Ambos marcos promueven la educación en seguridad como un componente esencial de la estrategia de seguridad de una organización.

En resumen, la aplicación de la ISO 27002 y el Marco de Ciberseguridad del NIST en el teletrabajo es esencial para garantizar la protección de datos y sistemas en un entorno donde los riesgos pueden ser más variados y desafiantes. Estos marcos proporcionan una base sólida para abordar los aspectos críticos de la seguridad de la información en un contexto de trabajo remoto, lo que contribuye a la continuidad de las operaciones y a la protección de los activos de la organización.

Figura 12. *Modelo de seguridad de información para las empresas en el marco del teletrabajo*



La relación entre los procesos COBIT 5 (APO 701 - APO 707) y la seguridad en el teletrabajo, utilizando la ISO 27002 y el Marco de Ciberseguridad del NIST, se basa en la necesidad de establecer un marco sólido de gobierno y gestión de TI para garantizar la seguridad de la información en un entorno de trabajo remoto.

Dentro de esteescrivbe modelo se evidencia los fundamentos teóricos, los componentes prácticos del teletrabajo y los componentes de seguridad, entre los cuales en conjunto con las dimensiones de COBIT 5 (APO 701 - APO 707) y la seguridad en el teletrabajo, utilizando la ISO 27002 y el Marco de Ciberseguridad del NIST debe existir una sinergia que permita fortalecer la seguridad información para el sector empresarial en el marco del teletrabajo.

La sinergia entre los fundamentos teóricos, los componentes prácticos del teletrabajo y los componentes de seguridad es fundamental para fortalecer la seguridad de la información en el sector empresarial en el contexto del teletrabajo. Esta combinación de conocimiento teórico, implementación práctica y estándares de seguridad sólidos garantiza que las organizaciones puedan aprovechar los beneficios del teletrabajo de manera eficiente y segura. Los fundamentos teóricos proporcionan la base conceptual necesaria, los componentes prácticos permiten la aplicación concreta de esta modalidad laboral, y los estándares de seguridad, como COBIT 5, ISO 27002 y el Marco de Ciberseguridad del NIST, brindan pautas específicas para proteger la integridad, confidencialidad y disponibilidad de los datos en un entorno de trabajo remoto. Esta sinergia es esencial para garantizar que el teletrabajo sea productivo y seguro en un entorno empresarial en constante evolución.

Ahora bien, es importa establecer la forma en como se complementan los estándares del modelo, como lo es APO con la ISO 27002 y NIST:

APO 701 - Gestionar el Marco de Gobierno de TI y la ISO 27002:

La ISO 27002 proporciona directrices específicas para el desarrollo de políticas de seguridad de la información. En el teletrabajo, es esencial tener políticas que aborden el uso de dispositivos personales, el acceso remoto a sistemas y la protección de datos confidenciales.

APO 702 - Gestionar la Estrategia de TI y la ISO 27002:

La ISO 27002 ayuda en la formulación de estrategias de seguridad de TI que son cruciales en el teletrabajo, donde se deben identificar oportunidades y riesgos relacionados con la tecnología y definir una estrategia de seguridad acorde.

APO 703 - Gestionar la Arquitectura Empresarial de TI y la ISO 27002:

La ISO 27002 se relaciona con la gestión de la arquitectura empresarial de TI al proporcionar directrices sobre la seguridad de la infraestructura y las aplicaciones de TI, asegurando que estén alineadas con las políticas de seguridad.

APO 704 - Gestionar la Innovación y la ISO 27002:

La ISO 27002 promueve la innovación en prácticas y tecnologías de seguridad, lo que es relevante para mantenerse al día con las amenazas emergentes, especialmente en el teletrabajo, donde las amenazas pueden evolucionar rápidamente.

APO 705 - Gestionar el Portafolio de Proyectos de TI y la ISO 27002:

La ISO 27002 puede ser utilizada para evaluar la seguridad de los proyectos de TI relacionados con el teletrabajo, asegurando que estén alineados con los estándares y políticas de seguridad.

APO 706 - Gestionar la Entrega de Servicios y la ISO 27002:

La ISO 27002 es relevante para garantizar que los servicios de TI entregados en el teletrabajo sean seguros, cumpliendo con los SLA de seguridad y protegiendo la integridad y confidencialidad de los datos.

APO 707 - Gestionar la Relación con los Proveedores y la ISO 27002:

La ISO 27002 puede aplicarse en la selección y contratación de proveedores de servicios de TI para el teletrabajo, asegurando que cumplan con los requisitos de seguridad.

Además, el Marco de Ciberseguridad del NIST complementa la ISO 27002 al proporcionar una serie de controles y prácticas recomendadas para mejorar la ciberseguridad, lo que es fundamental en el teletrabajo. Los controles del NIST ayudan a proteger los sistemas y datos en un entorno remoto, desde la autenticación y el cifrado hasta la detección y respuesta a incidentes.

En resumen, la combinación de los procesos COBIT 5 y las directrices de seguridad de la ISO 27002 y el NIST brinda un enfoque sólido y completo para garantizar la seguridad de la información en el teletrabajo. Los procesos de COBIT 5 proporcionan el marco de gobierno y gestión de TI, mientras que las normas y prácticas recomendadas de seguridad de la ISO 27002 y el NIST ayudan a implementar medidas específicas de seguridad en el entorno remoto. Esto es esencial para proteger los activos de información de la organización y minimizar los riesgos en el teletrabajo.

Por otro lado, NIST (National Institute of Standards and Technology) y ISO 27002 son dos marcos de referencia ampliamente utilizados en el campo de la seguridad de la información. Una de las contribuciones más destacadas de NIST en el campo de la ciberseguridad es la publicación del Marco de Ciberseguridad de NIST (NIST Cybersecurity Framework). Este

marco proporciona una estructura sólida para que las organizaciones evalúen, desarrollen e implementen prácticas efectivas de ciberseguridad. Su enfoque basado en el riesgo permite a las organizaciones personalizar sus estrategias de seguridad de acuerdo con sus necesidades y recursos específicos.

Además, NIST es conocido por su serie de publicaciones SP 800, que abordan una amplia variedad de temas relacionados con la seguridad de la información y la tecnología. SP 800-53, por ejemplo, define un conjunto de controles de seguridad que se utilizan ampliamente en todo el mundo para garantizar la integridad, confidencialidad y disponibilidad de los datos.

La colaboración de NIST con la industria, el gobierno y la comunidad académica es un pilar fundamental de su enfoque. Esta colaboración asegura que sus estándares y directrices sean prácticos y relevantes para una amplia gama de organizaciones y sectores. Además, NIST también trabaja en estrecha colaboración con organismos internacionales y está comprometido con la promoción de la ciberseguridad a nivel global.

NIST es una autoridad respetada en el mundo de la ciberseguridad y la tecnología de la información, y sus estándares y directrices desempeñan un papel crucial en la protección de datos y sistemas críticos en una era digital cada vez más compleja y desafiante. Su enfoque en la colaboración, la personalización y la adaptación a los riesgos actuales hace que sus recursos sean invaluables para organizaciones de todo el mundo que buscan fortalecer su postura de seguridad cibernética (Fernández, 2019).

NIST y la ISO 27002 Aunque no están directamente relacionados, se complementan de diversas maneras:

Enfoque en la Seguridad de la Información: Ambos marcos están diseñados para ayudar a las organizaciones a establecer y mantener prácticas efectivas de seguridad de la información. ISO 27002 se centra específicamente en la gestión de la seguridad de la información, mientras que NIST proporciona un conjunto más amplio de estándares y guías que abordan la seguridad de la información, así como otros aspectos tecnológicos y científicos (Zarate, 2021).

Estructura y Terminología Comunes: Ambos marcos utilizan una estructura y terminología comunes en sus directrices. Esto facilita la comprensión y la implementación conjunta de los estándares y mejores prácticas de seguridad de la información.

Complementariedad de Controles: ISO 27002 y NIST SP 800-53, una de las publicaciones de NIST, a menudo se utilizan juntos para cubrir un conjunto completo de controles de seguridad de la información. Mientras que ISO 27002 se centra en controles específicos de seguridad de la información, NIST SP 800-53 proporciona una amplia gama de controles que abarcan seguridad de la información, seguridad de sistemas y otros aspectos relacionados con la tecnología.

Marco de Referencia de Gestión de Riesgos: Ambos marcos proporcionan directrices para la gestión de riesgos de seguridad de la información. ISO 27002 se enfoca en los controles necesarios para mitigar riesgos, mientras que NIST incluye un proceso completo de gestión de riesgos en sus documentos, como NIST SP 800-37.

Contexto Global y Regional: ISO 27002 es un estándar internacional ampliamente adoptado y reconocido en todo el mundo. En contraste, NIST, aunque utilizado en todo el mundo, es un conjunto de estándares desarrollado por el gobierno de los Estados Unidos. Esto significa que, en algunos casos, las organizaciones pueden optar por cumplir con ISO 27002 para

cumplir con requisitos globales, mientras que las organizaciones que operan en los Estados Unidos pueden utilizar NIST en combinación con ISO 27002.

NIST ISO 27002 son dos marcos de referencia que comparten similitudes en términos de seguridad de la información, estructura y terminología. Se complementan bien para ayudar a las organizaciones a desarrollar y mantener prácticas efectivas de seguridad de la información, y la elección entre ambos depende de los objetivos específicos y los requisitos de cumplimiento de cada organización.

En el contexto actual, donde el teletrabajo ha adquirido una relevancia sin precedentes, las pautas y recomendaciones proporcionadas por el Instituto Nacional de Estándares y Tecnología (NIST) se han convertido en un recurso invaluable para garantizar la seguridad de la información y los sistemas de las organizaciones. NIST destaca la importancia de establecer prácticas de acceso seguro para los empleados que trabajan de forma remota. Esto incluye la implementación de la autenticación multifactor (MFA) y el uso de redes privadas virtuales (VPN) para salvaguardar las comunicaciones y los datos en tránsito. Además, se enfoca en la gestión de dispositivos, alentando a las organizaciones a mantener los dispositivos actualizados con parches de seguridad y a promover la adopción de contraseñas sólidas (Valencia, 2023).

La capacitación y concienciación de los empleados son elementos esenciales en la estrategia de seguridad en el teletrabajo. NIST reconoce que los trabajadores remotos deben estar equipados con los conocimientos necesarios para identificar y prevenir amenazas cibernéticas, como el phishing y el malware. Además, NIST aborda la seguridad de la red, proporcionando directrices sobre cómo segmentar adecuadamente las redes y el uso de firewalls para proteger los activos de la organización.

La protección de los datos, un aspecto crítico en cualquier entorno de trabajo, cobra especial relevancia en el teletrabajo. NIST aconseja cifrar y proteger minuciosamente los datos confidenciales y personalmente identificables tanto en dispositivos como durante su transmisión. Asimismo, subraya la necesidad de realizar evaluaciones continuas para verificar la eficacia de las prácticas de seguridad en el teletrabajo, ya que el panorama de amenazas cibernéticas sigue evolucionando. En resumen, las directrices de NIST se erigen como un faro de seguridad en el entorno laboral remoto, ofreciendo un marco sólido para proteger la información y los sistemas en una era de trabajo cada vez más distribuida (Artabia y Soto, 2023).

4.3 Validación el modelo de gobierno de ti orientado a la seguridad de la información mediante el juicio de expertos.

La validación del modelo es esencial para establecer la confianza en su futura implementación, lo que asegura la certeza de que los componentes del modelo tienen el potencial de optimizar y fortalecer los procedimientos asociados al modelo planteado. Las características de los expertos a considerar se muestran en la tabla a continuación.

Tabla 4. *Caracterización de los expertos*

Marque con una x el grado de escolaridad con relación a los años de experiencia y cargos que allá tenido	**Tipo de cargo y años de experiencia**		
¿Conoce el contexto sobre el cual se desarrolla el proyecto?	Si		**No**
Ultimo Grado de escolaridad	**No (años de experiencia)**	**Investigador**	**Profesor**
Profesional			
Licenciado			
Especialista			
Magister			
Doctor			

Postdoctor

Se contó con 5 evaluadores 3 magister, 1 doctor y 1 postdoctor con experiencia promedio de 15 años en investigación y 18 años en el área académica docente.

A continuación, se procede a validar el instrumento enviado a los expertos seleccionados para el diligenciamiento de la información.

El proceso para validar el modelo parte de los criterios que se exponen a continuación:

- Adaptación del modelo
- Uso de estándares reconocidos
- Pertinencia del modelo
- Correspondencia

Las respuestas se detallan a continuación

- MR: muy relevante.
- BR: bastante relevante.
- R: relevante.
- PR: poco relevante
- NR: no relevante.

Tabla 5. *Consolidado de respuestas de expertos*

PREGUNTAS	MR	BR	R	PR	NR
El modelo se sustenta en estándares internacionales					
Los elementos incorporados en el modelo son pertinentes de acuerdo al objeto de estudio					
Existe correspondencia entre el modelo diseñado y la definición					
El modelo podría ser adaptado en otras dependencias o I.E.S					
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características					

Tabla 6. *Respuesta de los expertos*

PREGUNTAS	MR	BR	R	PR	NR	TOTAL
El modelo se sustenta en estándares internacionales	5	0	0	0	0	5
Los elementos incorporados en el modelo son pertinentes de acuerdo al objeto de estudio	4	1	0	0	0	5
Existe correspondencia entre el modelo diseñado y la definición	4	1	0	0	0	5
El modelo podría ser adaptado	5	0	0	0	0	5
Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características	4	1	0	0	0	5

El instrumento se valida a través del Alpha de Cronbach que se estructura de acuerdo a la siguiente formula:

Figura 13. *Formula del Alpha*

$$\alpha = \frac{k}{k-1}\left[1-\frac{\sum s^2}{S_T^2}\right]$$

Donde,
k = El número de ítems
Σs^2 = Sumatoria de varianzas de los ítems.
sT^2= Varianza de la suma de los ítems.
α = Coeficiente de alfa de Cronbach

Fuente: Formula de Aplha.

El Alfa de Cronbach es una métrica de fiabilidad ampliamente empleada en la investigación social y científica para evaluar la coherencia interna de un conjunto de ítems o preguntas en una encuesta o escala de medición. Este método, concebido por Lee Cronbach en la década de 1950, se ha convertido en una herramienta esencial para evaluar la confiabilidad de instrumentos de medición.

El Alfa de Cronbach se fundamenta en la correlación entre los ítems dentro de una encuesta. Su cálculo mide la consistencia interna al evaluar en qué medida los ítems evalúan la misma característica o constructo. Los valores del Alfa de Cronbach oscilan entre 0 y 1, donde una puntuación más cercana a 1 refleja una mayor consistencia interna entre los ítems. El modelo dio una coeficiente de 0,88

La tabla 7 incluye la valoración de la fiabilidad de ítems según el coeficiente alfa de Cronbach.

Figura 14. *Valoración de la fiabilidad*

Intervalo al que pertenece el coeficiente alfa de Cronbach	Valoración de la fiabilidad de los ítems analizados
[0 ; 0,5[	Inaceptable
[0,5 ; 0,6[	Pobre
[0,6 ; 0,7[	Débil
[0,7 ; 0,8[	Aceptable
[0,8 ; 0,9[	Bueno
[0,9 ; 1]	Excelente

La evaluación de la confiabilidad del instrumento y las respuestas proporcionadas por los expertos han convergido en una conclusión positiva que respalda la replicabilidad e implementabilidad del modelo propuesto. Este veredicto se basa en sólidos argumentos que indican que el instrumento empleado en la investigación es consistente y preciso. La confiabilidad es un factor fundamental para garantizar que los resultados obtenidos sean confiables y estables, lo que, a su vez, fortalece la validez del modelo en cuestión.

La opinión favorable de los expertos añade un importante nivel de validación al modelo. La experiencia y conocimientos profundos que estos expertos poseen en el campo de estudio hacen que su aprobación sea un respaldo valioso. Esta aprobación sugiere que el modelo se alinea con las mejores prácticas y se adapta a las necesidades y estándares del campo, lo que es esencial para su credibilidad.

Además, la calificación positiva también apunta a la replicabilidad del estudio, lo que significa que otros investigadores en el mismo campo podrían llevar a cabo investigaciones similares y esperar obtener resultados coherentes. Este factor es crucial para el avance del conocimiento y la generalización de los hallazgos a través de diferentes contextos y poblaciones.

Finalmente, la implementabilidad del modelo se ve respaldada por la evaluación positiva, lo que significa que el modelo es práctico y viable de aplicar en situaciones reales. Los procedimientos y enfoques descritos en el modelo son adecuados y efectivos, lo que garantiza que el modelo no solo es teóricamente sólido, sino que también puede traducirse de manera efectiva en la práctica.

En conjunto, esta evaluación positiva respalda firmemente la idea de que el modelo propuesto es una herramienta confiable, válida y efectiva que puede ser replicada e implementada en el ámbito de la investigación o en aplicaciones prácticas.

Conclusiones

Relacionado con Caracterizar los fundamentos teóricos y prácticos del teletrabajo y los componentes de seguridad de la información requeridos, las consideraciones previas destacan la importancia de un enfoque integral en la implementación del teletrabajo en el ámbito empresarial. Esto involucra la conjunción de fundamentos teóricos sólidos que abordan los aspectos conceptuales y éticos del teletrabajo, componentes prácticos bien estructurados que aborden la infraestructura tecnológica, la gestión de recursos humanos y la evaluación de desempeño, y una seguridad de la información eficaz respaldada por normas y estándares reconocidos como COBIT 2019, ISO 27002 y el Marco de Ciberseguridad del NIST. La sinergia entre estos elementos es clave para garantizar una transición exitosa hacia el teletrabajo, maximizando la productividad y la seguridad en el entorno laboral remoto. Además, se resalta la necesidad de adaptabilidad y ajustes continuos, dada la evolución constante de las amenazas cibernéticas y la tecnología. Este enfoque integral y en constante evolución es esencial para el sector empresarial en su adopción del teletrabajo.

Para la estructuración de los componentes del modelo de gobierno TI orientado a la seguridad de la información para el sector empresarial en el marco del teletrabajo se consideraron fundamentos teóricos, leyes como la ley 1221 de 2.008 y la ley 2028 de 2.021 componentes prácticos y componentes de seguridad, se incluyeron estándares como la ISO 27002 para la seguridad de la información, NIST framework de ciberseguridad y los objetivos de gobierno y gestión de COBIT APO13 Gestionar la Seguridad y el APO07 Gestionar los recursos humanos.

La importancia de un Modelo de Gobierno de Seguridad de la Información (SGI) para el sector empresarial en el contexto del teletrabajo es innegable. Este modelo desempeña un papel fundamental en la protección de la información sensible, asegurando que los datos empresariales se mantengan seguros y confidenciales, incluso cuando los empleados trabajan fuera de las instalaciones físicas de la empresa. Además, es esencial para cumplir con las regulaciones y estándares relacionados con la privacidad y la protección de datos que afectan a muchas industrias. También contribuye a la gestión efectiva de los riesgos específicos asociados al teletrabajo, identificándolos y permitiendo la implementación de medidas preventivas y correctivas. Además de optimizar recursos y definir roles claros, promueve una cultura de seguridad entre los empleados, concienciándolos sobre la importancia de su papel en la protección de la información. La preparación para incidentes, la resiliencia empresarial y la mejora de la reputación son beneficios adicionales de un SGI sólido, lo que, en última instancia, mejora la competitividad de la empresa en el mercado.

Para la validación del modelo se hizo un juicio de expertos contando con 5 evaluadores tres con maestría, un doctor y un postdoctor con alta experiencia en promedio de 15 años de experiencia investigativa y 18 años de experiencia como docentes en el área de formación académica universitaria. Se utilizó el alfa de Cronbach con un resultado de 0,88 lo que lo ubica en el rango bueno.

Recomendaciones

Teniendo un modelo que es aplicable a las empresas, el paso siguiente es implementar el modelo por tanto se propone que como trabajos futuros se proyecte la evaluación del mismo aplicable en los sectores analizados en la investigación.

Referencias

Andrés-Rosales, R., Almonte, L. D. J., & Suárez, Y. C. (2023). Análisis espacial de la dinámica del salario, flexibilidad y productividad laboral en las entidades federativas mexicanas, 2000.1-2021.1. Nóesis. Revista de Ciencias Sociales, 32(64), 4-26.

Arévalo, P. A. O. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica-ESPOL*, *28*(3).

Arriola, A., & Chávez, C. (2023). Evaluación ergonómica en el teletrabajo: una revisión sistemática de herramientas utilizadas. CienciAmérica, 12(1).

Artavia León, J. A., & Soto Sotelo, M. G. (2023). Evaluación del sistema de gestión de resiliencia y de ciberseguridad en un proveedor de internet, utilizando el" Marco para la mejora de la seguridad del instituto nacional de estándares y tecnologías NIST 1.1" (Doctoral dissertation, Universidad Cenfotec).

Artavia León, J. A., & Soto Sotelo, M. G. (2023). Evaluación del sistema de gestión de resiliencia y de ciberseguridad en un proveedor de internet, utilizando el" Marco para la mejora de la seguridad del instituto nacional de estándares y tecnologías NIST 1.1" (Doctoral dissertation, Universidad Cenfotec).

Babativa Novoa, C. A. (2017). *Investigación cuantitativa*.[Tesis de grado, Fundación Universitaria del Área Andina].Colombia.

Bell, Daniel. The coming of post-industrial society; a venture in social forecasting. - New York, Basic Books [1973]. - xiii, 507 p. illus. 25 cm. [traducción: Advenimiento de La Sociedad Post-Industrial. - Alianza (January, 1992). - ISBN: 8420621498.] [traducción: Vers la société post industrielle. - Robert Laffont, 1976]

Beltrán, A. R. P., Bilous, A., Ramos, C. R. F., & Escobar, C. F. B. (2020). El impacto del

teletrabajo y la administración de empresas. RECIMUNDO: Revista Científica de la Investigación y el Conocimiento, 4(1), 326-335.

Botero, D. A. (2023). Flexibilidad laboral:¿ un legado que nos deja la pandemia?. Revista CEA, 9(19).

Burch, S. (2005). Sociedad de la información/Sociedad del conocimiento. *Palabras en juego*, *56*.

Bustos Guáqueta, C. A. (2015). *Seguridad informática para el teletrabajo en empresas privadas en Colombia* (Bachelor's thesis, Universidad Piloto de Colombia).

Carvajal, D. L., Cardona, A., & Valencia, F. J. (2019). Una propuesta de gestión de la seguridad de la información aplicada a una entidad pública colombiana. *Entre ciencia e ingeniería*, *13*(25), 68-76.

Castells, Manuel. 2002 “La dimensión cultural de Internet”, Universitat Oberta de Catalunya, julio.

Díaz, C. E. O., Taday, K. V. L., Maldonado, P. A. C., & Ramos, E. L. H. (2023). Aplicación de las tecnologías de la información y la comunicación en el teletrabajo. Estudios del Desarrollo Social: Cuba y América Latina, 11(Especial 2), 184-192.

Escobar, B. R. P., Salazar, C. A. H., Pantaleón, A. J. S., & Román, C. E. A. (2023). Teletrabajo en organizaciones: competencias y valoración de actividades en las empresas del norte de Amazonas-Perú. Revista de ciencias sociales, 29(7), 88-100.

Fernández Fernández, M. F. (2019). Diseño de un marco de trabajo para la gestión de riesgos de ingeniería social basado en los estándares ISO 27002 y NIST 800-50.

Freixo, J., & Rocha, Á. (2014). Arquitetura de informação de suporte à gestão da qualidade em unidades hospitalares. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (14), 1-15. http://dx.doi.org/10.17013/risti.14.1-15.

Jiménez Cervera, B. M., & Serrano Mejía, A. P. (2023). La flexibilidad laboral y su relación con la productividad de los profesionales dedidcados a la docencia superior universitaria de la

ciudad de Piura, año 2021.[Tesis de grado, UPAO]. Perú

Lee, R. M., & Yen, C. D. (2018). Financial Technologies and Applications. IEEE Computer Society.

Medina Rojas, E. F., & Ocampo Correa, S. L. (2021). Implementación de gobierno de seguridad de la información para la empresa SKG Tecnología con base en la norma NTC-ISO/IEC 27014: 2013.

Medina-Giacomozzi, A. I., del Pilar Gallegos-Muñoz, C., Ramírez-Muñoz, M. P., & Mora-Sepúlveda, C. S. (2022). Teletrabajo: su impacto en los trabajadores de la ciudad de Chillán, Chile. *Encuentros*, *20*(01-Enero-Junio-), 164-175.

Molina Bravo, S. P., & Quintero Sierra, J. D. Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Bonos y Descuentos SAS, a partir de la norma ISO 27001: 2013.

Monfort Casañ, R. (2016). *COBIT 5 y el cuadro de mando integral como herramientas de gobierno de TI* (Doctoral dissertation, Universitat Politècnica de València).

Mora Aristega, J. E., León Acurio, J. V., Huilcapi Masacon, M. R., & Escobar Mayorga, D. C. (2017). El modelo COBIT 5 para auditoría y el control de los sistemas de información.

Morales, F. (2012). Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. *Recuperado el*, *11*, 2018.

Nieto, L. A. F. (2020). El teletrabajo: de actor secundario a protagonista en el escenario del covid-

Nieves, A. C. (2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001: 2013*. [Tesis de grado, institución universitaria politécnico facultad de ingeniería y ciencias básicas]. Colombia

Párraga, M. M. C., & Mora, C. P. I. (2022). Teletrabajo e incidencia en el clima organizacional del Instituto Ecuatoriano de Seguridad Social, administración Portoviejo. *RECUS. Revista*

Electrónica Cooperación Universidad Sociedad. ISSN 2528-8075, *7*(1), 58-67.

Peiró, J. M.ySoler, A. (2020). El impulso al teletrabajo durante el COVID-19 y los retos que plantea. IvieLAB, 1, 1-10.

Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. Á. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *8*(16), 847-870.

Pinos, P., Yépez, G., Carguachi, J., & Saquinga, D. (2022). Expectativas y necesidades de SSO de la comunidad académica del IST Sucre, basado en la ISO 45001. *MEMORIAS SUCRE REVIEW*, *2*(1).

Pozos, F. and Acosta, M. (2016) 'Importancia y análisis del desarrollo empresarial', Pensamiento & Gestión, 40, pp. 184–202. doi: 10.14482/pege.40.8810.

Prieto, M. M. P., Vázquez, M. J. A., & Gutiérrez, D. A. R. (2022). Análisis del teletrabajo y sus componentes: estudio en industria de exportación de ciudad Chihuahua, México.

Prieto, M. M. P., Vázquez, M. J. A., & Gutiérrez, D. A. R. (2022). Análisis del teletrabajo y sus componentes: estudio en industria de exportación de ciudad Chihuahua, México.

Prince, D. (2018). Cibersecurity: the security and protection challenges of our digital world . IEEE Computer Societ

Reinoso, G. I. V., & Gómez, O. S. (2021). Propuesta de políticas de Ciberseguridad para el Teletrabajo. Caso de estudio Rectorado ESPOCH. Dominio de las Ciencias, 7(6), 63-82.

Reinoso, G. I. V., & Gómez, O. S. (2021). Propuesta de políticas de Ciberseguridad para el Teletrabajo. Caso de estudio Rectorado ESPOCH. Dominio de las Ciencias, 7(6), 63-82

Rodríguez Mejía, M. (2007). El teletrabajo en el mundo y Colombia. *Gaceta laboral*, *13*(1), 29-

42.

Rodríguez Mejía, M. (2007). El teletrabajo en el mundo y Colombia. *Gaceta laboral*, *13*(1), 29-42.

Santillan, W. (2020). El teletrabajo en el COVID-19. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica*, *9*(2), 65-76.

Silva Guevara, P. S. (2022). *Mecanismos de ciberseguridad en dispositivos de teletrabajo para una institución financiera* (Master's thesis, Pontificia Universidad Católica del Ecuador).

Suárez, D., & Fontalvo, A. Á. (2015). Una forma de interpretar la seguridad informática. *Journal of Engineering and Technology*, *4*(2).

Tubella, I. (2012). *Comprender los media en la sociedad de la información*. Barcelona: Universitat Oberta de Catalunya.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (22), 73.

Viancha & Sarmiento. (2021). Estrategia metodológica para minimizar riesgos de fuga de información empresarial en teletrabajo [Tesis de grado, Universidad Santo Tomas].

Villalón, J. C. (2021). Aspectos prácticos de la nueva regulación del teletrabajo. Estudios Latinoamericanos de Relaciones Laborales y Protección Social, (11), 33-48.

Zarate, I. J. (2021). Herramienta de armonización entre las normas 27001 y NIST-53 como pilares para la medición del nivel de madurez del SGSI. Diciembre de 2021.

Apéndices

Apéndice 1. Matriz de operacionalización de variables

Propósito	Conceptualización	Dimensiones	subdimensiones	Indicadores
Diseñar un instrumento para diagnosticar el cumplimiento de la normatividad asociada al teletrabajo en el marco de la seguridad de la información	Teletrabajo Seguridad de la información Gobierno de TI	NORMATIVIDAD	LEY 1221 DE 2008 LEY 2088 DE 2021	Capacidad Tecnológica Requisitos legales de contratación
		APO07 GESTIONAR LOS RECURSOS HUMANOS	APO0701. ADQUIRIR Y MANTENER UNA DOTACIÓN DE PERSONAL SUFICIENTE Y ADECUADA APO0702. IDENTIFICAR AL personal clave de TI Apo0703. Mnatener las habilidades y competencias del personal APO0704. Evaluar y reconocer/recomepensar el rendimiento laboral de los empleados APO0705. Planificar y hacer seguimiento del uso de los recursos humanos del negocio y de TI Apo0706. Gestionar al personal contratado	Procesos Estructuras organizativas Personas, Habilidades y Competencias Políticas y Procedimientos Cultura, ética y comportamiento Servicios, infraestructura y aplicaciones

		APO13 GESTIONAR LA SEGURIDAD	APO1301. Establecer y mantener un SGSI APO1302. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad APO1303. Monitorizar y revisar el SGSI	Procesos Estructuras organizativas Personas, Habilidades y Competencias Políticas y Procedimientos Cultura, ética y comportamiento Servicios, infraestructura y aplicaciones

Apéndice 2. Cuestionario

Instrumento de cumplimiento de normatividad de Teletrabajo y Trabajo en Casa

Propósito

Diseñar un instrumento para diagnosticar el cumplimiento de la normatividad asociada al teletrabajo en el marco de la seguridad de la información

Metodología

Para el desarrollo del cuestionario se tiene como referente COBIT 2019 de **ISACA** lo correspondiente a los objetivos de gobierno y gestión APO07 y APO13 para revisión de cumplimiento de niveles de capacidad

Instrucciones

(Por favor marque con una X la respuesta correcta)

Sector al cual pertenece

Empresas tecnológicas _____ Sector público _____

Instituciones de educación superior _____ Instituciones técnicas y tecnológicas _____

Por favor seleccione el nivel de madurez que corresponda con valores de

0 • Falta de cualquier capacidad básica • Estrategia incompleta para abordar el propósito de gobierno y gestión • La intención de todas las prácticas del proceso puede haberse definido o no.

1 El proceso logra más o menos su propósito a través de la aplicación de un conjunto de actividades incompleto que pueden caracterizarse como iniciales o intuitivas, no muy organizadas.

2 El proceso lograr su propósito a través de la aplicación de un conjunto de actividades básicas, pero completas, que pueden caracterizarse como realizadas.

3 El proceso logra su propósito de forma mucho más organizada usando activos para la organización. Los procesos están, por lo general, bien definidos.

4 El proceso lograr su propósito, está bien definido, y su rendimiento se mide (de forma cuantitativo).

5 El proceso lograr su propósito, está bien definido, su rendimiento se mide para mejorar el desempeño y se persigue la mejora continua.

Niveles de Capacidad (0,1,2,3,4,5)

PROCESO	ACTIVIDAD	Nivel de Capacidad
APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada.	1. Evaluar los requisitos de personal de forma periódica o ante cambios mayores Asegurar que tanto la empresa como la función de TI tengan los suficientes recursos para apoyar las metas y los objetivos empresariales, procesos y controles empresariales y las iniciativas habilitadas por I&T de forma adecuada y apropiada.	
	2. Mantener los procesos de contratación y retención de personal empresarial y de TI en línea con todas las políticas y procedimientos de personal de la empresa.	
	3. Establecer una estructura de recursos flexible, como el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, para apoyar el cambio en las necesidades empresariales.	
	4. Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad y/o criticidad de la función.	
APO07.02 Identificar al personal clave de TI.	1. Como precaución de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que tomarán las personas clave	
	2. Tomar las acciones pertinentes relativas a cambios laborales, en especial terminación de contratos.	
	3. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico.	
	4. Comprobar regularmente los planes de respaldo de personal	
APO07.03 Mantener las habilidades y competencias del personal.	1. Identificar las habilidades y competencias disponibles actuales, tanto de recursos internos como externos.	
	2. Identificar las brechas entre las habilidades requeridas y las disponibles Desarrollar planes de acción, como capacitación (habilidades técnicas y de conducta), contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.	
	3. Revisar los materiales y programas de capacitación de forma regular. Garantizar su idoneidad con respecto a los	

	requisitos en constante evolución de la empresa y su impacto sobre el conocimiento, capacidades y habilidades necesarias.	
	4. Proporcionar acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias	
	5. Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad.	
	6. Realizar evaluaciones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Evaluar la planificación de los reemplazos.	
APO07.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados.	1. Considerar las metas empresariales/funcionales como el contexto para establecer metas individuales	
	2. Establecer metas individuales alineadas con las metas empresariales y de I&T relevantes. Basar las metas en objetivos específicos, medibles, alcanzables, relevantes y en tiempo (SMART) que reflejen las competencias principales, los valores empresariales y las habilidades requeridas para los roles.	
	3. Proporcionar retroalimentación oportuna acerca del rendimiento comparado con las metas individuales	
	4. Proporcionar instrucciones específicas para el uso y el almacenamiento de la información personal en el proceso de evaluación, en cumplimiento de la legislación vigente sobre datos personales y laboral vigente.	
	5. Recopilar resultados de evaluación de rendimiento de 360 grados.	
	6. Proporcionar planes formales de planificación y de desarrollo profesional conforme a los resultados del proceso de evaluación para fomentar el desarrollo de competencias y las oportunidades para el avance personal y para reducir la dependencia de individuos clave. Proporcionar coaching a los empleados sobre el rendimiento y la conducta cuando sea apropiado.	
	7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, desarrollo de competencias y logro de las metas de desempeño. Asegurar que el proceso se aplique de forma consistente y en línea con las políticas organizativas.	
	8. Implementar y comunicar un proceso disciplinario.	
APO07.05 Planificar y hacer seguimiento del	1. Crear y mantener un inventario de recursos humanos empresariales y de TI.	

uso de los recursos humanos del negocio y de TI.	2. Entender la demanda actual y futura de recursos humanos para contribuir a lograr los objetivos de I&T y ofrecer servicios y soluciones conforme al portafolio de iniciativas relacionadas con I&T, al portafolio de inversión futura y necesidades operativas diarias.	
	3. Identificar las carencias y proporcionar recomendaciones sobre los planes de abastecimiento, así como de los procesos de contratación de personal empresarial y de TI. Crear y revisar la planificación de personal, mediante un seguimiento de su uso real.	
	4. Mantener una información adecuada sobre el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos.	
APO07.06 Gestionar al personal contratado	1. Implementar las políticas y procedimientos del personal contratado	
	2. Al inicio del contrato, obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de I&T empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación	
	3. Avisar a los contratistas de que los directivos se reservan el derecho a supervisar e inspeccionar todo el uso de los recursos de TI, incluido el correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.	
	4. Como parte de sus contratos, proporcionar a los contratistas una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados.	
	5. Revisar el trabajo de contratistas y basar la aprobación de los pagos en los resultados	
	6. En contratos formales y no ambiguos, definir todo el trabajo realizado por personal externo	
	7. Realizar revisiones periódicas para garantizar que el personal contratado haya firmado y aceptado todos los acuerdos necesarios.	
	8. Realizar revisiones periódicas para garantizar que los roles de los contratistas y los derechos de acceso sean adecuados y conforme a los contratos	
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.	

	Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa	
	Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad.	
	Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI.	
	Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	
	Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.	
	Comunicar la estrategia de SGSI.	
APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.	
	Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	
	Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades.	
	Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información.	
	Implementar programas de formación y concienciación sobre seguridad de la información y privacidad.	
	Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.	
	Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	
APO13.03 Monitorizar y revisar el sistema de	Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad.	

gestión de seguridad de la información (SGSI).	Realizar auditorías de SGSI a intervalos planificados.	
	Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.	
	Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	
	Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	

Gracias por su colaboración

Apéndice 3. Guion de preguntas

Guión de preguntas si desarrolla o desarrolló su trabajo como **Teletrabajo**

Conceptualización

Teletrabajo. Es 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 la comunicación - TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo. (Ley 1221 de 2008)

Como es su forma de trabajo según las definiciones plantadas:
. **Autónomos** son aquellos que utilizan su propio domicilio o un lugar escogido para desarrollar su actividad profesional, puede ser una pequeña oficina, un local comercial. En este tipo se encuentran las personas que trabajan siempre fuera de la empresa y sólo acuden a la oficina en algunas ocasiones.
. Móviles son aquellos teletrabajadores que no tienen un lugar de trabajo establecido y cuyas herramientas primordiales para desarrollar sus actividades profesionales son las Tecnologías de la Información y la comunicación, en dispositivos móviles.
. **Suplementarios**, son aquellos teletrabajadores que laboran dos o tres días a la semana en su casa y el resto del tiempo lo hacen en una oficina.
. **Teletrabajador.** Persona que desempeña actividades laborales a través de tecnologías de la información y la comunicación por fuera de la empresa a la que presta sus servicios.
Se encuentra dentro de la población vulnerable definiendo población vulnerable (Personas en situación de discapacidad, población en situación de desplazamiento forzado, población en situación de aislamiento geográfico, mujeres cabeza de hogar, población en reclusión, personas con amenaza de su vida).
Se cumple lo definido en la ley relacionado Garantías laborales, sindicales y de seguridad social para los teletrabajadores
1. A los teletrabajadores, dada la naturaleza especial de sus labores no les serán aplicables las disposiciones sobre jornada de trabajo, horas extraordinarias y trabajo nocturno. No obstante la anterior, el Ministerio de la Protección Social deberá adelantar una vigilancia especial para garantizar que los teletrabajadores no sean sometidos a excesivas cargas de trabajo.
2. El salario del teletrabajador no podrá ser inferior al que se pague por la misma labor, en la misma localidad y por igual rendimiento, al trabajador que preste sus servicios en el local del empleador.
3. En los casos en los que el empleador utilice solamente teletrabajadores, para fijar el importe del salario deberá tomarse en consideración la naturaleza del trabajo y la remuneración que se paga para labores similares en la localidad.

4. Una persona que tenga la condición de asalariado no se considerará teletrabajador por el mero hecho de realizar ocasionalmente su trabajo como asalariado en su domicilio o en lugar distinto de los locales de trabajo del empleador, en vez de realizarlo en su lugar de trabajo habitual
5. La asignación de tareas para los teletrabajadores deberá hacerse de manera que se garantice su derecho a contar con un descanso de carácter creativo, recreativo y cultural.
6. Lo dispuesto en este artículo será aplicado de manera que se promueva la igualdad de trato entre los teletrabajadores y los demás trabajadores, teniendo en cuenta las características particulares del teletrabajo y, cuando proceda, las condiciones aplicables a un tipo de trabajo idéntico o similar efectuado en una empresa.
La igualdad de trato deberá fomentarse, en particular, respecto de:
a) El derecho de los teletrabajadores a constituir o a afiliarse a las organizaciones que escojan y a participar en sus actividades;
b) A protección de la discriminación en el empleo;
c) La protección en materia de seguridad social (Sistema General de Pensiones, Sistema General de Seguridad Social en Salud y riesgos profesionales), de conformidad con lo previsto en la Ley 100 de 1993 y las normas que la modifiquen o adicionen o en las disposiciones que regulen los regímenes especiales;
d) La remuneración;
e) La protección por regímenes legales de seguridad social;
f) El acceso a la formación;
g) La edad mínima de admisión al empleo o al trabajo;
h) La protección de la maternidad. Las teletrabajadoras tendrán derecho a retornar al mismo puesto de trabajo o a un puesto equivalente con la misma remuneración, al término de la licencia de maternidad.
i) Respeto al derecho a la intimidad y privacidad del teletrabajador
7. Los empleadores deberán proveer y garantizar el mantenimiento de los equipos de los teletrabajadores, conexiones, programas, valor de la energía, desplazamientos ordenados por él, necesarios para desempeñar sus funciones.
8. Si el teletrabajador no recibe los paquetes de información para que realice sus labores, o los programas para desempeñar su función, o no son arreglados a pesar de haberlo advertido no podrá dejar de reconocérsele el salario que tiene derecho
9. El empleador, debe contemplar el puesto de trabajo del teletrabajador dentro de los planes y programas de salud ocupacional, así mismo debe contar con una red de atención de urgencias en caso de presentarse un accidente o enfermedad del teletrabajador cuando esté trabajando.

10. La vinculación a través del teletrabajo es voluntaria, tanto para el empleador como para el trabajador. Los trabajadores que actualmente realicen su trabajo en las instalaciones del empleador, y pasen a ser teletrabajadores, conservan el derecho de solicitar en cualquier momento, volver a la actividad laboral convencional.
11. Las empresas cuyas actividades tengan asiento en Colombia, que estén interesadas en vincular teletrabajadores, deberán hacerlo con personas domiciliadas en el territorio nacional, quienes desarrollarán sus labores en Colombia.
12. A todas las relaciones de teletrabajo que se desarrollen en el territorio nacional les será aplicada la legislación laboral colombiana, en cuanto sea más favorable para el teletrabajador.

Guion de preguntas para personas que realizan su actividad como **Trabajo en Casa**

Definición de Trabajo en Casa. Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones. Este no se limita al trabajo que puede ser realizado mediante tecnologías de la información y las comunicaciones, medios informáticos o análogos, sino que se extiende a cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la empresa o entidad. (Ley 2088 de 2.021)

Qué opinión tiene de los siguientes elementos contemplados en la Ley

. Garantías en la habilitación del ejercicio del trabajo en casa en las funciones y servicios públicos. Para el cumplimiento de las funciones públicas y la prestación de los servicios públicos, en la habilitación del trabajo en casa para los servidores públicos se garantizarán:
a. La satisfacción de los principios de igualdad, moralidad, eficacia, seguridad jurídica, economía, celeridad, imparcialidad y publicidad propios del ejercicio de la función administrativa;
b. La salvaguarda de las prerrogativas laborales y sociales de los trabajadores;
c. El respeto de los principios esenciales del Estado Social de Derecho y de los derechos fundamentales de las personas.
Criterios aplicables al trabajo en casa. La habilitación del trabajo en casa se regirá por los principios generales de las relaciones laborales señalados en la Constitución Política y en la ley, y por los siguientes criterios:

a. Coordinación. Las funciones, servicios y actividades laborales deberán desarrollarse de manera armónica y complementaria entre el empleador y el trabajador para alcanzar los objetivos y logros fijados. La coordinación deberá darse desde el momento mismo de la asignación de tareas o actividades, para lo cual se deberán fijar los medios y herramientas que permitan el reporte, seguimiento y evaluación, así como la comunicación constante y recíproca
b. Desconexión laboral. Es la garantía y el derecho que tiene todo trabajador y servidor público a disfrutar de su tiempo de descanso, permisos, vacaciones, feriados, licencias con el fin de conciliar su vida personal, familiar y laboral. Por su parte el empleador se abstendrá de formular órdenes u otros requerimientos al trabajador por fuera de la jornada laboral.
Elementos de la relación laboral en el Trabajo en Casa. La habilitación del trabajo en casa implica que se mantenga la facultad subordinante del empleador, junto con la potestad de supervisión de las labores del trabajador. Permanecerán todas las obligaciones, derechos y deberes derivados de la prestación personal del servicio. El empleador determinará los instrumentos, la frecuencia y el modelo de evaluación del desempeño, cumplimiento de metas, así como el mecanismo para el reporte y/o resultados de éstas, por el tiempo que dure el trabajo en casa. El Gobierno nacional determinará los instrumentos para la habilitación del trabajo en casa para los servidores públicos. El seguimiento de los objetivos y actividades de los servidores públicos y trabajadores del sector privado deberá obedecer a criterios concertados y establecidos con anterioridad.
. Jornada de Trabajo. Durante el tiempo que dure el trabajo en casa se mantendrán vigentes las normas previstas en el Código Sustantivo del Trabajo y en los reglamentos aplicables a los servidores públicos, relativos al horario y la jornada laboral. Estarán excluidos del cumplimiento de estas disposiciones y de la remuneración del trabajo suplementario los trabajadores de dirección, de confianza o de manejo, así como los niveles directivo y asesor, en el sector público
Término del trabajo en casa. La habilitación de trabajo en casa originada por circunstancias excepcionales, ocasionales o especiales se extenderá hasta por un término de tres meses prorrogables por un término igual por una única vez, sin embargo, si persisten las circunstancias ocasionales, excepcionales o especiales que impidieron que el trabajador pudiera realizar sus funciones en su lugar de trabajo se extenderá la habilitación de trabajo en casa hasta que desaparezcan dichas condiciones. En todo caso, el empleador o nominador conserva la facultad unilateral de dar por terminada la habilitación de trabajo en casa, siempre y cuando desaparezcan las circunstancias ocasionales, excepcionales o especiales que dieron origen a dicha habilitación

Elementos de Trabajo. Para el desarrollo del trabajo en casa y el cumplimiento de sus funciones, el servidor público o el trabajador del sector privado, podrá disponer de sus propios equipos y demás herramientas, siempre que medie acuerdo con el respectivo empleador y/o entidad pública. Si no se llega al mencionado acuerdo, el empleador suministrará los equipos, sistemas de información, software o materiales necesarios para el desarrollo de la función o labor contratada, de acuerdo con los recursos disponibles para tal efecto. El empleador definirá los criterios y responsabilidades en cuanto al acceso y cuidado de los equipos, así como respecto a la custodia y reserva de la información de conformidad con la normativa vigente sobre la materia. En todo caso el empleador es el primer responsable de suministrar los equipos necesarios para el desarrollo de las actividades, cumplimiento de funciones y prestación del servicio bajo la habilitación de trabajo en casa.
. Procedimientos necesarios para la implementación del Trabajo en Casa. Previo a la implementación del trabajo en casa, toda empresa y entidad pública o privada deberá contar con un procedimiento tendiente a proteger este derecho y garantizar a través de las capacitaciones a que haya lugar el uso adecuado de las tecnologías de la información y la comunicación - TIC o cualquier otro tipo de elemento utilizado que pueda generar alguna limitación al mismo. Para dar inicio a esta habilitación, el empleador deberá notificar por escrito a sus trabajadores acerca de la habilitación de trabajo en casa, y en dicha comunicación, se indicará el periodo de tiempo que el trabajador estará laborando bajo esta habilitación.
. Sobre los derechos salariales y prestacionales. Durante el tiempo que el servidor público o trabajador del sector privado preste sus servicios o desarrolle sus actividades bajo la habilitación de trabajo en casa, tendrá derecho a percibir los salarios y prestaciones sociales derivadas de su relación laboral. A los servidores públicos y trabajadores del sector privado que devenguen hasta dos salarios mínimos legales mensuales vigente y que se les reconozca el auxilio de transporte en los términos de las normas vigentes sobre el particular, durante el tiempo que presten sus servicios bajo la habilitación de trabajo en casa, se le reconocerá este pago a título de auxilio de conectividad digital. El auxilio de conectividad y el auxilio de transporte no son acumulables.
PARÁGRAFO 1. Para los servidores públicos, el auxilio de conectividad se reconocerá en los términos y condiciones establecidos para el auxilio de transporte.
PARÁGRAFO 2. Para los trabajadores del sector privado, el valor establecido para el auxilio de transporte se reconocerá como auxilio de conectividad digital y tendrá los mismos efectos salariales del auxilio de transporte.

. Garantías laborales, sindicales y de seguridad social. Durante el tiempo que se preste el servicio o actividad bajo la habilitación de trabajo en casa, el servidor público o trabajador del sector privado continuará disfrutando de los mismos derechos y garantías que rigen su relación laboral, entre otras, las que regulan la jornada laboral, horas extras, trabajo nocturno, dominicales y festivos, descansos dentro de la jornada laboral, derechos de asociación y negociación sindical y en general todos los beneficios a que tenga derecho en el marco de la respectiva relación laboral. Durante el tiempo que se presten los servicios o actividades bajo la habilitación del trabajo en casa el servidor público o trabajador del sector privado continuará amparado por las acciones de promoción y prevención, así como de las prestaciones económicas y asistenciales, en materia de riesgos laborales. Así mismo, la Administradora de Riesgos Laborales a la que se encuentre afiliado el empleador, deberá promover programas que permitan garantizar condiciones de salud física y mental, así como la seguridad en el trabajo, para lo cual los empleadores deberán comunicar y actualizar ante la Administradora de Riesgos Laborales los datos del trabajador y en aquellos casos en que sea necesaria la prestación del servicio o el desarrollo de actividades en un lugar diferente al inicialmente pactado en la relación laboral deberá informar la dirección en la que se efectuará el desarrollo de las actividades.
. Programas de bienestar y capacitación. Para la implementación de la habilitación de trabajo en casa, el empleador deberá promover la formación, capacitación y el desarrollo de competencias digitales, en los servidores públicos y trabajadores del sector privado cuando la actividad a desarrollar así lo requiera.
Implementación del trabajo en casa. El trabajo en casa como habilitación excepcional aquí regulada no requerirá modificación al Reglamento Interno de Trabajo ni al Manual de Funciones, salvo que fuera necesario para el desarrollo de las labores. PARÁGRAFO. En los eventos en que sea necesario modificar el reglamento interno no podrán variar las condiciones laborales establecidas o pactadas al inicio de la relación laboral
Canales oficiales de comunicación para ciudadanos y usuarios. Las entidades públicas y los empleadores del sector privado deberán adoptar las directrices necesarias para el desarrollo del trabajo en la habilitación del trabajo en casa, y en especia l darán a conocer a los ciudadanos y usuarios en su página web, los canales oficiales de comunicación e información mediante los cuales prestarán sus servicios de manera virtual, así como los mecanismos tecnológicos y/o virtuales que emplearán para el registro y respuesta de las peticiones. En todo caso la habilitación de trabajo en casa no implicará retroceso, demoras o falta de calidad en la atención y en el desempeño de funciones y prestación de servicios.

Apéndice 4. Categorías previas

Categorías Principales	**Subcategorías**
Salud Mental	Derecho a la intimidad Privacidad
Recursos	Financieros Temporales Físicos Tecnológicos
Productividad	
Clima laboral	Trabajo en equipo Aislamiento
Seguridad de la información	