Diseño de un nuevo dominio de seguridad de la información basado en la GTC-ISO-IEC 27002:2015 para los entornos de trabajo remoto emergentes por la COVID-19

German Andrés Gutiérrez Peña

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnología de Información

Bogotá D.C., 2021

Diseño de un nuevo dominio de seguridad de la información basado en la GTC-ISO-IEC 27002:2015 para los entornos de trabajo remoto emergentes por la COVID-19

German Andrés Gutiérrez Peña

Director:

Roberto Mauricio Cárdenas Cárdenas

Master Universitário en E-learning y Tecnología Educativa

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnología de Información

Bogotá D.C., 2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

Bogotá D.C., 2021

Dedicatoria

Dedico este proyecto principalmente a Dios quien me ha puesto en este camino, a mi familia paterna de la cual he heredado hábitos de estudio, a mi familia materna de la cual he conocido del grato camino del esfuerzo, a mi futura esposa por ser de gran apoyo en el desarrollo del presente proyecto y a mis hijos quienes son mi motivo de inspiración y legado.

Agradecimientos

Agradezco a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme las pautas de formación como profesional y magister, al Mg. Roberto Mauricio Cárdenas Cárdenas por su apoyo y acompañamiento en el proceso de desarrollo del presente proyecto, a la dra. Diana Marcela Cardona directora del curso Gestión de Seguridad en TI por su valiosa asistencia y aclaraciones en relación con la temática de su curso en el que se fundamenta el presente proyecto.

Resumen

Este proyecto de investigación aborda la adopción de nuevas directrices de seguridad de la información para los escenarios de trabajo remoto originados por la pandemia de la COVID-19, debido a que con la llegada del evento pandémico han aumentado de manera exponencial las amenazas informáticas y, también, han surgido diversos tipos de ataques informáticos; además, los sistemas de seguridad de algunas organizaciones se han visto vulnerables porque fueron diseñados originalmente para una operación local y no remota.

El objetivo principal de este proyecto se fundamenta en el diseño de un nuevo dominio de seguridad de la información, inspirado en el alcance limitado que tiene la actual norma colombiana GTC-ISO/IEC 27002:2015 para satisfacer las nuevas necesidades de protección de la información. Para el desarrollo del proyecto se planteó un caso de estudio y una metodología constituida por cuatro etapas, en las cuales se contempló la exploración e identificación del aumento de amenazas informáticas, estudio y análisis del actual código de prácticas de la GTC-ISO/IEC 27002:2015 y sus ciento catorce controles de seguridad. Igualmente, se exploró el desarrollo de un nuevo dominio de seguridad para el perfeccionamiento de la actual norma en el marco de los puestos de trabajo de forma remota y, por último, se procedió a elegir las mejores tecnologías y aplicación de buenas prácticas para la seguridad de la información empresarial, acorde con las directrices del nuevo dominio de seguridad propuesto.

Producto del nuevo dominio de seguridad planteado, se concluye que este contempla las herramientas de protección para los nuevos entornos de trabajo remoto, con el fin de beneficiar a ProCibernetica, asimismo, a cualquier otra organización que esté interesado en aplicar este nuevo dominio.

Palabras clave: amenaza, controles, COVID-19, seguridad de la información, trabajo remoto.

Abstract

This research project focuses on the adoption of new information security guidelines for remote work scenarios that were created due to the COVID-19 pandemic. With the advent of the pandemic, computer threats have increased exponentially and new types of attacks have also emerged, in addition, the security systems of some organizations were shown to be vulnerable since they were not designed for remote operation.

The main objective of this project is the design of a new information security domain that greatly improves the current Colombian standard GTC-ISO/IEC 27002:2015 to meet new information protection needs. For the development of the project a case study and a methodology consisting of four stages were applied; the exploration and identification of increasing computer threats, study and analysis of the current code of practice of the GTC-ISO/IEC 27002:2015 with its one hundred and fourteen (114) security controls, development of a new security domain for the refinement of the current GTC-ISO/IEC 27002:2015 in the context of remote workstations and finally, the best technologies and application of best practices for business information security were chosen, in line with the guidelines of the proposed new security domain.

As a product of the proposed new security domain, we have developed protection tools for new remote working environments implemented on the ProCibernetica company and potentially on any other organization.

Keywords: controls, COVID-19, information security, remote working, threat.

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

La información es un recurso intangible asociado a la composición de un conjunto de datos estructurado coherentemente para llevar, en este caso, a una organización hacia una acción determinada. De esta manera, la información es uno de los activos de mayor importancia para una organización y el tratamiento inadecuado de su seguridad podría impactar tanto la disponibilidad de la información para la continuidad del negocio como la confidencialidad para la credibilidad de sus clientes, y hasta implicaciones jurídicas por sanciones a incumplimientos regulatorios. Con el fin de que las organizaciones no se vean afectadas por algunos de estos inconvenientes, estas pueden acceder a recursos como un sistema de gestión y seguridad de la información SGSI o directamente poder aplicar algunos de los controles de seguridad de la norma colombiana GTC-ISO/IEC 27002:2015 Instituto Colombiano de Normas Técnicas [Icontec], 2015) para proteger la información.

A partir de la llegada de la pandemia COVID-19, en el primer semestre de 2020, el panorama de la ciberseguridad se volvió mucho más crítico debido a un aumento considerable en las amenazas informáticas. En medio de esto, los ciberdelincuentes han diseñado diferentes tipos de ataques basados en técnicas de ingeniería social, utilizando como principal medio el correo electrónico. Además, debido al creciente uso de las herramientas de videoconferencia y colaboración, los atacantes han puesto su punto de mira en estos instrumentos para intentar explotar nuevas vulnerabilidades y obtener información confidencial de las empresas y usuarios (Berrios, 2020; Rodríguez García, 2020).

Dado el evidente aumento de amenazas informáticas, producto del nuevo modelo de trabajo remoto poscovid, las empresas no están asumiendo una postura adecuada en el manejo de la seguridad de la información. Una de las principales causas de lo anterior, se apoya en que la

actual guía técnica colombiana GTC-ISO/IEC 27002:2015, originalmente no fue diseñada para amparar la seguridad de la información en medio de la variedad de escenarios de trabajo remoto y aislamiento social causados por pandemia; por lo tanto, la guía GTC-ISO/IEC 27002:2015 no cuenta con los controles de seguridad adecuados para proteger la información y mitigar cualquier tipo de amenaza sobre los sistemas, que ahora son más vulnerables en los entornos no protegidos (como el trabajo en casa). Es imprescindible disponer de los adecuados controles de seguridad para los escenarios de tipo pandemia porque existe la evidencia científica que afirma la posible aparición de un nuevo tipo de pandemia a partir de la gripe aviar H5N8 (Shi & Gao, 2021). Con relación a esto, incluso el reconocido y distinguido empresario estadounidense Bill Gates ha venido afirmando que podría presentarse una nueva pandemia, posiblemente propagándose en el 2024 (Micó, 2020).

Es importante destacar que la existencia de los adecuados controles de seguridad de la información favorecería el nuevo modelo de trabajo remoto, el cual ha demostrado buena aceptación por parte de los colaboradores de las organizaciones, ya que ha aumentado la productividad y ha reducido costos a los empleadores (Rodríguez García, 2020).

La actual realidad poscovid requiere la creación de un nuevo dominio de seguridad transversal para la protección de la información empresarial, el cual es presentado mediante el presente proyecto, en el cual se explorar nuevas prácticas para la seguridad y uso de tecnología específica con el fin de proteger los datos empresariales a través de los activos de información; para esto se llevarán a cabo las siguientes etapas:

1. Identificación de nuevas amenazas informáticas sobre los actuales escenarios de trabajo remoto a causa del confinamiento ocasionado por la COVID-19. Se presenta el caso de estudio de la empresa ProCibernetica.

2. Demostración de vacíos de la actual guía técnica colombiana GTC-ISO/IEC 27002:2015 frente a los nuevos desafíos de seguridad de la información empresarial poscovid, comprendiendo la brecha entre teletrabajo y trabajo remoto.
3. Diseñar y proponer nuevos controles de seguridad de la información para satisfacer las nuevas necesidades de protección de datos empresariales en el trabajo remoto poscovid.
4. Seleccionar una tecnología y unas prácticas adecuadas para la protección de la información a partir del nuevo dominio de seguridad presentado.

La investigación y diseño planteado en el presente proyecto sirve de apoyo y sustento para impulsar y promover la seguridad de la información sobre cualquier organización que esté interesada en proteger su información empresarial en el trabajo remoto y operación poscovid. Igualmente, como recurso en el proceso de implementación de un sistema de gestión y seguridad de la información en este nuevo escenario. No obstante, el dominio de seguridad presentado en este proyecto está sujeto a acciones de mejora y perfeccionamiento a partir de la experiencia de su implementación y surgimiento de nuevas tecnologías de ciberseguridad.

Planteamiento del problema

La situación económica del país actualmente atraviesa por una preocupante crisis financiera, gran parte de esto es debido a las obligadas y desesperadas medidas de confinamiento social, dictadas por el Gobierno colombiano, a las que se ha tenido que adherir la mayoría de la población, así como en otras naciones, causado por la pandemia COVID-19. Este virus causa una infección respiratoria aguda de tipo gripal el cual puede ser leve, moderado o severo. Ha sido catalogado por la Organización Mundial de la Salud como una emergencia en salud pública de importancia internacional por su rápida propagación; tanto es así que, se han identificado casos en todos los continentes y el 6 de marzo de 2020 se confirmó el primer caso en Colombia (Ministerio de Salud y Protección Social, s.f.).

Como resultado de esta gran calamidad de salud pública, las organizaciones colombianas y de otras naciones se han visto obligadas a que sus empleados den estricto cumplimiento a las medidas de confinamiento decretadas por los diferentes entes gubernamentales. Por lo anterior, algunas organizaciones han tenido que suspender sus actividades, mientras que otras intentan reactivar su productividad con el apoyo del trabajo remoto para que sus empleados puedan ejecutar actividades laborales desde los lugares donde residen, esto sobre las funciones y actividades que particularmente lo permitan.

Si bien la pandemia trajo cosas positivas como la cultura del trabajo remoto, tanto para el colaborador como el empresariado, también hay puntos negativos como la saturación de los servicios digitales, lo cual está afectando directamente a la disponibilidad de los servicios, asimismo, la confidencialidad e integridad de la información debido al aumento de riesgos por las amenazas en la habilitación de accesos remotos a los colaboradores, causada por la urgencia de mantener operativas las empresas. Hubo, además, un aumento considerable de fraudes y

ataques informáticos, gracias a la demanda de usuarios en Internet. En medio de la pandemia, los ciberdelincuentes han diseñado diferentes tipos de ataques basados en técnicas de ingeniería social, utilizando como principal medio el correo electrónico. Igualmente, por el creciente uso de herramientas de videoconferencia y colaboración, los ciberdelincuentes han puesto su mirada en estas aplicaciones, intentando explotar nuevas vulnerabilidades que puedan ser aprovechadas para obtener información confidencial de las empresas, cualquier tipo de credencial bancaria o datos personales de los usuarios (Berrios, 2020; García, 2020).

La información es el activo más útil, valioso e importante para todas las organizaciones colombianas, así como de otras naciones; sin embargo, actualmente no se le ha dado la importancia que esta debería tener, debido a que, desde un inicio, culturalmente no se ha despertado ni brindado un adecuado nivel de conciencia en las personas sobre su importancia. Esto ha resultado en la incapacidad para aplicar los adecuados y acertados controles de seguridad para la protección integral de la información empresarial, independientemente al tiempo, modo y lugar en el cual la información este siendo procesada.

Justificación

Gran parte de las empresas colombianas se encuentran, en la actualidad, operando bajo puestos de trabajo remoto, debido al aislamiento social, y la mayoría de estas no están asumiendo una postura adecuada frente al manejo de la seguridad de la información, desconociendo por completo la existencia de las nuevas amenazas y riesgos informáticos. En este sentido, la GTC-ISO/IEC 27002:2015 (Icontec, 2015), versión oficial, no cuenta con los controles adecuados para garantizar la seguridad de la información que conlleve a la mitigación de las amenazas y el apropiado tratamiento de riesgos, especialmente, en los nuevos escenarios de trabajo remoto poscovid para los miles, incluso millones, de trabajadores remotos en Colombia y del mundo entero, que vienen haciendo todo lo posible por dar continuidad a sus actividades laborales desde sus lugares de residencia, por medio del uso de un equipo de cómputo y conexión a Internet.

El presente trabajo propone la aplicación de mejores prácticas y uso de tecnología adecuada para el fortalecimiento de la seguridad de la información en medio de una situación de aislamiento social, causado por la rápida proliferación del virus SARS-CoV-2 (COVID-19). Ahora los sistemas se encuentran más vulnerables debido a la exposición sobre entornos no protegidos y aparición de nuevas amenazas informáticas, lo cual desencadena mayores riesgos para la seguridad de la información empresarial.

La seguridad de la información es un tema cada vez más importante para las organizaciones y, aún más, en medio de una situación poscovid, en el que las amenazas informáticas cada día van en aumento. Así que, el contar con los adecuados controles de seguridad de la información se vuelve imprescindible por las siguientes razones:

- Insuficiencia de controles de seguridad de la actual norma GTC-ISO/IEC 27002:2015: la actual versión de la GTC-ISO/IEC 27002:2015 (Icontec, 2015) no promueve el uso de

controles de seguridad para la protección de nuevos ambientes de trabajo, en donde la información es dinámica y está en constante movimiento. Según BSI Group (2021), la ISO 27002 no aborda adecuadamente el uso de controles de seguridad requeridos para el tiempo actual, asimismo, no cuenta con controles relacionados específicamente con los servicios en la nube.

- Proliferación de nuevos virus pandémicos futuros: tal como lo ha previsto el reconocido y distinguido empresario estadounidense Bill Gates, creador y fundador de la empresa Microsoft, ha venido afirmando que podría presentarse la propagación de una nueva pandemia posiblemente entre el 2024 y 2025; cabe destacar que este mismo también predijo en el 2015 sobre la catástrofe mundial por aparición de un virus de tipo pandemia, que finalmente surgió en el 2019 (Micó, 2020), adicionalmente ya existen evidencias científicas que indican que posiblemente de la gripe aviar pueda emerger otra nueva pandemia (Shi & Gao, 2021).
- Destacable acogida del trabajo remoto: el trabajo remoto ha presentado una buena aceptación por parte de los colaboradores de las empresas, ya que ha aumentado la productividad y ha logrado ahorrar los costos de buena parte de las empresas; por lo tanto, se proyecta que, pasada la pandemia, muchas empresas contemplan seguir operando bajo esta modalidad (García, 2020).

Objetivos

Objetivo general

Diseñar un dominio transversal para la seguridad de la información basado en la guía técnica colombiana GTC-ISO/IEC 27002:2015, con el fin de proteger la información empresarial frente a los nuevos desafíos del trabajo remoto en casa.

Objetivos específicos

Identificar las nuevas amenazas informáticas sobre los actuales escenarios de trabajo remoto a causa del confinamiento ocasionado por la COVID-19, basándose en el estudio de caso de la empresa ProCibernetica.

Demostrar los vacíos de la actual guía técnica colombiana GTC-ISO/IEC 27002:2015 frente a los nuevos desafíos de seguridad de la información empresarial poscovid, comprendiendo la brecha entre el teletrabajo y el trabajo remoto.

Diseñar nuevos controles de seguridad de la información para satisfacer las nuevas necesidades de protección de datos empresariales en el trabajo remoto poscovid.

Proponer el uso de tecnología y prácticas adecuadas para la protección de la información a partir del nuevo dominio de seguridad presentado.

Marco teórico

El apartado del marco teórico aborda la descripción de los conceptos en el que se basa el proyecto de investigación y los conceptos claves para facilitar la comprensión de la metodología y resultados de la investigación.

Definición de amenazas informáticas

La seguridad de la información contempla la aplicación de un conjunto de medidas preventivas, con carácter de correctivas, para proteger la disponibilidad, confidencialidad e integridad de la información que usualmente es afectada por actividades de cibercrimen.

El cibercrimen es toda actividad malintencionada, ilegal y delictiva que atenta contra los pilares de la disponibilidad, confidencialidad e integridad de la información, y que se lleva a cabo mediante el uso de las tecnologías de la información y comunicación (Castellanos Vega, 2020).

Algunas de las principales amenazas causadas por el cibercrimen se describen a continuación:

- *Denia of service* (DoS): este traduce "ataque de denegación de servicio" y es un tipo de ataque informático dirigido a un sistema o una red, el cual tiene el objetivo principal de interrumpir el tráfico y acceso a un servidor, y hacer que el servicio sea inaccesible para el usuario legítimo. Este tipo de agresión cibernética se deriva en la modalidad estándar y la modalidad de reflexión: en la primera, el ataque se lleva a cabo de manera directa entre el *boot* y el objetivo; en la segunda modalidad, el atacante esconde su identidad haciéndose pasar por la víctima, para posteriormente perpetuar su ataque mediante la inundación de solicitudes hacia el objetivo (Valenzuela Matutti, 2020).

- *Payment fraud*: este tipo de ataque traduce “fraude de pago electrónico” y es una de las actividades ilícitas más comúnmente usadas por los ciberdelincuentes, la cual se ha venido presentando con el auge de las transacciones en línea. El objetivo de este tipo de ataque es que el usuario atacado pierda su dinero y su información confidencial (Diaz Jiménez *et al*., 2018).
- *Sociallity engineered threats* (*phishing, fraud*): es un tipo de ataque a la seguridad de la información que se fundamenta en el empleo de técnicas persuasivas para obtener información confidencial y financiera para usar en beneficio del atacante. El termino *phishing* traduce “fraude electrónico” y es una modalidad de ataque informático basado en el empleo de técnicas de ingeniería social, que se aprovecha de situaciones y eventos sociales determinados para hacer el ataque y robar la información; estos eventos pueden ser desastres naturales, elecciones políticas, eventos deportivos, festividades culturales importantes, epidemias o crisis de salud (como la ocasionada por la COVID-19). El objetivo de estos tipos de ataques es influir en un usuario para ganar su confianza y hacer que este divulgue información confidencial como contraseñas, números de tarjeta de crédito u otros (Valenzuela Matutti, 2020). Las campañas de *phishing* son difundidas mediante los siguientes modos: correo electrónico, redes sociales, mensajes de texto, páginas web.
- *Malware*: traduce “*software* malicioso” y es un tipo de ataque informático que tiene el objetivo de dañar el equipo en el que se ha logrado alojar ese *software*, ya sea un equipo de cómputo o un dispositivo móvil. Existen varios tipos de *malware* dentro de los cuales se tienen los virus informativos, troyanos, gusanos, *spyware*, *adware*, *ransomware*; cada

uno de estos actúa de manera diferente, usualmente, se propaga por medio de correo electrónico (Fernández, 2020a).

- *Ransomware:* es un ataque informático muy común actualmente, es de tipo *malware*, es un *software* malicioso extorsivo, y su finalidad es el secuestro de la información cifrando los archivos del sistema para luego exigir el pago de dinero por el rescate de la información. Existen varios tipos de *ransomware*, no obstante, el *ransomware* usualmente es difundido mediante correo electrónico, mensaje instantáneo o sitio web (Castellanos Vega, 2020).
- *Zoombombing:* es un tipo de vulnerabilidad que atenta contra la confidencialidad de la información sobre las nuevas y ascendentes reuniones virtuales, en el cual personas no invitadas se infiltran e irrumpen en la comunicación (Nakamura *et al*., 2021).

Descripción de la norma GTC-ISO/IEC 27002:2015 y algunos de sus controles

La guía técnica colombiana ISO-IEC 27002, versión 2015, es el principal recurso al que generalmente se accede en el periodo final de diseño y construcción del sistema de gestión y seguridad de la información (SGSI), y se hace de manera posterior a la identificación de los activos de información y definición de la matriz de riesgos para la organización. La GTC-ISO-IEC 27002:2015 (Icontec, 2015) contiene un conjunto de directrices, controles y buenas prácticas para la gestión de la seguridad de la información empresarial teniendo en cuenta algunos entornos de operación. A continuación, se presenta la descripción de conceptos relevantes y correlacionados con la guía técnica colombiana ISO-IEC 27002:2015 para el desarrollo del presente proyecto.

GTC-ISO-IEC 27002:2015: la composición de sus siglas representa lo siguiente: GTC indica Guía técnica colombiana; ISO son las siglas en inglés de la Organización Internacional de Normalización; IEC son las siglas en inglés de la Comisión Electrónica Internacional; la numeración 27002 se relaciona con la pertenencia al grupo de normas compuestas por la serie 27000, las cuales guardan correspondencia con todo lo concerniente a la implementación de un SGSI; sus últimos caracteres, 2015, obedecen al año de publicación de la norma. En conjunto esta denominación representa a la última guía oficial para el establecimiento de buenas prácticas y recomendaciones compuesta por 14 dominios y 114 controles para considerar en la protección de los sistemas de información.

Control 6.2.1: este control, de acuerdo con la guía técnica GTC-ISO/IEC 27002:2015, pretende establecer una política de seguridad para dispositivos móviles, considerando los peligros internos y externos a los que se encontrarían expuestos, en los que se tendrían riesgos que afectarían la protección física, la seguridad del *software*, la seguridad de conectividad, la confidencialidad y los accesos seguros, la disponibilidad y el respaldo de datos, el uso seguro y la responsabilidad por parte del empleado. En términos generales, el control de seguridad para dispositivos móviles establece las pautas para el tratamiento de amenazas que se presentan en el ejercicio habitual de trabajo, entornos fuera de la organización (Icontec, 2015).

Control 6.2.2: este control, según la guía técnica GTC-ISO/IEC 27002:2015, hace referencia a todo lo concerniente con el teletrabajo por medio del cual se constituyen las medidas de seguridad para la información, independientemente de la ubicación donde se esté efectuando el teletrabajo. La habilitación de esta modalidad obliga al empleador a cumplir con una serie de requisitos legales. Este control evalúa los siguientes puntos:

- Seguridad física del sitio y entorno del teletrabajador.

- Seguridad en la conexión a los recursos de la organización.
- Uso de dispositivos personales en el trabajo.
- Seguridad del perímetro y protección contra ataques informáticos.
- Suministro de equipo de cómputo, conexión remota segura, puesto de trabajo y demás recursos para la ejecución de las actividades laborales.
- Fijación al horario de trabajo y controles de acceso a la información.
- Soporte técnico de *hardware* y *software*, copias de respaldo a los datos.
- Revocación de acceso a los datos corporativos en horarios no laborales (Icontec, 2015).

Control 7.2.1: en la guía técnica GTC-ISO/IEC 27002:2015, este control se refiere a las responsabilidades de la dirección y se contempla que la dirección establezca políticas, procedimientos y estrategias para fomentar la seguridad de la información; además de asegurarse que estas sean cumplidas por parte de los empleados (Icontec, 2015)

Control 9.1.1: este control, conforme a lo que indica la guía técnica GTC-ISO/IEC 27002:2015, habla sobre los procedimientos de control de acceso, tanto físico como lógico, para los colaboradores que entraran a interactuar con los activos de información de la organización. Asimismo, establece derechos de acceso y permisos de acceso por roles de usuario, reglas de autenticación y almacenamiento al registro de eventos (Icontec, 2015).

Control 10.1.1: la guía técnica GTC-ISO/IEC 27002:2015 refiere que este tipo de control trata sobre los controles de seguridad mediante el uso de criptografía. La criptográfica propuesta sobre este control se encuentra orientada a la protección del negocio sobre los datos que fluyen a través de los canales de comunicación o de los datos que se encuentran en estado de almacenamiento (Icontec, 2015).

Control 11.1.1: este control, tal y como señala la guía técnica GTC-ISO/IEC 27002:2015, hace referencia a la seguridad del perímetro físico. Este control se preocupa por la protección de la información de puertas para adentro y sugiere la aplicación de medidas de seguridad sobre la edificación o recinto donde se encuentren resguardados los activos de información de la organización, mediante diferentes estrategias como el control de acceso solo para personal autorizado y restricción a personal no autorizado, uso de puertas de seguridad, paredes reforzadas y uso de alarmas y sistema de monitoreo (Icontec, 2015).

Control 13.1.2: la guía técnica GTC-ISO/IEC 27002:2015 indica que este control se encarga de establecer las directrices para la seguridad de los servicios de red, a través del uso de tecnología para la seguridad de la red de datos de la organización; igualmente, mediante el uso de equipos *firewall* y parametrización técnica para el control de acceso a servicios y aplicaciones de red y conexiones seguras por medio del uso de soluciones de seguridad gestionada (Icontec, 2015).

Control 17.1.1: este control, en la guía técnica GTC-ISO/IEC 27002:2015, determina la necesidad de planificar la continuidad de la seguridad de la información sobre situaciones adversas como, por ejemplo, desastres, buscando mantener los requisitos de seguridad de la organización (Icontec, 2015).

Tecnologías y términos entorno al nuevo dominio de seguridad

La tecnología hace parte del conjunto de elementos creados por el hombre, en el cual su origen se fundamenta en el diseño y desarrollo de servicios y sistemas compuestos por una serie de técnicas estructuradas de manera lógica para transformar el entorno del ser humano, con el fin de favorecer su progreso social y económico, y, de esta manera, conducir a la satisfacción de necesidades y/o la solución de problemas. La tecnología hace parte de los elementos dentro de la

infraestructura de tecnologías de la información (TI) en una organización y se encarga de soportar el flujo, almacenamiento, procesamiento y análisis de la información. La infraestructura está constituida por las instalaciones físicas, redes y comunicaciones, forma de almacenamiento, servidores, herramientas de gestión y aplicaciones de la organización. La infraestructura tecnológica puede estar agrupada en el centro que reúne los datos (*datacenter*) de la organización o descentralizada por medio de un proveedor externo desde un ambiente de nube pública o nube privada (Millán, 2018).

Con el fin de lograr un adecuado entendimiento técnico y conceptual, a continuación, se relaciona de manera discriminada la diversa terminología utilizada para cada uno de los controles de seguridad en el desarrollo de la última etapa del proyecto. Es de precisar que esta terminología está directamente relacionada con la propuesta de nuevos controles de seguridad para la protección de la información en la era poscovid, el cual se desarrolló en este proyecto y se relaciona bajo el numeral diecinueve, y tiene como propósito la adición de un nuevo dominio de seguridad sobre la actual norma GTC-ISO/IEC 27002:2015, la cual actualmente cuenta con dieciocho dominios y carece de directrices de seguridad sobre eventos pandémicos.

- Ciberseguridad: el concepto de ciberseguridad se refiere al conjunto de técnicas y herramientas que se deberían utilizar para proteger la integridad, disponibilidad y confidencialidad de los datos, sobre la infraestructura en la que estos fluyen y reposan, salvaguardándolos de las diferentes amenazas, ataques y accesos no autorizados (Palo Alto Networks, s.f.).
- Activo de información: los activos de información de una organización son todos aquellos elementos que contienen información sensible y propia de la organización, estos se clasifican en activos tangibles y activos intangibles. Los activos tangibles son aquellos

de tipo material como equipos de cómputo, equipos de red, servidores, periféricos, dispositivos móviles, personas e instalaciones de la organización. Los activos intangibles son aquellos en los que circula y reposa la información, como las aplicaciones informáticas, sistemas operativos, canales de comunicación, bases de datos, entre otros. Con base en la importancia de la seguridad de la información para las organizaciones, sobre ambos activos, se deberían establecer medidas de seguridad preventiva para protegerlos ante la posible materialización de riesgos, tanto físicos como lógicos (ISO Win, 2017).

- Mitigación de riesgos informáticos: es un conjunto de medidas de seguridad preventiva dirigidas a disminuir y reducir, al mejor nivel posible, la aparición de eventos indeseados y controlar el nivel de impacto y probabilidad de ocurrencia; de esta manera, se podrá evitar poner en peligro la información empresarial. Los riesgos se determinan principalmente a partir de la identificación de amenazas y vulnerabilidades para un sistema, los riesgos se categorizan por nivel de importancia, probabilidad de ocurrencia e impacto. Un plan de mitigación y tratamiento de riesgos se constituye a partir de la aplicación de controles de seguridad (Castiblanco y Oviedo Regueros, 2017).
- La actual norma GTC-ISO/IEC 27002:2015 no cuenta con directrices de seguridad para la protección de dispositivos móviles sobre escenarios de tipo pandemia, es por esta razón que se presenta un nuevo control de seguridad bajo el enunciado diecinueve punto uno.

La terminología empleada para los nuevos controles del enunciado 19.1, el cual hace mención a la seguridad de la información sobre dispositivos móviles, son los siguientes:

Heatseat: es un término en ingles que hace referencia a un tipo de auriculares que incluye sistema de microfonía para apoyar las comunicaciones de tipo virtual, como lo son las videoconferencias, que se dan comúnmente en ambientes corporativos

Asistente de Google: es una aplicación de mensajería conversacional en ambas vías desarrollada por Google y lanzada al mercado en el 2016; la aplicación tiene la particularidad de asistir al usuario con tareas como hacer búsquedas en Internet, crear eventos en el calendario, hacer llamadas, recibir notificaciones audibles y escuchar y responder mensajes en aplicaciones de chat (Asistente de Google, 2021; Tillman, 2021).

Bose QuietComfort 35 II: es un tipo de auriculares inalámbricos creado por el fabricante Bose y lanzado al mercado en el 2016; es considerado uno de los mejores auriculares en el control de cancelación del ruido, duración de batería y por su gran facilidad para conectarse con la aplicación del Asistente de Google sin necesidad de decir "Ok Google". Adicionalmente, estos auriculares cuentan con la capacidad de leer automáticamente todas las notificaciones y mensajes que llegan al dispositivo móvil (Culturasonora, s.f.).

Debido a los obstáculos jurídicos y sobre carga operativa que presenta el actual control del teletrabajo en la norma GTC-ISO/IEC 27002:2015 se desarrolla un nuevo control de seguridad expuesto bajo en enunciado diecinueve punto dos.

La terminología considerada para los controles del enunciado 19.2, el cual hace mención al concepto de trabajo remoto consensuado, son los siguientes:

- Teletrabajo: el teletrabajo es una modalidad de trabajo densamente regulada bajo la Ley 1221 del 16 de julio de 2008 y actualmente vigente en materia laboral, la cual impone al empleador el cumplimiento de una serie de requisitos operativos y jurídicos, como el

amparar al colaborador con un puesto de trabajo, conexión a Internet, servicio de luz, agua, telefonía, inspección domiciliaria para la valoración de los riesgos laborales, modificación al contrato del colaborador, reporte ante la ARL, entre otros (Congreso de la República de Colombia, 2008; Redacción El País, 2020).

- Trabajo remoto en casa: el trabajo remoto es una modalidad laboral dispuesta gracias a la excepción del evento pandémico, habilitada mediante la circular 021 de 2020, la cual permite a las empresas contar con alivios operativos, jurídicos y económicos para implementar este tipo de trabajo (Ministerio del Trabajo, 2020).

Considerando la diferencia que existe actualmente entre estos dos conceptos y su relevancia en el desarrollo del presente proyecto, se presenta a través de la Tabla 1 los aspectos más sobresalientes entre el teletrabajo y el trabajo remoto, con el cual se pretende facilitar su entendimiento.

Tabla 1.

Tabla comparativa entre el concepto del teletrabajo y trabajo remoto en casa.

	Teletrabajo	**Trabajo remoto en casa**
Modalidad y regulación	Modalidad de trabajo no presencial definida por la Ley 1221 del 16 de julio de 2008.	Modalidad de trabajo no presencial definida mediante circular 021 de 2020, dictada por el Gobierno colombiano.
Propósito	Establecer las medidas regulatorias y contractuales para el contrato de trabajo que no requiere de la presencia física del colaborador en la organización.	Establecer las medidas para el trabajo remoto en casa por situación excepcional de emergencia sanitaria causada por la COVID-19.

Cobertura de protección en materia de seguridad y salud en el trabajo	A cargo del empleador.	A cargo del colaborador.
Determinación de riesgos en el desarrollo de las actividades de trabajo	El empleador determina los riesgos y brinda recomendaciones de seguridad.	El colaborador deberá comunicar los riesgos al empleador.
Puesto de trabajo	Amparado por el empleador.	Asumido por el colaborador.
Recursos como conexión a Internet, servicio de luz, agua y telefonía para el desarrollo de actividades laborales	A cargo del empleador.	El empleador no está obligado a suministrar estos recursos.
Equipo de cómputo	Suministrado por el empleador.	Puede ser suministrado por el empleador o el colaborador.
Condiciones del trabajo	Se determinan mediante el contrato de trabajo.	Las condiciones de trabajo se precisan mediante comunicación declarada por estado de emergencia.
Medios para el desarrollo de actividades	Mediante el uso de tecnologías de telecomunicaciones e Internet.	Mediante el uso de tecnologías de telecomunicaciones e Internet, si la naturaleza de las actividades lo permiten.
Lugar donde se realiza el trabajo	En el domicilio del colaborador o en el lugar que estime conveniente.	En el domicilio del colaborador o un lugar de aislamiento definido.

Fuente: elaboración propia a partir de Congreso de la República de Colombia (2008) y Ministerio de Trabajo (2020).

La actual norma GTC-ISO/IEC 27002:2015 no dispone de medidas de seguridad para proteger los activos de información como el recurso humano ante la eminente amenazas de tipo

pandemia, por este motivo se desarrolla un nuevo control de seguridad expuesto bajo en enunciado diecinueve punto tres.

Consideraciones para los controles del enunciado 19.3, el cual hace mención a la seguridad poscovid para el recurso humano:

Resolución 223 de 2021: mediante el cual se establecen las decisiones normativas de adopción del protocolo general de bioseguridad para mitigar la propagación del coronavirus COVID-19 y en el cual se establecen medidas de distanciamiento físico entre personas, lavado frecuente de manos, reporte y monitoreo de síntomas relacionados con el virus, el cual aplica para trabajadores del sector público y privado (Ministerio de Salud y Protección Social, 2021).

Gestiona2Latam: es una organización colombiana fundada en el 2013 que se dedica al desarrollo de *software* orientado a la optimización y automatización de procesos dentro de las diferentes áreas de una organización, mediante la gestión de sus bases de datos (Gestiona2, s.f.a).

Extreme Networks: es un fabricante estadounidense fundado en el 1996, este se dedica al desarrollo y venta de soluciones de conexión a red alámbrica e inalámbrica basadas en *hardware* y *software*. Extreme Networks cuenta actualmente con gran variedad en líneas de producto que denomina: ExtremeSwitching, ExtremeRouting, ExtremeWireless, ExtremeApplications, ExtremeAnalytics, ExtremeLocation, ExtremeCloud IQ y Extreme AirDefense (Extreme Networks, 2021a).

ExtremeLocation: es una solución tecnológica dentro de la línea de aplicaciones del fabricante Extreme Networks, esta permite el análisis de ubicación en interiores, la

cual admite, entre otras cosas, el control y flujo del personal en zonas determinadas dentro de las instalaciones de la organización (Extreme Networks, 2021b).

La actual norma GTC-ISO/IEC 27002:2015 no dispone de directrices de seguridad de la información sobre herramientas de videoconferencia y colaboración las cuales han sido altamente utilizadas en el ejercicio del trabajo remoto en medio del aislamiento social por COVID-19, por este motivo se desarrolla un nuevo control de seguridad expuesto bajo en enunciado diecinueve punto cuatro.

La terminología empleada para los controles del enunciado 19.4, el cual hace mención a la seguridad en videoconferencia y colaboración, se presenta a continuación:

Herramienta de colaboración: es una aplicación digital que brinda solución a los problemas de ubicación y limitación física, diseñada para facilitar la comunicación e integración de los colaboradores en el ámbito empresarial y, de esta manera, contribuir en el desarrollo del trabajo colaborativo.

Cifrado de datos: también mencionada como encriptación, se trata de una técnica de seguridad utilizada para proteger la información ante un evento de interceptación; en este caso, el cifrado se utiliza para proteger los datos a medida que estos son transmitidos sobre la herramienta de colaboración, Esta característica de seguridad hace que los caracteres del mensaje original sean modificados mientras estos salen de su origen y al momento de llegar a su destino son descifrados y reensamblados (Fernández, 2020b).

ATP: cuyas siglas representan *Advanced Threat Protection* o protección avanzada contra amenazas, es una característica de seguridad inmersa en la solución de

colaboración de Microsoft Teams, es un módulo de seguridad que centra sus esfuerzos en minimizar riesgos y prevenir la ocurrencia de ataques a la información.

Protocolo SIP: es un protocolo de inicio de sesión a través de una red IP mediante el cual se lleva a cabo el establecimiento, modificación y finalización de una comunicación entre dos dispositivos. SIP es empleado para las comunicaciones de voz, video y mensajería instantánea (Sánchez, 2018).

TLS: cuyas siglas representan *Transport Layer Security*, este protocolo se encarga de agregar cifrado a los datos para asegurar la transferencia de la información entre el cliente y el servidor (Microsoft, 2021a).

MTLS: siglas son la condensación de las palabras *Mutual Transport Layer Security*, este protocolo permite reconocer la identidad de un servicio mediante el intercambio de certificados de seguridad entre servidores (Microsoft, 2021a).

SRTP: cuyas siglas representan *Secure Real–Time Transport Protocol*, este protocolo es usado para asegurar la transmisión de datos multimedia y es usado por la aplicación Microsoft Teams para cifrar los datos multimedia en el tránsito de cliente a cliente (Microsoft, 2021a).

Rol de organizador: este tipo de participante debe contar con licencia de cuenta empresarial y tiene la capacidad de crear y programar reuniones, además puede tener el control sobre los demás participantes; el organizador de las reuniones también puede convertir a un asistente en moderador (Microsoft, 2021a).

Rol de moderador: este participante cuenta con la facultad de poder presentar la sesión, previa autorización del organizador (Microsoft, 2021a).

Rol de asistente: este participante es catalogado como un usuario invitado para presenciar la reunión, bajo este rol se encuentra impedido para actuar como moderador (Microsoft, 2021a).

HIPAA: estas siglas representan Ley de Responsabilidad y Portabilidad del Seguro de Salud (*Health Insurance Portability and Accountability Act*). Se trata de una ley del sector salud de los Estados Unidos y es la encargada de proteger la privacidad e integridad de la información de los usuarios.

GDPR: estas siglas significan el Reglamento General de Protección de Datos (*General Data Protection Regulation*) y hablan sobre el reglamento para la protección de datos de los individuos de la Unión Europea.

FedRAMP: estas siglas se refieren al Programa de Administración de Autorizaciones y Riesgos Federales. Se trata de un programa del Gobierno de los Estados Unidos para la evaluación de la seguridad y monitoreo de productos y servicios en la nube.

SOC: esta sigla simboliza al Centro de Operaciones de Seguridad (*Security Operations Center*).

FERPA: es la sigla de la Ley de los derechos educativos y la privacidad familiar (*Family Educational Rights and Privacy Act*).

ISO 27001: es el estándar de seguridad de la información que establece la estructura y requisitos para establecer, implementar, operar y mejorar un sistema de seguridad de la información (SGSI).

ISO 27018: es la norma que propone la aplicación de buenas prácticas para la protección de la información en la nube.

Acoustic Fence: es la tecnología de Polycom que integra el uso de un procesador digital DSP con múltiples micrófonos para la cancelación de ruidos y voces, de esta manera, el ruido de baja frecuencia es filtrado para que solamente la frecuencia de voz del participante de la sesión de videoconferencias pueda ser escuchado de manera clara por los demás usuarios (Polycom, s.f.).

A partir de los cambios culturales que se han dado tras la llegada de la pandemia de COVID-19 ycon el trabajo remoto en casa, han quedado obsoletas todas las medidas de seguridad de tipo perimetral para la protección de la información, originalmente propuestas en la actual norma GTC-ISO/IEC 27002:2015 por este motivo se desarrolla un nuevo control de seguridad expuestobajo en enunciado diecinueve punto cinco.

La terminología y programas empleados para los controles del enunciado 19.5, el cual hace mención a la extensión de la seguridad en el desvanecimiento del perímetro corporativo, se presenta a continuación:

Monitoreo GPS: es una tecnología de posicionamiento global que permite la identificación de ubicación y rastro geográfico de un bien o dispositivo en tiempo real.

Geoposicionamiento: es una técnica de seguimiento geográfico que permite precisar una determinada posición de un elemento o persona sobre un plano cartesiano con el mayor índice de precisión posible.

Prey: solución de *software* para el rastro y administración de equipos de cómputo y dispositivos móviles desarrollados por la empresa chilena Prey Inc, que actualmente opera en Chile y Estados Unidos. La solución es usada para la protección de

aproximadamente nueve millones de dispositivos alrededor de todo el mundo (Prey [software], 2021).

DLP: cuyas siglas representan *Data Loss Prevention*, en español, “prevención de perdida de datos”, esta es una solución de *software* que se encarga de monitorear, detectar y bloquear acciones atribuibles a las transmisiones de datos no autorizadas para la protección a alto nivel de los datos sensibles como información financiera, propiedad intelectual u otro tipo de información definida por la organización (Software de prevención de pérdida de datos, 2021).

ForcePoint: empresa estadounidense fundada en 1994, dedicada al desarrollo de productos de seguridad informática. Dentro de sus productos cuenta con soluciones de seguridad de tipo *firewall* de próxima generación, seguridad web, SASE (*secure access service edge*, “servicio de acceso seguro de borde”) y DLP (*data loss prevention*, “prevención de perdida de datos”). La solución DLP de ForcePoint es destacada en el mercado sobre otros fabricantes (Forcepoint, 2021).

Las directrices de seguridad propuestas por la actual norma GTC-ISO/IEC 27002:2015 para la protección a los servicios de red, tienen un alcance limitado y no contempla la aplicación de medidas de seguridad para los servicios de red de tipo distribuido; ahora requeridos para los escenarios del trabajo remoto, por este motivo se desarrolla un nuevo control de seguridad expuesto bajo en enunciado diecinueve punto seis.

Finalmente, la terminología empleada para los controles del enunciado 19.6, el cual hace mención a la seguridad en las comunicaciones distribuidas, es la siguiente:

VPN: cuyas siglas representan *Virtual Private Network* y hace referencia a una red privada de tipo virtual, es una tecnología que permite el redireccionamiento del tráfico de red a través de un canal seguro mediante la encriptación de los datos que son transmitidos. Las VPN pueden establecerse de modo sitio a cliente o sitio a sitio, estas últimas son implementadas para conectar oficinas remotas con la sede central de la organización (De Luz, 2019).

AP30: adaptador para la conexión de red corporativa segura mediante acceso VPN y que permite una conexión inalámbrica automatizada, extendiendo la red corporativa de la organización hacia cualquier sitio remoto.

Virtual Appliance: es un concepto utilizado en el campo del cómputo y se refiere a la optimización de recursos, el cual se crea para alojar un solo servicio o aplicación de red con un propósito específico (Virtual Appliance, 2021).

Materiales y métodos

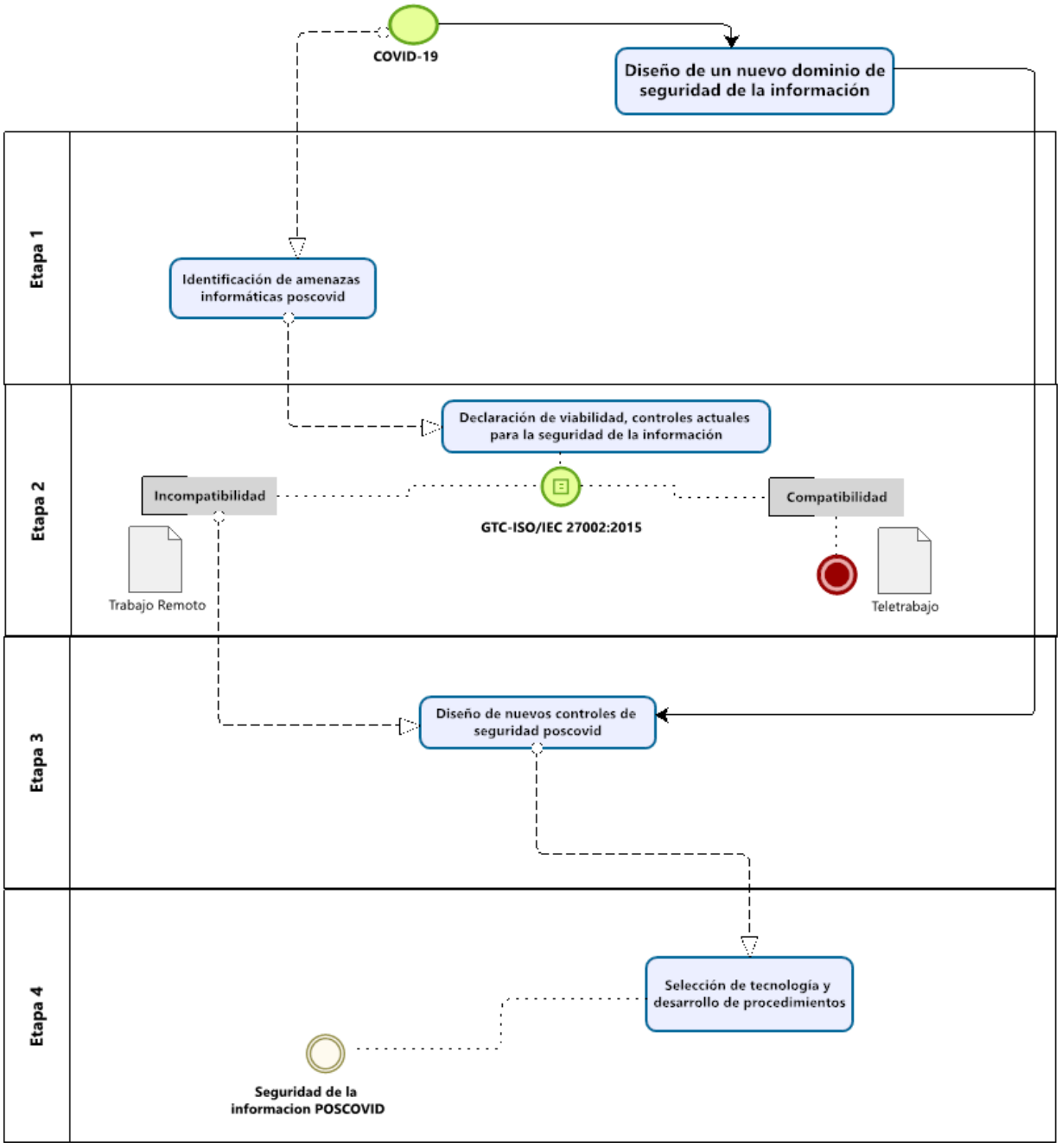
Metodología

El proceso metodológico que se llevó a cabo para el diseño del nuevo dominio de seguridad de lainformación propuesto en este proyecto, tal y como lo relaciona en la Figura 1, consistió en cuatro etapas principalmente, nombradas de esta manera: 1. Identificación de amenazas; 2.

Demostración de los vacíos de la actual norma GTC-ISO/IEC 27002:2015; 3. Diseño de nuevos controles de seguridad de la información; y 4. Selección de tecnologías y prácticas adecuadas para la protección de la información. A continuación, se describe con detalle la ejecución de cadaetapa planteada y el caso de estudio tomado como base para aplicación de esta metodología.

Figura 1.

Esquema del diseño metodológico.



Fuente: elaboración propia.

Caso de estudio

Esta metodología fue aplicada a la empresa ProCibernetica, para quienes la seguridad de la información es un asunto de alta importancia. ProCibernetica es una empresa colombiana y de tipo privada. La llegada de la pandemia COVID-19 en el primer semestre de 2020, obligó a ProCibernetica, a la sociedad colombiana y del mundo entero, en general, a establecer medidas de confinamiento y aislamiento social con el propósito de mitigar la rápida propagación del virus, y como medida de contingencia ProCibernetica tuvo que recurrir a la modalidad del trabajo remoto para lograr contar con el apoyo de sus colaboradores y dar continuidad a las actividades laborales; asimismo, contribuir con las medidas de aislamiento fomentadas por el Gobierno nacional. No obstante, para ProCibernetica siempre ha sido primordial y de muy alto valor la seguridad de su información y la de sus clientes, sin importar las dinámicas a las que esta deba adherirse para prolongar y reforzar la seguridad de la información, dando lugar a los controles de seguridad que su operación le demande. Ahora en medio de esta problemática de la COVID-19 y la modalidad de trabajo remoto desde casa, la organización precisó:

1. Disponer de la mejor tecnología de seguridad para proteger su información corporativa, sin importar las variables presentes en los escenarios de trabajo remoto de sus colaboradores.
2. Contar con una solución de tipo *plug & play* para facilitar la instalación y uso por parte de sus colaboradores de perfil no técnico.
3. Lograr reducir responsablemente los costos adicionales que le ocasionaría incursionar en la modalidad del teletrabajo en medio de la crisis poscovid.
4. Establecer medidas de seguridad poscovid para los dispositivos móviles de sus colaboradores.

5. Implementar una solución tecnológica que respalde la automatización en el reporte de síntomas de la COVID-19 de sus colaboradores.
6. Disponer de la tecnología y aplicación de prácticas adecuadas para proteger la información que se produce, recibe y transmite a través de las herramientas de videoconferencia y colaboración.
7. Disponer de una tecnología para controlar el inventario de cómputo que se encuentra distribuido geográficamente en medio de la operación del trabajo remoto.
8. Considerar el uso de una solución de seguridad para prevenir el robo y fuga de información sensible.
9. Contar con una solución tecnológica que le permita controlar los índices de ocupación para el aislamiento social al interior de la organización, al momento de retornar a la presencialidad.
10. Implementar un plan de sensibilización en seguridad de la información para que sus colaboradores logren actuar de manera responsable ante futuros eventos de crisis.

Este proyecto tuvo como reto principal el diseño de nuevos controles de seguridad para la protección de la información sobre los nuevos escenarios de trabajo remoto, ocasionados por las políticas de confinamiento social que ha generado la crisis actual, tanto mundial como local, a causa de la pandemia COVID-19 (Presidencia de la República de Colombia, 2020a).

Una vez formulado el caso de estudio, se procedió al diseño del nuevo dominio de seguridad de la información para los entornos de trabajo remoto, el cual se llevó a cabo mediante las siguientes etapas:

Etapa 1. Identificación de amenazas informáticas en el contexto de la COVID 19

Esta etapa consistió en la identificación del aumento de amenazas informáticas generadas por la aparición de la COVID-19. Con base en la revisión bibliográfica se afirmó que la pandemia ha dado origen al incremento de múltiples amenazas cibernéticas por parte de ciberdelincuentes y a la manifestación de nuevas vulnerabilidades sobre los diferentes sistemas de las organizaciones. La causa principal es que sus plataformas no estaban preparadas para operar apropiadamente ante este nuevo escenario, igualmente, es debido a que la seguridad de la información no es un concepto elemental ni básico en sí mismo, puesto que sería fácil su aplicación para resolver el problema, solamente con el uso de un hardware de seguridad determinado; sin embargo, esto va más allá y trasciende al empleo de procedimientos, políticas adecuadas, campañas de concientización para los usuarios y de un adecuado plan de gestión de riesgos (Berrios, 2020).

Por otra parte, con base en la revisión exhaustiva de diferentes fuentes, se logró identificar los vectores de ataque más significativos en el marco de la pandemia, tales como: *Denia of service* (DoS), *Payment fraud*, *Sociallity engineered threats* (*phishing*, *fraud*), *Malware* (*worms*, *viruses*, *spam*), *Ransonware*, *Zoombombing*, entre otros. Estos ataques han impactado económicamente a diferentes organizaciones y ha afectado sus activos informáticos, en consecuencia, su productividad, reputación e imagen corporativa y aspectos de tipo legal. Posterior a la identificación de amenazas se procedió a la etapa dos la cual se describe a continuación.

Etapa 2. Observación y declaración de limitaciones de seguridad de la GTC-ISO/IEC 27002:2015

Esta etapa consistió en el análisis de los ciento catorce controles expuestos por la norma GTC-ISO/IEC 27002:2015 (Icontec, 2015). De esta lista, se identificaron y extrajeron ocho controles que contienen directrices de seguridad para proteger los puestos de trabajo remoto y otras variables para la seguridad poscovid, los cuales se relacionan en la Tabla 2. Aunque, la guía contenga este tipo de controles para la protección de la información, en este escenario mundial de pandemia, mediante este análisis, se evidenció que estos controles tienen un alcance limitado, ya que no contemplan directrices de seguridad en el marco de las crisis de tipo pandémico.

Dado lo anterior, en esta etapa del proyecto, se describieron los vacíos identificados por cada control de seguridad mencionado en la Tabla 2. Mediante la ejecución de esta etapa, se consiguió resaltar las insuficiencias de cada control en la seguridad de la información en medio de las nuevas variables del trabajo remoto y otras variables para la seguridad poscovid.

Tabla 2.

Listado de controles de seguridad declarados insuficientes para la protección de la información poscovid.

ID Control	Dominio	Descripción
6.2.1	Organización de la seguridad de la información.	Política para dispositivos móviles.
6.2.2		Teletrabajo.
7.2.1	Seguridad de los recursos humanos.	Responsabilidades de la dirección.
9.1.1	Control de acceso.	Política para el control de acceso.
10.1.1	Criptografía.	Uso de controles criptográficos.
11.1.1	Seguridad física y de entorno.	Seguridad de perímetro físico.

13.1.2	Seguridad de las comunicaciones.	Seguridad a los servicios de red.
17.1.1	Seguridad de la información para la continuidad de negocio.	Continuidad a la seguridad de la información ante situaciones adversas o de crisis.

Fuente: elaboración propia.

Etapa 3. Diseño y desarrollo de un dominio de seguridad para satisfacer las necesidades de protección a la información poscovid

Concluida la etapa anterior y basándose en el alcance limitado de la actual GTC-ISO/IEC 27002:2015 se procedió al diseño de un nuevo dominio de seguridad de la información, el cual se compuso por una serie de nuevos controles de seguridad, los cuales tuvieron como finalidad perfeccionar la actual GTC-ISO/IEC 27002:2015 para resarcir los vacíos que en efecto tiene actualmente dicha norma, estos vacíos también han sido declarados por la organización BSI Group de España (BSI Group, 2021).

El diseño del nuevo dominio de seguridad se fundamentó en las necesidades de protección para los activos de información de la empresa ProCibernetica en el marco del escenario de trabajo remoto pospandemia; dichas necesidades obedecieron a los siguientes motivos:

Para el diseño del control 19.1.1 se establecieron planes de capacitación para la generación de conciencia en los colaboradores en cuanto a la manipulación de sus dispositivos móviles para mitigar los nuevos riesgos poscovid para los activos de información.

Para el diseño del control 19.1.2 se estableció, como política dentro de la organización, el uso de accesorios tecnológicos como auriculares inteligentes junto al asistente de voz para minimizar la exposición y manipulación de los dispositivos móviles por parte de los colaboradores.

En el control 19.2.1 se estableció el acuerdo político legal para el trabajo remoto en casa, bajo las mejores condiciones para la organización.

Para el control 19.3.1 se planteó una solución tecnológica para reportar los autodiagnósticos de síntomas de la COVID-19 de manera automatizada.

Para el control 19.3.2 se propuso el uso de tecnologías de geoposicionamiento dentro de las instalaciones de la organización para controlar los índices de aislamiento social y verificación de posibles contagios ante la retoma de actividades de forma presencial.

Estimando el incremento de uso de herramientas de videoconferencia y colaboración en medio de la operación de trabajo remoto, así como también de las vulnerabilidades y nuevas amenazas hacia estas plataformas, mediante los controles 19.4.1 y 19.4.2, se estableció la creación de un nuevo procedimiento de seguridad informática en la organización para la aplicación de buenas prácticas al momento de usar el sistema de videoconferencia y colaboración. Adicionalmente, sobre las herramientas de colaboración más destacadas del mercado se analizaron las características de seguridad de cada una de estas para que finalmente ProCibernetica pudiera implementar la herramienta de colaboración más segura y proteger su información.

Para el control 19.5.1 se estableció el uso de una tecnología para el control, monitoreo y movilidad de equipos de cómputo y dispositivos móviles asignados a los colaboradores para el trabajo remoto.

Para el control 19.5.2 se estableció el uso de una tecnología sobre los equipos de punto final para impedir cualquier intención de fuga de datos empresariales fuera del dominio corporativo.

Para el control 19.6.1 se determinó el uso de tecnología VPN, tipo *hardware*, de uso esencial para la protección de los canales de comunicación en el domicilio de los trabajadores remotos.

Para el control 19.7.1 se estableció la creación de una nueva política dentro de la organización para promover la cultura de la ciberseguridad, mediante capacitaciones de sensibilización para la protección de la información en medio de nuevas situaciones de crisis e impacto social.

Etapa 4. Determinar el uso de tecnología y aplicación de procesos con base en el nuevo dominio de seguridad

La etapa final se llevó a cabo a partir de los controles de seguridad definidos en la etapa tres, con base en estos se derivó la elección de tecnologías adecuadas y el desarrollo de buenas prácticas para la protección de la información poscovid.

Para la identificación de las diferentes tecnologías requeridas, se tuvo en cuenta el objetivo de cada uno de los once controles propuestos en la etapa tres del presente proyecto; de los cuales siete de estos obedecen a la incorporación de nuevas tecnologías para ProCibernetica y los cuatro controles restantes hacen referencia al desarrollo y ejecución de nuevas prácticas de seguridad.

La elección de las tecnologías apropiadas se basó en la exploración inicial de varios fabricantes, junto a sus características y funcionalidades, con el objetivo principal de hallar soluciones especializadas que cuenten con: alta calidad, respaldo técnico, prestigio, visión y experiencia. A continuación, se presentan algunas de las necesidades más relevantes que se consideraron para la elección de los diferentes fabricantes, con el fin de dar solución a los siete controles mencionados anteriormente.

La elección de la tecnología para el control 19.1.2 se centró en descubrir una composición tecnología que apoyara una de las políticas de bioseguridad expuesta en la Resolución 223

(Ministerio de Salud y Protección Social, 2021), que hace referencia a evitar la exposición de los teléfonos celulares.

La elección de la tecnología para el control 19.3.1 se apoyó en la necesidad de controlar con precisión y rigurosidad los registros y estadísticas de reporte de síntomas de la COVID-19, tal como fue establecido oficialmente a través de la Resolución 223 de 2021.

La elección de la tecnología para el control 19.3.2 se sustentó en la necesidad de dar cumplimiento al protocolo de bioseguridad establecido mediante la Resolución 223 (Ministerio de Salud y Protección Social, 2021), con el cual también se promueve el uso de las tecnologías para controlar el distanciamiento social y evitar aglomeraciones.

La elección de la tecnología para el control 19.4.1 se realizó bajo el criterio de proteger la confidencialidad de la información, al mejor nivel posible, con base en el nuevo formato de audio y video en las herramientas de colaboración a través de Internet.

La elección de la tecnología para el control 19.4.2 se fundamentó en la necesidad de disponer de una solución que garantizara la integridad de la información mediante la eliminación de ruidos en las comunicaciones de voz.

La elección de la tecnología para el control 19.5.1 se sustentó en contar con una solución de gran trayectoria y experiencia para el control y monitoreo de inventario distribuido geográficamente.

La elección de la tecnología para el control 19.5.2 se fundamentó en encontrar la solución de mejor reputación y solidez con tecnología avanzada para prevenir, de la mejor manera posible, cualquier tipo de fuga de información sin importar que esta se encuentre fuera del perímetro físico de la organización.

La elección de la tecnología para el control 19.6.1 se apoyó en la necesidad de encontrar una solución que lograra extender la conexión hacia la sede principal de ProCibernetica, manteniendo la seguridad de extremo a extremo y que eludiera las vulnerabilidades presentes en algunas conexiones wifi, además de ser de fácil instalación para los colaboradores de perfil no técnico y que fuera provista por un fabricante destacado en el ofrecimiento de soluciones de red.

Análisis de resultados

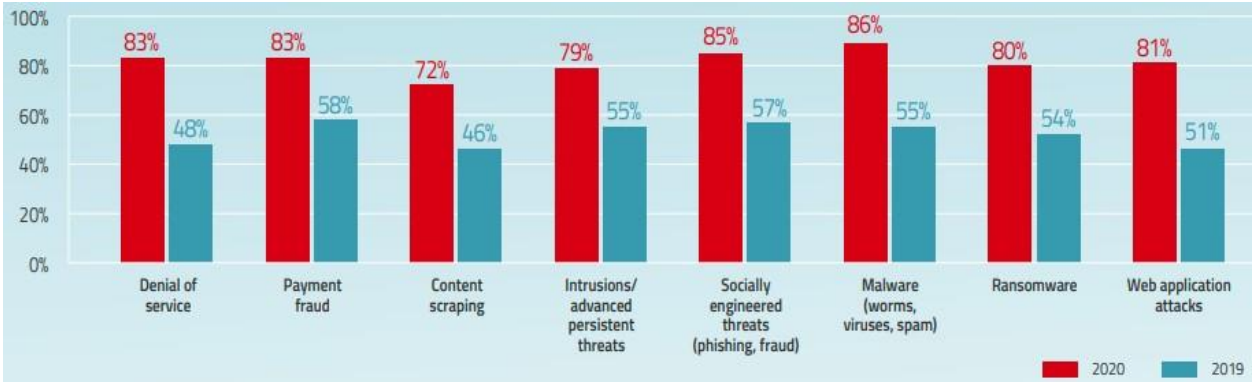
Comportamiento de amenazas informáticas poscovid

Descritas algunas de las amenazas informáticas más comúnmente destacadas en el ámbito cibernético, es importante precisar que según Radware, reconocido fabricante de servicios avanzados de seguridad cibernética, se concluye que la pandemia COVID-19 ha afectado notoriamente la seguridad de la red y los incidentes de seguridad no resueltos pueden ser aún más desastrosos que la misma pandemia; además que las organizaciones tienen un importantereto en la seguridad de sus datos a medida que adaptan sus operaciones remotas a gran escala (Radware, 2020).

En la Figura 2, se relacionan los vectores de ataque que más aumentaron como resultado de la pandemia, los cuales fueron identificados a partir de la exploración bibliográfica realizada durante la primera etapa de este proyecto.

Figura 2.

Vectores de ataque en creciente aumento según el fabricante Radware.



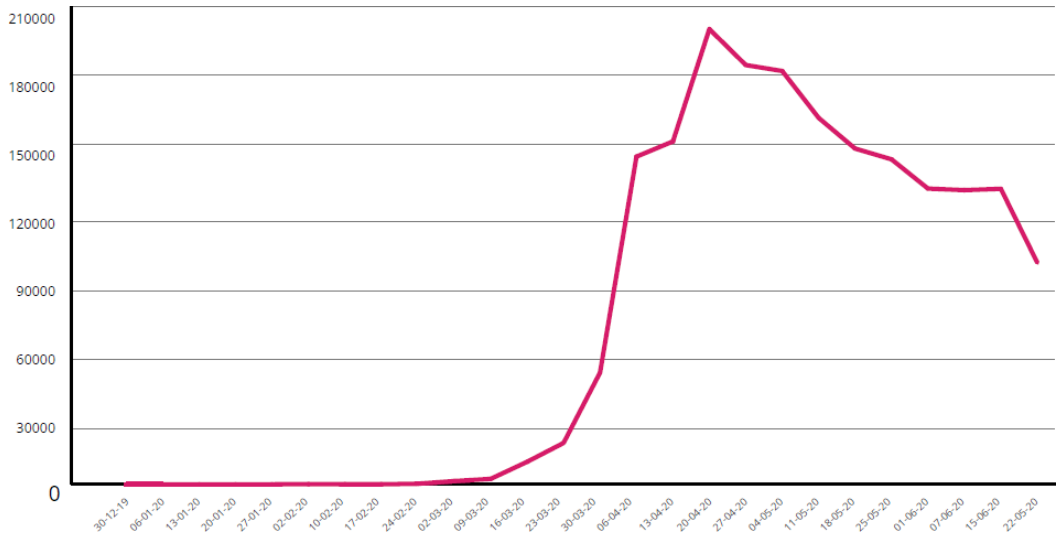
Fuente: tomado de Radware (2020, p. 15).

Por otra parte, de acuerdo con el mapa mundial de amenazas cibernéticas publicadas por el fabricante Check Point —proveedor de soluciones de seguridad de TI y pionero en la industria

de la seguridad de perímetro—, encontró que, en las primeras semanas en las que se masifico la proliferación de la pandemia COVID-19, aumentaron considerablemente los ataques de tipo *malware*, los cuales utilizaron técnicas de *socially engineered* relacionadas a la COVID-19. En la Figura 3, se evidencia el drástico y exponencial aumento de ataques informáticos tras la llegada del coronavirus (Check Point Software Technologies, 2020).

Figura 3.

Aumento de ataques informáticos relacionados con el coronavirus presentada por el fabricante Check Point.



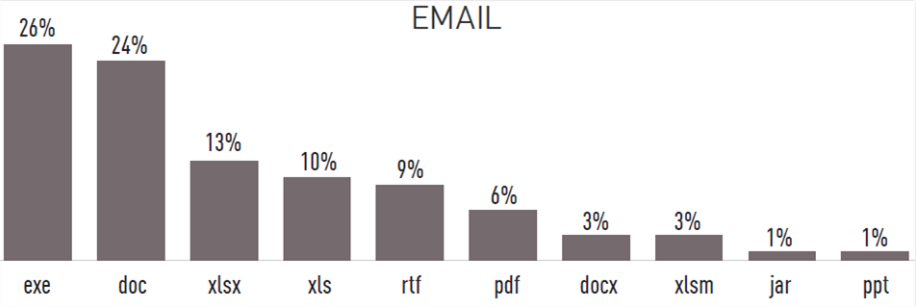
Fuente: tomado de Check Point Software Technologies (2020, p. 4).

En la anterior figura, se observa con claridad que desde la segunda semana de marzo de 2020 inició el aumento de ataques informáticos de tipo malware que utilizaron técnicas de ingeniería social con trampas de temáticas relacionadas con la COVID-19, y a mediados de abril de 2020 se registró el pico máximo de estos ataques.

De acuerdo con un estudio realizado por Check Point, el cual rastreo los ciberataques producidosen tiempo real sobre su plataforma tecnológica; además detectó, como se ve en la Figura 4, los principales tipos de archivos maliciosos recibidos mediante el correo electrónico.

Figura 4.

Tipos de archivos maliciosos recibidos mediante el correo electrónico.



Fuente: tomado de Check Point Software Technologies (2020, p. 11).

El crecimiento de las amenazas informáticas también viene siendo una constante que va en aumento sobre el territorio colombiano, mucho más a partir de la llegada de la COVID-19, junto con los nuevos hábitos del trabajo remoto desde casa. Estos son escenarios que en la gran mayoría de casos se habilitaron sin las debidas medidas de seguridad informática, claramente lo vemos reflejado en el aumento de los delitos informáticos e incidentes cibernéticos que detecto la Policía Nacional de Colombia desde su centro cibernético policial. En la Tabla 3, se enlistan los diferentes delitos informáticos manejados por la Policía Nacional y, adicionalmente, se muestra el aumento de denuncias entre el 2019 y 2020 (Castellanos Vega, 2020).

Tabla 3.

Registro de denuncias por infracción a la ley de delitos informáticos.

Infracciones a la Ley 1273 de 2009	Denuncias año 2019	Denuncias año 2020	Aumento
Hurto por medios informáticos y semejantes.	466	670	144 %
Acceso abusivo a un sistema informático.	159	433	272 %
Violación de datos personales.	183	314	172 %
Suplantación de sitios web para capturar datos personales.	51	308	604 %
Transferencia no consentida de activos.	90	120	133 %
Interceptación de datos informáticos.	27	92	341 %
Uso de ***software*** malicioso.	39	47	121 %
Daño informático.	7	27	386 %
Obstaculización ilegítima de sistema informático o red de telecomunicación.	3	5	167 %
Total:	1025	2016	197 %

Fuente: adaptado de Castellano Vega (2020).

Reconocimiento de vacíos de seguridad en la GTC-ISO/IEC 27002:2015 con relación a los nuevos desafíos de seguridad poscovid

A continuación, se describen las insuficiencias que contienen los controles de seguridad relacionados en la tabla 2, los cuales fueron extraídos de la actual guía técnica GTC-ISO/IEC 27002:2015 (versión oficial). Estos controles presentan vacíos al pretender hacer uso de las

actuales directrices sobre los nuevos entornos de trabajo remoto y otras variables para la seguridad poscovid.

Insuficiencia del control 6.2.1 de la GTC-ISO-IEC 27002:2015 para la seguridad sobre los dispositivos móviles

El control 6.2.1 de la guía GTC-ISO/IEC 27002:2015 (Icontec, 2015) es insuficiente para lograr una cobertura de aplicación en cuanto a las adecuadas medidas de seguridad que propendan a garantizar la mitigación de la propagación del virus SARS CoV-2 (COVID-19), debido a la falta de conciencia por parte de los usuarios a la hora de usar físicamente los dispositivos móviles, los cuales habitualmente son manipulados y exhibidos a una constante movilidad física por parte de los usuarios, por lo que estos dispositivos son frecuentemente expuestos a diferentes ambientes y lugares. De este modo, se deberían tener en cuenta los nuevos riesgos inherentes a los que se encuentran expuestas las personas en general sobre determinados ambientes, los cuales pueden afectar el adecuado estado de salud de cualquier trabajador. Se habla de esta manera reconociendo que el enfoque principal de SGSI se centra en la protección de sus activos, en el que todo activo de información es aquel elemento que contiene información de la empresa y habitualmente los colaboradores cuentan con un alto conocimiento sobre la empresa y sus negocios en su mente, por lo tanto, las personas son también claramente un activo para las organizaciones (ISO Win, 2017).

En este caso, se hace alusión al riesgo de salubridad al que está sujeta la humanidad desde el segundo semestre de 2019, gracias a la pandemia de la COVID-19.

Existen estudios científicos que demuestran que el aire es la principal ruta de transmisión para el contagio de la COVID-19 y en lugares poco ventilados este virus puede permanecer por varias horas flotando en el aire (de Quiroga, 2020; Rodriguez Mega, 2020).

A partir de esto, se debería crear una nueva directriz de seguridad sobre los dispositivos móviles, tanto a nivel de procedimiento que conlleve a evitar dejar los dispositivos móviles sobre superficies que podrían estar infectadas con el virus COVID-19, como también la incorporación de nuevos accesorios tecnológicos como un kit de manos libres para mitigar cualquier tipo de exposición para el colaborador; evitando que este tenga que manipular y exponer continuamente el dispositivo móvil sobre ambientes inseguros, con el fin de minimizar la propagación del virus el cual puede llegar a afectar a este u otro colaborador.

Insuficiencia del control 6.2.2 de la GTC-ISO-IEC 27002:2015 en relación con los entornos de teletrabajo

El control 6.2.2 de la guía GTC-ISO/IEC 27002:2015 (Icontec, 2015) habla sobre los entornos de teletrabajo. La aplicación de este control exige al cumplimiento de requerimientos de tipo jurídico para las empresas, puesto que el teletrabajo es una modalidad de trabajo densamente regulada y actualmente está vigente en materia laboral, establecido bajo la Ley 1221 (Congreso de la República de Colombia, 2008).

El esquema del teletrabajo, tal como se presentó en la tabla 1 en la cual se precisan las condiciones de esta modalidad de trabajo, dificultaría y prolongaría las posibilidades de que una empresa se adhiera a esta modalidad, sobre todo en medio de una situación de emergencia como la que se afronta en la actualidad, la cual fue oficialmente formalizada por medio del Decreto 417 (Presidencia de la República de Colombia, 2020a).

Es importante que un empleador tenga total claridad sobre lo concerniente al teletrabajo y lo que se viene conociendo como trabajo remoto, en pro de reanudar la economía del país en medio de la política de aislamiento social obligatorio, determinada por el Gobierno Nacional en el decreto 457 (Presidencia de la República de Colombia, 2020b).

Una importante y destacada agremiación colombiana con más de 45 años, orientada a contribuir al crecimiento económico del país y que cuenta con amplio conocimiento de la sociedad en general, ha identificado que a causa de la situación de la pandemia COVID-19 hay actualmente entre dos y tres millones de personas trabajando desde sus casas, obviando el cumplimiento normativo del teletrabajo (Rojas Castañeda, 2020).

Es preciso afirmar que, el teletrabajo, establecido mediante la Ley 1221 de 2008 y el Decreto 884 (Presidencia de la República de Colombia, 2012), consagra que tanto empresas públicas como privadas tengan que contribuir económicamente al teletrabajador para garantizar los recursos de conexión a Internet, servicio de energía, servicio de agua y de telefonía, como también, las herramientas imprescindibles para que el teletrabajador pueda realizar su trabajo adecuadamente (Castro de la Torres, 2021; Rojas Castañeda, 2020).

A partir de esto, se debería crear un nuevo control autónomo e independiente a lo establecido por el control A.6.2.2, en donde se establezcan las políticas de seguridad aplicables sobre la nueva figura de trabajo remoto en casa, reglamentada por medio de la Ley 2088 (Congreso de la República de Colombia, 2021) y, anteriormente, por la circular 21 del Ministerio del Trabajo (2020), la cual es considera como medida ocasional y transitoria mientras esté vigente la emergencia sanitaria (Mintrabajo, 2020).

La creación de un nuevo control alivianaría la carga operativa, jurídica y administrativa de las organizaciones y, a su vez, contemplaría la aplicación de nuevas tecnologías de seguridad

para la protección de los datos sobre los nuevos entornos donde será procesada, fuera de las oficinas.

Insuficiencia del control 7.2.1 de la GTC-ISO-IEC 27002:2015 en relación con las nuevas responsabilidades de la dirección

El control 7.2.1 de la guía GTC-ISO/IEC 27002:2015 (Icontec, 2015) se refiere a las responsabilidades de la dirección. Tal como se encuentra actualmente en la guía no se contempla la ejecución de medidas de control para que la organización se cerciore sobre el estado de salud de sus empleados, en medio de la situación de pandemia actual. Para esto se identifica que este control debería proponer una solución tecnológica que obligué al empleado a informar sobre su reporte de salud y síntomas previo a iniciar sus actividades laborales y a entrar en interacción con los demás colaboradores.

Insuficiencia del control 9.1.1 de la GTC-ISO-IEC 27002:2015 sobre las medidas de control de acceso

El control 9.1.1 de la guía GTC-ISO/IEC 27002:2015 (Icontec, 2015) evidentemente no contempla la aplicación de un control de acceso con el fin de verificar los casos de personas que posiblemente este infectadas con el coronavirus (COVID-19), y de este modo controlar y prevenir la propagación del virus dentro de la organización. En la actual situación, toda organización debería gestionar adecuadamente las condiciones de salubridad ante la COVID-19. Para el control de acceso se debe contar con una tecnología adecuada para medir y controlar tanto los niveles de distanciamiento como la interacción entre colaboradores, de modo que, estas puedan registrarse y ser verificadas para que al momento de conocerse un caso positivo con

COVID-19, la trazabilidad de este colaborador quede en el registro y sea parte de la solución, ya que permitiría identificar rápidamente las personas con las que el trabajador con coronavirus interactuó. Lo anterior, para lograr generar una alerta preventiva con los otros colaboradores que pudiesen haberse visto comprometidos.

Insuficiencia del control 10.1.1 de la GTC-ISO-IEC 27002:2015 para la aplicación de controles criptográficos

Este control es insuficiente y se queda escasa su aplicación sobre los nuevos escenarios de trabajo remoto, en los que se encuentra actualmente inmersa la sociedad a causa de la propagación del virus de la pandemia COVID-19. En especial, este control 10.1.1 (Icontec, 2015), excluye la aplicación de técnicas de criptografía sobre las aplicaciones de voz para los puestos de trabajo de los colaboradores de las organizaciones de tipo *callcenter*, que se encuentran trabajando remotamente desde sus casas; como el caso de las grandes organizaciones de *callcenter* de este país Teleperformance y Konecta Colombia, quienes tienen más de la mitad de su planta de colaboradores trabajando desde casa (Neira Marciales, 2020).

Las organizaciones deberían concientizar a sus colaboradores que atienden llamadas remotamente, a operar desde un recinto reservado con un adecuado nivel de aislamiento acústico, con el fin de evitar poner en riesgo la confidencialidad de la información que se comparte telefónicamente con los clientes y proveedores. La organización debería proveer la adecuada tecnología que propenda por la seguridad informática sobre las herramientas de voz y colaboración utilizadas por los colaboradores desde sus hogares; adicionalmente proporcionar las adecuadas herramientas físicas de audio y microfonía para perfeccionar la integridad y confidencialidad de la información que se comparte de manera audible.

Insuficiencia del control 11.1.1 de la GTC-ISO-IEC 27002:2015 relacionado con la habitual seguridad de perímetro

La aplicación de este control deja al descubierto los escenarios de trabajo remoto en casa, en los cuales se observa que los colaboradores ya no se encuentran aglomerados en una misma ubicación física o en una misma edificación para la ejecución de sus actividades laborales, sino que, a causa de la pandemia COVID-19, gran cantidad de organizaciones tuvieron que reinventar su manera de operar, permitiendo que sus colaboradores trabajaran desde sus casas (Redacción El País, 2020).

Por lo tanto, no son suficientes las directrices de seguridad determinadas por este control para las organizaciones que buscan proteger su información en la actualidad. Este control debería considerar los nuevos escenarios de trabajo donde los colaboradores se encuentra distribuidos cada uno de ellos en ubicaciones geográficas independientes, por lo que el concepto de perímetro ha venido desvirtuándose tanto desde la perspectiva física como lógica. Igualmente, este control debería contemplar el uso de una tecnología para controlar el inventario de dispositivos mediante monitoreo GPS, pues es importante mantener el control sobre los activos de la organización.

Insuficiencia del control 13.1.2 de la GTC-ISO-IEC 27002:2015 en relación con la seguridad en los servicios de red

La aplicación de este control se encuentra netamente enfocado a la seguridad de red corporativa, de tipo perimetral, para la protección de datos dentro de la organización. Este punto deja por fuera el brindar directrices de seguridad para los nuevos modelos de trabajo remoto, impulsados por la propagación del coronavirus (COVID-19). Este control debería contemplar el uso de herramientas tecnológicas que permitan asegurar las redes de tipo residencial (el hogar del

trabajador) desde donde se conectan los colaboradores para realizar su trabajo, por lo tanto, se puede considerar, por ejemplo, el uso de soluciones de servicio de acceso seguro de borde, de tipo *cloud* u otras.

Insuficiencia del control 17.1.1 de la GTC-ISO-IEC 27002:2015 en relación con las nuevas necesidades de seguridad

Aunque este control propone dar continuidad a las políticas de seguridad de la información sobre situaciones adversas, conservando los requisitos de seguridad de la información de la organización, su planteamiento es muy superficial y no contempla una situación adversa de pandemia. Tampoco se puede asumir que los requisitos de seguridad de una organización van a permanecer inmóviles, puesto que se ha comprobado con la pandemia COVID-19 que el impacto en materia de ciberseguridad fue muy importante y sigue afectando en diferentes escenarios la disponibilidad, integridad y confidencialidad de la información (Berrios, 2020).

Cabe entender que, toda situación adversa suele ser una condición difícil de sobrellevar y esta requiere de un tiempo determinado para implementar un plan de recuperación y continuidad. No obstante, para este tipo de situaciones, lo más efectivo y beneficioso para la organización es contar con un plan de educación y sensibilización para los colaboradores, acerca del manejo apropiado y cuidadoso de la información para mejorar continuamente la seguridad.

Dominio y controles de seguridad de la información propuestos para la era poscovid

El siguiente dominio de seguridad propuesto tiene como finalidad perfeccionar la actual guía técnica colombiana GTC-ISO/IEC 27002:2015, buscando llenar los vacíos que en efecto

tiene dicha guía, la cual en su etapa de diseño inicial no contemplo directrices de seguridad sobre la información frente a situaciones de crisis de salubridad por pandemias. Por lo tanto, de ninguna manera se pretende desvirtuar ni desvalorar la actual guía GTC-ISO/IEC 27002:2015. En cambio, se presenta la propuesta de un nuevo dominio de seguridad continuo al último presentado por la actual guía, es por este motivo que el nuevo dominio de seguridad propuesto inicia a partir del numeral diecinueve (19) y de esta manera dar continuidad a la guía actual.

19. Seguridad transversal para los contextos de tipo pandemia

19.1 Seguridad poscovid sobre dispositivos móviles

Objetivo: establecer lineamientos de seguridad física preventiva para la aplicación de procedimientos seguros y uso de tecnología para mitigar la propagación del virus pandémico.

- 19.1.1 Buenas prácticas poscovid para la seguridad preventiva sobre dispositivos móviles.

  Control**:** en caso de movilidad, se deberían establecer planes de capacitación para la generación de conciencia en los colaboradores, en cuanto a la manipulación responsable de los dispositivos móviles, reconociendo que los virus de tipo pandémico podrían estar presentes en cualquier superficie, sobre todo en recintos cerrados y con poca ventilación. Se debería desinfectar previamente los nuevos espacios donde los dispositivos móviles entrarían en contacto con superficies externas o desinfectar periódicamente el o los dispositivos.

- 19.1.2 Fortalecimiento de la seguridad con incorporación de accesorios tecnológicos para dispositivos móviles.

  Control**:** en caso de movilidad, se debería incorporar tecnología complementaria como lo puede ser un kit de manos libres o headset para interconectar con el dispositivo móvil y de

esta manera minimizar la exposición de los dispositivos móviles sobre superficies externas y así mitigar la propagación del virus.

19.2 Trabajo remoto consensuado

Objetivo: moderar las sobrecargas operativas, económicas y jurídicas para las organizaciones en medio de situaciones de crisis que exigen una reacción inmediata para el sostenimiento económico de la sociedad.

- 19.2.1 Acogerse al modelo de trabajo permitido en situación de crisis.

  Control**:** las organizaciones que, por asuntos de fuerza mayor de tipo natural como desastres, pandemias, crisis de salubridad, climáticas u otras, se vean impulsadas a la continuidad de sus actividades de negocio de manera remota deberían adherirse a los nuevos reglamentos permitidos por el respectivo ente gubernamental, con el fin de dar continuidad a sus operaciones de negocio.

19.3 Seguridad poscovid para el recurso humano

Objetivo: disponer de los recursos y medidas de control y gestión del recurso humano para promover la seguridad de los colaboradores.

- 19.3.1 Gestión y control del recurso humano ante amenazas de contagio.

  Control: la organización debería contar con una política responsable de autodiagnóstico para el reporte de síntomas de manera diaria, con el objetivo de controlar de forma automatizada el estado de salud de los colaboradores por medio del uso de tecnologías adecuadas.

- 19.3.2 Medidas de seguridad para la retoma a la presencialidad.

Control: ante la retoma progresiva a la presencialidad, la organización debería disponer dentro de sus instalaciones de una tecnología adecuada para medir y controlar la interacción social entre los colaboradores, de modo que se logre registrar la geoposición de estos para, posteriormente, alertar a los colaboradores que estuvieron en contacto con alguna persona afectada por el virus.

19.4 Seguridad en la videoconferencia y colaboración

Objetivo: proveer los lineamientos de seguridad para los puestos de trabajo remoto que se fundamentan en la operación del audio y video para su funcionamiento.

- 19.4.1 Plan de concientización para el uso apropiado de herramientas de colaboración.

  Control: la organización deberá establecer un plan de concientización a sus colaboradores para la ejecución responsable de las actividades laborales que involucran la voz y el video, desde los puestos de trabajo remoto, y así evitar poner en riesgo la integridad y confidencialidad de la información, sobre todo, cuando esta es transmitida de manera audible.

- 19.4.2 Suministro de herramientas seguras para la colaboración.

  Control*:* la organización debería garantizar el uso de la tecnología más segura disponible del mercado en herramientas de voz y colaboración para sus trabajadores que se encuentran en forma remota y, complementariamente, proveer *hardware* de audio y microfonía adecuado para perfeccionar la integridad y confidencialidad de la información que se transmite de manera audible.

19.5 Extensión de la seguridad en el desvanecimiento del perímetro corporativo

Objetivo: facilitar una solución para el control de los activos distribuidos en el trabajo remoto y evitar la difusión no autorizada de información empresarial sensible.

- 19.5.1 Control y gestión de los activos distribuidos.

  Control*:* la organización debería disponer de una solución tecnológica que le permita controlar la distribución física de sus equipos de cómputo por medio de monitoreo de tipo GPS.

- 19.5.2 Prevención de pérdida de datos.

  Control: considerando el desprendimiento de la información sobre el perímetro de la organización, se debería estimar el uso de tecnología que supervise el estado y el flujo de la información empresarial sensible, de modo que se bloquee cualquier intento de salida de los datos sobre el dominio corporativo.

19.6 Seguridad en las comunicaciones distribuidas

Objetivo: asegurar las operaciones de red y conectividad distribuida de los colaboradores.

- 19.6.1 Seguridad distribuida para conexiones remotas.

  Control: la organización debería contar con una solución tecnológica para la seguridad de los datos que son transmitidos por las redes remotas de tipo residencial, desde donde los colaboradores establecen la conexión a Internet para la realización de su trabajo.

19.7 Seguridad informática persistente

Objetivo: planificar la continuidad de la seguridad de la información ante futuras condiciones desconocidas.

- 19.7.1 fundamentos de seguridad predictiva.

  Control: la organización debería establecer un plan de educación y sensibilización sobre los fundamentos de la seguridad de la información y su continuidad en medio de situaciones de crisis e impacto social, entre ellas escenarios de pandemia, considerando el dinamismo de las nuevas y cambiantes necesidades de seguridad emergentes.

Elección de tecnologías y desarrollo de procedimientos a partir del nuevo dominio de seguridad propuesto

A partir del dominio de seguridad de la información propuesto en el presente proyecto, se consideró que un apropiado SGSI, además de proponer el uso de algunas herramientas tecnológicas de ciberseguridad, también debería ir complementado la aplicación de procedimientos y políticas de buenas prácticas, en el cual la participación y el apoyo del recurso humano de la organización juega un papel trascendental para su éxito.

A continuación, se enuncia la aplicación de las buenas prácticas inclinadas a extender la protección de la información en medio de una situación de crisis por la propagación de un virus de tipo pandémico; puesto que este tipo de escenarios quebranta las estructuras sociales, generando la movilización de colaboradores hacia un ámbito de resiliencia con el empeño de mantener la economía nacional activa, por medio del trabajo remoto.

Adicionalmente, se planteó el uso de tecnologías ideales para la protección de la información sobre los nuevos desafíos para la seguridad. Las prácticas y tecnologías descritas a

continuación se encuentran fundamentadas y orientadas a cumplir con las directrices expuestas en cada uno de los controles creados y propuestos bajo el nuevo dominio de seguridad, relacionado en el presente proyecto.

Dentro del dominio número 19, nombrado como “Seguridad transversal para los contextos de tipo pandemia”, se presentan las tecnologías y procedimientos descritos a continuación para cada control.

Control 19.1 Seguridad poscovid sobre dispositivos móviles

Para el control 19.1.1

Este control habla de las buenas prácticas de seguridad en la manipulación de los dispositivos móviles frente a las nuevas necesidades de seguridad poscovid. Mediante la Tabla 4, se presenta el siguiente procedimiento:

Tabla 4.

Presentación de procedimiento requerido en el control 19.1.1 para la seguridad poscovid sobre dispositivos móviles.

1. Objetivo del procedimiento
Generación de nuevo conocimiento para la aplicación de prácticas seguras en la manipulación de dispositivos móviles.
2. Alcance del procedimiento
El empleo de prácticas seguras en la manipulación de dispositivos móviles para mitigar la propagación de contagio en contextos pandémicos está destinado principalmente para las áreas dentro de la organización que, por su actividad de negocio, asiduamente requieren de desplazamientos e interacción con otras personas, tanto internas como externas.
3. Criterios

Los criterios a tener en cuenta para el desarrollo de la capacitación son los siguientes:

- El contenido de la capacitación deberá ser intuitivo y vinculado mediante la representación de actividades cotidianas del trabajo.
- La capacitación deberá ser concreta y con una duración igual o menor a 20 minutos.
- La capacitación deberá ser de tipo virtual y presentada mediante contenido multimedia.

4. Procedimiento

Actividad	**Descripción**	**Responsable**
Lograr aprobación de la Dirección.	Relacionar los riesgos y perjuicios para la organización que podrían derivarse de un contagio en el contexto de una pandemia sobre un colaborador que es considerado activo de información.	Área de TI
Determinar el público objetivo.	El área directiva de la organización deberá determinar el público al que principalmente está dirigida la capacitación.	Dirección
Buscar proveedor de la capacitación.	Realizar la respectiva búsqueda de un proveedor consultor o especialista en seguridad de la información que pueda ofrecer el desarrollo del contenido en formato multimedia.	Área de Compras
Ejecución del plan de capacitación.	Establecer el cronograma y periodicidad para efectuar la capacitación dentro de la organización.	Área de Recursos Humanos

Fuente: elaboración propia.

Con la llegada de una amenaza desconocida sobre el territorio colombiano como lo fue la COVID-19 en el primer semestre de 2020, las organizaciones no lograban entender con claridad cómo esta amenaza podría afectar la disponibilidad de su información. Mediante este proyecto, se tomó como referencia el comportamiento de la empresa ProCibernetica ante el nuevo escenario causado por el coronavirus. Allí, sus colaboradores ignoraban los riesgos de seguridad ante una manipulación inadecuada de los dispositivos móviles en medio de ambientes contaminados con el virus pandémico. Esto se determinó a partir de lo anterior y del vacío presente en el control 6.2.1 para la seguridad de los dispositivos móviles, expuesto en la norma GTC-ISO/IEC 27002:2015 (Icontec, 2015). Gracias a este proyecto, se creó el procedimiento de seguridad para la implementación de buenas prácticas y hábitos de seguridad relacionados con la mitigación de propagación de virus en los dispositivos móviles. Con la aplicación de este procedimiento, ProCibernetica logró actuar de manera precavida eludiendo la exposición de los dispositivos móviles sobre entornos posiblemente contaminados, evitando que los móviles fueran contaminados y pudieran retrasmitir el virus del colaborador a otras personas.

Para el control 19.1.2

Este control habla del fortalecimiento de la seguridad con la incorporación de accesorios tecnológicos para dispositivos móviles, se propuso aprovechar el uso de la tecnología, presentada en la Figura 5 (Asistente de Google y Auriculares inteligentes Bose), para mitigar los riesgos de contagio a causa de la exposición de los dispositivos móviles sobre superficies externas y respaldar la disponibilidad e integridad de la información empresarial.

Figura 5.

Recursos tecnológicos para la seguridad poscovid en dispositivos móviles.

Fuente: tomado de Google (s.f.a; s.f.b).

Implementar el uso de auriculares inteligentes de tipo inalámbrico compatibles con el Asistentede Google permitirá eliminar totalmente la exposición de los dispositivos sobre ambientes posiblemente contaminados. La adaptación de esta tecnología habilita el uso interactivo del teléfono móvil sin siquiera tocar y manipular físicamente el dispositivo.

Una vez ajustado y activado las notificaciones del Asistente de Google, así como, también sincronizado los auriculares con el dispositivo móvil, bastara solo con presionar un botón en uno de los costados de los auriculares para activar la interacción con el Asistente de Google, mediante el uso de comandos de voz. De esta manera y sin tener que manipular físicamente el dispositivo móvil, el colaborador puede crear eventos en el calendario, hacer llamadas, recibir notificaciones audibles y escuchar y responder mensajes en aplicaciones de chat (Tillman, 2021).

ProCibernetica cuenta con dos áreas principales dentro de su estructura organizacional, las cuales frecuentemente realizan desplazamientos a nivel nacional para interactuar con los diferentes clientes, estas son el área comercial y el área de servicios. En el ejercicio de estas interacciones, los colaboradores junto con sus accesorios, como lo son los dispositivos móviles,

siempre se han visto expuestos a diferentes entornos y variables del ambiente. Tras la llevada de la COVID-19 algunos de estos desplazamientos disminuyeron, pero muchos otros tuvieron que seguirse llevando a cabo en medio de la presencia del coronavirus. Aplicando todas las medidas de bioseguridad pertinentes, ProCibernetica fortaleció la seguridad informática mediante la incorporación de la tecnología avanzada propuesta en este proyecto, la cual recomienda el uso de auriculares inteligentes, esta medida brindó a los colaboradores un menor nivel de exposición de los dispositivos móviles frente al virus; de esta manera se consiguió actuar responsablemente frente a la intención de mitigar la propagación del coronavirus y proteger el activo de información para la organización, es decir, el colaborador.

Control 19.2 Trabajo remoto consensuado

Basado en el enunciado “19.2 Trabajo remoto consensuado”, se propone la aplicación del siguiente procedimiento que se describirá en la Tabla 5, para satisfacer lo citado por el control “19.2.1 Acogerse al modelo de trabajo permitido”. El cual se propone que:

> Las organizaciones que, por asuntos de fuerza mayor de tipo natural como desastres, pandemias, crisis de salubridad, climática u otras. Se vean impulsadas a la continuidad de sus actividades de negocio de manera remota, deberían adherirse a los nuevos reglamentos flexibles permitidos por el respectivo ente gubernamental para dar continuidad a sus operaciones de negocio (p. 61, en este trabajo).

Tabla 5.

Presentación del procedimiento para el trabajo remoto como está expuesto en el control 19.2.1.

1. Objetivo del procedimiento

Llevar a la organización a la adopción de medidas de protección al empleo mediante las disposiciones legales permitidas por el ente gubernamental, para la preservación económica en medio de situaciones de crisis sociales.

2. Alcance del procedimiento

Viabilizar la implementación de la modalidad del trabajo remoto en casa haciendo valer las bondades dispuestas por los decretos, circulares o reglamentos emitidos por el ente gubernamental.

3. Criterios

Los criterios a tener en cuenta para la puesta en marcha del trabajo remoto son los siguientes:

- Reconocer el estado de emergencia derivado por una situación de pandemia.
- Programar un plan de contingencia para la continuidad del negocio.
- Habilitar canales de comunicación para mantener el contacto con los colaboradores.

4. Procedimiento

Actividad	Descripción	Responsable
Aprobación de la Dirección.	Acordar con la dirección la nueva operación de trabajo remoto y definir los lineamientos.	Gerencia
Sustento legal.	Explorar y confirmar vigencia de la reglamentación permitida para la situación ocasional y excepcional de trabajo remoto.	Área Jurídica
Planeación de ejecución.	Establecer los cargos y funciones de los colaboradores que podrán trabajar remotamente.	Recursos Humanos

Fuente: elaboración propia.

Control 19.3 Seguridad poscovid para el recurso humano

Previo a la llegada de la COVID-19 al país, ProCibernetica no tenía a ninguno de sus colaboradores operando remotamente. La organización se enfrentó a la modalidad de teletrabajo cuando el Gobierno Nacional estableció la medida de aislamiento social mediante el Decreto 457 (Presidencia de la República de Colombia, 2020b) para mitigar la rápida propagación del virus, ante este escenario la compañía y varias organizaciones desconocían las condiciones y los extensos requisitos, tanto legales como operativos, para trabajar mediante la modalidad de teletrabajo. Adicionalmente, existen vacíos en la guía GTC-ISO/IEC 27002:2015, específicamente en el control 6.2.2 (Icontec, 2015), al no brindar directrices para que las organizaciones operen mediante la modalidad de trabajo remoto en situaciones de crisis y de fuerza mayor. Dado lo anterior y mediante este proyecto, se propuso a ProCibernetica acogerse a la medida del trabajo remoto y permitida legalmente bajo la Circular 021 (Ministerio del Trabajo, 2020) para no impactar la economía de la organización y continuar su operación por medio del trabajo remoto en casa. Con la aplicación de esta medida la organización logró optimizar el uso de sus recursos y dar continuidad a sus actividades laborales sin impactar negativamente su operación.

Basado en el enunciado “19.3: Seguridad poscovid para el recurso humano”, y con el fin de dar cumplimiento a lo expuesto en el control “19.3.1 Gestión y control del recurso humano ante las amenazas de contagio”, se impulsó a que la organización cuente con una política responsable de autodiagnóstico para el reporte de síntomas de manera diaria y así controlar de manera automatizada el estado de salud de los colaboradores con el uso de las tecnologías adecuadas.

Para el control 19.3.1

Se propone el uso de la siguiente solución tecnológica para este control: sistema automatizado para el reporte de síntomas.

Con el objetivo de establecer las pertinentes medidas de seguridad y mitigación del virus COVID-19, el Gobierno Nacional determinó, mediante la Resolución 223 del 25 de febrero de 2021, la aplicación de medidas de bioseguridad para todo tipo de colaboradores de empresas del sector público y privado, por ende, las organizaciones deben implementar un sistema para el control y reporte de síntomas de sus colaboradores (Ministerio de Salud y Protección Social, 2021).

Con la llegada de la COVID-19, ProCibernetica tuvo que adherirse responsablemente a las medidas de bioseguridad ordenadas inicialmente para todas las actividades económicas y sociales mediante la Resolución 666 (Ministerio de Salud y Protección Social, 2020), dentro de las cuales se ordenaba la implementación de un sistema para el control y reporte de síntomas de la COVID-19 de los colaboradores. A partir de esto y del vacío del control 7.2.1 para la seguridad del recurso humano, expuesto en la guía GTC-ISO/IEC 27002:2015, se propone el uso de una tecnología concreta para respaldar la seguridad del recurso humano. Inicialmente, ProCibernetica implemento el diligenciamiento de una encuesta mediante formularios de Google; sin embargo, esta medida no fue efectiva, debido a que gran parte de los colaboradores olvidaban realizar dicha encuesta, para otros colaboradores sin conexión a Internet les era imposible realizar el registro y para el área encargada del control, al no tener información precisa y oportuna, le era ineficaz al momento de presentar estadísticas al área directiva.

La solución tecnológica propuesta para la automatización al proceso del reporte de síntomas permitió a ProCibernetica disponer de los resultados del proceso de reporte de síntomas

en un horario preciso y de manera completa, ya que la solución propuesta hace uso de la tecnología de omnicanalidad y recordatorios persistentes hasta que el proceso fuera llevado a cabo.

Gestiona2 Latam fue el proveedor de la solución tecnológica para la automatización del proceso de reporte de síntomas diarios, mediante la disposición de diversos canales de comunicación apoyados con asistentes virtuales encargados de solicitar a los colaboradores la realización del reporte mediante una notificación de tipo pop-up (Gestiona2, s.f.b). De esta manera se liberó la carga laboral en las áreas responsables y además se consiguió que la organización contara con el reporte de síntomas de todos sus colaboradores en un horario específico.

La solución de Gestiona2 hace uso de los siguientes canales de comunicación, evidenciados en la Figura 6, para el registro de síntomas por parte de los colaboradores: mensaje de texto MSN, llamada telefónica a número móvil, vía WhatsApp o Telegram.

Figura 6.

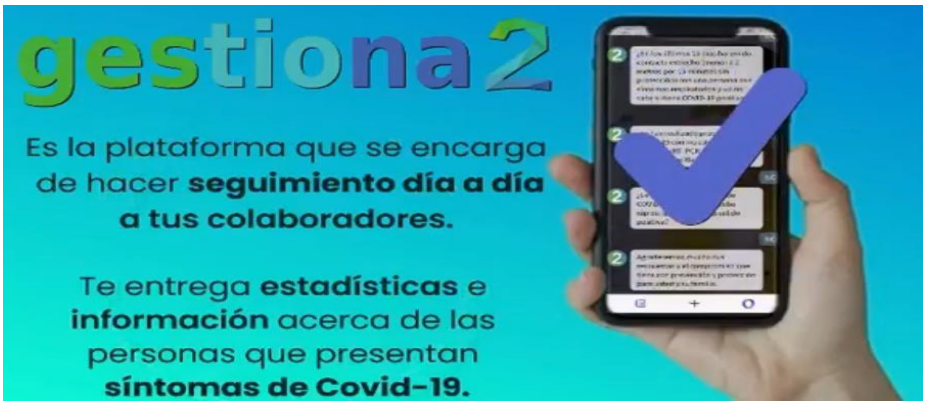
Representación de los medios de comunicación de la solución de reporte de síntomas del fabricante Gestiona2 Latam.

Fuente: tomado de Gestiona2 (2020).

Para los casos en que algún colaborador registrara positivo para síntomas de la COVID-19, la plataforma tecnológica de Gestiona2 notificaba al área encargada de la organización para entregar información estadística, como se refleja en la Figura 7, mediante una alerta por medio de los siguientes canales: mensaje de texto MSN, email, vía WhatsApp o Telegram.

Figura 7.

Representación de la solución automatizada para el reporte de síntomas de la COVID-19.



Fuente: tomado de Gestiona2 (2020).

Para el control 19.3.2

Este hace mención a las medidas de seguridad para la retoma de la presencialidad y en el cual, se expone que ante la retoma progresiva de la presencialidad, la organización deberá disponer dentro de sus instalaciones de una tecnología adecuada para medir y controlar la interacción social entre los colaboradores; de modo que, se logre registrar la geoposición de estos para posteriormente alertar a los colaboradores sobre quiénes estuvieron algún contacto con un colaborador que pueda estar infectado por el virus.

Para el control 19.3.2 se propone el uso de la siguiente solución tecnológica: Extreme Networks, cuenta con una novedosa y avanzada solución de analítica y posicionamiento basada en la nube llamada ExtremeLocation.

ExtremeLocation es una solución de servicios de ubicación basada en red que trabaja de manera conjunta con la tecnología Wireless de Extreme y permite a las organizaciones tener un control y trazabilidad de los visitantes y usuarios que llegan a sus instalaciones y, además, permite hacer el seguimiento a sus desplazamientos y recorridos en las zonas determinadas dentro de su perímetro. La aplicación de esta tecnología ha cobrado un mayor sentido con la llevada del coronavirus (COVID-19), ya que sus funcionalidades, que se describen de manera generalizada en la Figura 8, permite que las organizaciones dispongan de un recurso tecnológico para controlar las medidas de aislamiento social y así limitar el número máximo de visitantes permitidos dentro de sus instalaciones y, al mismo tiempo, cotejar las interacciones sociales que se presenten para alarmar y tomar acciones ante los posibles casos de contagio del virus COVID-19 o a futuro de las posibles pandemias.

Figura 8.

Solución de ExtremeLocation para controlar la aglomeración de personal.

Fuente: tomado de Extreme Networks (2019).

A continuación, en la Figura 9 se presenta la interfaz de administración de la solución en la cual se evidencia la interacción y aglomeración de personal dentro de la organización, cabe

destacar que el reconocimiento de cada persona depende de la conexión de los dispositivos móviles del personal hacia la red wifi de la organización.

Figura 9.

Representación de la interfaz de monitoreo de la solución ExtremeLocation.

Fuente: tomado de Extreme Networks (2021c, p. 82).

A finales del segundo semestre de 2020, ProCibernetica decidió acogerse a las medidas de retoma progresiva a la presencialidad permitidas bajo la Resolución 223 (Ministerio de Salud y Protección Social, 2021), para lo cual estableció contar con la presencia física de solo algunos de sus colaboradores en las instalaciones. Esta decisión obligó a la organización a implementar el

protocolo de bioseguridad y aplicar estrategias para garantizar el distanciamiento físico dentro de su sede principal. Dichas estrategias se apoyaron en la sensibilización del personal e implementación de carteles y avisos alusivos al distanciamiento físico; sin embargo, esta medida no fue del todo efectiva, ya que en el ejercicio de retoma de la presencialidad se presentó uno de los primeros casos de contagio de la COVID-19, el cual se presume que fue procedente por la visita de un proveedor.

Basado en esto y en el vacío del control 9.1.1 expuesto en la norma GTC-ISO/IEC 27002:2015 para el control de acceso, se propone el uso de la tecnología ExtremeLocation con la cual ProCibernetica logrará:

Controlar las áreas y hacer seguimiento a las zonas dentro de la organización para detectar la cantidad de personas que se encuentran en las instalaciones de la empresa, por medio del enlace wifi de sus dispositivos móviles y así identificar al personal interno y visitante (Extreme Networks, 2021c).

Recopilación de datos de localización para el seguimiento a los activos y determinación de zonas de mayor aglomeración de personal para la toma de medidas correctivas y preventivas (Extreme Networks, 2021c).

Visualización de eventos de congestión y aglomeración de personal en tiempo real para la toma de medidas con el personal interno y/o visitante (Extreme Networks, 2021c).

Parametrizar en la interfaz de la solución (ExtremeLocation) el umbral máximo de personal permitido dentro de la organización y en cada una de sus áreas (Extreme Networks, 2021c).

Activación de alarmas y envió de alertas en casos en los que el umbral de cantidad de personas se supere (Extreme Networks, 2021c).

Análisis del contexto de ubicación y desplazamiento de visitantes y colaboradores de la organización (Extreme Networks, s.f.).

Determinar tendencias comportamentales en la afluencia e interacciones generales del personal sobre las diferentes áreas de la organización (Extreme Networks, s.f.).

Control 19.4 Seguridad en la videoconferencia y colaboración

Basado en el enunciado del control "19.4 Seguridad en la videoconferencia y colaboración", se propone la aplicación del siguiente procedimiento y uso de tecnología.

Para el control 19.4.1

En este control, el cual indica crear el plan de concientización para el uso apropiado de herramientas de colaboración, la organización debería establecer un plan de concientización a sus colaboradores para una ejecución responsable de las actividades laborales que involucran la voz y el video desde los puestos de trabajo remoto, y así evitar poner en riesgo la integridad y confidencialidad de la información, sobre todo, cuando esta es transmitida de manera audible.

Previo a la llegada de la pandemia COVID-19, ProCibernetica eventualmente hacia uso de las herramientas de colaboración para llevar a cabo reuniones, tanto internas como con algunos de sus clientes y proveedores, debido a que comúnmente estas se llevaban a cabo de manera presencial. Por lo tanto, la organización y sus colaboradores no contaban con la cultura de seguridad y buenas prácticas al momento de llevar a cabo una sesión de videoconferencia, en especial, con personal externo. Teniendo en cuenta lo anterior, se creó el procedimiento de concientización presentado a través del control 19.4.1 Tabla 6), con el fin de fortalecer la seguridad de la información empresarial desde la aplicación de buenas prácticas.

Tabla 6.

Presentación del procedimiento para la aplicación de prácticas seguras en la videoconferencia y herramientas de colaboración.

1. Objetivo del procedimiento

Llevar a que los colaboradores de manera procedente ejecuten las mejores prácticas de seguridad para garantizar que las reuniones virtuales, que se efectúan de manera remota, sean seguras y privadas.

2. Alcance del procedimiento

Generar conciencia y criterio en los colaboradores para que cuenten con las competencias requeridas a fin de respaldar la privacidad y propiedad intelectual de la organización, mientras se utiliza la herramienta de colaboración elegida por la organización.

3. Criterios

Los principios a tener en cuenta para contribuir a la integridad y confidencialidad en el manejo de la información, cuando se emplean herramientas de colaboración en el trabajo remoto, son:

- Reconocer el nuevo sitio de trabajo y las posibles fuentes generadoras de ruido.
- Disponer de una conectividad de tipo segura brindada por la organización antes de iniciar la videoconferencia.
- Prever la divulgación involuntaria de la información del negocio a través del video proyectado.

4. Procedimiento

Actividad	Descripción	Responsable
Controlar el acceso a la reunión.	Tener en cuenta con quién se comparte el enlace de la reunión, quién puede unirse a ella y limitar el reenvió del link.	Colaborador

Verificar participantes.	Confirmar que en la sesión se encuentren los participantes exclusivamente invitados.
Presentación de contenido.	Por defecto, tener deshabilitado la opción de compartir pantalla para los participantes invitados.
Grabación de sesión.	Impedir que los asistentes diferentes al organizador puedan grabar la sesión.
Integridad de audio.	Posicionarse en la mejor ubicación libre de ruidos e interferencias para no perturbar la integridad y confidencialidad de la información trasmitida.

Fuente: elaboración propia.

Para el control 19.4.2

El cual habla sobre el suministro de herramientas seguras para la colaboración, en este control se establece que la organización garantice el uso de la tecnología más segura disponible del mercado en herramientas de voz y colaboración, para los colaboradores remotos, y, adicionalmente, proveer el hardware de audio y microfonía adecuado con el fin de perfeccionar la integridad y confidencialidad de la información que se transmite de manera audible. De esta manera, se podrá mitigar el mayor número posible de ciberataques por medio del *zoombombing* y otros, los cuales atentan contra la confidencialidad y disponibilidad de la información (Lazar, 2021).

ProCibernetica, históricamente, ha utilizado la herramienta de colaboración que por defecto le suministro su proveedor de cuentas de correo electrónico, debido a que este recurso no era utilizado en gran medida de manera previa a la pandemia COVID-19. No era relevante para ProCibernetica conocer si el nivel de seguridad brindado por dicha herramienta era el adecuado o no para la protección de su información empresarial. Sin embargo, a partir de esto y del vacío

expuesto en el control 9.1.1 de la guía GTC-ISO/IEC 27002:2015, se propone a la organización la incorporación y uso de la tecnología más segura del mercado en la actualidad para la protección de la información, a través de la videoconferencia y colaboración, la cual es Microsoft Teams; por otro lado, se puede ofrecer respaldo a la integridad de la información de tipo audible mediante la tecnología Acoustic fence.

Sobre Microsoft Teams se puede decir que, fue lanzada mundialmente a producción en el 2017 y es una plataforma de comunicación unificada para la colaboración, que comprende el uso de audio y video para las reuniones en línea de modo sincrónico, chats, almacenamiento de nube, que se integra con la suite de Office y aplicaciones de terceros.

Microsoft Teams (MS Teams) es un fabricante muy comprometido con la seguridad de la información, el cual, por estar ligado a la nube de Microsoft, cuenta con fuertes características de seguridad y, además, continuamente hace uso de diversas técnicas de seguridad avanzada las cuales son descriptas a continuación:

1. Seguridad de extremo a extremo mediante encriptación de datos: Teams blinda la comunicación en la capa de transporte mediante los protocolos TLS, MTLS y SRTP, para garantizar el cifrado de toda la comunicación SIP sobre la red y, al mismo tiempo, prevenir los ataques de interceptación y desvío de la comunicación. La Tabla 7 presenta los protocolos aplicados en los diferentes tipos de comunicación para la seguridad de los datos.

Tabla 7.

Protocolos de cifrado para la seguridad de la comunicación con MS Teams.

Tipo de trafico	Técnica de cifrado
Servidor - Servidor	MTLS
Cliente – Servidor (chat)	TLS

Señalización	TLS
Elementos multimedia audio y video	SRTP/TLS

Fuente: elaboración propia con base en Microsoft (2021a).

2. Autenticación multifactor: Microsoft Teams cuenta con técnicas de seguridad avanzada para la confidencialidad de la información, mediante la protección de identidad a las cuentas, con un acceso condicional por medio de la autenticación moderna de dos factores en la comunicación de tipo cliente-servidor. Esta característica de seguridad está disponible para la aplicación de escritorio, versión para dispositivos móviles y cliente web. La autenticación multifactorial debe habilitarse en la configuración de la herramienta (Microsoft, 2021a; Microsoft, 2021b).
3. Controles de privacidad: los controles de privacidad de Microsoft Teams permiten la habilitación de políticas para la prevención de amenazas sobre las reuniones, las políticas permiten:

    - Hacer que los invitados externos deban esperar autorización de ingreso a la sesión.
    - Permitir solo que algunos participantes puedan unirse directamente a la sesión sin tener que esperar autorización.
    - Expulsar participantes de la sesión.
    - Habilitar o denegar permisos para presentar y compartir pantalla (Conzultek, 2020; Garache Rizo, 2020).

Como se observa en la Tabla 8, el control de acceso a la videoconferencia puede ser parametrizado de acuerdo con las siguientes disposiciones y tipo de cuentas:

Tabla 8.

Parámetros para el control de acceso de participantes en las sesiones de MS Teams.

Tipos de configuración	Participantes que se pueden unir directamente	Participantes que deben esperar para unirse
Participantes de la organización.	• Cuentas corporativas. • Invitados.	• Participante federado. • Participante anónimo. • Acceso telefónico.
Participantes de otra organización.	• Cuentas corporativas. • Participante federado.	• Anónimos. • Acceso telefónico. • Invitados.

Fuente: elaboración propia.

Un control de seguridad adicional, como lo vemos en la Tabla 9, permite administrar la experiencia de los participantes mediante la designación de permisos de operación sobre la sesión.

Tabla 9.

Listado de acciones permitidas por tipo de usuario en la sesión de MS Teams.

Acción	Moderador	Asistente
Participar en el chat de la sesión.	✓	✓

Silenciar a otros participantes.	✓	X
Eliminar a otros participantes.	✓	X
Compartir contenido.	✓	X
Permitir a otros participantes unirse a la sesión.	✓	X
Iniciar o detener una grabación.	✓	X
Hacer que otros participantes sean moderadores.	✓	X

Fuente: adaptado de Microsoft (2021a).

Teams permite que los usuarios corporativos inviten a usuarios externos que no tengan cuenta con Microsoft y que estos puedan participar de las reuniones sin inconveniente alguno. Los roles de los participantes en una sesión se definen como organizador, moderador y asistente.

4. Seguridad cibernética y defensa contra amenazas: Microsoft Teams por medio de la licencia Microsoft 365 E5 dispone de solidas funciones de seguridad para la protección contra amenazas persistentes, asegurando el entorno de acciones malintencionadas, tanto de manera local como en la nube, mediante técnicas de inteligencia adaptativa. El módulo ATP de Microsoft posibilita diagnosticar y resolver si el contenido que fluye por la aplicación es de naturaleza maliciosa o no, en caso de serlo bloqueará automáticamente dicho contenido para evitar el acceso de los usuarios (Garache Rizo, 2020; Microsoft, 2021b; Microsoft, s.f.).

Microsoft Teams cuenta con funcionalidades de seguridad para la comprobación y detección de amenazas informáticas sobre los datos adjuntos y, de esta manera, evitar que un usuario de Teams ejecute el documento y sea víctima de un ataque (Microsoft, 2021b).

Igualmente, Microsoft Teams promueve la confidencialidad de la información por medio de las etiquetas de confidencialidad de Teams para que los administradores regulen el acceso al contenido corporativo producido durante una sesión de colaboración, las etiquetas de confidencialidad deben ser habilitadas y configuradas por el administrador (Microsoft, 2021b). Por otro lado, en cuanto a DLP (prevención de perdida de datos), Teams permite la protección de datos y documentos confidenciales por medio de las directivas DLP, con el fin de garantizar la confidencialidad previniendo que los datos confidenciales, tanto mensajes como documentos sean entregados a personal no autorizado (Microsoft, 2021b).

5. Cumplimiento de normativas y estándares regulatorios: Microsoft Teams respalda el cumplimiento a más de 90 estándares y leyes regulatorias de la industria (Garache Rizo, 2020; Microsoft, 2021b), dentro de los cuales se destacan: HIPAA, GDPR, FedRAMP, SOC, FERPA, ISO 27001, ISO 27018, entre otros.

Según Conzultek (2020) y Novacloud (Garache Rizo, 2020), Microsoft Teams es la mejor herramienta de comunicación y colaboración efectiva para el trabajo remoto, además cuenta con la incorporación de tecnología segura para la protección de la información y prevención de amenazas sobre los entornos de videoconferencia y colaboración. A continuación, en la Tabla 10, se presenta un consolidado comparativo de la herramienta Microsoft Teams en relación con otras marcas.

Tabla 10.

Comparativo entre las soluciones de videoconferencia y colaboración MS Teams, Zoom y Google Meet.

	Ms Teams	**Zoom**	**Google Meet**

Protección contra amenazas.	✓	*X*	✓
Interoperabilidad	✓	✓	*X*
Control a la funcionalidad de compartir pantalla.	✓	*X*	*X*
Control a la coautoría de documentos.	✓	*X*	*X*
Autenticación avanzada.	✓	*X*	*X*
Acreditación de seguridad ISO27001.	✓	*X*	✓
Cifrado de extremo a extremo.	✓	✓	*X*
Administración de dispositivo.	✓	✓	*X*
Control de tiempo de la sesión.	✓	*X*	*X*
Marcación telefónica.	✓	*X*	✓
Poner en sala de espera.	✓	✓	*X*
Silenciar a los participantes.	✓	✓	*X*
Conexión con salas de reuniones.	✓	*X*	*X*
Flexibilidad para ejecutar en web browser.	✓	*X*	✓

Fuente: elaboración propia.

Los resultados presentados anteriormente, se encuentran respaldados por las siguientes entidades consultoras de tecnología: It Support Guys, G Cloud Devoteam, Obsessed Efficiency y Ricoh.

Microsoft Teams es la herramienta de colaboración más distinguida, robusta y con destacadas características de seguridad, que la lleva a sobresalir de otras herramientas alternativas como Zoom y Google Meet (Caicedo, 2020; Hopper, 2021; Morpeth, 2020; Verbrugghe, 2020).

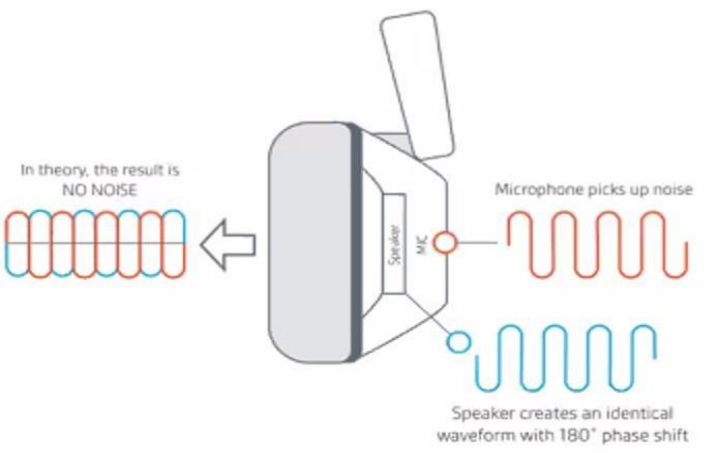
De manera complementaria, el control 19.4.2 propone junto con la herramienta de colaboración, la inclusión de un *hardware* de audio y microfonía adecuado para perfeccionar la integridad de la información cuando esta es transmitida de manera audible.

Para el control 19.4.2

Se propone el uso de la siguiente herramienta tecnológica para el control del punto 19.4.2: la tecnología Acoustic Fence del fabricante Polycom. Esta tecnología es ideal para operar en los entornos de trabajo remoto en casa, los cuales son propensos a los ruidos de fondo y voces externas que afectan la claridad de la voz para quienes se encuentran participando en la sesión de videoconferencia. La reciente tecnología Acoustic Fence permite la cancelación de ruidos de fondo mediante el filtrado de frecuencias, tal como se ve en la Figura 10, en la cual se representa un prototipo del funcionamiento de la tecnología.

Figura 10.

Representación de la tecnología Acoustic Fence de Polycom para el filtrado de ruido.

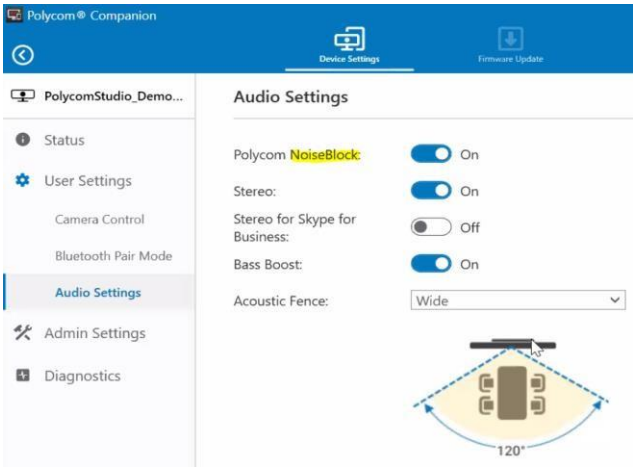


Fuente: Polycom, evento privado.

Es importante resaltar que dicha funcionalidad debe ser ajustada y activada en la interfaz de configuración de la solución tecnológica, tal como se observa en la Figura 11:

Figura 11.

Interfaz de la solución de Polycom para activar el bloqueo de ruido.



Fuente: Polycom, evento privado.

La incorporación de la tecnología Acoustic Fence está disponible solamente sobre algunos auriculares: Voyager 4300 (Figura 12), Blackwire 8225 y el Voyager focus 2.

Figura 12.

Representación de headset *disponible con la tecnología Acoustic fence.*

Fuente: tomado de Poly.com (2021).

Control 19.5 Extensión de la seguridad en el desvanecimiento del perímetro corporativo

Se propone el uso de la siguiente tecnología para satisfacer lo citado por el control 19.5.1, el cual hace referencia al control y gestión de los activos distribuidos, en el cual se promueve que la organización debe disponer de una solución tecnológica que le permita controlar la distribución física de sus equipos de cómputo por medio de monitoreo de tipo GPS.

Previo a la llegada de la pandemia COVID-19, ProCibernetica contaba con una operación 100 % centralizada y presencial en sus instalaciones y de ninguna manera contemplaba una operación de tipo remoto; por lo tanto, el inventario de sus activos tecnológicos era realizado y controlado de manera local. Sin embargo, con la llegada del nuevo modelo de trabajo remoto, al que obligatoriamente tuvo que acogerse, ProCibernetica empezó a experimentar dificultades al momento de requerir controlar el estado y ubicación de su inventario de equipos de cómputo,

distribuidos para el trabajo remoto de sus colaboradores. Basado en esto y en el vacío del control 11.1.1 referente a la seguridad física y de entorno presentado en la guía GTC-ISO/IEC 27002:2015, se propone el uso de la siguiente solución tecnológica para el control y monitoreo GPS de los activos equipos de cómputo.

Para el control 19.5.1

Se propone el uso de la siguiente solución tecnológica: monitoreo GPS de equipos de cómputo. En medio de la nueva normalidad del trabajo remoto se hace importante disponer de una solución tecnológica que permita que la organización logre gestionar y tener visibilidad de los activos de *hardware* de la organización, como lo son los equipos de cómputo asignados a los colaboradores que trabajan de manera remota.

Para esta necesidad se propone el uso del *software* de rastreo y administración de dispositivos Prey, el cual es una solución tecnológica de origen chileno. Prey surgió inicialmente como una solución antirrobo para el rastreo de dispositivos móviles y equipos de cómputo. El *software* cuenta con soporte sobre plataformas Windows, MacOS, Ubuntu, Android y iOS (Seguridad América, s.f.).

La solución de Prey puede ser adquirida mediante diferentes tipos de licenciamiento como lo pueden ser: uso personal, empresarial o educativo. Prey es una solución de *software* para el rastreo de equipos de forma proactiva y detección de movimiento, adicionalmente permite parametrizar el funcionamiento de los equipos sobre un rango de operación georreferenciado (Prey Project, s.f.). Las funcionalidades más destacadas de esta solución son:

Rastro inteligente:

- El rastreo por defecto de la solución permite trazar y registra las ubicaciones de los dispositivos cada vez que se detecta un movimiento.
- La solución tecnológica utiliza los métodos: GPS, GeoIP y triangulación Wifi para proyectar la mejor precisión de rastreo.
- La solución dispone de una interfaz de monitoreo para visualizar el despliegue de los equipos de manera simultánea sobre una vista satelital (Prey Project, s.f.).

Detección y reacción:

- La solución permite la delimitación de áreas geográficas en las cuales pueden operar ciertos equipos y notificar cuando algún equipo se mueva por fuera del área permitida.
- Configuración de zonas de seguridad para la activación de políticas de bloqueo de equipos en el evento en que algún equipo se mueva por fuera de la zona permitida (Prey Project, s.f.).

Trazabilidad de ubicaciones:

- La solución permite el registro de todas las ubicaciones detectadas y las organiza cronológicamente por año, mes, día y hora.
- Visibilidad al historial de ubicaciones sobre mapa de calor para la detección rápida de eventos de mayor actividad (Prey Project, s.f.).

Acciones de seguridad:

- La solución dispone de una funcionalidad de seguridad mediante la activación del modo emergencia, el cual permite el bloqueo del equipo ante un evento de pérdida del equipo.

- El modo emergencia permite forzar la activación de una alarma que no se puede silenciar para asistir la localizar del equipo ante caso de pérdida.
- En caso de ser necesario, la solución permite etiquetar un equipo como perdido en la plataforma de gestión para correlacionar evidencias con información que conlleve a su recuperación (Prey Project, s.f.).

La solución propuesta por Prey permite que la organización cuente con un control de inventario detallado del *hardware* de la organización como equipos *laptops*, tablets y dispositivos móviles, manteniendo un control de asignación de equipos por colaborador y visibilidad georreferenciada en la interfaz de administración de la solución, como se evidencia en la Figura 13 (Seguridad América, s.f.). Esta funcionalidad cuenta con características como:

Tablero de visibilidad de dispositivos.

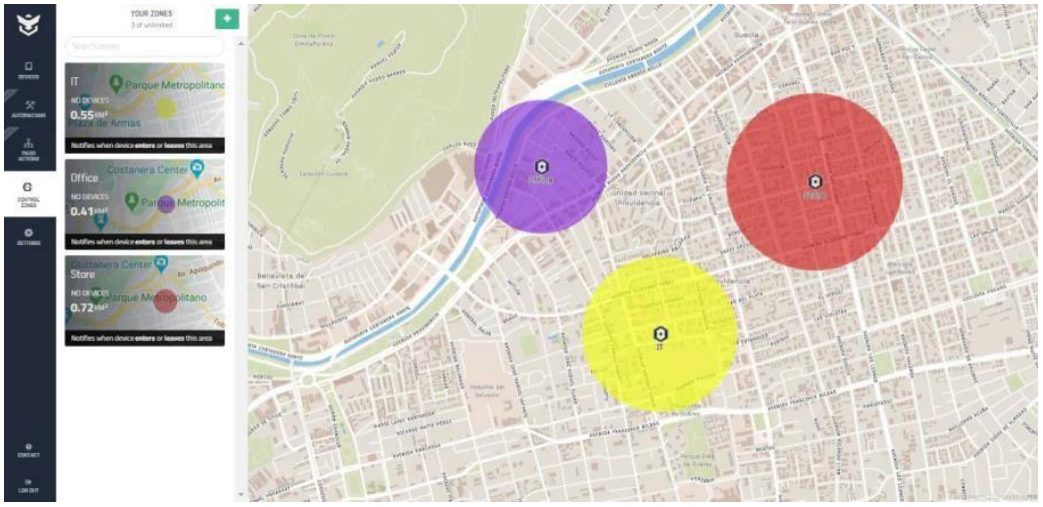
Control de asignación de dispositivos.

Visibilidad de utilización de equipos.

Etiquetado y agrupación de dispositivos.

Figura 13.

Representación de interfaz de Prey para el control de inventario de equipos.



Fuente: tomada de Google (s.f.c).

Para el control 19.5.2

Para el control “19.5.2: Prevención de perdida de datos” en el cual se considera que, a causa del desprendimiento de la información sobre el perímetro de la organización, se debería considerar el uso de tecnología que supervise el estado y flujo de la información empresarial de tipo sensible, de modo que, se bloquee cualquier intento de salida de los datos sobre el dominio corporativo.

Previo a la llegada de la pandemia COVID-19, ProCibernetica contaba con una operación completamente centralizada y la seguridad de su información sensible se apoyaba en una plataforma de seguridad de perímetro, mediante un dispositivo de *firewall* y algunas otras políticas de directorio activo. Ambas medidas eran apropiadas a la organización solo mientras sus equipos de cómputo estuvieran dentro del perímetro de la edificación.

A causa de la operación de trabajo remoto fuera del perímetro, la protección a la información sensible de ProCibernetica quedo expuesta. Es por esto que, para esta nueva necesidad de seguridad se propone el uso de la tecnología DLP descrita a continuación.

La fuga de datos puede causar consecuencias catastróficas para las organizaciones, tanto en el daño de su imagen corporativa como en la posibilidad de incurrir en sanciones jurídicas por el incumplimiento regulatorio.

La solución de prevención de perdida de datos de ForcePoint permite blindar y proteger la información sensible, confidencial y de propiedad intelectual de la organización. La solución de seguridad cibernética DLP de ForcePoint permitiría a la organización:

Reducir el riesgo de robo de datos permitiendo mayor visibilidad sobre los mismos por medio de la adopción de servicios en la nube.

Aplicación de controles efectivos para el cumplimiento normativo y reglamentario comprendido por más de 370 políticas aplicables a las exigencias de 83 países.

Reconocimiento de información sensible presente en imágenes y capturas de pantalla mediante el reconocimiento óptico de caracteres.

Análisis de comportamiento para la identificación de amenazas.

Descubrimiento de nuevas pequeñas fugas de datos.

Identificar a los colaboradores de alto riesgo mediante la identificación de actividad sospechosa.

Visibilidad total y control avanzado para el monitoreo de los datos sin importar donde estos residan.

Automatización en la clasificación y etiquetado de los datos empresariales para impulsar la productividad de la organización.

La tecnología de protección de datos DLP seleccionada pertenece al fabricante ForcePoint y es reconocida como una de las mejores tecnologías para DLP, la cual se encuentra dentro de las primeras cuatro posiciones sobre un listado de fabricantes evaluados y reconocidos a nivel mundial. ForcePoint es reconocido como uno de los fabricantes líderes en seguridad cibernética que impulsa la transformación digital mediante el fortalecimiento de la seguridad a través de un análisis profundo del comportamiento del usuario con respecto a su interacción con los datos en tiempo real (Forcepoint, 2019; Myservername.com, s.f.).

Control 19.6 Seguridad en las comunicaciones distribuidas

Basado en el enunciado del control 19.6, el punto 19.6.1, menciona que la organización cuente con una solución tecnológica para la seguridad de los datos que son transmitidos por las redes remotas de tipo residencial desde donde los colaboradores establecen la conexión a Internet para la realización de su trabajo.

Previo a la llegada de la pandemia COVID-19, ProCibernetica contaba con una operación 100 % centralizada en el cual sus actividades de trabajo de cómputo se realizaban dentro de sus instalaciones y estas se regían bajo las políticas de seguridad establecidas por su plataforma de seguridad de perímetro. Es decir que, la comunicación hacia Internet, establecida por cada colaborador, estaba protegida y asegurada dentro de la organización. No obstante, la nueva modalidad de trabajo remoto expuesta por la COVID-19 desvirtuó todo este modelo, por lo tanto, debido a esto y al vacío del control 13.1.2 de la seguridad de las comunicaciones expuesto en la

guía normativa GTC-ISO/IEC 27002:2015, se propone el uso de una nueva solución tecnológica para ProCibernetica.

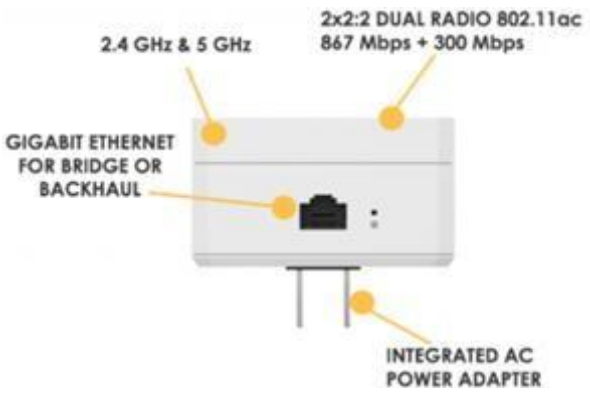
Para el control 19.6.1

Se propone el uso de la siguiente solución tecnológica: conexión remota segura con ExtremeWireless AP30. La elección de una tecnológica propicia para el respaldo de la seguridad de la información en medio de los nuevos escenarios de trabajo remoto, distribuidos en las redes de tipo residencial de los colaboradores, principalmente considera que debe contar con características de fácil uso y que pueda ser implementada de manera intuitiva por cualquier tipo de usuario.

La tecnología seleccionada se compone de una solución de acceso remoto seguro VPN *site-to-site* y Wifi *plug and play*. Esta solución permitió para ProCibernetica extender de manera instantánea la red corporativa hacia cualquier sitio remoto. La puesta en funcionamiento en el lado remoto fue absolutamente simple y solo requirió que el colaborador conectara el dispositivo la toma de corriente y a la conexión de red con el CPE que entrega su proveedor de servicio a Internet. Inmediatamente, el dispositivo de manera automática estableció una conexión de tipo VPN sitio a sitio contra la plataforma tecnológica de administración de la solución en la sede principal de ProCibernetica para ser auto aprovisionada y habilitar su funcionamiento en el hogar del colaborador, bajo los mismos parámetros Wifi SSID y controles de seguridad establecidos localmente por la organización. A continuación, en la Figura 14, se presenta el componente de *hardware* de la solución propuesta.

Figura 14.

Adaptador wifi AP30 de extreme para la seguridad de red en el trabajo remoto.



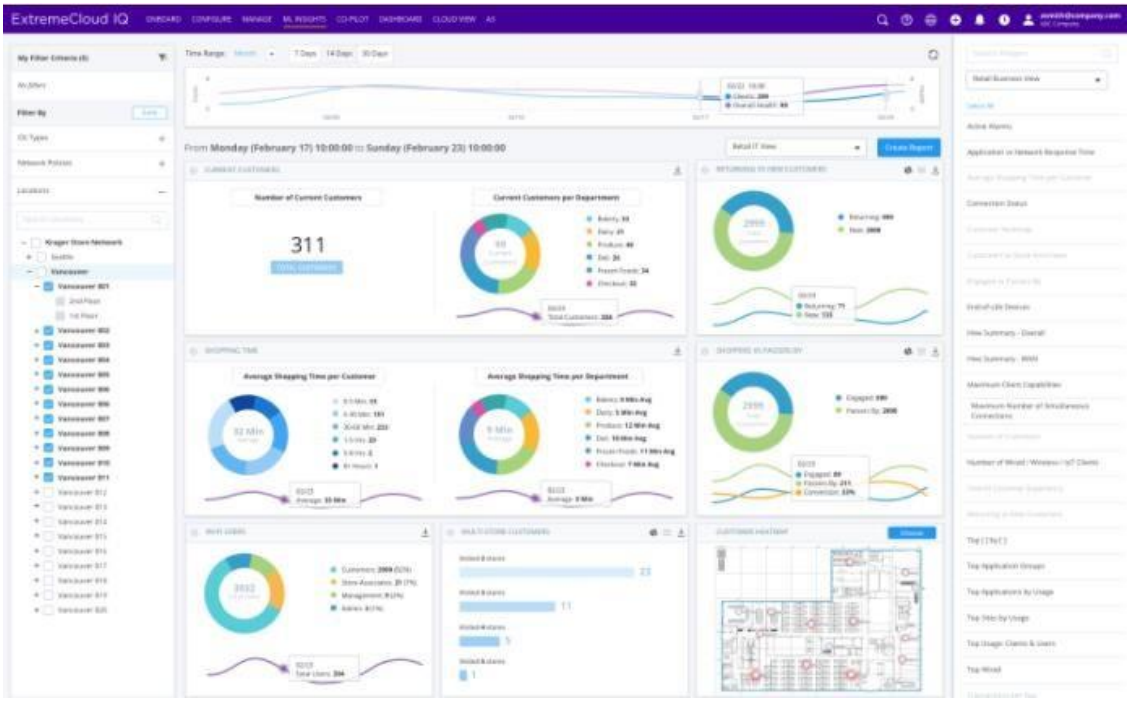
Fuente: tomado de Wi-Fi Now (2018).

La nueva solución propuesta se encuentra compuesta por un componente de *hardware*, en el lado remoto, y un componente de *software*, en el sitio central, de red LAN de la organización.

En la Figura 15, se presenta el componente de *software* de la solución, el cual es entregado por el fabricante bajo una arquitectura de tipo *virtual appliance* para ser instalado dentro del *datacenter*, en la sede principal de la organización.

Figura 15.

Interfaz de gestión y administración de la solución de trabajo remoto seguro.



Fuente: tomado de ChanelBuzz.ca (2020).

La puesta en marcha de la solución de acceso remoto seguro VPN Wifi *plug and play* exigió un esfuerzo técnico por parte del área de TI solo en el lado de la sede principal, en el cual se parametrizo la plataforma para que los dispositivos remotos AP30 operaran de manera automática y fueran auto aprovisionados. Desde el lado del colaborador remoto, no se requirió de conocimientos técnicos y bastó solamente con establecer una conexión física al dispositivo. Bajo este esquema de red se estableció un enlace lógico cifrado de extremo a extremo, en el que el lado remoto se convirtió en una réplica exacta de la configuración local de red y de acuerdo con las políticas de seguridad con las que contaba la sede principal de la organización. De este modo, la información logró estar protegida y libre de amenazas atribuibles a la manipulación y

perjuicios por parte del usuario y su entorno. La Figura 16 representa el diagrama topológico operativo de la solución.

Figura 16.

Arquitectura general de la solución tecnológica para el trabajo remoto seguro.

Fuente: elaboración propia.

Control 19.7 Seguridad informática persistente

Previo a la llegada del virus pandémico de la COVID-19, ProCibernetica no contaba con ningún tipo de plan de continuidad de la seguridad de la información, así que ninguno de sus colaboradores disponía de conocimientos y habilidades para dar un tratamiento seguro a la información en medio de nuevos escenarios de trabajo (teletrabajo y trabajo remoto). A partir de esto y del vacío del control 17.1.1 expuesto la guía GTC-ISO/IEC 27002:2015, se propuso a ProCibernetica la aplicación de un nuevo procedimiento para favorecer la seguridad de la información ante la aparición de nuevos escenarios y eventualidades que pudiesen poner en riesgo la seguridad de la información de la organización.

Para el control 19.7.1

Los fundamentos de seguridad predictiva del control 19.7.1, se incentiva a la organización a establecer un plan de educación y sensibilización sobre los fundamentos de la seguridad de la información y su continuidad en medio de situaciones de crisis e impacto social, entre estas situaciones la de pandemia, considerando el dinamismo de las nuevas y cambiantes necesidades de seguridad emergentes. Se propone la aplicación del siguiente procedimiento para la seguridad persistente (Tabla 11):

Tabla 11.

Presentación de procedimiento de seguridad persistente del control 19.7.1.

1. Objetivo del procedimiento
Establecer una política de cultura de ciberseguridad en toda la organización en la cual los colaboradores adquieran nuevo conocimiento de tipo preventivo, correctivo y analítico para responder acertadamente ante los nuevos riesgos.
2. Alcance del procedimiento
Los servicios de capacitación y sensibilización deberán brindarse de manera periódica como mínimo una vez por semestre y será destinada a todas las áreas y colaboradores de la organización.
3. Criterios
Las pautas a tener en cuenta en el desarrollo y ejecución del procedimiento son las siguientes: • Identificar el estado de conocimiento y posición actual del personal de la organización en relación con la ciberseguridad. • Involucrar a todas las áreas de la organización y priorizar su participación de acuerdo con la importancia, relación y vínculo que se maneje con la información sensible.

- Comprobar la experiencia y resultados del proveedor que se decida seleccionar para la capacitación de los colaboradores.

4. Procedimiento

Actividad	Descripción	Responsable
Establecer la cultura de ciberseguridad.	Implantar una política de seguridad de la información en la cual se vean involucrados y comprometidos todos los colaboradores.	Dirección
Proveer los recursos y herramientas.	Buscar un proveedor acreditado y experimentado en servicios de capacitación con visión futurista en las nuevas necesidades de seguridad y que pueda ofrecer contenido intuitivo de fácil entendimiento para diferentes tipos de usuarios no técnicos.	Área de Recursos Humanos y Área de TI
Establecer cronograma.	Programar la ejecución de las jornadas de capacitación para que sean recibidas de manera estratégica como mínimo en dos sesiones.	Área de Recursos Humanos
Capacitación.	Ejecución a las jornadas de educación que deberán ser de obligatoria participación por parte de los colaboradores.	Colaboradores
Evaluación de conocimiento.	Corroborar la adquisición del nuevo conocimiento que el personal obtuvo.	Área de Recursos Humanos

Fuente: elaboración propia.

Conclusiones

El control de seguridad propuesto para la protección de los dispositivos móviles permiteque las organizaciones cuenten con recursos adicionales de responsabilidad social en la misión de mitigación del virus COVID-19, por medio de una nueva visión en el manejo de la seguridadde la información empresarial, con la que se propone la aplicación de prácticas estrictas para minimizar la exposición de los dispositivos móviles sobre los entornos que puedan conllevar al contagio de los virus de tipo pandémico.

El control de seguridad propuesto para regular la modalidad del trabajo remoto cuenta con atributos de sustento jurídico que favorecen el sostenimiento económico de las organizaciones, en medio de una situación de crisis social y de impacto en la operación de la organización, por cuenta de la propagación de virus de tipo pandemia. La modalidad del trabajo remoto difiere al teletrabajo en cuanto a sus deberes de tipo jurídico, operativo y administrativo.

La solución tecnológica propuesta por el proveedor Gestiona2 Latam, para el reporte de síntomas de contagio de la COVID-19 de manera automatizada, se distingue de otras alternativas de registro como lo son el registro manual y registro mediante Google Forms. La diferencia se encuentra en el sentido en que se sostiene en la precisión de la tecnología y desiste de la dependencia de la voluble voluntad humana. Esto permite a la organización ser más responsable y exacta en el manejo de registros y eventos de contagio de sus colaboradores.

El control de seguridad A.19.3.2 se crea para resarcir el vacío de la directriz actual (GTC-ISO-IEC 27002:2015) para el control de acceso de personas a las organizaciones. Este nuevo control propone la aplicación de tecnología altamente innovadora de uso muy reciente y particular para controlar los índices de aglomeración de personal, mediante el monitoreo de

geoposicionamiento; asimismo, se considerar su uso ante los eventos de retoma a la presencialidad en las instalaciones de la organización.

El control de seguridad propuesto para el uso de herramientas de videoconferencia y colaboración proyecta la aplicación de hábitos seguros al momento de hacer uso de las herramientas de colaboración en el trabajo remoto. Además, propone el uso de la herramienta Microsoft Teams, la cual dispone de mayores capacidades de seguridad en comparación a las herramientas Zoom y Google Meet. De manera complementaria, se sugiere agregar el *hardware* de voz y audio para garantizar la integridad de la información que se transmite de manera audible.

Los controles de seguridad A.19.5.1 y A.19.5.2 se crean para resarcir el vacío de la directriz actual frente al control de seguridad de perímetro, en la GTC-ISO-IEC 27002:2015, para controlar por medio de la tecnología el uso y movilidad del inventario de cómputo distribuido para el trabajo remoto y, además, impedir la fuga de datos en los entornos remotos donde la organización carece de una visibilidad física de sus activos.

Las conductas formuladas en el control 19.7.1 promueven la existencia de una cultura de ciberseguridad en una organización para que sus colaboradores cuenten con las aptitudes y capacidades de reacción que ampare la seguridad de la información empresarial, ante el surgimiento de nuevos eventos y escenarios desconocidos, en los cuales pueda verse comprometida la información de la organización.

En el presente trabajo, se ha puesto en evidencia el impacto que ha traído para la seguridad de la información empresarial las nuevas condiciones de trabajo remoto a las que obligatoriamente ha sido conducida la sociedad, a causa del confinamiento obligatorio por la propagación de la COVID-19.

El esquema del nuevo control de seguridad propuesto tiene como finalidad brindar las adecuadas directrices de seguridad de la información para las organizaciones que requieran proteger su información y aspiren a la implementación de SGSI, en medio del actual escenario de trabajo remoto derivado por la COVID-19.

En general, se encontró que la implementación de un esquema de seguridad de la información va más allá de la adquisición de una solución tecnológica y debe complementarse con la aplicación de procesos adecuados y oportunos que pueden favorecer los asuntos jurídicos de la organización.

En cuanto a la solución tecnológica presentada, esta fue descubierta mediante un ejercicio investigativo. No obstante, se confirma la existencia de otras tecnologías de seguridad de red con opción de despliegue en nube, como lo es la solución SASE (*Secure Access Service Edge*), la cual también podría ser compatible para los escenarios de trabajo remoto. Sin embargo, esta no aplica para las necesidades específicas de ProCibernetica, ya que SASE cuenta con características de seguridad de puerta de enlace de manera nativa, mientras que, en el caso de estudio, se requiere habilitar un enlace totalmente seguro de extremo a extremo para replicar la seguridad de perímetro actualmente existente en la sede principal de ProCibernetica.

Referencias

Asistente de Google. (2021, 22 de junio). En Wikipedia. https://es.wikipedia.org/wiki/Asistente_de_Google

Rojas Castañeda, D. (2020, 11 de agosto). Conozca cuáles son las diferencias legales que hay entre quienes teletrabajan y aquellos que trabajan en casa. *Asuntos Legales*. https://www.asuntoslegales.com.co/consumidor/conozca-las-diferencias-legales-que-hay-entre-quienes-teletrabajan-y-aquellos-que-trabajan-en-casa-3043356

Berrios, C. (2020). Impacto del COVID-19 en la ciberseguridad de América Latina. *Ciberseguridad Latam*. https://www.ciberseguridadlatam.com/2021/02/14/impacto-del-covid-19-en-la-ciberseguridad-de-america-latina/

BSI Group. (2021). Norma ISO/IEC 27017 - Controles de seguridad para servicios cloud. *BSI Group*. https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Caicedo, N. (2020, 3 de abril). ¿Qué sistemas de videoconferencias hay para empresas? Comparativa 2020. *Ricoh*. https://digital.ricoh.es/sistemas-videoconferencia-profesionales-comparativa-2020/?utm_source=linkedin&utm_medium=postimagen

Castellanos Vega, C. J. (2020). *Modalidades de cibercrimen en tiempos de Pandemia Covid-19 en Bogotá (Colombia).* Universidad Militar Nueva Granada. http://hdl.handle.net/10654/37304

Castiblanco, F. y Oviedo Regueros, L. A. (2016). *Análisis de riesgos informáticos y sugerencia de controles para la mitigación del riesgo empleando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 sobre los activos críticos de T.I. en la sede administrativa de la*

empresa Modanova S.A.S [tesis de especialización, Universidad Piloto de Colombia]. Repositorio Institucional. http://repository.unipiloto.edu.co/handle/20.500.12277/2660

Castro de la Torre, C. (2021, 25 de enero). Entender la diferencia entre teletrabajo y trabajo remoto. *Asuntos Legales*. https://www.asuntoslegales.com.co/consultorio/entender-la-diferencia-entre-teletrabajo-y-trabajo-remoto-3114944

ChanelBuzz.ca. (2020, 14 de abril). *Extreme Networks boosts ExtremeCloud IQ with new portable subscription, curated kits*. https://channelbuzz.ca/2020/04/extreme-networks-boosts-extremecloud-iq-with-new-portable-subscription-curated-kits-33591/

Check Point Software Technologies. (2020). *Cyber attack trends: 2020 mid-year report*. https://pages.checkpoint.com/cyber-attack-2020-trends.html

Congreso de la República de Colombia. (2008, 16 de julio). *Ley 1221. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones*. Diario Oficial 47052. http://www.secretariasenado.gov.co/senado/basedoc/ley_1221_2008.html

Congreso de la República de Colombia. (2021, 12 de mayo). *Ley 2088. Por la cual se regula el trabajo en casa y se dictan otras disposiciones*. Diario Oficial 51672. http://www.secretariasenado.gov.co/senado/basedoc/ley_2088_2021.html

Conzultek. (2020). *Cómo mejorar la privacidad y seguridad de sus videoconferencias empresariales con Microsoft Teams*. https://blog.conzultek.com/privacidad-seguridad-videoconferencias-microsoft-teams

Culturasonora. (s.f.). *Auriculares Bose QuietComfort 35 II: opiniones, precio y características de los Bose QC35 II*. Consultado 20 de julio de 2021. https://www.culturasonora.es/auriculares/bose/bose-quietcomfort-ii/

De Luz, S. (2019, 9 de octubre). Diferencias entre las VPN Site-to-Site de las VPN de acceso remoto (Road Warrior). *RZ Redes Zone* https://www.redeszone.net/tutoriales/vpn/vpn-site-to-site-acceso-remoto-road-warrior/

De Quiroga, S. (2020, 15 de noviembre). ¿Es el aire la principal vía de transmisión del coronavirus SARS-CoV-2? *Gaceta Médica*. https://gacetamedica.com/opinion/la-contra/es-el-aire-la-principal-via-de-transmision-del-coronavirus-sars-cov-2/

Díaz Jiménez, S. D., Angulo Cabrales, J. C. y Barboza Camelo, M. M. (2018). *Análisis del delito de fraude electrónico: modalidad tarjeta de crédito* [trabajo de grado, Universidad Cooperativa de Colombia]. Repositorio Institucional. http://hdl.handle.net/20.500.12494/8381

Extreme Networks. (s.f.). *Advance your business and IT goals with ExtremeApplications*. Consultado 20 de julio de 2021. https://www.extremenetworks.com/products/extremeapplications/#cat-108

Extreme Networks. (2019). *ExtremeLocation*. https://cloud.kapostcontent.net/pub/cce75af5-aa54-4b3b-a9db-d21be01a9e75/extremelocation-datasheet.pdf

Extreme Networks. (2021a, 28 de octubre). En Wikipedia. https://en.wikipedia.org/wiki/Extreme_Networks

Extreme Networks. (2021b). *Cloud-based. Location analytics solution - extremelocation.* Consultado 13 de junio de 2021. https://www.extremenetworks.com/product/extremelocation/

Extreme Networks. (2021c). *ExtremeLocation Essentials user guide.* Versión 5.0. https://documentation.extremenetworks.com/extremelocation/essentials/5.0/ExtremeLoca

tion_Essentials_v5.0_User_Guide.pdf?_ga=2.60920620.1013203745.1636076981-1371540372.1631156031

Fernández, Y. (2020a, 2 de junio). Malware: qué es, qué tipos hay y cómo evitarlos. *Xataka Basics*. https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Fernández, Y. (2020b, 6 de marzo). Encriptar: qué es, para qué sirve y cómo cifrar tus archivos. *Xataka Basics*. https://www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

ForcePoint. (2019). *Forcepoint Data Loss Prevention (DLP)*. https://www.forcepoint.com/sites/default/files/resources/brochures/brochure-dlp-en.pdf

Forcepoint. (2021, 11 de octubre). En Wikipedia. https://en.wikipedia.org/wiki/Forcepoint

Garache Rizo, J. (2020, 8 de abril). Microsoft Teams la herramienta más segura para Teletrabajo y videoconferencias. *Nova Cloud*. https://novacloud.business/microsoft-teams-la-herramienta-mas-segura-para-teletrabajo-y-videoconferencias/

García, V. (2020, 30 de diciembre). Estos son los 10 hitos sobre ciberseguridad en INCIBE en 2020. *Revista Byte*. https://revistabyte.es/ciberseguridad/ciberseguridad-2020/

Gestiona2. (s.f.a). *¿Qué es Gestiona2?* Consultado 18 de mayo de 2021. https://gestionados.co/que-es-gestiona2/

Gestiona2. (s.f.b). *Nuestros servicios*. Consultado 16 de mayo de 2021. from https://gestionados.co/servicios/

Gestiona2. (2020, 22 de septiembre). *Gestiona2* [Nuestra plataforma hace seguimiento a los síntomas de covid 19 de tus empleados para que tu ambiente laboral este seguro] Facebook. Consultado 20 de julio de 2021. https://www.facebook.com/watch/?v=333777764530850

Google. (s.f.a). *Google Assistant*. https://bit.ly/2ZW4NM8

Google. (s.f.b). *Bose QuietComfort 35 II.* https://bit.ly/3EOuInI

Google. (s.f.c). *Prey Reviews 2021: Details, pricing & features*. https://bit.ly/3CQjm1T

Hopper, A. (2021, 18 de mayo). Microsoft Teams vs Google Meet vs Zoom: the definitive videoconferecing battle. *IT Support Guys.* https://itsupportguys.com/it-blog/teams-vs-meet-vs-zoom/

Instituto Colombiano de Normas Técnicas (Icontec). (2015). *GTC_ISO/IEC 27002:2015. Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información*. Icontec.

ISO Win. (2017). *Los activos de información en la norma ISO 27001 2017*. https://isowin.org/blog/activos-ISO-27001/

Lazar, I. (2021, 24 de marzo). Collaboration tool security: how to avoid common risks. *Search Unified Commuications*. https://searchunifiedcommunications.techtarget.com/tip/Collaboration-tool-security-How-to-avoid-common-risks

Micó, A. B. (2020, 23 de noviembre). Bill Gates predice cuando llegará la próxima pandemia. *Periódico As*. https://as.com/diarioas/2020/11/23/actualidad/1606122301_572190.html

Microsoft (s.f.). *Microsoft 365 E5*. Consultado 22 de agosto de 2021. https://www.microsoft.com/es-co/microsoft-365/enterprise/e5?activetab=pivot:overviewtab

Microsoft. (2021a, 27 de octubre). *Seguridad y Microsoft Teams*. https://docs.microsoft.com/es-es/microsoftteams/teams-security-guide

Microsoft. (2021b, 31 de agosto). *Seguridad y cumplimiento en Microsoft Teams*. https://docs.microsoft.com/es-es/microsoftteams/security-compliance-overview

Millán, A. (2018) *Componentes de la infraestructura TI (OVI)* [video]. http://hdl.handle.net/10596/19310

Ministerio de Salud y Protección Social (Minsalud). (s.f.). *Coronavirus (COVID-19). Reportes y tableros de control*. https://www.minsalud.gov.co/salud/publica/PET/Paginas/Covid-19_copia.aspx

Ministerio de Salud y Protección Social (Minsalud). (2020, 24 de abril). *Resolución 666. Por medio de la cual se adopta el protocolo general de bioseguridad para mitigar, controlar y realizar el adecuado manejo de la pandemia del Coronavirus COVID-19*. https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%20666%20de%202020.pdf

Ministerio de Salud y Protección Social (Minsalud). (2021, 25 de febrero). *Resolución 223. Por medio de la cual se modifica la Resolución 666 de 2020 en el sentido de sustituir su anexo técnico*. Diario Oficial 515599. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30041616

Ministerio del Trabajo (Mintrabajo). (2020, 17 de marzo). *Circular externa 0021. Medidas de protección al empleo con ocasión de la fase de contención del COVID-19 y de la declaración de emergencia sanitaria*. https://www.mintrabajo.gov.co/documents/20147/0/Circular+0021.pdf/8049a852-e8b0-b5e7-05d3-8da3943c0879?t=1584464523596

Morpeth, A. (2020, 10 de marzo). Microsoft Teams vs Zoom for online meeting. *Obsessed Efficiency*. https://ucgeek.co/2020/03/microsoft-teams-vs-zoom-for-online-meetings/

Myservername.com. (s.f.). *Las 11 mejores soluciones DLP de software de prevención de pérdida de datos en 2021*. Consultado 12 de septiembre de 2021. https://es.myservername.com/11-best-data-loss-prevention-software-dlp-solutions-2021#4_Forcepoint_DLP

Nakamura, L., Stiverson, H. y Lindsey, K. (2021). *Racist zoombombing*. Routledge.

Neira Marciales, L. (2020, 10 de septiembre). Los call centers invierten hasta $2.000 millones al mes en las adecuaciones por la pandemia. *Diario La República*. https://www.larepublica.co/empresas/call-centers-invierten-hasta-2000-millones-al-mes-en-adecuaciones-por-la-pandemia-3057965

Palo Alto Networks. (s.f.). *What is Cybersecurity?* Consultado 20 de julio de 2021. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

Polycom. (s.f.). *Polycom acoustic fence for VVX business media phones*. Consultado 20 de julio de 2021. https://www.polycom.com/content/www/en/video-collaboration/innovations/acoustic-fence.html

Poly.com. (2021). *Bluetooth office headsets*. https://www.poly.com/content/dam/www/products/headsets/voyager/voyager-4300/doc/voyager-4300-uc-series-ds-en.pdf

Presidencia de la República de Colombia. (2012, 30 de abril). *Decreto 884. Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposicione*s. Diario Oficial 48417. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1183842

Presidencia de la República de Colombia. (2020a, 17 de marzo). *Decreto 417. Por el cual se declara un Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional*. https://coronaviruscolombia.gov.co/Covid-19/docs/decretos/general/51_Presidencia_Decreto_417.pdf

Presidencia de la República de Colombia. (2020b, 22 de marzo). *Decreto 457. Por la cual se imparte instrucciones en virtud de la emergencia sanitaria generada por la pandemia del coronavirus COVID-19 y el mantenimiento del orden público*. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20457%20DEL%2022%20DE%20MARZO%20DE%202020.pdf

Prey (software). (2021, 12 de octubre). En Wikipedia. https://es.wikipedia.org/wiki/Prey_(software)

Prey Project. (s.f.). *Cómo Funciona*. Consultado 22 de agosto de 2021. https://preyproject.com/es/como-funciona/?s=menu

Radware. (2020). *C-suite perspectives. Accelerated cloud migration but lagging security*. https://www.radware.com/resources/c-suite-2020/

Redacción El País. (2020, 26 de mayo). En Colombia hay seis millones de personas trabajando desde casa por la pandemia de covid-19. *El País*. https://www.elpais.com.co/economia/en-colombia-hay-seis-millones-de-personas-trabajando-desde-casa-por-la-pandemia-de-covid-19.html

Rodríguez García, O. (2020). Home Office en la nueva normalidad: retos y futuro del Home Office. *Revista Latinoamericana de Investigación Social*, *3*(3), 94-99. http://revistasinvestigacion.lasalle.mx/index.php/relais/article/view/2834

Rodriguez Mega, E. (2020, 14 de julio). El coronavirus sí permanece en el aire, pero no como te lo imaginas. *Salud con lupa*. https://saludconlupa.com/comprueba/el-coronavirus-si-permanece-en-el-aire-pero-no-como-te-lo-imaginas/

Sánchez, A. (2018, 4 de julio). SIP para dummies… Una breve guía práctica. *3CX*. https://www.3cx.es/blog/guia-protocolo-sip/

Seguridad América. (s.f.). *Prey - Protección y localización de dispositivos en piloto automático*. Consultado 22 de agosto de 2021. https://www.seguridadamerica.com/soluciones/prey-proteccion-y-localizacion-de-dispositivos-en-piloto-automatico/

Shi, W. & Gao, G. F. (2021). Emerging H5N8 avian influenza viruses. *Science*, *372*(6544), 784-786. https://doi.org/10.1126/science.abg6302

Software de prevención de pérdida de datos. (2021, 29 de abril). En Wikipedia. https://es.wikipedia.org/wiki/Software_de_prevención_de_pérdida_de_datos

Tillman, M. (2021, 22 de enero). Los mejores auriculares del Asistente de Google 2021: sonidos inteligentes de bose, Sony y más. *Pocket-lint*. https://www.pocket-lint.com/es-es/auriculares/guias-del-comprador/143305-los-mejores-audifonos-del-asistente-de-google-audifonos-y-audifonos-mejor-calificados-que-funcionan-con-el-asistente-de-google

Valenzuela Matutti, J. (2020). *Ciberataques en tiempos de coronavirus* [video]. Repositorio Institucional INICTEL. http://repositorio.inictel-uni.edu.pe:8080/xmlui/handle/123456789/28

Verbrugghe, C. (2020, 10 de abril). Comparing Zoom, Microsoft Teams and Google Meet. *Devoteam G Cloud*. https://gcloud.devoteam.com/blog/comparing-zoom-microsoft-teams-and-google-meet

Virtual appliance. (2021, 7 de enero). En Wikipedia. https://en.wikipedia.org/wiki/Virtual_appliance

Wi-Fi Now. (2018, 9 de febrero). *New roundup: Aerohive launches 'Atom' & Japan's KDDI goes 802.11ax*. https://wifinowglobal.com/news-and-blog/news-roundup-aerohives-atom-ap-japans-kddi-goes-802-11ax/