Decanato de Ingenierías e Informática

Escuela de Informática

Curso Monográfico

PROPUESTA DE ESTRATEGIAS PARA LA MEJORA DE LA CIBERSEGURIDAD DURANTE EL TELETRABAJO EN *CONTACT CENTERS/BPOS* DE SANTO DOMINGO.

Sustentada por:

Ydelky Alexandra Ulerio Contreras	**A00066846**
Luis Alberty Comas Rosario	**A00070796**
Johan Ferreira Serrata	**A00077938**

Asesor:

Willy Padua

Monografía para optar por el título de:

Ingeniería de Sistemas de Computación

Santo Domingo, D. N., 2021

ÍNDICE DE CONTENIDO

Dedicatorias

Agradecimiento

Resumen

Abstract

CAPÍTULO 1: ASPECTOS GENERALES DE LA INVESTIGACIÓN 1

INTRODUCCIÓN 1

1.1 Justificación 2

1.2 Delimitación 2

1.3 Selección y definición del tema 2

1.4 Planteamiento del problema 2

1.5 Objetivo 3

1.5.1 General 3

1.5.2 Específicos 3

1.6 Marco metodológico 4

CAPÍTULO 2: DESCRIPCIÓN DEL ÁMBITO GENERAL DEL TELETRABAJO EN *CONTACT CENTER* 5

2.1 Marco teórico 5

2.2 Definición 5

2.3 Antecedentes del teletrabajo 6

2.4 Historia de los *Contact Centers* 7

2.5 Normas internacionales 8

2.6 Ataques informáticos 9

2.6.1 Malware 9

2.6.2 Amenazas persistentes avanzadas 10

2.6.3 Puerta trasera 10

2.6.4 Fuerza bruta 10

2.6.5 Ingeniería social 10

2.6.6 Phishing 10

2.6.7 Spoofing 10

CAPÍTULO 3: APLICACIÓN DE LA CIBERSEGURIDAD, LOS CONTROLES Y SITUACIÓN ACTUAL DEL TELETRABAJO EN *CONTACT CENTER* SANTO DOMINGO 11
3.1 Que es la ciberseguridad 11
3.2 Controles críticos de ciberseguridad 11
3.2.1 Control protección del navegador web y del correo electrónico 12
3.2.2 Control defensas contra malware 12
3.2.3 Control Gestión de la infraestructura de red 12
3.3 Situación actual del teletrabajo en *Contact Center*, Santo Domingo 13
3.3.1 Comienzos 13
3.3.2 Posibles riesgos 14
3.3.3 Caso actual de “Contact Centers” en el parque de zona franca San Isidro, en Santo Domingo Este. 14
3.3.4 Entrevista a un supervisor de área de Contact Center 15
3.4.5 Encuesta 16
CAPÍTULO 4: IMPLEMENTACIÓN DE ESTRATEGIAS EN LA CIBERSEGURIDAD DURANTE EL TELETRABAJO 21
4.1. Elementos que conforman la estrategia 22
4.2 Plataforma Secure Remote Worker 23
4.2.1 Que es Secure Remote Worker? 23
4.2.2 Objetivos de Secure Remote Worker 23
4.3 Característica de la plataforma THINSCALE *Secure Remote Worker* 24
4.4 ¿Como funciona Secure Remote Worker? 28
4.5 Planteamiento de mejores practicas 29
4.6 Instalación de la plataforma *Secure Remote Worker* 32
4.6.1 Requerimientos de sistema 32
4.6.2 Guía de instalación en servidor 32
4.7 Políticas propuestas 33
4.7.1 Políticas de cuentas de usuarios de Windows 33
4.7.2 Políticas de grupo de Windows 33

CAPÍTULO 5: EVALUACIÓN DEL IMPACTO EN EL TELETRABAJO DE LOS *CONTACT CENTER* DE SANTO DOMINGO 35
5.1 Análisis de problemática actual 35
5.2 Análisis comparativo de situación actual versus propuesta 35
CONCLUSIÓN 37
Recomendaciones 38
Bibliografia 40
ANEXOS 44

ÍNDICE DE FIGURAS

Figura 1: Norma para implementar un SGSI 9
Figura 2: Primera repuesta encuesta 16
Figura 3: Segunda repuesta encuesta 16
Figura 4: Cuarta repuesta encuesta 17
Figura 5: Sexta repuesta a encuesta 18
Figura 6: Octava repuesta encuesta 19
Figura 7: Propuesta infraestructura teletrabajo 21
Figura 8: Implementación básica SRW 29

ÍNDICE DE TABLAS

Tabla 1: Elementos de la estrategia 22
Tabla 2: Controles para accesos remotos 30
Tabla 3: Requisitos de instalacion SWR 32

INDICE DE ANEXOS

Anexo A: Norma ISO/IES 27002-2013..... 44
Anexo B: Norma ISO/IES 27005-2008..... 46
Anexo C: Norma ISO/IES 27003-2010..... 48
Anexo D: Control de proctección navegador y correos electronicos..... 49
Anexo E: Control de defensas con *malware* 50
Anexo F: Gestión de infraestructura de red 51
Anexo G: Guía de instalacíon servidor SWR 52
Anexo H: Encuesta 55

LISTA DE ACRÓNIMOS

Acrónimo	Significado
BPO	Business Process Outsourcing
TIC	Tecnologías de la información y comunicación
USB	Universal Serial Bus
SGSI	Sistema de Gestión de Seguridad de la Información.
ISO	Organización Internacional de Normalización
IEC	Comisión Electrotécnica Internacional
CIS	Center for Internet Security
RDS	Remote Desktop Service
SQL	Structured Query Language
DMZ	Demilitarized Zone
BYOD	Bring Your Own Device
PCI	Payment Card industry
HIPAA	Health Insurance Portability and Accountability Act
TI	Tecnología de la Información
AEP	Prevención de ejecución de aplicaciones
SEP	Prevención de ejecución de servicios
PC	Computador Personal
NIST	Instituto Nacional de Estándares y Tecnología
FISMA	Modernización Federal de la Seguridad de la Información
TLS	Transport Layer Security
TIC	Conexiones a Internet de Confianza

Dedicatoria

Dedico primeramente este trabajo a Dios, por haberme dado la vida, como guía presente en el camino de mi vida, bendiciéndome y dándome las fuerzas para continuar en este proceso y metas trazadas tan importante de mi formación profesional.

A mi madre querida la señora **María Milagros Contreras Ayala**, por ser el más importante pilar en mi vida, porque ha estado ayudándome en las buenas y en las malas y lo continúa haciendo, por todo su apoyo incondicional, su amor y confianza depositadas todas en mí, que me permitieron lograr la culminación de mi formación profesional.

A mi hijo **Axel David de la Cruz Ulerio**, posiblemente en estos momentos no entiendas mis palabras, sé que algún día las entenderás, eres esa luz que me mantiene a flote cada día, eres esa motivación por la cual me esfuerzo más por el presente y el mañana, este logro es por ti.

A mis abuelos la señora **Leonora Ayala** y **Pedro Antonio Contreras Castaños**, nunca voy a poder devolverle todo el esfuerzo que hicieron por mí, por su apoyo incondicional, por enseñarme siempre a no detenerme.

-Ydelky Alexandra Ulerio Contreras

Dedicatoria

Le dedico este trabajo a las tres damas de mi vida, mi hija **Alyssa Comas** la cual ha sido la fuerza que me motivo a regresar a mis estudios luego de mi retiro, a mi madre **Zeneida Rosario** quien siempre ha sido un apoyo incondicional en todo este proceso de crecimiento personal que he experimentado y a mi amada esposa **Nancy López** quien ha sido mi complemento, apoyo, consejera y compañera de esta aventura llamada vida.

También a mi padre **Luis Batista** el gran hombre que me enseño que, con trabajo duro, amor, esfuerzo y honestidad se logra echar adelante, mi hermano **Carlos Batista**, mi hermana **Darlene Batista**, a mi hermana **Jerelee Batista**, mi hermana menor **Ana Celia Batista**, mi sobrina **Sarah Sophia Batista**.

Finalmente, pero no menos importante a tres personas muy importantes en mi vida las cuales siempre han estado a mi lado desde mi niñez mi querido primo H**enry Bido, Douglas Saldaña** y **Moisés Padilla** quienes siempre han demostrado que la hermandad va más allá de la sangre.

-Luis Alberty Comas Rosario

Dedicatoria

Dedico esta investigación a mi familia, en especial a mis padres, mi esposa y mi hijo, que me han brindado su apoyo y amor incondicional. A mis compañeros de la universidad, que han aportado a mi crecimiento profesional y personal durante este trayecto.

-Johan Ferreira

Agradecimiento

El presente trabajo agradezco a Dios por ser mi guía, por darme esa paciencia y sabiduría para llegar al término de esta meta propuesta.

A mi **madre** por todo su esfuerzo, paciencia, dedicación, confianza que me ha brindado durante toda mi vida.

A mi **hijo** por comprenderme durante el desarrollo de la carrera misma, por entender ese sacrificio necesario de no estar todo el tiempo para ti.

A mis **abuelos** maternos por ser esas personas después de mi madre que más se han ocupado de mí.

A mi **esposo** te encontré en el camino y ha sido un apoyo incondicional, por medio de tus consejos, amor y paciencia ayudándome para ver concluida esta meta.

Mis tías las cuales a cada una tengo que agradecer este logro, **Ybelky** por siempre apoyarme y ayudarme en todo momento durante esta meta, **Soraida** por darme ese apoyo al inicio de mi carrera, **Deysi** por todo el tiempo que me ha apoyado y me has dado de tu tiempo en todo lo que necesito para ayudarme a terminar este logro, tío **Polín** aun desde lejos siempre atento y brindándome su cariño en todo momento.

A todas esas personas que no he podido mencionar que de alguna manera estuvieron presente, gracias.

A mis compañeros, **Luis Comas** y **Johan Ferreira** porque no se es equipo solo, por su paciencia y su ayuda en todo momento esto no sería posible. Al **Dr. Rubén Darío Pimentel**, por su ayuda en cuanto a las orientaciones recibidas para la terminación de este trabajo.

A la Universidad APEC en conjunto con los profesores, por permitirme concluir con esta etapa de mi vida y guiarme durante el desarrollo de esta investigación.

-Ydelky Alexandra Ulerio Contreras

Agradecimiento

Agradezco en primer lugar a Dios por permitirme concluir este ciclo, a mi familia por siempre estar a mi lado, a mis compañeros de monografía **Ydelky Ulerio** y **Johan Ferreira** por su gran compromiso en este trabajo.

Agradecimientos especiales a **Henry Bido** por darme el apoyo en los momentos más difíciles, a **Douglas Saldaña** por ser un ente motivador y apoyo moral en todo momento, al señor **Ángel Pérez** por esos valiosos consejos y por ser un gran líder y guía.

-Luis Alberty Comas Rosario

Agradecimiento

Agradezco a mi madre, **Suleika Serrata**, por todo el apoyo que me ha brindado. A mi esposa, **Charina Rosado**, por su amor y complicidad para conmigo. A mis compañeros de la universidad que se han convertido en muy buenos amigos: **Esmil Contreras**, J**ose Moya**, **Edwin Castillo** y **Francisco Deño**. A los maestros, que a lo largo de mi paso por UNAPEC contribuyeron en mi crecimiento profesional. De manera especial a mis compañeros de monográfico, **Ydelky Ulerio** y **Luis Comas**, por haber hecho esto posible.

-Johan Ferreira

Resumen

La monografía titulada “Propuesta de estrategias para la mejora de la ciberseguridad durante el teletrabajo en *Contact Centers/BPO* de Santo Domingo”, fue un trabajo de investigación basado en la experiencia que vivieron este tipo de negocios, para lograr la implementación del teletrabajo durante el confinamiento obligatorio a causa de la pandemia por coronavirus (COVID-19). Con la finalidad de analizar cuáles fueron las amenazas y los riesgos que tuvieron desde el punto de vista informático y a partir de este análisis, presentar una propuesta de implementación de una solución de software de THINSCALE que proporcionará un ambiente controlado por las empresas que garantice realizar el trabajo de agente de Contact Center en formato remoto con la aplicación de políticas y controles recomendados por los institutos internacionales de tecnología y las guías de mejores prácticas.

Palabras Claves: Teletrabajo, “Contact Centers”, Ciberseguridad, Agentes

Abstract

The monograph entitled "Proposal of strategies for the improvement of cybersecurity during teleworking in "Contact Centers/BPO" of Santo Domingo", was a research work based on the experience that lived this type of business, to achieve the implementation of teleworking during mandatory confinement due to the coronavirus pandemic (COVID-19). In order to analyze what were the threats and risks that had from the computer point of view and from this analysis, present a proposal for the implementation of a software solution of THINSCALE that provide an environment controlled by companies that guarantees to perform the work of Contact Center agent in remote format with the application of policies and controls recommended by the international institutes of technology and best practices guides.

Keywords: *Teleworking, "Contact Centers", Cybersecurity, Agent*

CAPÍTULO 1: ASPECTOS GENERALES DE LA INVESTIGACIÓN

INTRODUCCIÓN

Desde finales del año 2019 el mundo se vio sacudido por un evento que cambio la manera en que nosotros los seres humanos nos relacionamos, compartimos y hasta como trabajamos. Partiendo de este evento muchas empresas trataron de sobrevivir aplicando procesos que facilitaran la conectividad de sus colaboradores y así poder generar valor en medio de un mundo detenido por la pandemia COVID-19.

Los *Contact Centers* no son una excepción a la regla, los mismos se vieron forzados a cambiar sus operaciones y enviar muchos agentes a sus hogares para poder seguir operando. Esto generó retos en los departamentos de TI como la conectividad y la seguridad de la misma, también se generan inquietudes de como mitigar los riesgos provenientes de dichos cambios en las operaciones.

Esta investigación se basa en el enfoque de cómo enfrentar esos retos haciendo un análisis de los precedentes, trazando una propuesta tecnológica la cual pueda suplir faltas en el proceso, se proponen políticas y controles para eficientizar dicha propuesta y elevarla a niveles en los cuales se pueda trabajar de forma segura en un entorno no seguro y usando BYOD.

En el presente trabajo podrá ver un análisis de la situación inicial de los Contact Center, tocando un poco la historia, los aspectos fundamentales del teletrabajo. Luego del análisis se enfocarán los esfuerzos en el diseño de una solución tecnológica que se acople a las necesidades de este modelo de negocio, junto con la propuesta de solución las cuales están guiadas por políticas, controles y mejores prácticas que garantizaran el buen funcionamiento del entorno.

Para finalizar se hará un análisis del impacto que se tendría con la implementación de la solución propuesta tomando en cuenta todos los criterios aprendidos durante el análisis del problema.

1.1 Justificación

- Aumentar los conocimientos teóricos y prácticos en infraestructura y ciberseguridad para ayudar en la toma de decisiones al momento de la adquisición o implementación de softwares.
- Mitigar las vulnerabilidades de la infraestructura tecnológica actual de los *Contact Center/BPO* que mantiene a los agentes laborando de forma remota en Santo Domingo, República Dominicana.

1.2 Delimitación

Mejora de la ciberseguridad durante el teletrabajo, como medio de prevención de fraudes y malas prácticas por parte de los agentes de los *Contact Center/BPOs* en Santo Domingo, República Dominicana, que se encuentran trabajando de forma remota dentro de la provincia Santo Domingo con un computador de la empresa y con acceso a internet.

1.3 Selección y definición del tema

Los *Contact Center* son un servicio indispensable hoy en día para cualquier compañía. En sus comienzos principalmente era informativo y era más un accesorio a la oferta principal del producto. Pero las empresas vieron la oportunidad de un nicho sin explotar y su utilización se expandió notablemente. La constante aparición de competencia dejaba claro que ya no era algo “de lujo” comunicarse con el cliente, sino que más bien debía ser un canal habitual y necesario para que el usuario se sintiese atendido y satisfecho.

Esto y la fuerte demanda del cliente particular, aunado al boom tecnológico, dieron como resultado un departamento de atención al cliente que hoy en día sigue dando de qué hablar y que ve cómo diariamente alzan las expectativas, por eso siempre están buscando reinventarse junto a las mejores innovaciones.

1.4 Planteamiento del problema

En vista de la situación sanitaria que se vive a nivel mundial, muchos *Contact Center* han tenido que implementar el teletrabajo para poder seguir operando. Esta nueva modalidad trae consigo riesgos informáticos a causa de que los empleados que se encuentren trabajando de forma remota dentro de la provincia Santo Domingo, tienen

menos controles y supervisión por parte de la institución. Motivo por el cual planteamos el problema de investigación: Estrategia para la mejora de la ciberseguridad durante el teletrabajo en *Contact Center/BPO* de Santo Domingo.

En la actualidad algunas instituciones carecen de una plataforma de conexión segura desde la computadora del agente hacia los servidores de la compañía, esto permite que el agente tenga acceso a capturas/grabación de pantalla, copiar datos sensitivos de clientes, acceder a correos/redes sociales personales y compartir por esa vía los datos ya mencionados.

Agregado a esto, está el hecho de que los agentes tienen la posibilidad de acceder a su teléfono personal en horas de trabajo, lo cual le permite tomar fotos y videos en vivo de la información mostrada en pantalla en los diferentes sistemas de uso de trabajo. Esto representa un reto mayor, ya que fuera del computador, no tenemos posibilidad de mecanismos de control más allá de los controles persuasivos.

¿Cómo podemos reducir el riesgo de filtración de información sensible de nuestros clientes por parte de nuestros agentes?

¿Cuáles son los riesgos que existen en torno al teletrabajo en empresas de tipo *Contact Center o BPO*?

1.5 Objetivo

1.5.1 General

Diseñar un ambiente de trabajo seguro y confiable para los agentes de *Contact Center* que se encuentran trabajando de forma remota dentro de la provincia Santo Domingo.

1.5.2 Específicos

- Analizar la situación actual del teletrabajo en *Contact Center*.
- Proponer una solución tecnológica que permita el teletrabajo, bajo la implementación de controles y mejores prácticas.
- Evaluar el impacto que tendrá la adopción e implementación de la solución tecnológica propuesta.

1.6 Marco metodológico

El enfoque de nuestra investigación es cualitativo, ya que está basada en la extracción de conclusiones a partir de datos no estructurados.

Es de carácter no experimental, puesto que los datos obtenidos durante la investigación no son alterados.

Es de tipo descriptiva, ya que se explican las situaciones actuales y la evolución del tema a tratar. Proyectiva porque se da solución a un problema actual con la elaboración de una propuesta.

Para esta investigación nos auxiliamos de las técnicas de investigación siguientes: encuesta, entrevista, documentaciones y publicaciones periodísticas.

CAPÍTULO 2: DESCRIPCIÓN DEL ÁMBITO GENERAL DEL TELETRABAJO EN *CONTACT CENTER*

2.1 Marco teórico

Riesgos de filtración de información sensible de clientes de empresas subcontratadas en *Contact Center o BPO*.

2.2 Definición

Teletrabajador es la persona que, bajo una relación de subordinación, presta sus servicios al empleador para el desarrollo de actividades laborales, a través del uso de herramientas tecnológicas y medios digitales en un establecimiento distinto del local habitual del empleador. (Ministerio de trabajo, 2020, pág. 5).

Tecnologías de la información y comunicación (TIC) es el conjunto de servicios, herramientas, redes, dispositivos y softwares, que permiten la ejecución del contrato de trabajo bajo la modalidad del teletrabajo, así como una comunicación efectiva entre el empleador y el trabajador. (Ministerio de trabajo, 2020).

Contact Center es una plataforma telefónica que facilita la comunicación entre agentes y clientes a través de diferentes medios: teléfono, email, chat, web, fax, beeper, etc. Y, además, garantiza en una misma base de datos el registro de cada uno de los contactos realizados, que permite mejorar la atención al cliente. (Conde del Oso, 2005).

El teletrabajo es una modalidad que se apoya en el uso de las TIC, para permitirle al empleado trabajar a distancia de las instalaciones de la empresa. Su etimología procede de la palabra griega tele (lejos) y de la palabra latina trabajo, que es realizar alguna labor física o intelectual de manera continua. (OPTIC, 2020, p. 12).

Existen diferentes modalidades de teletrabajo, según (Organización Internacional del Trabajo, 2016) entre ellas:

- Escritorio multiusuario (*hot desking*, nombre en inglés) donde el empleado labora un tiempo a distancia y el resto en las oficinas de la empresa, en esta modalidad el empleado no tiene un escritorio fijo asignado/reservado para su uso.

- Escritorio multiusuario con reserva (*hotelling*, nombre en inglés) parecido a multiusuario, pero los trabajadores deben realizar una reserva previa para ir a las oficinas.
- Telecentros, instalaciones que ofrecen estaciones de trabajo y otro equipo de oficina a los trabajadores de diversas entidades, también conocido como *working space*.
- Oficinas colaborativas, que son entornos de trabajo virtuales en los que los trabajadores pueden trabajar en colaboración desde distintos lugares gracias a una red de telecomunicaciones.

2.3 Antecedentes del teletrabajo

El teletrabajo permite realizar nuestra actividad laboral desde una ubicación distinta a la sede de la empresa para la cual laboramos. Regularmente se realiza desde el domicilio del colaborador, pero puede darse desde otras ubicaciones tales como un hotel, una cafetería, un medio de transporte mientras viaja, etc. Las organizaciones han adoptado este método de trabajo porque permite la adaptación ante posibles situaciones excepcionales, como el confinamiento obligatorio causado por la pandemia del COVID-19.

La seguridad es un tema de suma importancia durante el teletrabajo, puesto que el colaborador estará fuera de la red de la empresa y el nivel de exposición a las amenazas será mayor, según documentación publicada por el (INCIBE Instituto Nacional de Ciberseguridad, 2020):

> La seguridad durante el teletrabajo está vinculada a la tecnología utilizada para el acceso remoto y para la actividad diaria. Por tanto, dependerá de los riesgos asociados a los mecanismos de acceso remoto a la red y a los servidores de la empresa, y de los relativos al uso de ordenadores de sobremesa, portátiles, teléfonos inteligentes o tabletas, medios de almacenamiento extraíbles (memorias USB, discos duros, etc.), herramientas colaborativas y aplicaciones en la nube. En ocasiones esta tecnología es compartida para usos domésticos lo que conlleva riesgos específicos. (p.2)

Autorizar este método de trabajo sin contar con las medidas de seguridad necesarias puede ser un riesgo para la empresa, puesto que los colaboradores podrían utilizar aplicaciones y dispositivos no autorizados, propiciando el acceso de los ciberdelincuentes a la red privada de la empresa y a la información gestionada por la misma, lo cual pone en riesgo la continuidad del negocio.

Para disminuir estos riesgos (INCIBE Instituto Nacional de Ciberseguridad, 2020) hace algunas recomendaciones, entre las cuales podemos destacar:

> Para disponer de un entorno de teletrabajo seguro, necesitamos establecer una política de seguridad en la que se contemplen las directrices a seguir respecto al uso de los distintos sistemas y métodos de acceso, contemplando todos los posibles escenarios. Esta política debe definir las medidas necesarias para proteger los dispositivos de teletrabajo, garantizar conexiones remotas seguras. (p.2)

2.4 Historia de los *Contact Centers*

Los *Contact Centers* surgieron básicamente como funcionalidades nuevas que, empresas interesadas en la atención al cliente o televentas, ya ejercían. Pronto este servicio empezó a ofrecer en modalidad de *outsourcing* por nuevas empresas que surgieron para dedicarse de manera integra a desarrollar las practicas diversas de los *Contact Centers*. (Micheli Thirión, 2007).

Según dice (Garcia Encarnacion & Freites Mejia, 2018):

> Desde sus inicios, en la década de 1970, los *Contact Centers* aceleraron las transacciones del mercado mediante el concepto del telemarketing, y a partir de entonces los centros de llamadas y sus proveedores tecnológicos se han expandido hasta representar un sector económico global. (p. 5)

Los primeros *Contact Centers* de gran tamaño fueron el resultado de una reestructuración interna de organizaciones con una gran base de clientes, como bancos, compañías de seguros, de telecomunicaciones, informática, comercio, pero actualmente

son también proveedores independientes y especializados que abarcan todos los servicios y países que requieren una plataforma de TIC. (Garcia Encarnacion & Freites Mejia, 2018).

En la actualidad, con las innovaciones tecnológicas digitales, los *Contact Centers* son operadores de la relación empresa-clientes mediante comunicación en más de un canal, mejor conocida como omnicanalidad, que no es más que el uso de múltiples canales de comunicación, pero de una manera unificada.

2.5 Normas internacionales

Las normas de seguridad son reglas que nos ayudan a poder implementar de manera exitosa un sistema de gestión de la seguridad de la información (SGSI), y se apoya en pautas y políticas para control, implementación y gestión de riesgos. Según nos indica (Duque & Orozco Alzate, 2017):

> Uno de los requisitos para implementar un SGSI en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos. Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC). (p. 75)

Está compuesta por aproximadamente 17 normas, clasificadas en cuatro categorías:

i. La norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000.
ii. Las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006.
iii. Las normas guía desarrolladas a través de 10 normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032.
iv. Las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017.

Las categorías mencionadas que se citan en esta investigación son normas las cuales servirán como guías de consultas para la implementación exitosa del sistema de gestión de la seguridad de la información (SGSI), (ver anexos A, B, C).

Figura 1

Principales normas para implementar un SGSI basado en los estándares de la familia de normas ISO/IEC 27001:2013

Nota: Como se puede observar entre todas las normas existente la en la familia ISO/IEC 27000 la combinación de las citadas en la anterior imagen representa los pilares para la implementación de un SGSI (Sistema de gestión de la seguridad de la información).

2.6 Ataques informáticos

2.6.1 Malware

(ISACA, 2015) “También llamado código malicioso, es el software diseñado para tener acceso a sistemas informáticos específicos, robar información o interrumpir las operaciones informáticas” (p.30).

2.6.2 Amenazas persistentes avanzadas

(ISACA, 2015) “Ataques complejos y coordinados dirigidos a una entidad u organización específica. Estos requieren una enorme cantidad de investigación y tiempo, a menudo se toman meses o incluso años para ejecutarse plenamente” (p. 31).

2.6.3 Puerta trasera

(ISACA, 2015) “Un medio de recuperar el acceso a un sistema comprometido mediante la instalación de software o la configuración de software existente para permitir el acceso remoto bajo condiciones definidas por el atacante” (p. 31).

2.6.4 Fuerza bruta

(ISACA, 2015) “Un ataque realizado al intentar todas las combinaciones posibles de contraseñas o claves de cifrado hasta encontrar la correcta” (p. 31).

2.6.5 Ingeniería social

(ISACA, 2015) “Cualquier intento de explotar las vulnerabilidades sociales para tener acceso a la información y/o sistemas” (p. 32).

2.6.6 Phishing

(ISACA, 2015) “Un tipo de ataque vía correo electrónico (e-mail) que intenta convencer a un usuario de que el origen es genuino, pero con la intención de obtener información para su uso en ingeniería social.” (p. 32).

2.6.7 Spoofing

(ISACA, 2015) “Falsificación de la dirección de envío de una transmisión con el fin de obtener la entrada ilegal a un sistema seguro” (p. 32).

CAPÍTULO 3: APLICACIÓN DE LA CIBERSEGURIDAD, LOS CONTROLES Y SITUACIÓN ACTUAL DEL TELETRABAJO EN *CONTACT CENTER* SANTO DOMINGO

3.1 Que es la ciberseguridad

Cuando se habla de aplicar la ciberseguridad tenemos que tener conocimiento de que es, para ello la definimos según nos dice (UIT, 2010):

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. (p. 20)

Otra fuente consultada expresa en que consiste la ciberseguridad, (González Ferreras, Reyes Matos, Rodriguez Asencio, & Padua Ruiz, 2020) plantean que:

> La ciberseguridad consiste en la protección de activos de información mediante el manejo de los riesgos y amenazas a los datos que son procesados, almacenados y transportada en sistemas de información que se encuentran conectados con redes, tanto locales como el Internet. (p. 20)

3.2 Controles críticos de ciberseguridad

Los controles CIS o controles críticos de ciberseguridad según (Center for Internet Security (CIS), 2021) “Son un conjunto priorizado de salvaguardias para mitigar los ciberataques más frecuentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y de políticas”.

Esta lista está conformada actualmente en su versión 8 por 18 controles los cuales están orientados para la ciberdefensa, cada control se dirige a áreas especifica como lo son: controles básicos, controles funcionales y controles organizacionales.

3.2.1 Control protección del navegador web y del correo electrónico

Este control permite mejorar las protecciones y las detecciones de amenazas del correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través del compromiso directo. Este control es crítico ya que es un punto de entrada muy común en los atacantes. El contenido puede ser diseñado para atraer o engañar a los usuarios para que revelen credenciales, proporcionen datos confidenciales o proporcionar un canal abierto para permitir que los atacantes obtengan acceso, aumentando así el riesgo para la empresa. (ver anexo D)

3.2.2 Control defensas contra malware

Este control previene o controla la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en los activos empresariales. Su propósito va desde capturar credenciales, robo de datos, identificación de otros objetivos dentro de la red y cifrado o destruir datos. El malware está en constante evolución y se adapta, a medida que las variantes modernas aprovechan técnicas de aprendizaje automático. (ver anexo E)

3.2.3 Control Gestión de la infraestructura de red

Este control permite establecer, implementar y administrar activamente (Rastrear, informar, corregir) dispositivos de red, para evitar que los atacantes exploten servicios de red y puntos vulnerables. Este es una defensa esencial contra los ataques. Este control incluye una arquitectura de seguridad adecuada, que aborda las vulnerabilidades que a menudo, son introducida con configuraciones predeterminadas, monitoreo de cambios y reevaluación de las configuraciones. La infraestructura de red incluye dispositivos físicos y virtualizados. Pasarelas, cortafuegos, puntos de accesos inalámbricos, enrutadores y conmutadores. (ver anexo F)

3.3 Situación actual del teletrabajo en *Contact Center*, Santo Domingo

3.3.1 Comienzos

Desde el inicio de la pandemia de Sars-Cov 19 a inicios de 2020, muchas empresas se vieron forzadas a cambiar su modelo de trabajo debido a la crisis que el brote pandémico estaba generando a nivel mundial y a la necesidad de evitar el contacto directo entre cliente y colaboradores con el fin de mitigar la tasa de contagio que en esas fechas estaba en un ascenso alarmante.

Dicho cambio de modelo llevó a los departamentos de ciberseguridad a nuevos retos entre los cuales se pueden citar:

- Cómo mover la mayor cantidad de colaboradores a trabajar de manera remota de la manera más segura posible.
- Cómo mantener la plataforma de seguridad de la empresa asegurada teniendo menos controles sobre los usuarios, ya que estos están laborando fuera del entorno seguro de la institución.
- Cómo mitigar el riesgo de fuga de información y su subsiguiente mal uso.

En este caso los *Contact Centers* no fueron la excepción pues debido al modelo de trabajo de los mismo y la información sensible que manejan. Tanto de cliente como de terceros, les crea todo un reto para poder mitigar las distintas amenazas que se pueden presentar en el proceso de cambio de presencial a remoto.

En la actualidad, la mayoría de los *Contact Center* de la República Dominicana se han visto en la obligación de suspender a una parte de sus agentes sin disfrute salarial dadas las medidas de distanciamiento y reducción del número de personas permitidas para los espacios públicos y privados dispuestas por el gobierno.

Pocos han podido lograr que los agentes puedan continuar laborando de manera remota (teletrabajo o trabajo a distancia) debido a la falta de una solución tecnológica que permita la realización del trabajo de manera segura, garantizando la confidencialidad de los datos de los clientes.

Esto a su vez se traduce en una baja productividad y no cumplimiento de métricas, dado que una de las cláusulas más comunes en los contratos de Outsourcing es el

headcount (cantidad de agentes disponibles para atender las llamadas) exigido por el cliente.

3.3.2 Posibles riesgos

Todo cambio trae consigo ciertos riesgos de los cuales actualmente los estafadores aprovechan estas oportunidades entre los posibles riesgos a mitigar:

- Posible robo de información usando dispositivos móviles.
- Redes de hogar compartidas y poco seguras.
- Posibles infecciones de equipos remotos por errores del usuario.

3.3.3 Caso actual de "Contact Centers" en el parque de zona franca San Isidro, en Santo Domingo Este.

A partir de marzo de 2020 debido a la pandemia generada del COVID-19 llevó a los gobiernos a tomar medidas drásticas, como el cierre casi total de las actividades industriales y económicas, obligando a las empresas a suspender la mayoría de sus empleados por un periodo indefinido y sin disfrute de salario.

En el caso de José el coronavirus le cambia la vida no solo a él sino a miles más, estos han vivido muchos estragos y más de un 30% a 40% pierden sus empleos. Según lo comentado por (Listin Diario, 2020):

> La parte emocional de José se mantiene ecuánime, pero por momentos la asusta el futuro cercano ante una situación sanitaria que cada vez se sale de control. Todos sus ahorros se han ido a pique por el impacto de la pandemia y la obligación de cerrar la compañía que administraba y que en 2018 tenía cerca de 200 trabajadores hasta finalmente quedarse con 35 colaboradores la última semana de junio. "Todo se ha ido a pique" y no fue por mala administración. Fue que el negocio cambió y no había la demanda suficiente y por más que se luchó por no cerrar durante cuatro meses no fue posible, dice. Los compradores no estaban buscando lancetas, tirillas ni glucómetros. Ni mucho menos alarmas, estaban comprando insumos para contrarrestar el impacto del coronavirus y no era posible mantener esa cantidad de empleados que fueron disminuyendo muy

a su pesar, apunta. Actualmente, de 24,000 empleados laborando en los centros de contactos en el país desde antes de la crisis sanitaria se estima que hayan alrededor de 18,000 trabajadores activos, según explicaciones del presidente del clúster de centros de contactos o llamadas (*Call Centers*), David Crow. Desde el inicio de la crisis en marzo, dice David Crow, presidente del clúster de centros de contactos o centros de llamadas, “fuimos forzados hacer transicional a trabajo remoto. Como industria, llegamos a habilitar 74% de nuestros empleados trabajar desde sus casas.

3.3.4 Entrevista a un supervisor de área de Contact Center

En la entrevista realizada al Ingeniero Johan Polanco (comunicación personal, 30 de junio, 2021), el cual tiene 15 años de experiencia en el área de *Contact Center*, estando en el cargo de supervisor.

De acuerdo a las preguntas realizadas (ver anexo H) nos dice:

El trabajo antes del COVID-19 era algo muy mínimo, se basaba en realizar conexiones VPN, para acceder a realizar backup o accesos a programas y estos se hacía a través de llamadas móviles, iniciamos con el proceso para trabajar de manera remota desde marzo 2020, motivo en el cual las empresas se vieron obligadas a cerrar debido a la pandemia. En cuanto al crecimiento no hubo alguno dentro de la institución ya que no fue necesario, porque en vez de incrementar se disminuyó, como hemos vistos muchas empresas se vieron obligadas a cerrar sus operaciones y otras a disminuirlas. En cuanto al proceso y tiempo de implementación se utilizó para acceder Cisco Any Connect Secure Mobility Client y la aplicación de voz Cisco Jabber, el tiempo implementado aun con limitaciones ya el departamento de TI antes tenía previamente la solución agenda y se tomó 72 horas aproximadas. Se estipuló el uso del Bring Your Own Device (BYOD), con el cual se les permitía a los usuarios la utilización de sus propios equipos ya sea laptop o PC y si el agente no tenia se traslada directamente a la empresa. En el proceso de configuración de usuarios no hubo incidencias ya que se le facilitaron manuales para la instalación y mediante servidores que utilizan el protocolo File Transfer Protocol (FTP) se le agregaron los programas a instalar. Entre los posibles problemas fueron de

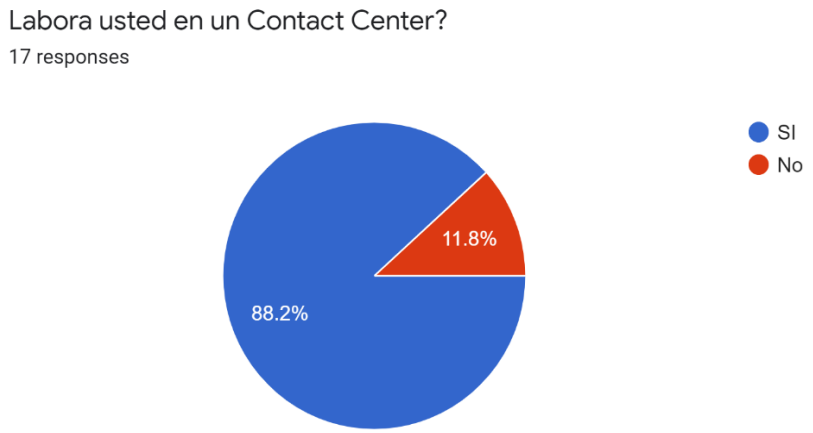
conexión a internet por motivo de lentitud ya que se necesitaba una mínima ancho de banda, el cual fue resuelto la empresa se hizo responsable del aumento del costo de los servicios de los agentes.

3.4.5 Encuesta

Pregunta 1

Figura 2

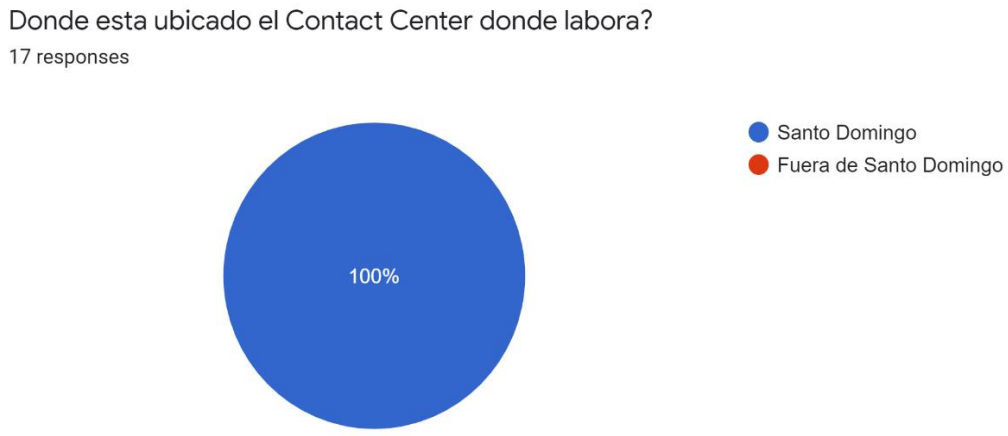
Repuestas obtenidas por encuesta realizada relación si labora en Contact Center



Pregunta 2

Figura 3

Repuestas obtenidas por encuesta realizada relación a ubicación del Contact Center



Pregunta 3

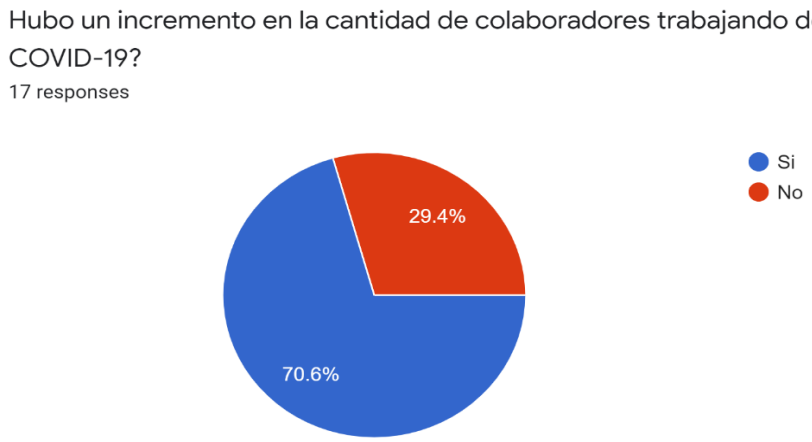
¿Cómo era el teletrabajo antes del COVID-19?

Al analizar las 17 respuestas obtenidas de los encuestados, podemos constatar que el teletrabajo era inexistente, o reservado para personal contratado en el exterior del país, antes de que el país fuera afectado por la pandemia del COVID-19, lo que evidencia una falta de preparación para este tipo de eventualidades por parte de los “Contact Centers” de la ciudad de Santo Domingo.

Pregunta 4

Figura 4

Repuestas obtenidas por encuesta realizada relación al crecimiento en Contact Center



El incremento en la cantidad de colaboradores habilitados para trabajar de forma remota a partir de la pandemia por el COVID-19 es notable, 12 de nuestros encuestados pudieron constatar este aumento en las empresas donde laboran.

Pregunta 5

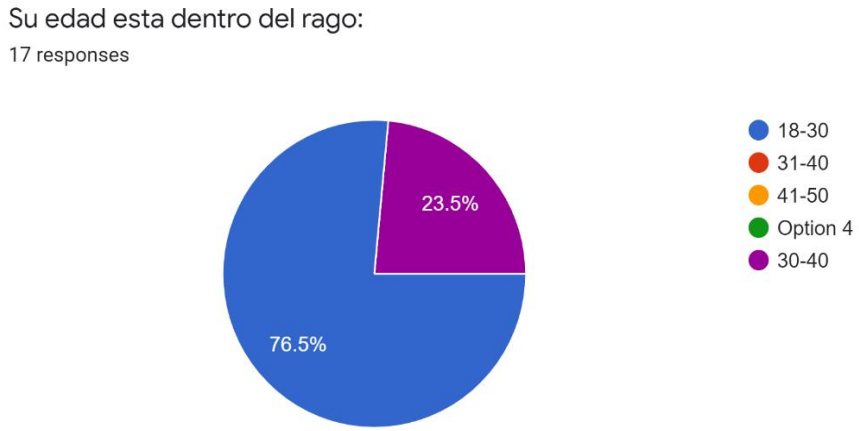
¿Cuánto tiempo ha estado usted laborando de forma remota?

De los 17 encuestados, solo 3 no fueron colocados para trabajar remotamente durante el cierre por la pandemia, el resto, ha estado trabajando de forma remota desde marzo 2020. Algunos ya se encuentran laborando desde las oficinas de la empresa gracias a la reapertura económica por parte del gobierno y el aumento en la cantidad de ciudadanos vacunados. Esto confirma que las empresas se vieron forzadas a implementar esta forma de trabajo para poder continuar con las operaciones, evitando así pérdidas económicas mayores y garantizando la continuidad del negocio.

Pregunta 6

Figura 5

Repuestas obtenidas por encuesta realizada relación al rango de edad en Contact Center



Pregunta 7

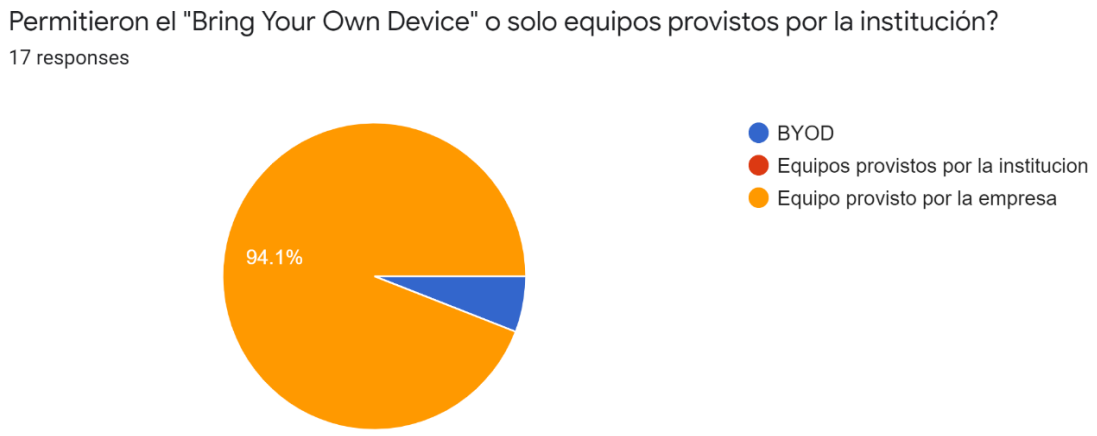
¿Cuál fue el proceso llevado a cabo para colocar a los colaboradores a trabajar remotamente y cuánto tiempo llevo implementarlo?

El proceso seguido por cada empresa fue distinto y el tiempo de implementación vario entre 48 horas y 2 semanas, de acuerdo con las respuestas obtenidas. Mayoría coincidían en que la empresa preparaba los equipos tecnológicos y luego los entregaba en el domicilio de los agentes, en algunos casos habilitando un canal de comunicación con el departamento de IT para guiar a los agentes en el proceso conexión y configuración de estos.

Pregunta 8

Figura 6

Repuestas obtenidas por encuesta realizada relación al rango de edad en Contact Center



Solo un colaborador trabaja en una empresa donde está permitida esta política, que le permite a los empleados hacer uso de sus equipos tecnológicos personales para realizar las labores de la empresa. Desde el punto de vista de seguridad, es más recomendable usar estrictamente equipos provistos por la empresa.

Pregunta 9

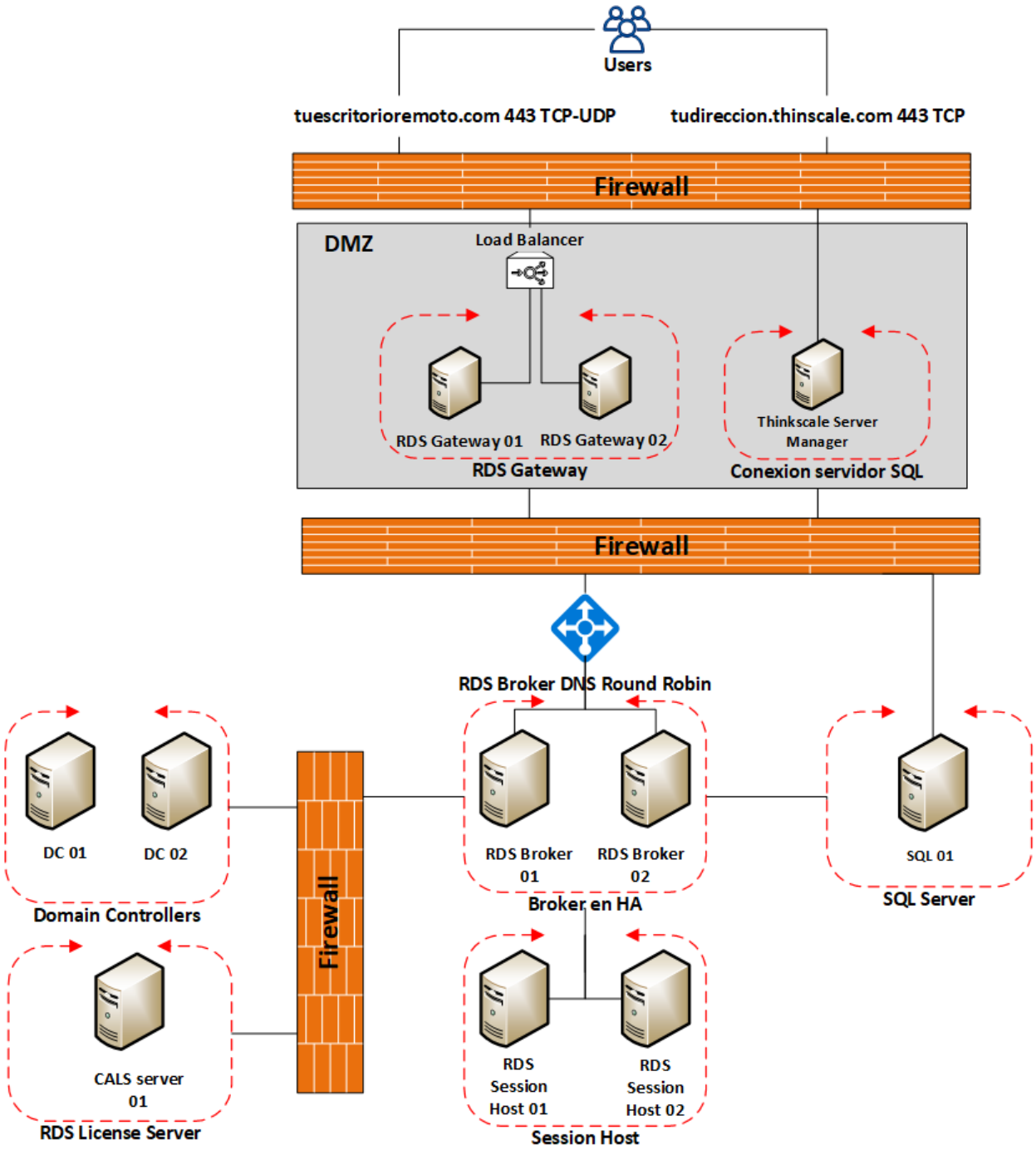
¿Tuvo usted, o sus agentes, incidencias en el proceso de pasar de presencial a remoto? ¿Qué tan complicada fue la transición?

Cinco encuestados coinciden en que el proceso de transición fue muy complicado y con muchas incidencias, mencionando la inestabilidad en la conexión a internet, deficiencia en el servicio eléctrico y la falta de un ambiente adecuado para trabajar dentro de su domicilio. Los doce restantes tuvieron una experiencia distinta, detallan que fue sencillo el proceso de transición y que recibieron el soporte necesario por parte del departamento de IT de la empresa.

CAPÍTULO 4: IMPLEMENTACIÓN DE ESTRATEGIAS EN LA CIBERSEGURIDAD DURANTE EL TELETRABAJO

Figura 7

Propuesta de infraestructura para teletrabajo seguro en Contact Centers/BPOs



4.1. Elementos que conforman la estrategia

Tabla 1

Elementos que conforman la estrategia

Nombre	Descripción
Secure Remote Worker	Es una solución de software que se instala y se ejecuta en el dispositivo personal de un usuario de *Microsoft Windows*, ofreciéndole al usuario un entorno de espacio de trabajo seguro para el acceso remoto y el trabajo en casa. (THINSCALE, 2020)
Remote Desktop Service (RDS)	Es la plataforma elegida para crear soluciones de virtualización para todas las necesidades de los clientes finales, incluida la entrega de aplicaciones virtualizadas individuales, el acceso seguro a escritorios remotos y la posibilidad de que los usuarios finales ejecuten sus aplicaciones y escritorios desde la nube. (Microsoft Corporation, 2017)
DMZ	*Demilitarized Zone* o zona desmilitarizada traducido al español, es una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo. (Instituto Nacional de Ciberseguridad Incibe, 2019)
RDS Broker	Administra las conexiones entrantes de escritorio remoto a la granja de servidores RDS. Maneja las conexiones a colecciones de escritorios completos y colecciones de aplicaciones remotas. Puede equilibrar la carga en los servidores de la colección al realizar nuevas conexiones. (Microsoft Corporation, 2018)
Gateway	(puerta de enlace) en términos generales son dispositivos que interconectan redes o dispositivos que traban con tecnología de comunicación diferentes. Se usan estos dispositivos para interconectar centrales VoIP con la red PSTN o la red celular. (Heiliger Ruiz, Hiraldo Santos, & Guzmán Hernández, 2018)

Firewall	Un firewall o cortafuegos es un sistema o dispositivo diseñado para para prohibir o permitir el acceso desde o hacia una red. (Reyes, Arias, & Correa, 2020)
RDS Host	Contiene las aplicaciones y los escritorios basados en sesiones que comparte con los usuarios. Los usuarios acceden a estos escritorios y aplicaciones a través de uno de los clientes de escritorio remoto que se ejecutan en Windows. (Microsoft Corporation, 2018)

4.2 Plataforma Secure Remote Worker

4.2.1 Que es Secure Remote Worker?

La herramienta que se ha seleccionado para esta propuesta es *Secure Remote Worker de* THINSCALE de la cual se detallaran sus principales características para justificar su selección dentro de las distintas ofertas existentes en el mercado.

Según lo indicado por (THINSCALE, 2020) *Secure Remote Worker* es una solución de software que se instala y se ejecuta en el dispositivo personal de un usuario de *Microsoft Windows*, ofreciéndole al usuario un entorno de espacio de trabajo seguro para el acceso remoto y el trabajo en casa.

4.2.2 Objetivos de Secure Remote Worker

Entre los objetivos que se persiguen con la implementación de esta solución están:

1. **Entrega de informática al cliente más allá de los límites de la oficina**

Con este objetivo (THINSCALE, 2020) expresa que la Secure Remote Worker “persigue ofrecer la flexibilidad a los colaboradores el de poder de llevar las funcionalidades de la oficina a cualquier lugar con la seguridad sé que requiere”.

2. **Garantizar la seguridad y el cumplimiento para los trabajadores remotos y BYOD**

En este objetivo (THINSCALE, 2020) nos asegura que trabajando con la solución *Secure Remote Worker*, “podemos tener los estándares de seguridad lo más cercanos a los existentes dentro del entorno corporativo de nuestra empresa, por otra parte, además, asegura el cumplimiento de estándares de seguridad como son *Security Payment Card industry* (PCI), Health *Insurance Portability and Accountability Act* (HIPAA) dándole a los equipos BYOD cumplirlos sin problema alguno”.

3. **Clientes ligeros definidos por software.**

Según (THINSCALE, 2020) La implementación de *Secure Remote Worker* “permite a los equipos de TI ofrecer entornos de espacio de trabajo seguros, basados en políticas, segregados y temporales en dispositivos de punto final basados en Windows de propiedad personal, y todo independientemente de dónde trabaje el usuario final”.

4.3 Característica de la plataforma THINSCALE *Secure Remote Worker*

1. **Bloqueo completo del dispositivo**

Según (THINSCALE, 2020) el inicio y ejecución de *Secure Remote Worker* “en el dispositivo Windows de un usuario final le deniega el acceso al sistema operativo Windows subyacente, lo que lo deshabilita de forma efectiva mientras usan el entorno de área de trabajo segura”.

En lugar de la interfaz de escritorio del sistema operativo Windows, un usuario final tendrá acceso al área de trabajo remota segura, una interfaz de usuario sencilla y fácil de navegar desde donde puede conectarse a sus entornos remotos de forma segura.

También tienen la capacidad de tener acceso a aplicaciones locales si tienen el permiso pertinente de TI para hacerlo. Su dispositivo solo se bloquea durante la sesión segura y se devuelve el control total al usuario una vez que cierra la sesión.

2. Herramienta de validación segura de trabajadores remotos

(THINSCALE, 2020) asegura que *Secure Remote Worker* “incluye una solución única que permite a los administradores de TI comprobar el dispositivo del usuario final antes de conectarse para asegurarse de que cumple el mínimo Requisitos”.

La herramienta de validación de punto final inspecciona el dispositivo de usuario final para poder determinar los niveles actualización de sistema operativo, parches, el *software* instalado y si el antivirus está presente. La comprobación proactiva de los dispositivos antes de la incorporación significa que cualquier problema se puede rectificar de antemano, lo cual reduce drásticamente los tiempos de incorporación y reduce las llamadas al soporte.

3. Prevención de ejecución de aplicaciones (AEP)

La característica AEP de *Secure Remote Worker* agrega una capa adicional de seguridad al impedir la ejecución de aplicaciones no autorizadas.

Según lo expresado en la documentación de (THINSCALE, 2020) al emplear un sistema basado en reglas, los administradores de TI ahora pueden configurar exactamente qué aplicaciones se pueden iniciar los usuarios finales en su dispositivo de punto final mientras *Secure Remote Worker* estas en ejecución y activo. Estas reglas permiten a los administradores de TI crear listas blancas y listas negras las cuales posean reglas que dan la posibilidad de tener un control granulado en las aplicaciones que se desean ejecutar y cuáles no.

4. Prevención de ejecución de servicios (SEP)

Según (THINSCALE, 2020) refiere dicha característica como:

> Que permite controlar qué servicios de Windows pueden ejecutarse cuando una sesión de *Secure Remote Worker* está activa y se ejecuta en "modo de trabajo. Si un servicio se está ejecutando y no coincide con las directivas de prevención de ejecución de servicios definidas, el servicio se detendrá automáticamente o el usuario final tendrá que detener manualmente el servicio antes de que pueda iniciar *Secure Remote Worker* en su dispositivo.” (p.3)

5. Administración de revisiones de *Windows*

(THINSCALE, 2020, pág. 3) *Secure Remote Worker* permite a los departamentos de TI controlar fácilmente la característica *Windows Update* para asegurarse de que los usuarios finales ejecutan las revisiones y actualizaciones correctas antes de conectarse al entorno corporativo.”

6. Bloqueo de dispositivos USB

Cuando hablamos de dispositivos de bloqueo (THINSCALE, 2020) dice:

> Los dispositivos USB a menudo se ven como una de las principales causas de violaciones de seguridad y fugas de datos dentro de una organización. Los usuarios conectan sus propias memorias USB y otros dispositivos multimedia habilitados para escritura y copian datos potencialmente confidenciales en ellos y los eliminan del entorno corporativo. *Secure Remote Worker* puede evitar que estos dispositivos se puedan usar con su función de bloqueo de dispositivos USB. Habilitar esta característica significa que los usuarios finales no pueden acceder a dispositivos de almacenamiento basados en USB al acceder a sistemas corporativos y datos desde el espacio de trabajo seguro. (p.3)

7. Windows Firewall Control

La aplicación *Secure Remote Worker* de (THINSCALE, 2020, pág. 3) “permite a administradores de TI configurar completamente la característica Firewall de Windows automáticamente. Pueden eliminar cualquier regla de firewall existente o configurar nuevas reglas de firewall y administrarlas de forma centralizada desde THINSCALE *management platform* y el editor de perfiles”.

8. Controles para ubicación y tiempo de la conexión.

(THINSCALE, 2020) plantea que aparte de ofrecer las facilidades del acceso remoto seguro, también ofrece una excelente gestión de tiempo y lugar. Ofreciendo información y récord de la ubicación y el tiempo de las conexiones usando la sesión de trabajo, dándole suficientes herramientas de los administradores de TI para poder dar los niveles

adecuados de acceso en los momentos adecuados y en las ubicaciones permitidas por las políticas de la organización.

9. Experiencia de usuario final mejorada

Para (THINSCALE, 2020) la experiencia del usuario final es clave para la productividad y la velocidad de acceso a la información y los datos. *Secure Remote Worker* ofrece una apariencia familiar de Windows junto con una interfaz de usuario intuitiva y segura del espacio de trabajo que permite un acceso rápido y fácil a entornos remotos. También permite a los usuarios finales tener acceso a las aplicaciones instaladas localmente (en función de la directiva del conjunto de administradores) en caso de que necesite trabajar sin conexión.

10. Administración, soporte e incorporación simplificados

Como *Secure Remote Worker* es una solución solo de software, los usuarios finales simplemente descargan la aplicación, iniciarla, cambiar al 'modo de trabajo' y se conectan de forma segura a el entorno corporativo en minutos según lo indicado en la documentación de (THINSCALE, 2020).

11. Navegación segura

(THINSCALE, 2020) Incluye como parte del software *ThinKiosk Client*, este es un navegador web integrado, completo con una interfaz de usuario totalmente personalizable, que permite a los usuarios navegar de forma segura por los sitios de Internet en función de la política establecida por el departamento de TI.

12. Detección de Windows Security Center

(THINSCALE, 2020) saca provecho de que *Secure Remote Worker* comprueba y supervisa de forma proactiva los componentes de seguridad del sistema operativo del dispositivo. Todos los componentes, como la protección con cortafuegos, antivirus y *spyware* se pueden supervisar.

En caso de que uno de estos componentes no sea compatible o no esté configurado correctamente, *Secure Remote Worker* puede tomar las medidas adecuadas para la corrección de la incidencia, asegura (THINSCALE, 2020) en su documentación oficial.

4.4 ¿Como funciona Secure Remote Worker?

(THINSCALE, 2020) explica que *Secure Remote Worker* permite a un usuario final usar su dispositivo Windows de propiedad personal mejor también conocido como BYOD. De forma predeterminada, un usuario final seguirá trabajando con normalidad y tendrá acceso completo a su PC o portátil con Windows local, por lo que cuando inicie sesión en su dispositivo, todavía tiene un menú de inicio y acceso completo a sus recursos, aplicaciones y configuraciones.

En el momento que *Secure Remote Worker* se inicia en su PC con Windows o portátil, y el usuario final habilita el *Secure Remote Worker*, su PC o portátil se coloca en modo "trabajador".

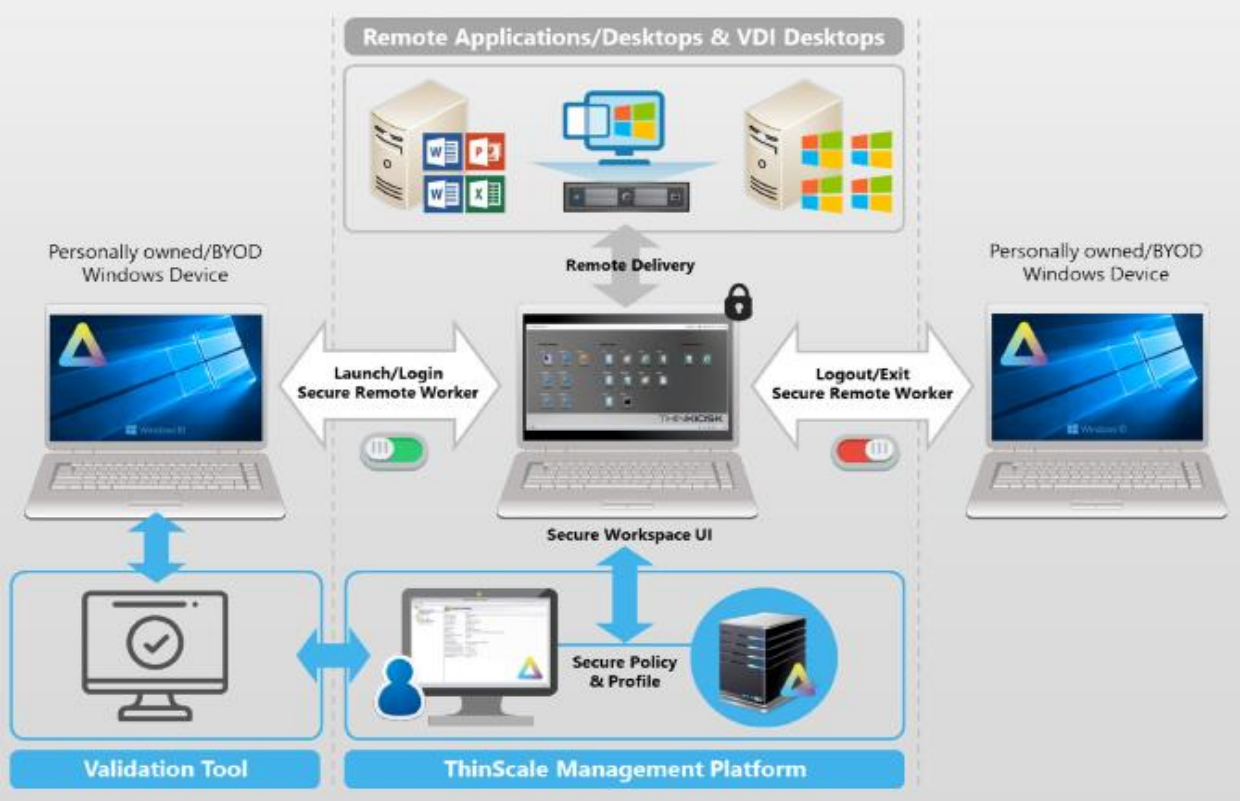
Desde ese momento las políticas de bloqueo son entonces aplicadas, se quita el Explorador de Windows y se inicia la interfaz de usuario de *Secure Remote Workspace* o modo trabajador.

Adicionalmente (THINSCALE, 2020) nos informa que una vez que el usuario final ha terminado de trabajar con sus aplicaciones y escritorios remotos, simplemente cierra la sesión del entorno remoto y sale *de Secure Remote Worker*.

Todas las restricciones de dispositivo que se aplicaron mientras se ejecutaba *Secure Remote Worker* ahora se levantan y el usuario final tiene de nuevo el control total de su PC local, en la figura 8 veremos de manera más detallada este proceso.

Figura 8

Funcionamiento básico de implementación solución Secure Remote Worker.



Nota: En la figura provista claramente muestra el proceso de una conexión remota segura desde un dispositivo *Bring Your Own Device* (BYOD) y su proceso completo desde la activación de la herramienta *Secure Remote Worker*, se hace la validación correspondiente y las revisiones de lugar y al ser estas validadas se inicia la sesión remota en el modo trabajador con el *secure workspace* teniendo acceso a las herramientas autorizadas por el departamento de TI y ceñidas a las políticas pautadas. Luego de finalizar este proceso cierras tu sesión de *Secure Remote Worker* y la sesión temporal de la herramienta se elimina y el computador vuelve a su estado original al de antes de ser ejecutado el *Secure Remote Worker*. Fuente: (THINSCALE, 2020)

4.5 Planteamiento de mejores practicas

El Instituto Nacional de Estándares y Tecnología, o NIST por sus siglas en inglés, es una agencia no reguladora del Departamento de Comercio de los Estados Unidos, que desarrolla y emite estándares, pautas y otras publicaciones para ayudar a las agencias federales a implementar la Ley Federal de Modernización de la Seguridad de la

Información de 2014 (FISMA) y para ayudar con la gestión de programas rentables para proteger su información.

La (NIST National Institute of Standards and Technology, 2020) en su publicación especial 800-53 Rev. 5, “en lo adelante SP 800-53, provee un catálogo de controles de seguridad y privacidad para todos los sistemas de información federal de los Estados Unidos, excepto para aquellos relacionados con la seguridad nacional”.

De los controles de acceso remoto publicados en dicho documento, recomendamos la aplicación de los siguientes:

Tabla 2

Controles de acceso remoto NIST Publicación Especial 800-53 Rev. 5

ID	Tipo	Control	Descripción
AC-17(1)	Acceso Remoto: Control de Acceso	Monitoreo y Control	El monitoreo y control de los métodos de acceso remoto permite a las organizaciones detectar ataques y ayudar a garantizar el cumplimiento de las políticas de acceso remoto al auditar las actividades de conexión de los usuarios remotos en una variedad de componentes del sistema, incluidos servidores, computadoras portátiles, estaciones de trabajo, teléfonos inteligentes y tabletas.
AC-17(2)	Acceso Remoto: Control de Acceso	Protección de la confidencialidad e integridad mediante el cifrado	Las redes privadas virtuales se pueden utilizar para proteger la confidencialidad y la integridad de las sesiones de acceso remoto. *Transport Layer Security* (TLS) es un ejemplo de protocolo

			criptográfico que proporciona seguridad en las comunicaciones de un extremo a otro en las redes y se utiliza para las comunicaciones por Internet y las transacciones en línea.
AC-17(3)	Acceso Remoto: Control de Acceso	Puntos de control de acceso administrados	Las organizaciones consideran los requisitos de la iniciativa *Trusted Internet Connections* (TIC) para las conexiones de red externas, ya que limitar el número de puntos de control de acceso para el acceso remoto reduce las superficies de ataque.
AC-17(4)	Acceso Remoto: Control de Acceso	Comandos y accesos privilegiados	El acceso remoto a los sistemas representa una vulnerabilidad potencial significativa que los adversarios pueden aprovechar. Como tal, restringir la ejecución de comandos privilegiados y el acceso a información relevante para la seguridad a través del acceso remoto reduce la exposición de la organización y la susceptibilidad a las amenazas de los adversarios a la capacidad de acceso remoto.

Nota: Información obtenidas de (NIST National Institute of Standards and Technology, 2020)

4.6 Instalación de la plataforma *Secure Remote Worker*

Se ha de tener en cuenta que en toda instalación de nuevas soluciones es requerido tener las herramientas necesarias para su correcta implementación.

4.6.1 Requerimientos de sistema

Estos son los requerimientos necesarios para la instalación de la solución *Secure Remote Worker.*

Tabla 3

Requisitos de instalación Secure Remote Worker

Nombre	Descripción
.NET Framework	4.5 o superior
Sistema operativo	Windows 7 SP1, “Windows” 10 1803 o superior
Memoria RAM	Mínimo 4GB de RAM
Disco duro	Mínimo 500 MB de RAM
Firewall	Reglas de firewall que permita a *Secure Remote Worker* tomar conexiones entrantes (creadas por el instalador)
Internet Explorer	Versión 7 o superior

Nota: Si en una maquina con Windows 7, se requiere este parche **KB4516065** y **KB4524752.** Fuente (THINSCALE, 2021)

4.6.2 Guía de instalación en servidor

Esta guía de instalación fue tomada de la web oficial de (THINSCALE, 2020) y detalla todos los aspectos de la instalación del *Secure Remote Worker*.

Para la ejecución de exitosa de la instalación se requiere tener accesos de administrador del equipo en el cual se instalará la herramienta. (ver anexo G)

4.7 Políticas propuestas

Es de suma importancia la aplicación de políticas de grupo en Windows, basándonos en el principio de menor privilegio, que establece que para garantizar la seguridad del sistema los usuarios deben tener estrictamente los permisos necesarios para realizar su trabajo. Dentro de las políticas más comunes y aceptadas por las normas usadas como guía en esta investigación, tenemos:

4.7.1 Políticas de cuentas de usuarios de Windows

- Contraseña compleja para los usuarios del dominio de la empresa, con los siguientes requerimientos mínimos: longitud mínima 12 caracteres, un carácter especial, un carácter numérico, una letra mayúscula.
- Bloqueo de cuenta del dominio luego de 5 intentos de acceso fallidos.
- Cambio de contraseña cada 45 días calendario.
- Horario para el acceso a los servidores de la empresa, de acuerdo con el horario de trabajo del departamento al que pertenece el colaborador y/o el asignado de manera directa al colaborador.

4.7.2 Políticas de grupo de Windows

- Prohibir el acceso a Configuración y Panel de control.
- Bloquear el acceso al símbolo del sistema o CMD.
- Bloquear el acceso a bandeja de notificaciones de “Windows”.
- Deshabilitar las unidades extraíbles.
- Apagar “Windows Defender” para evitar conflictos con el software de seguridad de terceros que se utilice.
- Deshabilitar reinicios forzados.
- Desactivar “Windows Installer” para evitar la instalación de software no autorizado.
- Prohibir cambiar la zona horaria, la hora y fecha del sistema.
- Prohibir apagar y reiniciar el sistema.
- Renombrar la cuenta de administrador local en todos los servidores de RDS.
- Habilitar el registro de eventos de “Windows”

- Habilitar el control de cuentas de usuario.
- Deshabilitar el uso del botón derecho del ratón.
- Permitir inicio de sesión a través de Servicios de Escritorio remoto solo para los colaboradores previamente autorizados.

CAPÍTULO 5: EVALUACIÓN DEL IMPACTO EN EL TELETRABAJO DE LOS *CONTACT CENTER* DE SANTO DOMINGO

5.1 Análisis de problemática actual

Los riesgos se pueden mitigar aplicando mecanismos que garanticen una conexión segura entre el agente remoto y el *Contact Center*, asegurarse que en ese proceso de conexión exista un entorno el cual pueda ser moldeado en base a políticas y buenas prácticas las cuales serán la salvaguarda de la integridad de la información.

Asegurarse que dicho entorno cumple con los requerimientos de operación y los estándares que el *Contact Center* requiere para sus operaciones sin comprometer su infraestructura.

Cuando no hay un control establecido en torno a las conexiones SSL existe la probabilidad de riesgo de que un paquete de datos sea interceptado o haya sido manipulado por una tercera persona cuando estos son enviados a través de internet.

5.2 Análisis comparativo de situación actual versus propuesta

En nuestra investigación se ha estado buscando la mejora del acceso remoto en *Contact Centers/BPOs* en Santo Domingo, lo cual nos ha llevado a la revisión y replanteamiento en el proceso de conexiones remotas tenemos que:

1. **Conexiones a través de VPN SSL**

Actualmente las conexiones remotas se están realizando con conexión VPN SSL, las cuales no están siendo monitoreadas ni permiten la implementación de políticas necesarias para preservar la seguridad del entorno.

Con nuestra propuesta se busca no solo poder acceder a los servidores de escritorio remoto de la empresa de forma segura, sino también garantizar que el agente haga dicha conexión desde cualquier equipo Windows (personal o provisto por la institución) utilizando un software que habilite una sesión de trabajo controlada y que solo permita los accesos previamente autorizados por la empresa.

2. Implementación de controles

En la actualidad, los controles son aplicados única y exclusivamente dentro de los servidores de escritorio remoto de la empresa, permitiendo a los agentes que puedan realizar acciones no permitidas en el computador que estén usando para conectarse, lo que se traduce en una brecha de seguridad muy grande.

Aplicando nuestra propuesta se podrán implementar controles para los usuarios que estarían usando el *Secure Remote Worker*, para así permitir o bloquear acciones dentro de la sesión de Windows local controlada por la aplicación. De esta forma nos aseguraremos de que solo se utilicen los softwares autorizados por la empresa y la navegación a los portales web que definamos.

3. Posibilidad de usar el equipo privado del agente

En caso de ser necesario, el agente podrá utilizar su computador personal para conectarse a los servidores de escritorio remoto de la empresa, esto es posible gracias a la forma en la que trabaja *Secure Remore Worker*, que bloquea de manera temporal el equipo del usuario mientras la aplicación se esté ejecutando, permitiendo solo el uso de las aplicaciones dispuestas para el perfil del agente.

Una vez terminada la sesión, el agente podrá regresar a utilizar su computador de la manera habitual y sin haber alterado su data.

CONCLUSIÓN

Según los datos obtenidos en nuestra encuesta, el teletrabajo en *Contact Centers* de Santo Domingo era muy bajo, inexistente o estaba reservado para empleados contratados en el exterior del país antes de la pandemia por coronavirus (COVID-19). Durante la pandemia, se produjo un aumento significativo en la cantidad de empleados trabajando en formato remoto, esto debido al confinamiento obligatorio dictado por el gobierno dominicano y a las medidas de distanciamiento social para evitar la propagación del virus.

Para lograr la implementación de este formato de trabajo, los *Contact Centers* tuvieron un plazo de tiempo muy corto y se vieron forzados a tomar medidas excepcionales para poder garantizar la continuidad del negocio, tales como permitir al empleado trabajar con su computador personal, asignar equipos de escritorio de la empresa para que fueran trasladados a los domicilios de los agentes, adquirir servicios de internet inalámbricos para ser asignados a los agentes que se encontraban trabajando desde casa, entre otras.

Conforme a este análisis, hemos identificado las amenazas y el nivel de riesgo de estas, por tanto, hemos diseñado una propuesta de ambiente de trabajo seguro y confiable, que permite la implementación de políticas de grupo y usuarios, las cuales pueden ser revisadas y modificadas con frecuencia de acuerdo con la necesidad de la empresa, permitiendo así un mayor control en los dispositivos personales que los empleados están usando para acceder a los servidores de la institución.

Se ha hecho mención a los controles de accesos que son un punto importante en esta investigación ya que, si existen los controles de usuarios esto a su vez le da a la empresa las herramientas necesarias en la búsqueda de proteger toda la infraestructura tanto física como virtual de personas malintencionadas.

Recomendaciones

- Se recomienda que el *Contact Center* provea los equipos que serán utilizados por los agentes que trabajan desde casa, los equipos deben tener una versión de sistema operativo actualizada, un software de antivirus y una cuenta de usuario sin privilegios de administrador.
- Se recomienda el uso de una solución de software que se instale y se ejecute en el dispositivo Windows del agente, para brindar un entorno de trabajo seguro para el acceso remoto y el trabajo desde casa, como el *Secure Remote Worker* de THINSCALE.
- Se recomienda la aplicación de políticas de acceso a correo institucional solo cuando se esté conectado a los servicios de escritorio remoto, evitando así el acceso desde fuera de la red de la empresa.
- Se recomienda la aplicación de políticas de grupo para los usuarios del dominio que usaran los servicios de escritorio remoto, para evitar que estos se conecten a los servidores de la empresa fuera de su horario laboral establecido.
- Se recomienda la aplicación de políticas de uso aceptable para los dispositivos y sistemas puestos a disposición del agente, debe ser un documento bien redactado y de manera formal, detallando también las consecuencias en caso de hacer uso indebido.
- Se recomienda establecer controles disuasivos para la prevención de acciones no deseadas por parte de los agentes que se encuentran trabajando desde casa, mediante la demostración de posibles castigos o coerción.
- Se recomienda auditar con frecuencia los equipos usados por los agentes que trabajan desde casa, para asegurar que las políticas de uso aceptable están siendo aplicadas de manera correcta.
- Se recomienda crear un plan de capacitación sobre temas de ciberseguridad, que será impartido a través de una plataforma online cada 3 meses para asegurar que los agentes se mantengan informados sobre las amenazas existentes y como cuidarse de ellas.

- Se recomienda implementar la política de privacidad de geolocalización para obtener las coordenadas geográficas de las conexiones de los agentes y garantizar que se mantengan laborando dentro de la ciudad de Santo Domingo.

Bibliografia

Center for Internet Security (CIS). (2021, mayo). *CIS Controls Version 8*. Retrieved from https://www.cisecurity.org/controls/v8/

Centro Nacional de Ciberseguridad (CNCS). (2020, julio 31). *Guía de Controles Críticos de Ciberseguridad.* Retrieved from Centro Nacional de Ciberseguridad (CNCS) República Dominicana: https://cncs.gob.do/wp-content/uploads/2020/07/Guia-de-Controles-Criticos-de-Ciberseguridad-Controles-CIS-V7.pdf

Conde del Oso, L. E. (2005, diciembre 05). Diseño e implementación de un Call Center y su evolución hacia un Contact Center. *Técnica De La Empresa De Telecomunicaciones De Cuba S.A*, 30-34. Retrieved from http://www.revistatonoetecsa.cu/index.php/tono/article/view/243

Duque, F. J., & Orozco Alzate, M. (01 de 03 de 2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información, 22*(6), 72-77. Obtenido de https://pdfs.semanticscholar.org/ff97/978e09c5bc3f1ca826017e9f34490d4e5c19.pdf

Garcia Encarnacion, Y., & Freites Mejia, E. (2018). *Propuesta de implementación de un plan de capacitación para empleados empresa Alorica 2018.* Santo Domingo: Universidad APEC.

González Ferreras, C. V., Reyes Matos, J., Rodriguez Asencio, R. A., & Padua Ruiz, W. A. (2020). *Controles de Ciberseguridad del servicio de Internet en centros comerciales de un aeropuerto.* Santo Domingo, D. N.: Universidad APEC.

Heiliger Ruiz, J. E., Hiraldo Santos, H. F., & Guzmán Hernández, C. (2018). *Propuesta de aplicación de un sistema de voz sobre IP, utilizando Raspberry pi, Asterisk, Open-VPN y DNS dinámico en Campus II.* Santo Domingo: Universidad APEC. Retrieved from https://bibliotecaunapec.blob.core.windows.net/tesis/TESIS_CI_IEL_02_2018_ET180220.pdf

INCIBE Instituto Nacional de Ciberseguridad. (2020). *Politicas de seguridad para la PYME: Teletrabajo seguro.* Retrieved from INCIBE Web Site.

Instituto Nacional de Ciberseguridad Incibe. (2019, Septiembre 19). *Qué es una DMZ y cómo te puede ayudar a proteger tu empresa*. Retrieved from Incibe Web Site: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

ISACA. (2015). Malware y Tipos de Ataque. In *Fundamentos de Ciberseguridad* (pp. 30-32). ISACA.

Listin Diario. (2020, julio 13). *El coronavirus le cambió la vida a la familia de José y a miles más.* (C. Acosta, Ed.) Retrieved from https://listindiario.com/economia/2020/07/13/625978/el-coronavirus-le-cambio-la-vida-a-la-familia-de-jose-y-a-miles-mas

Micheli Thirión, J. (2007). Los call centers y los nuevos trabajos del siglo XXI. 51.

Microsoft Corporation. (2017, Febrero 22). *Welcome to Remote Desktop Services*. Retrieved from Microsoft Corporation Web Site: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

Microsoft Corporation. (2018, Julio 6). *Remote Desktop Services roles*. Retrieved from Microsoft Corporation Web Site: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-roles

Ministerio de trabajo. (2020, 11 12). *RESOLUCION 23-2020 SOBRE REGULACION DEL TELETRABAJO COMO MODALIDAD ESPECIAL DE TRABAJO.* Retrieved from ministerio de trabajo: https://www.mt.gob.do/images/documentos/RESOLUCION%2023-2020%20SOBRE%20REGULACION%20DEL%20TELETRABAJO%20COMO%20MODALIDAD%20ESPECIAL%20DE%20TRABAJO.pdf

NIST National Institute of Standards and Technology. (2020, Diciembre 10). *Security and Privacy Controls for Information Systems and Organizations.* Retrieved from NIST Web Site: https://csrc.nist.gov/CSRC/media/Projects/risk-

management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

OPTIC. (2020, agosto 12). *Guía sobre el Teletrabajo para los Organismos del Estado Dominicano.* Retrieved from http://optic.gob.do/wp-content/uploads/2020/08/Guia-de-Teletrabajo-OPTIC.pdf

Organización Internacional del Trabajo. (2016, octubre 24-26). *Foro de diálogo mundial sobre las dificultades y oportunidades del teletrabajo para los trabajadores y empleadores en los sectores de servicios de tecnología de la información y las comunicaciones y financieros.* Retrieved from https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/meetingdocument/wcms_547101.pdf

Reyes, R., Arias, A., & Correa, M. (2020). *Análisis e implementación de un sistema web de reserva de rutas, pago de transporte y adquisición de carnets para abordaje de autobús e integración de GPS para el seguimiento en vivo para el transporte institucional del Instituto Tecnológico de Las Améric.* Santo Domingo: Universidad APEC.

The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework. (2021, agosto 3). *Scientific Figure ResearchGate*. Retrieved from Process model of ISO/IEC 27005: https://www.researchgate.net/figure/Process-model-of-ISO-IEC-27005_fig3_326554343

THINSCALE. (2020, julio 20). *Secure Remote Worker Data Sheet.* Retrieved from thinscale.com: https://www.thinscale.com/hubfs/5670453/Thinscale%20July2020/Pdf/secure-remote-worker-overview%20(1).pdf

THINSCALE. (2021, febrero 15). *Secure Remote Worker Requirements.* Retrieved from kb.thinscale.com: https://kb.thinscale.com/secure-remote-worker-knowledge-base/secure-remote-worker-requirements

UIT. (2010). Definiciones y terminología relativas a la creación. *Ciberseguridad*, 20. Retrieved from https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

ANEXOS

Anexo A

Norma ISO/IEC 27002:2013

Esta norma de control para el SGSI. Según lo planteado por (Duque & Orozco Alzate, 2017):

Esta norma se denomina formalmente como:

- Tecnología de información
- Técnica de seguridad
- Código de prácticas para controles de seguridad de la información

Ha sido diseñada de acuerdo con ISO (2015) para ser usada en organizaciones que intentan:

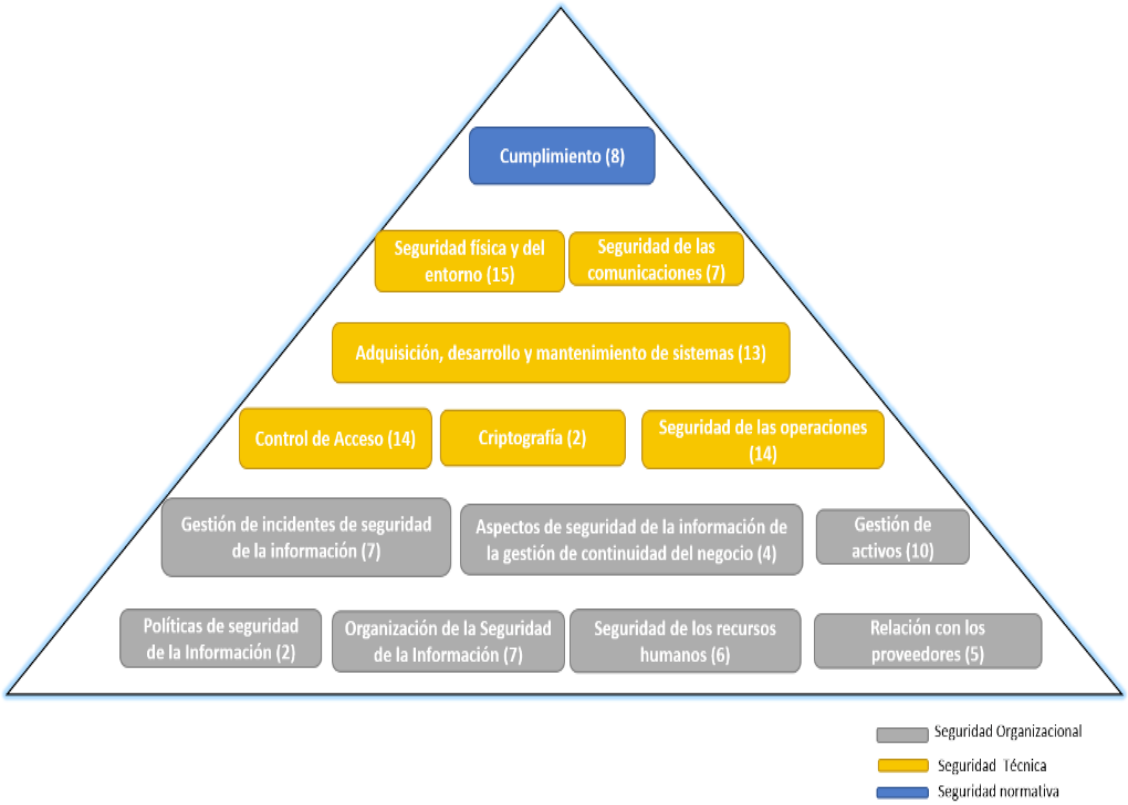
- Seleccionar controles dentro de un proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 2700.
- Implementar controles de seguridad de la información comúnmente aceptados.
- Desarrollar sus propias guías de gestión de seguridad de la información.

La estructura de los controles de seguridad de la información se encuentra conformada por 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos, como se puede apreciar en la figura anexa A-1 que se encuentra a continuación.

Con la norma ISO/IEC: 27002:2013 trazamos las principales políticas que nos guiarán en todo el proceso y serán las que mantiene al sistema con control como vemos en la figura A-1.

Figura A-1

Estructura de los controles de la norma ISO/IEC 27002:2013



Nota: La imagen anterior refiere a la norma ISO/IEC27002 podemos observar las capas de los controles que dicha normal sugiere. Se aprecia que existen 3 niveles de seguridad, la organizacional, la técnica y la normativa, siendo el cumplimiento la seguridad normativa principal y única de la normal, seguida por la seguridad técnica la cual sugiere distintos controles tanto físicos como lógicos para proteger la información. Seguido por la seguridad organizacional como la base de la pirámide en la cual es donde se gestionan las políticas de seguridad de la información, la gestión de incidentes, la continuidad del negocio, entre otras. Fuente: (Duque & Orozco Alzate, 2017, pág. 76)

Anexo B

Norma ISO/IEC 27005:2008

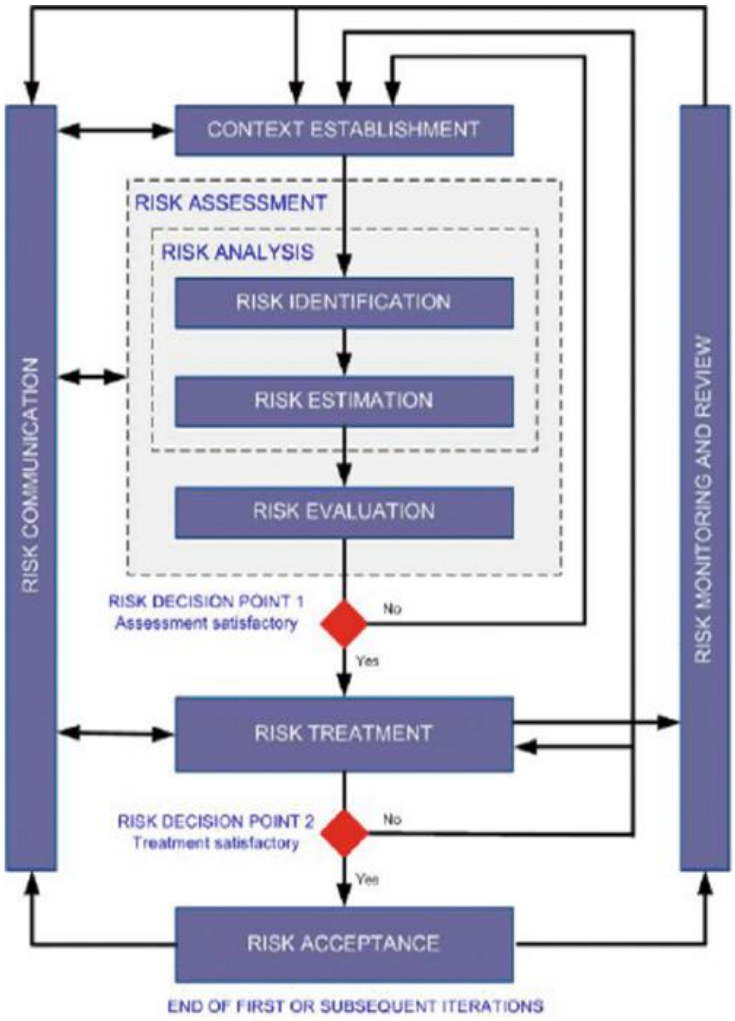
Esta norma se denomina formalmente como:

- Tecnología de la información
- Técnicas de seguridad
- Gestión del riesgo en la seguridad de la información

La norma nos proporciona directrices para la gestión del riesgo de la seguridad de la información, sin proporcionar metodologías específicas para tal fin. El componente de gestión del riesgo es uno de los insumos esenciales para desarrollar un SGSI. Si bien existen múltiples marcos de referencia, en su mayoría presentan los mismos elementos. (Duque & Orozco Alzate, 2017, pág. 76)

Figura B-1

Estructura de los controles de norma ISO/IEC 27005:2008



Nota: La norma ISO/IEC 27005:2008 es la encargada de gestionar, evaluar y dar pautas para la toma de decisiones con relación a los riesgos existente en un sistema de gestión de la seguridad de la información (SGSI). Fuente (The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework, 2021)

Anexo C

Norma ISO/IEC 27003:2010

Esta norma se denomina formalmente como:

- Tecnología de información
- Técnica de seguridad
- Guía de implementación de un sistema de gestión de seguridad de la información

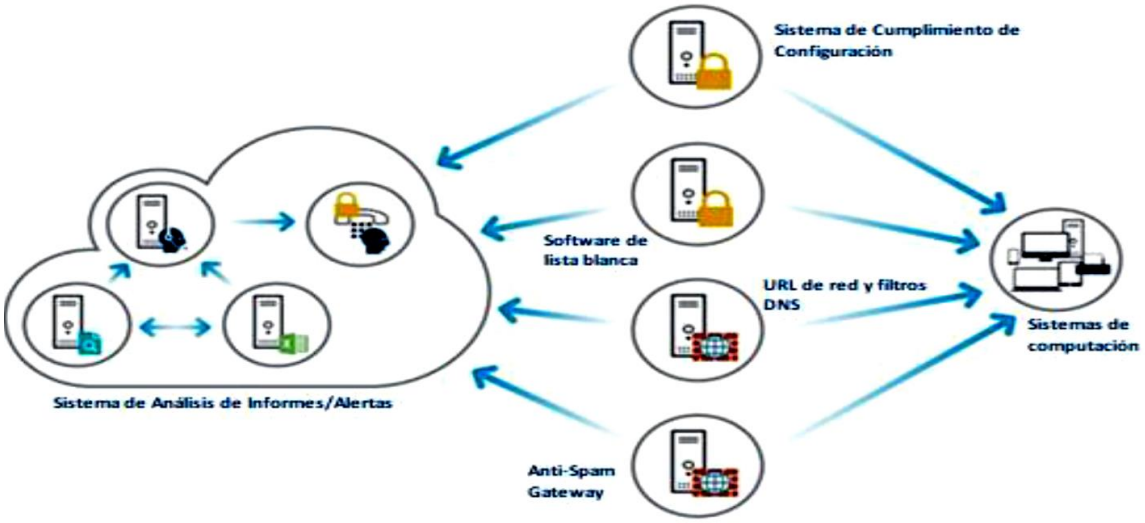
Su principal objetivo “es el establecimiento de las especificaciones y diseño de un SGSI, la cual será el referente para esta propuesta metodológica”. (Duque & Orozco Alzate, 2017, pág. 77)

Anexo D

Control de protección del navegador y el correo electrónico

Figura D-1

Diagrama de relación de entidad de sistema



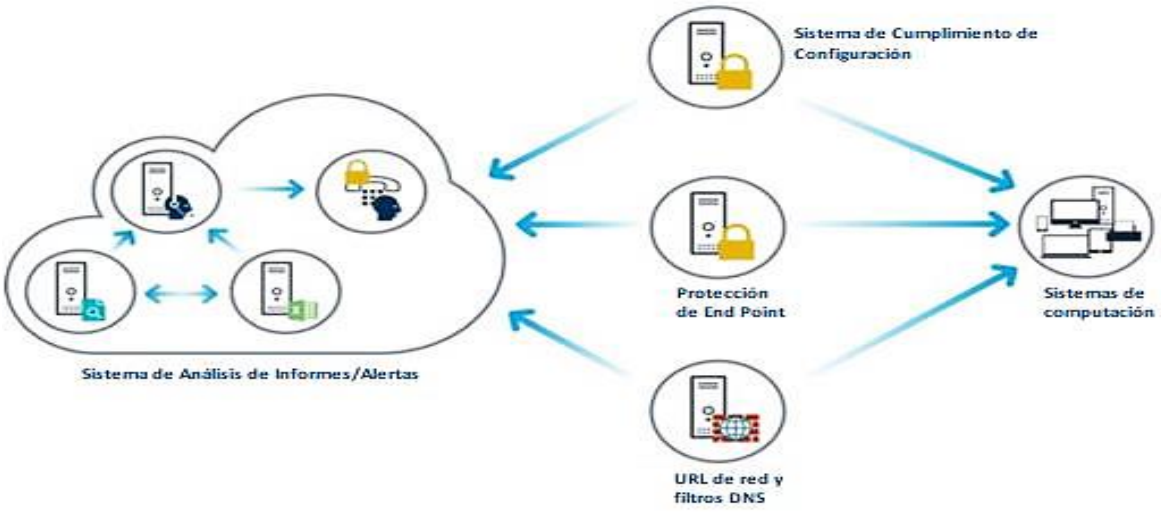
Nota: La figura muestra un control de protección del navegador web y del correo electrónico. Fuente: (Centro Nacional de Ciberseguridad (CNCS), 2020)

Anexo E

Control defensas contra malware

Figura E-1

Diagrama de relación de entidad de sistema



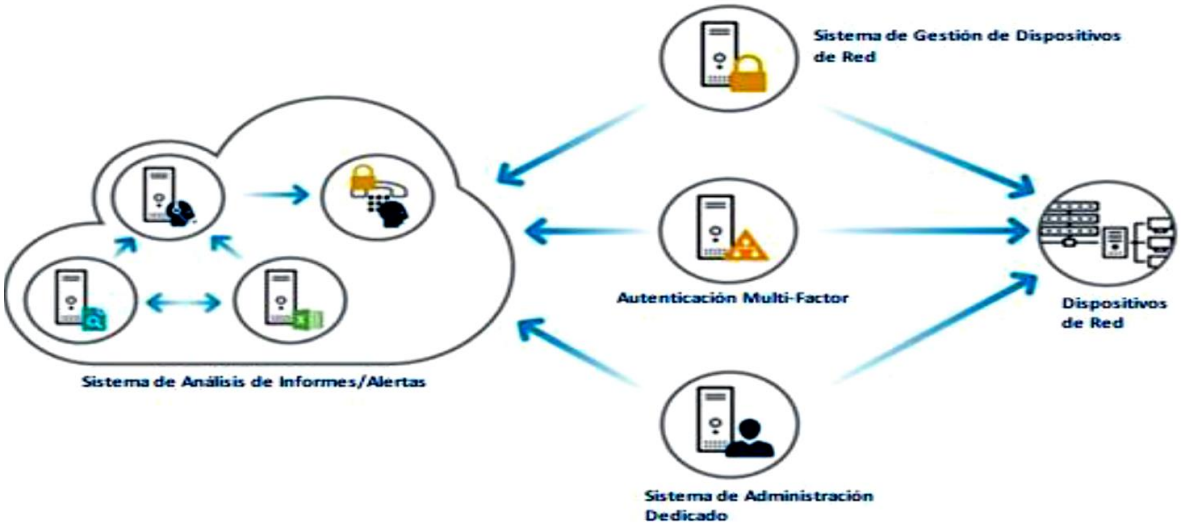
Nota: La figura muestra un control defensas contra malware. Fuente: (Centro Nacional de Ciberseguridad (CNCS), 2020)

Anexo F

Control gestión de la infraestructura de red

Figura F-1

Diagrama de relación de entidad de sistema

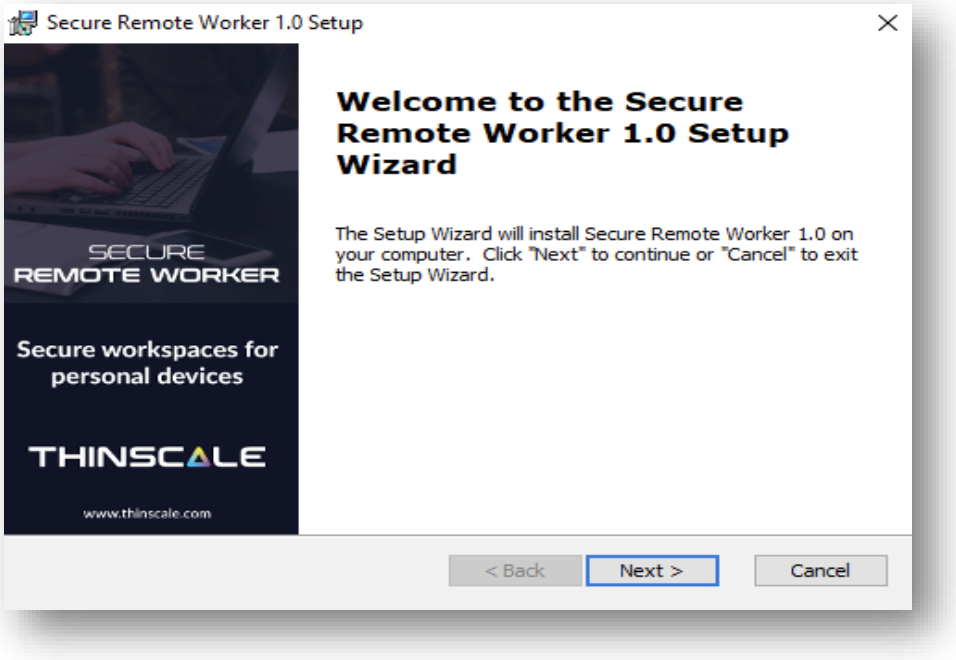


Nota: La figura muestra un control gestión de la infraestructura de red. Fuente: (Centro Nacional de Ciberseguridad (CNCS), 2020)

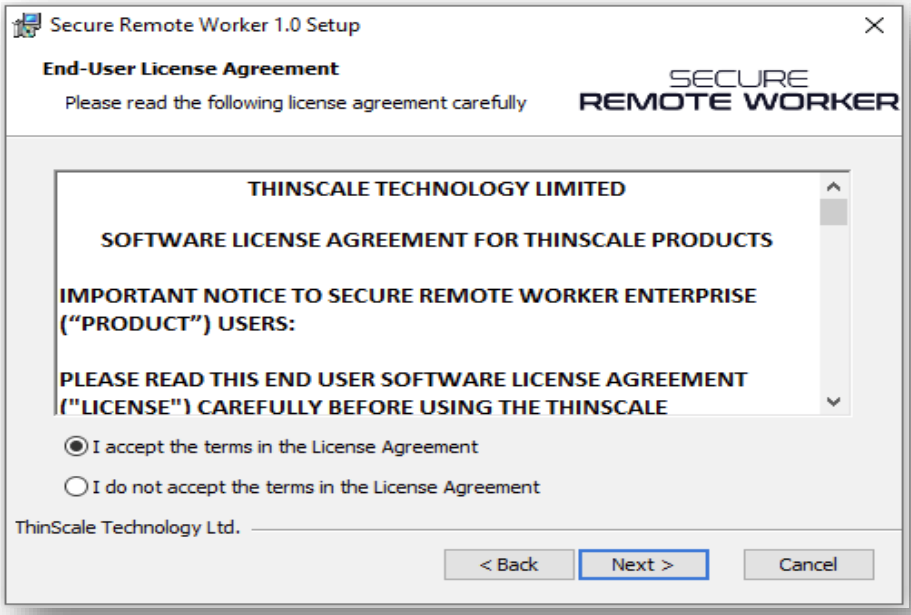
Anexo G

Guía de instalación en servidor

Copie el archivo de instalación en una carpeta temporal de una unidad local del servidor y ejecute el medio de instalación (SecureRemoteWorker-1.x.msi) Haga clic en *Next*

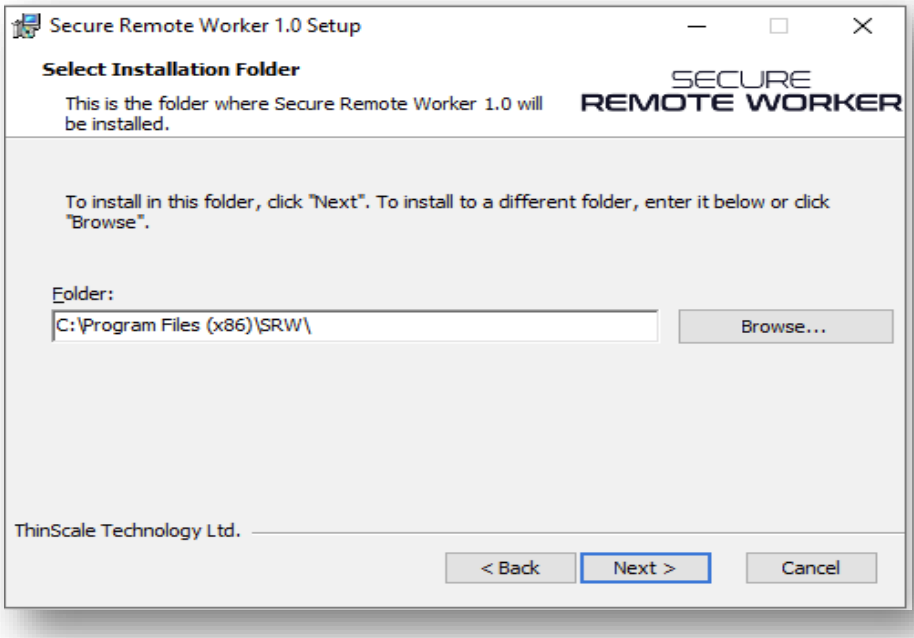


Nota: la versión del software puede cambiar con el tiempo.



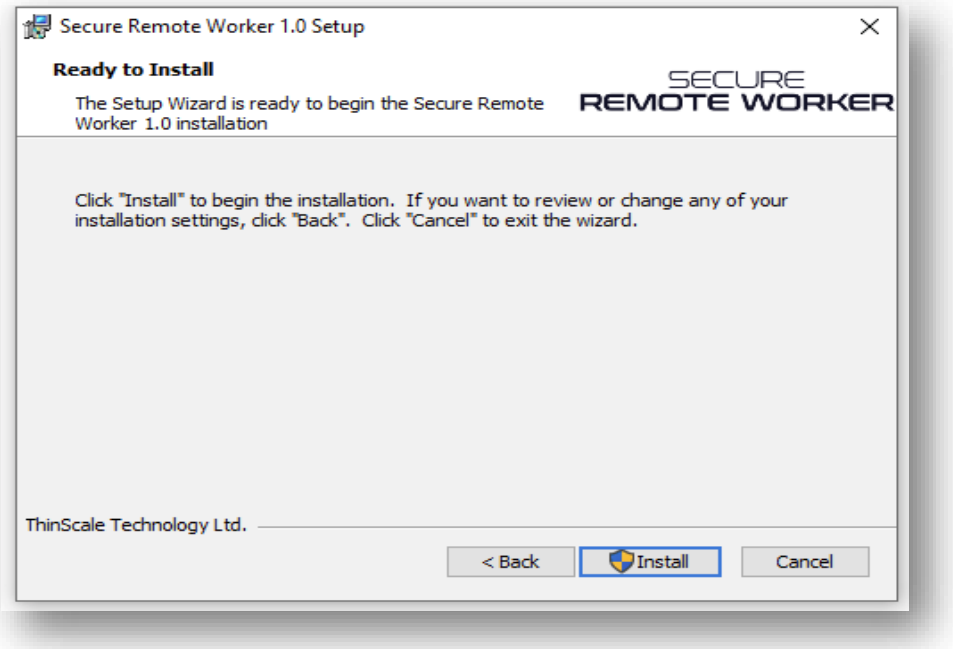
Nota: Seleccionar la opción *Next*.

Selecciona donde instalaras la aplicación dentro de tu servidor.



Nota: Seleccionar la opción *Next* para ir a la próxima ventana.

Seleccionar *Install*, para iniciar la instalación.



Nota: “Durante la instalación, se iniciará el Asistente de configuración de *Secure Remote Worker*, consulte la sección a continuación *Secure Remote Worker Setup Wizard* para obtener detalles de las opciones de configuración disponibles.

Secure Remote Worker puede solicitar que se reinicie el dispositivo si se requiere un reinicio.” (THINSCALE, 2020)

Anexo H

Encuesta trabajo remoto Contact Center Santo Domingo

Encuesta para trabajo monográfico: Propuesta de estrategias para la mejora de la ciberseguridad durante el teletrabajo en “Contact Centers/BPOs” de Santo Domingo.

1. ¿Labora usted en un Contact Center?
   - ☐ Si
   - ☐ No
2. ¿Dónde está ubicado el Contact Center donde labora?
   - ☐ Santo Domingo
   - ☐ Fuera de Santo Domingo
3. ¿Cómo era el teletrabajo antes del COVID-19?
4. ¿Cuánto tiempo ha estado usted laborando de forma remota?
5. ¿Hubo un incremento en la cantidad de colaboradores trabajando de forma remota luego del COVID-19?
   - ☐ SI
   - ☐ NO
6. Su edad está dentro del rango:
   - ☐ 18-30
   - ☐ 31-40
   - ☐ 41-50
7. ¿Cuál fue el proceso llevado a cabo para colocar a los colaboradores a trabajar remotamente y cuánto tiempo llevo implementarlo?
8. ¿Permitieron el “Bring Your Own Device” o solo equipos provistos por la institución?
   - ☐ BYOD
   - ☐ Equipos provistos por la institución
9. ¿Tuvo usted, o sus agentes, incidencias en el proceso de pasar de presencial a remoto?,¿Que tan complicada fue la transición?

Control plagio

Se ha utilizado la herramienta de plagio plagscan.com

https://www.plagscan.com/doc?140650812&sharekey=N4khxW8kRKbkw9TBuqeW

14.0% Resultados del Análisis de los plagios del 2021-08-08 23:40 UTC

Monografia Final.docx

Fecha: 2021-08-08 23:32 UTC

✱ Todas las fuentes 52 | Fuentes de internet 51

- [1] docplayer.es/58594773-Issn-aisti-no-22.html — 4.4% 34 resultados
- [2] pdfs.semanticscholar.org/ff97/978e09c5bc3f1ca826017e9f34490d4e5c19.pdf — 4.0% 33 resultados
- [3] www.researchgate.net/publication/318204876_A_methodology_for_implementing_an_information_security_management_system_based_ — 4.0% 33 resultados
- [4] listindiario.com/economia/2020/07/13/625978/el-coronavirus-le-cambio-la-vida-a-la-familia-de-jose-y-a-miles-mas — 1.9% 13 resultados
- [5] www.incibe.es/sites/default/files/contenidos/politicas/documentos/teletrabajo_seguro.pdf — 2.1% 13 resultados; ⊞ 1 documento con coincidencias exactas
- [7] 1library.co/document/q5w5mxwq-diseno-politica-seguridad-informacion-tecnologia-informacion-cooperativa-chibuleo.html — 1.7% 19 resultados
- [8] gaz.wiki/wiki/es/NIST_Special_Publication_800-53 — 1.1% 9 resultados
- [9] es.abcdef.wiki/wiki/NIST_Special_Publication_800-53 — 1.1% 9 resultados
- [10] esdeguelibros.edu.co/index.php/editorial/catalog/download/63/78/934?inline=1 — 1.2% 13 resultados
- [11] softevolution207546676.wordpress.com/2018/08/30/conoce-los-call-center-que-roban-identidad-descubre-como-no-caer-en-su-trampa/ — 1.0% 6 resultados; ⊞ 3 documentos con coincidencias exactas
- [15] ciberseguridad.com/guias/higiene-cibernetica/ — 0.6% 7 resultados
- [16] bibliotecaunapec.blob.core.windows.net/tesis/TESIS_CI_IEL_02_2018_ET180220.pdf — 0.5% 4 resultados
- [17] www.coursehero.com/file/95440783/POLITICA-DE-TELETRABAJOdocx/ — 0.5% 2 resultados
- [18] www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa — 0.4% 3 resultados
- [19] www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf — 0.3% 6 resultados
- [20] www.researchgate.net/publication/334114871_Auditorias_en_Ciberseguridad_Un_modelo_de_aplicacion_general_para_empresas_y_nac — 0.4% 6 resultados
- [21] repository.javeriana.edu.co/bitstream/handle/10554/7455/tesis629.pdf?sequence=1 — 0.3% 5 resultados
- [22] docs.vmware.com/es/VMware-Workspace-ONE-UEM/services/WS1_Android_Platform.pdf — 0.1% 4 resultados
- [23] www.welivesecurity.com/la-es/2015/04/09/backup-empresas-enfoque-normativo/ — 0.3% 3 resultados
- [24] silo.tips/download/arquitectura-integrada-de-seguridad-de-la-red-firewall-de-proxima-generacion-enf — 0.3% 5 resultados
- [25] searchdatacenter.techtarget.com/es/definicion/Amenaza-persistente-avanzada-o-APT — 0.2% 4 resultados
- [26] docplayer.es/10635826-Universidad-politecnica-de-valencia.html — 0.2% 3 resultados
- [27] repository.unad.edu.co/bitstream/10596/13631/1/Las competencias gerenciales en el desarrollo organizacional de la empresa de contact — 0.2% 4 resultados
- [28] hi-in.facebook.com/107487097280501/posts/398817121480829/ — 0.3% 2 resultados
- [29] prezi.com/i/plluvpbronrq/untitled/ — 0.2% 3 resultados

[30] repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4642/Diseño de un plan de contingencia para el sistema de gestión de turnos d
0.2% 2 resultados

[31] www.researchgate.net/publication/328562680_Ciberseguridad_en_la_Sociedad_Digital
0.2% 3 resultados

[32] www.studocu.com/co/document/universidad-nacional-abierta-y-a-distancia/seguridad-en-redes/trabajo-tutorial/toaz-ghgfhfg/13438354/viev
0.2% 3 resultados

[33] repositorio.upn.edu.pe/bitstream/handle/11537/13701/Diaz Morales Lilia Magdalena del Carmen.pdf?sequence=5
0.2% 3 resultados

[34] de.slideshare.net/PanchoE/la-norma-iso-9000-2008
0.1% 3 resultados

[35] slideplayer.es/slide/13621657/
0.2% 2 resultados

[36] dspace.ups.edu.ec/bitstream/123456789/15922/1/UPS-GT002230.pdf
0.1% 4 resultados

[37] searchdatacenter.techtarget.com/es/noticias/252475985/Consejos-de-seguridad-para-trabajar-remotamente-durante-las-vacaciones
0.1% 2 resultados

[38] docs.microsoft.com/es-es/microsoftteams/teams-on-rdp
0.2% 1 resultados

[39] repositoriotec.tec.ac.cr/bitstream/2238/10086/1/propuesta_para_implementar_oficina_administracion_proyectos_unidad_defensa_poder.p
0.1% 3 resultados

[40] repository.icesi.edu.co/biblioteca_digital/bitstream/10906/84786/1/T01700.pdf
0.2% 2 resultados

[41] www.linktoworks.com/secure-remote-worker-install
0.1% 3 resultados

[42] icoca.gorodovoy.pp.ua/72.html
0.2% 1 resultados

[43] www.incibe.es/protege-tu-empresa/blog/no-estes-en-las-nubes
0.1% 1 resultados

[44] mobile.twitter.com/josefinaromanv/status/1384651672236949510
0.1% 1 resultados

[45] books.google.co.in/books?id=_z2GcBD3deYC&pg=PA72&lpg=PA72&dq="'información comúnmente aceptados"'&source=bl&ots=wtjqxGF0
0.1% 2 resultados

[46] www.ilo.org/wcmsp5/groups/public/@americas/@ro-lima/@ilo-buenos_aires/documents/publication/wcms_248685.pdf
0.1% 2 resultados

[47] sites.google.com/view/jcgniihp7e/jvlnew-dmz-libro-tres-dmz-o-c-pdfepub
0.1% 1 resultados

[48] www.scribd.com/document/484618334/RESOLUCION-23-2020-SOBRE-REGULACION-DEL-TELETRABAJO-COMO-MODALIDAD-ESPEC
0.1% 1 resultados

[49] www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/meetingdocument/wcms_795523.pdf
0.1% 1 resultados

[50] www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/meetingdocument/wcms_780075.pdf
0.1% 1 resultados

[51] context.reverso.net/translation/english-spanish/fully customisable
0.1% 1 resultados

[52] www.revistatonoetecsa.cu/index.php/tono/user/setLocale/en_US?source=/index.php/tono/article/view/321
0.1% 1 resultados
⊞ 1 documento con coincidencias exactas

[54] mt.gob.do/transparencia/images/docs/oai/indice/2021/INDICE DE DOCUMENTOS DISPONIBLES PARA ENTREGA - MARZO 2021.xlsx
0.1% 1 resultados

[55] www.slideshare.net/yeniferblanco/proyecto-de-aula-8156666
0.0% 1 resultados

[56] core.ac.uk/download/pdf/71396435.pdf
0.0% 1 resultados

71 páginas, 11902 palabras

Nivel del plagio: 14.0% seleccionado / 53.8% en total

347 resultados de 57 fuentes, de ellos 56 fuentes son en línea.

Configuración

Directiva de data: *Comparar con fuentes de internet, Comparar con documentos propios*

Sensibilidad: *Media*

Bibliografia: *Considerar Texto*

Deteción de citas: *Reducir PlagLevel*

Lista blanca: --

Segundo control de plagio

Plagiarism Checker X Originality Report

Plagiarism Quantity: 3% Duplicate

Date	Sunday, August 08, 2021
Words	336 Plagiarized Words / Total 11744 Words
Sources	More than 55 Sources Identified.
Remarks	Low Plagiarism Detected - Your Document needs Optional Improvement.

/ Decanato de Ingenier&#65533;as e Inform&#65533;tica Escuela de Inform&#65533;tica Curso Monogr&#65533;fico PROPUESTA DE ESTRATEGIAS PARA LA MEJORA DE LA CIBERSEGURIDAD DURANTE EL TELETRABAJO EN CONTACT CENTERS/BPOS DE SANTO DOMINGO. Sustentada por: Ydelky Alexandra Ulerio Contreras A00066846 Luis Alberty Comas Rosario A00070796 Johan Ferreira Serrata A00077938 Asesor: Willy Padua Monograf&#65533;a para optar por el t&#65533;tulo de: Ingenier&#65533;a de Sistemas de Computaci&#65533;n Santo Domingo, D. N.,

2021 &#65533;NDICE DE CONTENIDO Dedicatorias Agradecimientos Resumen Abstract CAP&#65533;TULO 1: ASPECTOS GENERALES DE LA INVESTIGACI&#65533;N 1 INTRODUCCI&#65533;N 1 1.1 Justificaci&#65533;n 2 1.2 Delimitaci&#65533;n 2 1.3 Selecci&#65533;n y definici&#65533;n del tema 2 1.4 Planteamiento del problema 2 1.5 Objetivo 3 1.5.1 General 3 1.5.2 Espec&#65533;ficos 3 1.6 Marco metodol&#65533;gico 4 CAPITULO&#65533;2: DESCRIPCI&#65533;N DEL &#65533;MBITO GENERAL DEL TELETRABAJO EN CONTACT CENTER 5 2.1 Marco te&#65533;rico 5 2.2 Definici&#65533;n 5 2.3 Antecedentes del teletrabajo 6 2.4 Historia de los Contact Centers 7 2.5 Normas internacionales 8 2.6 Ataques inform&#65533;ticos 9 2.6.1 Malware 9 2.6.2

Amenazas persistentes avanzadas 10 2.6.3 Puerta trasera 10 2.6.4 Fuerza bruta 10 2.6.5 Ingenier&#65533;a social 10 2.6.6 Phishing 10 2.6.7 Spoofing 10 CAP&#65533;TULO 3: APLICACI&#65533;N DE LA CIBERSEGURIDAD, LOS CONTROLES Y SITUACI&#65533;N ACTUAL DEL TELETRABAJO EN CONTACT CENTER SANTO DOMINGO 11 3.1 Que es la ciberseguridad 11 3.2 Controles cr&#65533;ticos de ciberseguridad 11 3.2.1 Control protecci&#65533;n del navegador web y del correo electr&#65533;nico 12 3.2.2 Control defensas contra malware 12 3.2.3 Control Gesti&#65533;n de la infraestructura de red 12 3.3

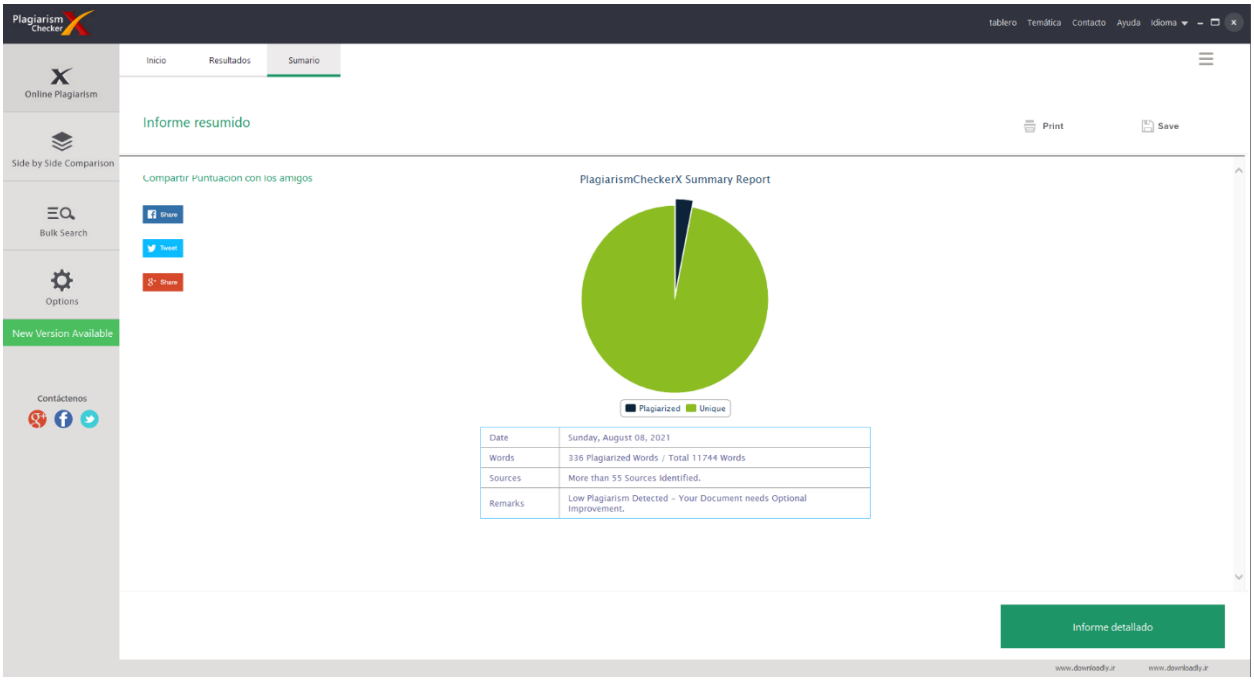
Situaci&#65533;n actual del teletrabajo en Contact Center, Santo Domingo 13 3.3.1 Comienzos 13 3.3.2 Posibles riesgos 14 3.3.3 Caso actual de &#65533;Contact Centers&#65533; en el parque de zona franca San Isidro, en Santo Domingo Este. 14 3.3.4 Entrevista a un supervisor de &#65533;rea de Contact Center 15 3.4.5 Encuesta 16 CAP&#65533;TULO 4: IMPLEMENTACI&#65533;N DE ESTRATEGIAS EN LA CIBERSEGURIDAD DURANTE EL TELETRABAJO 21 4.1. Elementos que conforman la estrategia 22 4.2

Sources found:

Click on the highlighted sentence to see sources.

Internet Pages

<1% https://industrialfreezone.com/
<1% http://repositorio.uchile.cl/bitstream/h
<1% https://www.facebook.com/SoyMayraMurriet
<1% http://riul.unanleon.edu.ni:8080/jspui/b
<1% https://www.lanacion.com.ar/el-mundo/esp
<1% https://www.mondaq.com/employment-and-wo
<1% https://www.coursehero.com/file/pscv7u/1
<1% https://docs.bentley.com/LiveContent/web
<1% https://www.reeditor.com/pdf/19815/29/mi
<1% https://www.laestrella.com.pa/opinion/co
<1% https://www.bbc.com/mundo/noticias-57582
<1% https://www.isotools.org/2020/09/23/hse-
<1% https://comunidad.movistar.es/t5/user/vi
<1% https://revista.aenor.com/348/isoiec-270
<1% https://www.researchgate.net/publication
<1% https://www.entrepreneur.com/article/261
<1% https://inmuebles.mercadolibre.com.do/so
<1% https://emotion.tirgy.com/28365/como-se-
<1% https://listindiario.com/economia/2020/0
<1% https://www.linguee.es/espanol-ingles/tr
<1% https://lahora.gt/pandemia-causa-quiebra
<1% https://www.instagram.com/p/CAvb-mhh5AZ/
<1% https://1library.co/document/y93xxrly-fi
<1% http://www.ieu.unal.edu.co/en/medios/not
<1% https://manglar.uninorte.edu.co/bitstrea


Plagiarism Checker
tablero Temática Contacto Ayuda Idioma
Online Plagiarism
Side by Side Comparison
Bulk Search
Options
New Version Available
Contáctenos
Inicio
Resultados
Sumario
Informe resumido
Print
Save
Compartir Puntuacion con los amigos
Share
Tweet
Share
PlagiarismCheckerX Summary Report
Plagiarized
Unique
Date
Sunday, August 08, 2021
Words
336 Plagiarized Words / Total 11744 Words
Sources
More than 55 Sources Identified.
Remarks
Low Plagiarism Detected - Your Document needs Optional Improvement.
Informe detallado
www.downloadly.ir
www.downloadly.ir