DISEÑO DE LINEAMIENTOS, ARQUITECTURA DE SEGURIDAD E IMPLEMENTACIÓN DE LA POLÍTICA ORIENTADA AL TRABAJO DESDE CASA PARA EL INSTITUTO NACIONAL DE CANCEROLOGÍA

Cortes Hernandez, Andres Mauricio
a.cortesh@uniandes.edu.co
Zapata Vargas, Rafael Humberto
rh.zapata@uniandes.edu.co

Resumen **– Desde el 2019 que empezó la pandemia Covid-19 y aproximadamente a finales de marzo del 2020. En Colombia se dio la orden de cuarentena general en todas las empresas, las cuales tuvieron que adaptarse a nuevos modelos de trabajo e incursionaron en nuevas tecnologías y medios digitales, para poder trabajar de manera remota. No obstante, esto generó un esfuerzo muy grande en todas las empresas. Este suceso, no fue diferente para el Instituto Nacional de Cancerología ya que, al ser una entidad de salud, su prioridad está centralizada en cuidar y preservar las vidas de sus pacientes.**

Teniendo en cuenta, lo anteriormente expuesto, el instituto cancerológico optó por mandar a la mayor parte de sus funcionarios a trabajar desde sus casas, esto conllevó a que el área de tecnología doblara los esfuerzos para poder exponer los servicios a internet y darle continuidad a la operación, sin tener en cuenta las mejores prácticas de seguridad al momento de generar algún cambio sobre la infraestructura, así mismo, no se generó ningún lineamiento para la salida de los usuarios a teletrabajo. El siguiente documento cubrirá los lineamientos de seguridad, política de teletrabajo que se pueden implementar en el Instituto Nacional de Cancerología.

Abstract **-** Since 2019 the pandemic started Covid-19 and approximating the ends of March from 2020. In Colombia the order of quarantine was given to all companies, which had to adapt to new models of work, new technologies and new digital media to be able to keep working remotely. However this generated a new effort on the part of technologies of every companies. This event was no different for the National Cancer Institute since, being a health entity, its priority is centered on caring for and preserving the lives of its patients.

Taking into account the above said, the cancer institute chose to send most of its employees to work from their homes, this led to the technology area doubling its efforts to expose the services to the internet and give continuity to The operation, without taking into account the best security practices at the time of generating any change on the infrastructure, likewise, no guidelines were generated for the exit of users to telework. The following document will cover the safety guidelines, telework policy that can be implemented in the National Cancer Institute.

I. Introducción

El uso de nuevas tecnologías, cambios económicos y las nuevas tendencias mundiales hacen que sea necesario cambiar las formas tradicionales de trabajo, a unas más flexibles que permitan garantizar los elementos esenciales de la relación laboral. Nadie predijo que la revolución del teletrabajo llegaría de golpe, ni que sería casi obligatoria. En medio de la pandemia, la adopción de tecnologías para trabajar desde casa ayuda a garantizar tanto la seguridad de los empleados como la continuidad de las actividades de negocio de las empresas, pero esta multitud de nuevos trabajadores remotos y móviles que carecen de preparación ha traído consigo riesgos de ciberseguridad sin precedentes.

La problemática del teletrabajo en el cancerológico se centra en los incidentes presentados por efectuar de manera masiva la salida a trabajo en casa, por este hecho se puede identificar la carencia de buenas prácticas de TI, como también oportunidades de mejora en su estrategia para escoger una modalidad en que la operación pueda continuar cuando los funcionarios estén por fuera de las instalaciones del Instituto Nacional de Cancerología.

Este documento cubrirá los aspectos generales para la creación de una política de teletrabajo, diseño de los servicios críticos y toda la respectiva documentación para el esquema de conexión remota a la red corporativa del Instituto Nacional de Cancerología,

II. Antecedentes

Entre enero y marzo de 2020, a medida que las infecciones por COVID-19 se extendieron por todo el mundo, en Colombia se dieron instrucciones a los empleadores de cerrar sus operaciones y de ser posible, aplicar el teletrabajo a tiempo completo para sus trabajadores, con muy poco tiempo de preparación tanto para los empleadores como para los trabajadores, algo que se planeó como una solución temporal y a corto plazo ha estado sucediendo desde hace meses esto ha dejado muy mal parado a las áreas de TI, que se han visto forzadas a implementar esquemas de teletrabajo en tiempos récord, sin tener en cuenta una arquitectura sólida y un diseño exhaustivo de los componentes informáticos que asegure la disponibilidad de la información, y mucho menos sin tener en cuentas las múltiples amenazas de seguridad que esto conlleva para la operación de las organizaciones, generando desconfianza y falta de expectativas de los usuarios hacía las áreas de tecnología.

En Colombia, según el más reciente estudio de penetración de teletrabajo, realizado en julio de 2018 para el MinTIC por la Corporación Colombia Digital y el Centro Nacional de Consultoría, el número de teletrabajadores en nuestro país se ha incrementado en más de 385 % en los últimos años, pasando de 31.500 en 2012, a más de 122 mil teletrabajadores en el año 2018 [11]. El estudio también señala que Bogotá se consolida como la ciudad con mayor número de individuos que operan bajo esta modalidad y de acuerdo con este enorme crecimiento de trabajadores remotos ahora impulsados por la pandemia del Covid-19, hace que las organizaciones deban generar esquemas de conexión para que los usuarios puedan acceder desde cualquier lugar a los sistemas corporativos, y esto principalmente abre nuevas puertas para la fuga de datos y en general posibilita la materialización de nuevos riesgos de ciberseguridad en las que muchas empresas e instituciones de toda índole no están preparadas. Como es el caso del Instituto Nacional de Cancerología, que actualmente adolece una cantidad importante de incidentes en la seguridad a raíz de la implementación de medidas improvisadas para poder mitigar las necesidades de conexiones remota de sus funcionarios, y que como consecuencia se han multiplicado los accesos de información por usuarios no autorizados, caídas en sus sistemas críticos de información, descargas de programas maliciosos, lentitud en la consulta de sus sistemas, etc.

III. Problemática Actual

Par el Instituto Nacional de Cancerología o también llamado INC se han presentado una serie de problemáticas tanto tecnológicas como administrativas asociadas a la rápida proliferación del trabajo desde casa, dichas problemáticas se han distribuido en 3 principales focos, el primero de ellos son los equipos de cómputo, casi la totalidad de colaboradores del Cancerológico cuentan con computadores de escritorio y no laptops, por tal motivo fue necesario que los médicos y funcionarios en general trabajarán desde sus casas con dispositivos personales, estas computadoras no tienen los mismos mecanismos de seguridad y controles que un computador corporativo; y esta falta de revisión ha provocado que documentos sensibles del instituto como por ejemplo historias clínicas se almacenen en las computadoras personales de los empleados y adicionalmente que esta información sensible también se transmita por medios de comunicación diversificados y no vigilados, como por ejemplo correos electrónicos personales.

Todo esto ha representado al INC múltiples incidentes de fuga de información, ya que según nuestra investigación, desarrollada en conjunto con el coordinador de la mesa de ayuda y el oficial de seguridad del instituto, desde mayo del 2020 a la fecha se han identificado 15 incidentes relacionados a imágenes diagnosticas de pacientes con cáncer en computadoras de hijos o familiares de los empleados, y esto puede representar un impacto tremendo debido a sanciones por mal manejo de datos personales extremadamente sensibles.

El segundo foco de problemas que identificamos en el Cancerológico, lo denominamos exposición de servicios, en el INC, con el afán de seguir manteniéndose operativo pese a las restricciones propias de la contingencia sanitaria, se realizaron configuraciones improvisadas en las que se expusieron a Internet las aplicaciones que los usuarios requieren para trabajar, como lo es la gestión documental, la herramienta de casos de mesa de ayuda, el sistema de planificación de recursos, sistemas de gestión de clientes, imágenes diagnósticas y otras aplicaciones especializadas de patología. Estas publicaciones sin planificación han afectado mayormente la disponibilidad de aplicaciones críticas que requieren los usuarios internos y externos. Se encontró en el informe del mes de julio de 2021, realizado por el administrador de seguridad informática del INC, que al menos 200 intentos de explotación de vulnerabilidades y ataques de denegación de servicio fueron dirigidos a dichas aplicaciones expuestas a Internet, en donde según el mismo informe, se les atribuyen que los servidores experimenten intermitencias de red y un estado de CPU entre el 80 y 90%. Esta conducta anómala es ratificada con reiterativos casos registrados en la mesa de ayuda, que manifiestan múltiples desconexiones y en general un funcionamiento inestable, además, como resultado del mismo informe se

encontró que el alto consumo remoto de las aplicaciones internas afecta negativamente el ancho de banda en upload del INC, lo que provoca que otros servicios se degraden y en general la experiencia de Internet de los usuarios no sea óptima. Adicionalmente se identificó que los servidores que atienden las aplicaciones expuestas no se encuentran dentro de una red DMZ, y por tal motivo facilita a atacantes llegar a otros servidores del INC, mediante movimientos laterales desde una aplicación vulnerada.

El tercer foco identificado, lo nombramos conexión remota, como se mencionó anteriormente, la gran mayoría de equipos de cómputo asignados a los usuarios del INC son de escritorio, estos equipos tienen instalados software muy especializado con licencias muy costosas que se distribuyen especialmente en unidades médicas, programas de software son esenciales para el trabajo de muchos usuarios en unidades como patología. Con la llegada de la pandemia y la necesidad de que los funcionarios trabajaran desde sus casas, era inviable por costos y control de inventario de licenciamiento, la instalación de los programas médicos en equipos personales o laptops rentadas, por esta razón se adoptó la medida de instalar el software Anydesk, en la mayoría de equipos del Cancerológico, este software permite la conexión remota desde otras computadoras a través de Internet, y de esta manera permitía a los usuarios conectarse desde sus casas a los equipos del Cancerológico como si estuvieran en la oficina, esta medida se adoptó rápidamente y funcionó sin novedades durante algunas semanas, sin embargo, no había una instrucción clara de qué software instalar, qué versión ni a qué usuarios.

Como resultado de la problemática que está pasando en el Cancerológico, se presenta un tremendo desorden en su red de datos a consecuencia de la implementación de una gran cantidad de reglas y configuraciones no documentadas, ni alineadas a un plan, falta de auditoría y desconocimiento total de los usuarios que tienen permitido conectarse desde sus casas. Tampoco hay control en el acceso de la información a la que ingresa cada funcionario, lo que ha generado gran cantidad de los incidentes mencionados, provocando un impacto cada vez mayor en la imagen, la atención y las finanzas del instituto.

IV. Propuesta

En esta sección describimos en un nivel amplio todo lo necesario para permitir que los empleados trabajen desde casa, las siguientes definiciones representan los procesos para definir quién es elegible para trabajar desde casa, el proceso para solicitar privilegios, así como el proceso de aprobación.

Estos componentes de alto nivel son indispensables para la elaboración de la política de trabajo remoto del INC, debido a que esta política es un acuerdo entre el Cancerológico y el empleado donde se declararán las expectativas y responsabilidades de los empleados que trabajan remotamente.

A. Elegibilidad De Trabajo En Casa.

No todas las funciones dentro del Instituto Nacional de Cancerología pueden realizarse a distancia, mientras que un desarrollador de software puede desempeñar fácilmente sus funciones desde casa a través de un ordenador y una conexión a Internet, un conductor de carretilla elevadora para la farmacia no puede hacerlo. Por eso uno de los pilares de la política de trabajo en casa es determinar desde el principio qué funciones pueden pasar de la oficina al hogar, con fluidez.

Se identificarán qué puestos están disponibles para el trabajo a distancia dentro del INC teniendo en cuenta las responsabilidades de cara a los pacientes, las limitaciones del software y los riesgos de seguridad del trabajo a distancia. Esto ayudará al instituto a reducir las solicitudes excesivas o innecesarias de trabajo desde casa.

Se tendrán en cuenta los siguientes criterios para que tanto los empleados como los directivos tengan en cuenta estos elementos antes de pedir o aprobar el trabajo desde casa, esto será un primer insumo para el oficial de seguridad y recursos humanos:

- ¿E l trabajador requiere presencia física para cumplir con su labor en el INC, como por ejemplo funciones de fabricación?
- ¿EL trabajador presenta alguna una restricción tecnológica como, por ejemplo, centro de llamadas o ventas?
- ¿Existe alguna restricción de seguridad que implique al funcionario no deba salir de las instalaciones del INC, como, por ejemplo, contratos con proveedores o historias clínicas impresas?
- ¿Existen problemas de ciberseguridad y privacidad de datos?
- ¿Cuáles son las condiciones del domicilio del empleado o del lugar de trabajo alternativo (ruido, conexión a internet, etc.)?

B. Proceso Aprobatorio De Trabajo En Casa

El proceso aprobatorio de las solicitudes para trabajar desde casa en el Instituto Nacional de Cancerología consta de tres pasos. En primer lugar, la solicitud del funcionario a su jefe inmediato, centrándose en si su puesto y sus características personales son adecuadas para el trabajo en casa. El segundo paso del proceso consiste en la evaluación mediante el diligenciamiento de un formato del entorno doméstico del empleado, para identificar si es adecuado para el trabajo en casa. Y el tercero es el diligenciamiento de un nuevo formato para tener consignadas las condiciones del domicilio y las características técnicas de la conexión a Internet del funcionario.

Las solicitudes de trabajo desde casa serán aprobadas por

recursos humanos y el oficial de seguridad con el visto bueno u observaciones del jefe inmediato, la respuesta de esta solicitud en caso de ser positiva mencionará con qué modalidad el funcionario del INC podrá trabajar desde casa:

- En determinadas ocasiones.
- Tiempo completo.
- Alternancia, repartiendo su tiempo entre el lugar de trabajo físico y su puesto de trabajo a distancia.

C. Equipamiento & Soporte Técnico

Una vez se haya aprobado la solicitud de trabajo en casa, se iniciará un proceso de alistamiento en la mesa de ayuda, la política de trabajo desde casa es clara en no permitir bajo ningún motivo el uso de computadoras personales para el trabajo remoto, por esta razón la mesa de ayuda identificará inicialmente si el funcionario ya cuenta con un equipo portátil corporativo asignado y en caso de que no, se le asignará uno, en conjunto con su respectivo cargador, mouse, pad-mouse y opcionalmente un teclado si el funcionario lo indica. Las computadoras alistadas para trabajo a distancia, determinadas características técnicas como el cifrado de disco y el bloqueo de los puertos USB y antivirus entre otros.

Tampoco está permitido para el trabajo desde casa, la asignación o alistamiento de impresoras, monitores u otro tipo de hardware al declarado anteriormente. Como resultado de este proceso se cargará o descontará en el inventario el hardware asignado y se le enviará la novedad a RRHH.

Al trabajar desde casa, los empleados del instituto dependerán más que nunca de la tecnología. La realización de las funciones de comunicación y de trabajo más básicas requiere el uso de TI, por esta razón la operación de la mesa de ayuda para el soporte de TI es más importante y logísticamente más difícil para una plantilla dispersa, debido a la incorporación remota. Todo esto se ideó un plan de comunicaciones y un esquema de soporte remoto que asegure que los empleados a distancia puedan recibir ayuda y atención a sus solicitudes de forma eficaz.

D. Acuerdos.

Siempre que una solicitud de trabajo en casa haya superado con éxito el proceso de evaluación, al funcionario del INC se le entregará un acuerdo de trabajo en casa. Este acuerdo será emitido por la dirección de recursos humanos junto con cualquier modificación del contrato. Se pedirá al empleado que firme y devuelva una copia del acuerdo de trabajo en casa, que se conservará en su expediente personal.

E. Canales De Comunicación.

Dado que en el INC la comunicación en persona ya no es una opción para todos, las comunicaciones internas deben definirse estrictamente. Esto significa que se auditarán los canales de comunicación existentes y se designará el propósito principal de cada uno. Esto también implicará la eliminación de los canales redundantes, por ejemplo, el uso simultaneó de Slack, Teams y G-chat. Se exigirá a los miembros del instituto que se ciñan a los canales de comunicaciones propuestos para reducir la ineficacia:

- Microsoft Teams para una comunicación rápida, ligera e informal, y como segundo contacto para anuncios puntuales.
- El correo electrónico Outlook para comunicaciones más formales, largas, anuncios para todo el equipo y programación interna.

F. Seguridad & Privacidad

De acuerdo con el manual del empleado y el acuerdo de confidencialidad firmado por el funcionario al momento de su contratación, la seguridad de los datos y la información del instituto debe ser de máxima preocupación y prioridad. Cualquier infracción del protocolo de seguridad dará lugar a medidas disciplinarias estrictas e inmediatas.

Los empleados que trabajen desde casa están obligados a cumplir de igual manera con la política de seguridad y privacidad del Instituto Nacional de Cancerología y con todos los requisitos de seguridad y confidencialidad informática propuestos en la política de trabajo en casa. El trabajador remoto tendrá una responsabilidad directa sobre todo el material que tenga en su en su casa y debe asegurarse de que no sea accesible a personas no autorizadas, como, por ejemplo, otros miembros de su hogar.

Los empleados tendrán acceso a un medio de conexión remoto hacia los servidores y redes del instituto. Este esquema de conexión debe usarse en todo momento durante las horas de trabajo, este esquema de conexión remota contendrá una serie de medidas de ciberseguridad para salvaguardar la integridad y confidencialidad de la información.

V. ANÁLISIS

Esta sección es clave para el desarrollo de nuestro planteamiento debido a que acá se condensan las investigaciones y análisis realizados para poder plantear y desarrollar la solución de este proyecto. Inicialmente se aborda la selección del marco de referencia, esta selección tiene como finalidad elegir la guía más apropiada para ayudar mitigar los riesgos asociados a las tecnologías empresariales utilizadas para el teletrabajo, siendo un insumo para el diseño de la política y la arquitectura propuesta.

Como segunda parte se detalla la selección de la tecnología

remota, esta selección muestra el análisis realizado para determinar cuál es la tecnología o solución integral que responda las necesidades de conexión de los trabajadores remotos en el cancerológico.

Los demás componentes como los servicios expuestos, redes de datos, organigrama y tipos de usuario hacen referencia al levantamiento de información de los aspectos técnicos más relevantes necesarios para poder entender la situación actual del Cancerológico y con este insumo poder identificar todas las posibles variables para desarrollar la solución de este proyecto.

A. Identificación Marcos De Referencia.

Se tendrán en cuenta los diferentes marcos de referencia relacionados con la seguridad de la información. Se analizará cuál de estos ayudará para con el desarrollo de la política de teletrabajo que se implementará en el Instituto Nacional de Cancerología, para ello se realizará el análisis con los siguientes marcos de referencia:

1. ISO 27001:2013: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa, tiene como fundamento los tres pilares de la seguridad de la información como es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace analizando cuáles son los potenciales problemas que podrían afectar la información con la evaluación de los riesgos presentados en la empresa y luego de los riesgos generados en la evaluación del sistema. [1]
2. SOC 2 tipo 2: Una auditoría de los Controles de Servicio y Organización 2 (service organization control 2 – SOC 2) es una herramienta eficaz para evaluar los controles de seguridad de un proveedor. Es un estándar internacional desarrollado por el Instituto americano de contables públicos certificados (American Institute of Certified Public Accountants), en el caso de los informes SOC 2 Tipo 2, los controles de la compañía son evaluados durante un período de tiempo, que puede abarcar un año. Es una revisión histórica de los sistemas, para determinar si los controles están apropiadamente diseñados funcionan correctamente a lo largo del tiempo. [2]
3. NIST 800-46: (National Institute of Standards and Technology) ayuda a empresas de todos los tamaños, sectores e industrias a proteger sus sistemas y datos de TI, de las amenazas de seguridad asociadas con las tecnologías de teletrabajo y acceso remoto, incluida la seguridad de las tecnologías Bring Your Own Device (BYOD). Se considera la mejor práctica, especialmente porque las tecnologías de teletrabajo y acceso remoto a menudo requieren seguridad adicional debido a su mayor vulnerabilidad a amenazas externas. [3]
4. COBIT 5: (Control Objectives for Information and related Technology) Es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información de una organización, así como evaluar el estado en que se encuentran las TI en la empresa, también se puede definir como un conjunto de herramientas de soporte empleadas por los gerentes para reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. [4]

Para poder determinar los criterios de evaluación, se realizó una mesa de seguridad con el coordinador de sistemas y el oficial de seguridad, en la cual se pautaron los 10 criterios con base a los conocimientos que se tenían sobre los estándares y cual está en mayor sincronía con el Instituto Nacional de Cancerología para poder construir la política de teletrabajo. El valor que se otorgó para cada uno de los criterios está dado por porcentajes de mayor a menor, dando un valor mayor a los criterios que están enfocados a seguridad de la información y a la construcción de la política de teletrabajo, la sumatoria de todos los valores de los diferentes criterios dan como resultado 100%, los cuales se pueden observar en la tabla 1. Criterios de evaluación Marcos de Referencia.

CRITERIOS DE EVALUACIÓN	VALOR
El estándar está enfocado en seguridad de la información	15%
El estándar está enfocado a la política de teletrabajo	15%
El estándar ayudara a la creación de los controles de la política de teletrabajo	12%
El estándar ayuda a proteger los sistemas de teletrabajo y acceso remoto	12%
El estándar ayuda a mitigar la problemática del proyecto	12%
El estándar es una guía para la planificación de la política de seguridad de teletrabajo	8%
El estándar es fácil para la implementación	3%
El INC puede certificarse con el estándar	8%
El INC está familiarizado con el estándar	5%
El oficial de seguridad conoce el estándar	10%

Tabla 1. Criterios de evaluación Marcos de Referencia.

La calificación para cada uno de los estándares y criterios se dio en consenso con el oficial de seguridad y el coordinar de sistemas, los puntajes que se expusieron en la mesa de seguridad. El promedio resultante de cada estándar es la sumatoria de cada uno de los criterios evaluados por el producto de la calificación y el valor porcentual de cada criterio de

evaluación.

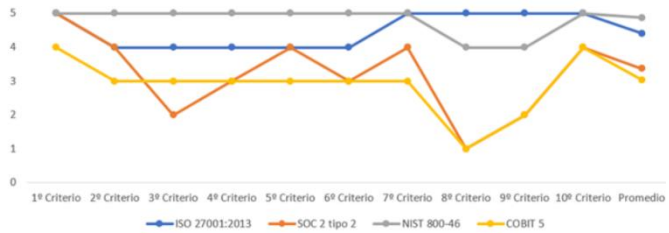

Ilustración 1. Grafica Multicriterio Estándares de Seguridad.

Para cada uno de los criterios evaluados en la mesa de seguridad, se obtuvo el resultado ponderado que el estándar NIST 800-46 con un valor ponderado de 4,87 es el marco más apropiado para tener como referencia para creación de la política de teletrabajo, rediseño de los servicios expuestos y el modelamiento del esquema de conexión remoto.

B. Identificación Tecnologías De Conexión Remota.

Las conexiones remotas son un punto esencial para realizar el modelamiento de como los funcionarios podrán acceder a la infraestructura corporativa para poder cumplir con sus labores diarias para esto se optaron por las siguientes soluciones:

1. AnyDesk: Programa de software de escritorio remoto desarrollado que provee acceso remoto bidireccional entre computadoras personales y está disponible para todos los sistemas operativos comunes. [6]
2. TeamViewer: Es un software de fácil acceso que permite conectarse remotamente a otro equipo. Entre sus funciones están: compartir y controlar escritorios, reuniones en línea, videoconferencias y transferencia de archivos entre ordenadores. Existen versiones para los sistemas operativos Microsoft Windows, Mac OS X,1 2 Linux,3 iOS,4 Android,5 Windows Phone 8, Windows RT y BlackBerry. [7]
3. VPN: Es una red virtual privada la cual será utilizada por los funcionarios para poder acceder a la red interna de la organización y a los recursos corporativos, con esta solución se habilitará el acceso a los escritorios para la manipulación remota y uso de los servicios de la compañía.
4. Escritorios virtuales: Es una solución en la cual virtualiza escritorios con las características necesarias para que los empleados puedan tener un fácil acceso a las aplicaciones y datos corporativos, independiente de donde se encuentren, esta solución protege el acceso a las aplicaciones y los recursos son protegidos por la compañía. [8]

Los criterios que se utilizaron para construir la matriz fueron establecidos de acuerdo con la problemática que posee Instituto Nacional de Cancerología que se basa en el acceso a los servicios y aplicaciones que solo están en la red corporativa, para ello se evaluaron las principales tecnologías que se encuentran en el mercado, se analizó y otorgo un mayor valor a los criterios que cumplen con el aseguramiento de la información para que estén alineados con la confidencialidad de los datos sensibles que se manejan en el INC y la administración centralizada sobre la herramienta para poder generar controles de seguridad sobre la misma, con ello se obtuvieron 9 criterios de evaluación en el cual la sumatoria total es del 100%.

CRITERIOS DE EVALUACIÓN	VALOR
Acceso remoto a la infraestructura del INC	10%
Protocolos seguros para el acceso remoto	15%
Control sobre la información sensible del INC	15%
Control sobre los recursos corporativos (performance)	15%
Facilidad para el despliegue de nuevas aplicaciones	8%
Facilidad para la implementación de controles de seguridad que resguarden la fuga de información	15%
Arquitectura On Premise y Cloud	3%
Costo para la implementación	15%
Rápida implementación	4%

Tabla 2. Criterios de Evaluación Tecnologías Remotas.

Para la calificación se optó el mismo método en la matriz multicriterio de los estándares de seguridad efectuando un consolidado del valor para cada tecnología, el promedio dado por cada tecnología de conexión remota es la sumatoria de cada uno de los criterios dados por el producto de la calificación y el valor porcentual de cada criterio de evaluación.

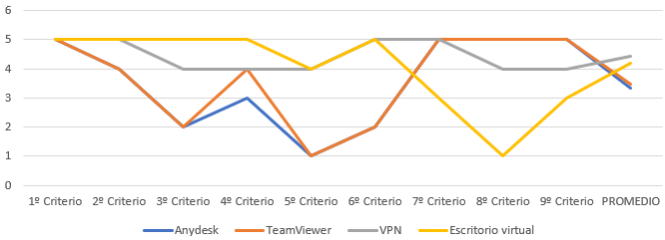

Ilustración 2. Grafica Multicriterio Soluciones Tecnológicas de Conexión Remota.

Al obtener los resultados se puede observar que la tecnología que se puede implementar para solucionar la problemática de acceso a la red corporativa es la VPN con un valor ponderados de 4,43, esta herramienta es la más apropiada analizándolo desde varios puntos de vista, desde costo, fácil implementación y seguridad de la información corporativa.

C. Organigrama.

Como resultado final del levantamiento de información realizado en conjunto con el área de talento humano, se identificó que el organigrama del INC está compuesto por las siguientes 5 secciones principales, organizadas por jerarquía:

- Junta directiva
- Dirección general
- Oficinas
- Subdirecciones
- Grupos área

Con base al análisis del organigrama del INC, fue posible realizar una agrupación más detallada de los usuarios para que con este insumo sea posible segregar o segmentar roles y funciones de acuerdo con las características o naturaleza de cada puesto de trabajo.

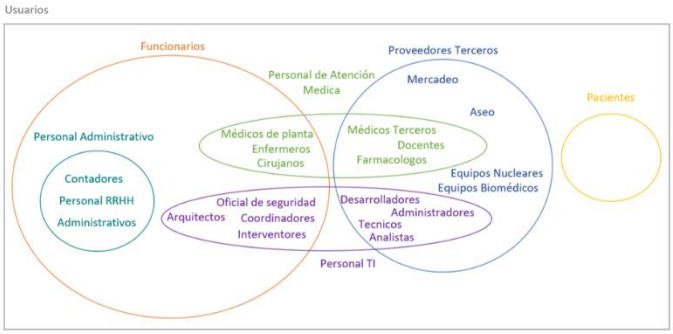

Ilustración 3. Tipos de Usuarios.

1. Funcionarios
    a. Personal Administrativo
        i. Contadores
        ii. RRHH
        iii. Administrativos
2. Personal Atención Medica
    a. Médicos de planta
    b. Enfermeros
    c. Cirujanos
3. Personal TI
    a. Oficial de seguridad
    b. Arquitectos
    c. Coordinadores
    d. Interventores
    e. Desarrolladores
    f. Administradores
    g. Técnicos
    h. Analistas
4. Proveedores Terceros
    a. Mercadeo
    b. Aseo
    c. Equipos
    d. Nucleares
    e. Equipos biomédicos
5. Pacientes

D. Controles A Nivel De Host

Las acciones y tareas que realiza el Instituto Nacional de Cancerología generan un gran volumen de información confidencial recogida en forma de distintos documentos asociados principalmente a datos clínicos de los pacientes. Implementar las medidas de seguridad a nivel de host es de vital importancia para que el INC pueda trabajar de forma correcta y pueda cumplir con normativas vigentes sobre protección de datos y otras reglamentaciones del ministerio de salud. Los controles de seguridad propuestos refuerzan la posición del Cancerológico en la gestión contra de virus, spywares, malwares o troyanos que pueden alterar totalmente el funcionamiento de los dispositivos y son capaces de generar daño severo en los equipos.

1. Antivirus & Antimalware

Todos los ordenadores corporativos conectados a la red del INC deberán contar con antivirus con su respectiva licencia. Los antivirus aportan medidas de protección efectivas ante la detección de un malware o de otros elementos maliciosos, cierran posibles amenazas y son capaces de poner el dispositivo en cuarentena para evitar males mayores. Otro aspecto muy importante en este control propuesto es el proceso de actualización de este, de lo contrario el instituto podría incurrir en una falsa sensación de seguridad debido a que se sienta protegido por tener antivirus, pero en realidad no debido a que esta desactualizado.

2. Bloqueo de puertos USB

Todas las maquinas deben contar con el control de bloqueo de puertos USB, este control se realizará a partir del módulo “Device Control” del antivirus corporativo, este bloqueo impide que personas inescrupulosas puedan extraer información o instalar malware para afectar el funcionario cuando no esté en el computador, con esto se evita que los computadores corporativos se infecten de software malicioso.

3. Firewall

Con este control propuesto es posible escanear los paquetes de red entrantes y salientes de cada uno de los ordenadores de la red del INC y de acuerdo con su comportamiento bloquearlos o no según un análisis de tráfico previamente identificado, estas configuraciones nuevas tienen que estar aprobadas por la supervisión.

4. Control de navegación WEB

Sin un control adecuado sobre la navegación, los empleados del INC pueden hacer un mal uso de Internet, y este mal uso puede generar problemas como

por ejemplo pérdidas de información o la infección de los equipos con malware. El control propuesto se basa en generar perfiles de navegación web en el firewall, de acuerdo con las áreas identificadas en el organigrama y de esta manera que cada área funcional acceda a Internet con su propio perfil basado en sus necesidades laborales y dejar de permitir el acceso libre a la web, por ejemplo, el área de contabilidad podrá tener acceso a páginas web de tipo bancario, pero áreas médicas no podrán realizar ninguna clase de transacción en Internet.

5. Antispam

Actualmente en el INC una gran parte de las comunicaciones se realiza utilizando el correo electrónico, por lo tanto, otra medida de seguridad propuesta es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de los datos en especial de las historias clínicas o en general datos médicos.

6. Respaldos

Tener un sistema de copias de seguridad periódico le permitirá al Cancerológico poder recuperar los datos ante una incidencia moderada o incluso de carácter catastrófico, impidiendo la pérdida de estos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.

7. DLP

La prevención de pérdida o fuga de datos (DLP) se propone cómo medida de seguridad en el INC para supervisar que ningún usuario esté copiando o compartiendo información o datos que no están aprobados por el INC. El DLP monitorizaría la red de la organización para evitar las fugas de información antes de que se lleguen a producir. Una vez que detecte una posible fuga, se alertaría al usuario para que sea consciente de que la acción que está realizando atenta contra la confidencialidad del instituto.

8. Cifrado

La seguridad de los equipos portátiles o de mesa es fundamental para que las historias clínicas y otros datos sensibles estén a salvo. Las amenazas a las que los ordenadores del INC pueden ser sometidos son muy variados y con orígenes muy distintos, uno de las más graves es el robo de información cuando un equipo portátil es robado o perdido.

VI. Arquitectura

A. *Topología Física Actual.*

De acuerdo con la investigación realizada junto con el administrador de redes del cancerológico, se identificó inicialmente dos enrutadores, configurados de manera independiente, es decir, que entre ellos no conforman ninguna clase de redundancia, estos equipos de red se conectan directamente a un firewall, este cortafuegos se comporta como el dispositivo capa 3 principal del instituto, se encarga de enrutar todas las redes LAN entre sí y hacia Internet. Adicionalmente el firewall está conectado a otro enrutador para establecer una conectividad y así dar conexión de red a una sede satélite.

B. *Topología Lógica Actual.*

La topología lógica se compone de múltiples redes que conforman la LAN del INC, dichas redes se ubican detrás de un firewall y son enrutadas a través de este, el cual delimita el perímetro hacia Internet.

C. *Exposición De Servicios Actual.*

La arquitectura actual para exponer los servicios en el INC se basa principalmente en el NAT, la configuración utilizada en este caso se le domina Destination NAT, en la cual la IP que se traslada es la destino, es decir, la IP publica a la cual el usuario remoto hace las consultas se cambia a nivel del firewall a la dirección privada que tiene el servidor en la red interna del INC, todo esto sin que el usuario remoto se entere.

La gran desventaja a nivel de seguridad de este tipo de arquitecturas y de configuraciones, es que en caso de que algún servidor se comprometa, el atacante podría hacer movimientos laterales en la red, es decir, con el acceso a algún servidor comprometido, se podría utilizar esa ubicación en la red para expandir el ataque e intentar infectar o alterar a otros servidores cercanos o redes a las que le permita el acceso, logrando así ampliar su superficie y causar más daño, fugar más información u otras acciones de acuerdo con las intenciones del atacante.

D. *Topología Física Propuesta.*

La topología física propuesta comienza en realizar el HSRP de los dos enrutadores, el HSRP es un protocolo que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red, este protocolo evita la existencia de puntos de fallo únicos mediante técnicas de redundancia y de esta manera tener mayor disponibilidad en los servicios que dependen de la WAN. Como segundo paso, se propone conectar los mismos enrutadores del ISP a un switch WAN y no directamente al firewall, esto proporciona flexibilidad para pruebas de conexión, por ejemplo, algún canal adicional o la configuración de un enlace WAN con otro dispositivo capa 3, además proporciona la capacidad de centralizar las VLAN de las redes MAN como MPLS o en general demás conexión de área muy amplia.

Con respecto a la red LAN, se propone no conectar los servidores a switches de distribución, sino que los servidores se

conecten a un switch TOR con mayores prestaciones de conmutación.

E. Topología Lógica Propuesta.

Con respecto al diseño lógico, se propone un esquema basado en zonas, las zonas son un grupo de una o más interfaces, tanto físicas como virtuales, a las que se puede aplicar políticas de seguridad para controlar el tráfico entrante y saliente. Agrupar las interfaces o VLAN en zonas simplifica la creación de políticas de seguridad, donde varios segmentos de red pueden usar la misma configuración de políticas o pueden manejarse de forma independiente, además, tienen la gran ventaja de que posibilitan el establecimiento de permisos de red preconfigurados.

Adicionalmente, el esquema de zonas propuesto estará acompañado del enfoque de microsegmentación. La microsegmentación es un método para crear zonas seguras en centros de datos, que les permite aislar las cargas de trabajo entre ellas y protegerlas individualmente. Está dirigido a hacer que la seguridad de la red sea más granular, es decir, la red se dividirá en múltiples redes más pequeñas para minimizar brechas. Estas redes se agrupara por zonas, por ejemplo, el enfoque tradicional usualmente refiere a una única red de servidores aislado el tráfico de los mismos de la red de usuarios finales, sin embargo, un servidor comprometido podría exponer a todos los servidores que comparten la misma red, mientras que con la arquitectura propuesta basada en zonas y microsegmentación, la red de servidores pasaría a ser una zona o en otras palabras una agrupación de redes más pequeñas que contendrían los servidores que conforman la red, de esta manera si un servidor se expone o compromete no hay más servidores en dicha red y minimizaría el riesgo de un ataque exitoso, la ilustración 4 ilustra el concepto de microsegmentación.

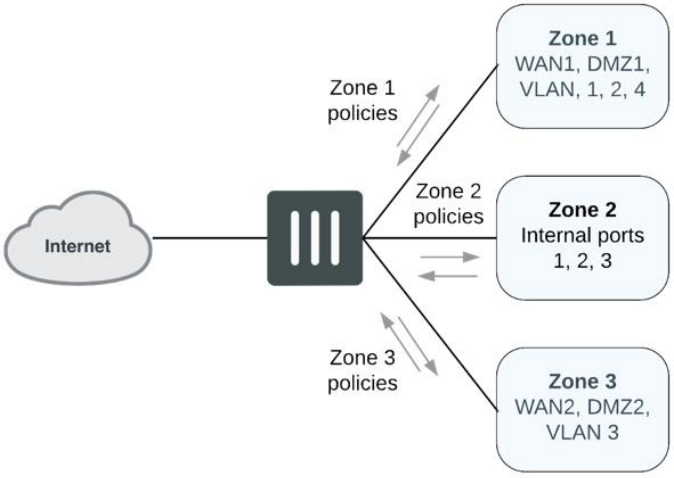

Ilustración 4. Topología Zonas

F. Exposición De Servicios Propuesta.

La exposición se servicios propuesta se basa en la creación de una zona DMZ que contenga múltiples redes DMZ agrupadas por servicios o funciones en común. La red DMZ estará diseñada para los servidores que expongan servicios hacia redes hostiles como Internet, usualmente en los enfoques de seguridad tradiciones se utiliza una única red DMZ, la cual contiene todos los servidores que se pueden acceder desde Internet o que exponen servicio ahí, y de esa manera se aísla ese tráfico posiblemente malicioso hacia otras redes internas, como la de usuarios o la red de servidores. sin embargo, una red que comparte múltiples servidores hace que compartan medios en común, por ejemplo, el broadcast, y eso puede ser utilizado para ataques en capa 2, pero con el esquema de exposición de servicios propuesto con una DMZ basada en zonas y microsegmentación cada red DMZ será una habitación aislada con permisos de red rigurosas evitando así que si un servidor en una red DMZ se comprometa no represente un riesgo para otros servidores DMZ.

VII. METODOLOGÍA

La metodología a utilizar son los lineamientos que se encuentran en la NIST 800 – 46 que es la guía de teletrabajo empresarial, acceso remoto y brindar la Seguridad de sus propios dispositivos (BYOD).

A. Fuente de información para el proyecto

El levantamiento de información dentro del instituto y con el estudio de los estándares de seguridad que se pudieran acoplar al proyecto tenemos que:

1. Fuentes primarias

Se tienen las siguientes fuentes de información después del estudio de cuál es el mejor estándar de seguridad que se ajuste con la creación de la política de teletrabajo y la normativa colombiana:

- Para la metodología se tomó el marco de referencia la NIST SP 800-46 ya que es la guía que nos ayudará con la problemática del proyecto.
- Teniendo como base la normatividad colombiana se utilizó el, Libro Blanco, ABC del teletrabajo en Colombia, la Ley 1221 de 2008 y el Decreto 0884 de 2012.

2. Tipos y métodos de investigación

El proyecto se realizó en base al siguiente tipo de investigación:

- Método inductivo – deductivo.

De esta manera, se realizará el análisis partiendo de una

premisa general, evaluando así el marco de referencia seleccionado y después el análisis de los principios generales para llegar a la conclusión específica, para validar que lo desarrollado funcione correctamente, esto también aplica al rediseño de los servicios expuestos y a los esquemas de conexión remota.

B. Técnicas para el desarrollo

Se realizó las siguientes actividades para el desarrollo de la problemática del INC:

1. Mesa de trabajo con el grupo de seguridad, gerencia de TI, mesa de ayuda y funcionarios.
2. Capacitaciones en las diferentes áreas.
3. Prototipos, con manual para la implementación del acceso remoto a la red corporativa.
4. Seguir los mejores estándares para la creación de las plantillas de hardening, tales como: CIS Benchmarcks [12], Statement on Auditing Standards (SAS) [13]y OWASP [14].

C. Entregables del proyecto

En esta sección estarán los entregables generales del proyecto.

1. Documento Política de trabajo en casa: En este documento se establecen los lineamientos de seguridad para que los funcionarios puedan establecer una conexión segura fuera de la red corporativa.
2. Documento con las topologías de los servicios: Se definieron las topologías de los servicios se entregará las topologías físicas y lógicas de las aplicaciones críticas del instituto.
3. Formato de solicitud de trabajo remoto: En este documento se tiene relacionado la lista de chequeo que debe cumplir el computador corporativo para poder tener la modalidad de teletrabajo, este documento lo deberá diligenciar el usuario con el apoyo de mesa de ayuda.
4. Matriz de acceso: En este documento se encuentran los diferentes grupos del directorio activo en los cuales se podrán evidenciar los permisos que tendrán los usuarios cuando se conecten a la VPN, con esta matriz se tendrá la descripción generalizada de mecanismos de protección en sistemas operativos y del sistema de información.
5. Configuraciones seguras: Se realizará el análisis y la implementación de los permisos que tendrán cada uno de los usuarios y los accesos al sistema, cumpliendo con el principio de mínimo privilegio.
6. Manual de conexión remoto por medio de VPN: En este documento se encuentra el paso a paso para la conexión y configuración de la VPN en el equipo del funcionario.
7. Documento Resolución de problemas: Este documento se tendrá el paso a paso para poder realizar un diagnóstico rápido del error presentado en la conexión de las VPN y accesos a los sistemas de información, este documentó lo tendrán que utilizar mesa de ayuda.
8. Capacitaciones: Es necesario realizar la concientización a los usuarios para el correcto uso de la política de teletrabajo, con ello se dictarán las mejores prácticas para el cambio y la elaboración de contraseñas seguras, el debido uso del correo corporativo y la identificación de correos maliciosos, el delicado uso y fuga de la información sensible, entre otros. Sin embargo, también se realizará capacitaciones a la mesa de ayuda para que esta área pueda apoyar cuando se presente algún problema con la VPN.

VIII. RIESGOS

La gestión de riesgos realizada es este proyecto en el INC consistió en identificar, planificar y controlar los riesgos potenciales. Se realizó una evaluación proactiva de los riesgos con el objetivo de estar preparados y corregir el curso rápidamente en caso de necesitarlo; y, así, cumplir con los objetivos del proyecto a tiempo y dentro del presupuesto.

Como primer paso reunimos una lista de todos los casos en los que se podrían presentar, potencialmente, riesgos que podrían afectar al proyecto. Con el oficial de seguridad del instituto se definió caso de riesgo como cualquier cosa que pudiese afectar negativamente al programa, al presupuesto o, en definitiva, al éxito del proyecto en sí.

Para determinar los riesgos identificados se utilizaron las siguientes tres herramientas en varias sesiones junto con el equipo del proyecto:

1. Juicio de expertos
2. Lluvia de ideas
3. Lista de verificación

Como resultados se obtuvieron los siguientes riesgos:

R#	RIESGO
R1	No identificar la totalidad de servicios digitales expuestos en el INC.
R2	No identificar la totalidad de las áreas elegibles para trabajo desde casa.
R3	El tiempo requerido para la identificación de servicios se extienda más de lo planeado teniendo en cuenta la disponibilidad de los recursos de los administradores del INC genere desfases en el cronograma.

R4	La tecnología remota escogida no cumpla con todas las necesidades del INC.
R5	La arquitectura de seguridad supere las habilidades técnicas del administrador de seguridad.
R6	La plantilla de endurecimiento o hardening propuesta no sea implementada por completo en el INC.
R7	Que los usuarios del INC continúen usando canales de comunicación diferentes a los establecidos.
R8	La implementación de la tecnología remota sea muy disruptiva y genere rechazo por parte de los usuarios.
R9	No encontrar disponibilidad necesaria de los usuarios para impartir las capacitaciones para la conexión remota.
R10	Pasar por alto componentes de infraestructura que no se identifiquen en las fases de inicio, lo que genere incompatibilidad con la arquitectura de seguridad en fases posteriores del proyecto.
R11	No estar alineado con la estrategia de la alta dirección.

Tabla 3. Tabla de riesgo

A cada riesgo identificado se le realizó un análisis de la probabilidad de su materialización y su gravedad o impacto en el Cancerológico. Teniendo en cuenta la complejidad de los riesgos de este proyecto, se consideró llevar a cabo el análisis con el equipo del proyecto y con algunos involucrados claves como el coordinador de sistemas y el administrador SAP debido a su larga carrera y experiencia en el INC. Para determinar la gravedad, se pensó el impacto que tendría el riesgo en los objetivos del proyecto, si retrasaría lo programado con el cronograma, afectará al presupuesto o reducirá el alcance que tendrían las entregas del proyecto.

MATRIZ DE RIESGOS

RIESGO	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
R1	3	4	12	Importante
R2	4	4	16	Muy grave
R3	4	4	16	Muy grave
R4	2	4	8	Apreciable
R5	4	3	12	Importante
R6	4	3	12	Importante
R7	2	3	6	Apreciable
R8	5	2	10	Importante
R9	4	4	16	Muy grave
R10	5	2	10	Importante
R11	5	1	5	Apreciable

			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.

Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.

Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las

Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Ilustración 5. Matriz de riesgos

Con base a esta matriz de riesgo realizada fue posible realizar un análisis más detallado de cada uno de los riesgos, se identificó que los riesgos más urgentes de tratar están relacionados con la fase de planificación del proyecto, más exactamente con la no identificación de áreas o servicios además de no encontrar la disponibilidad de los usuarios para capacitarlos en cuanto al uso de las tecnologías remotas para el acceso al trabajo remoto. La respuesta al riesgo ideada para estos riesgos etiquetados como "muy graves" es la mitigación, se realizaron varias iteraciones para identificar a todos los posibles interesados en el proyecto, de esta manera poder recopilar requisitos y expectativas como también posibles variables a fin de que no pasar por alto ninguno. Con respecto a la disponibilidad del personal para capacitarlo se involucró a la alta dirección como también a los líderes de cada área para que estuvieran enterados y muy atentos al proyecto y de esta manera poder contar con su apoyo a la hora de tener la disponibilidad de sus equipos y realizar las capacitaciones de manera satisfactoria.

IX. Trabajo Futuro

La continuación del proyecto de la implementación de la política de trabajo en casa para los funcionarios del Instituto Nacional de Cancerología es realizar los controles establecidos en la política, para poder mantener el correcto orden de los funcionarios que están trabajando desde el hogar.

A. Proceso de solicitud

Todos los funcionarios que tienen la posibilidad de optar por el trabajo desde casa deberán diligenciar los 3 formatos que se encuentra en la política para poder realizar el análisis a profundidad sobre la viabilidad para poder estar en esta modalidad de trabajo.

B. Evaluación del entorno del hogar

Un funcionario que trabaja en casa recibe la misma protección bajo la legislación de salud y seguridad que un funcionario que trabaja en una oficina. Por lo tanto, es vital asegurarse de que el entorno de trabajo en el hogar sea adecuado antes de llegar a un acuerdo sobre el trabajo a domicilio.

C. Acuerdo de trabajo en casa

Siempre que una solicitud para trabajar en casa haya pasado con éxito el proceso de evaluación de dos pasos descritos anteriormente, se debe emitir un acuerdo de trabajo en casa al empleado. Esto será emitido por la sección de recursos humanos junto con cualquier enmienda al contrato que pueda ser necesaria. Se le pedirá al empleado que firme y devuelva una copia del contrato de trabajo en casa y esto se conservará en su archivo personal.

Después de tener a las personas trabajando en el hogar, es necesario que el oficial de seguridad realice sesiones de seguimiento con cada una de las áreas del Instituto Nacional de Cancerología, para validar si se está cumpliendo con todas las metas y objetivos, ya que es necesario dar continuidad con el negocio y los funcionarios que estén con esta modalidad tienen que cumplir con todas sus actividades por más que no estén trabajando en la oficina.

Estos seguimientos son importantes para validar la viabilidad

de mantener la modalidad de trabajo en casa para los funcionarios.

REFERENCIAS

[1] ¿Qué es norma ISO 27001? (s. f.). 27001Academy. https://advisera.com/27001academy/es/que-es-iso-27001/

[2] SOC 2: la auditoría para los controles de ciberseguridad - Instituto Nacional de Contadores Públicos de Colombia. (s. f.). Instituto Nacional de Contadores Públicos de Colombia. https://incp.org.co/soc-2-la-auditoria-para-los-controles-de-ciberseguridad/

[3] NIST 800-46 Compliance & Scoring | Centraleyes. (s. f.). Centraleyes. https://www.centraleyes.com/nist-800-46/

[4] Los cinco principios de COBIT 5. (s. f.). ESAN | Graduate School of Business. https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/

[5] Sitio oficial del Consejo sobre Normas de Seguridad de la PCI (Industria de tarjetas de pago) - Verificar las normas de Cumplimiento, de seguridad de descarga de datos y de seguridad de tarjetas de crédito. (s. f.). Sitio oficial del Consejo sobre Normas de Seguridad de la PCI (Industria de tarjetas de pago) - Verificar las normas de Cumplimiento, de seguridad de descarga de datos y de seguridad de tarjetas de crédito. https://es.pcisecuritystandards.org/minisite/env2/

[6] The Fast Remote Desktop Application – AnyDesk. (s. f.). AnyDesk. https://anydesk.com/en

[7] Home. (s. f.). TeamViewer. https://www.teamviewer.com/en-us/

[8] Solución de acceso remoto seguro para aplicaciones empresariales - Citrix México. (s. f.). Citrix.com. https://www.citrix.com/es-mx/products/citrix-gateway/

[9] Misión, Visión, Valores, Principios y Código de integridad - Instituto Nacional de Cancerología. (s. f.-b). Inicio - Instituto Nacional de Cancerología. https://www.cancer.gov.co/somos-inc/nuestra-institucion/mision-vision-valores-principios-codigo

[10] Teletrabajo - Inicio. (s. f.). Teletrabajo. https://teletrabajo.gov.co/622/w3-channel.html

[11] Todo lo que se debe saber sobre el teletrabajo. (2021). MINTIC Colombia. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo

[12] CIS (Center for Internet Security). (2021, 3 diciembre). Benchmarks. CIS. https://www.cisecurity.org/cis-benchmarks/

[13] Audit and Attest Standards, Including Clarified Standards. (2021). AICPA. https://us.aicpa.org/research/standards/auditattest.html

[14] OWASP Foundation | Open Source Foundation for Application Security. (2021). OWASP. https://owasp.org/

Autores

Mauricio Cortes. Ingeniero Electrónico de la Universidad Los Libertadores, año 2015, Especialista en Telecomunicaciones con seminario de investigación aplicada en Seguridad de la Informática de la Universidad Piloto de Colombia, año 2019, Ha sido analista en seguridad de la información realizando la atención de requerimientos e incidentes para diferentes proyectos, destacándose en el análisis de malware. También se ha desempeñado como especialista de seguridad de la información, siendo administrador de diferentes consolas de Antivirus. Estudiante de la Maestría en Seguridad de la Información, año 2020.

Rafael Zapata, Ingeniero electrónico y telecomunicaciones con amplia experiencia en seguridad de la información y ciberseguridad además de un vasto dominio en plataformas Fortinet, Certificado en Project Management Professional (PMP), certified ethical hacker v10 (CEH), IPV6 Silver Certified, Cisco CCNA R&S, ITIL Fundation V3, Fortinet NSE4 & NSE1, auditor interno ISO/IEC 27001, A10 Networks Application Delivery, McAfee Risk and Compliance Suite y la certificación de especialista en tecnologías open source sobre Microsoft Azure. Estudiante de la Maestría en Seguridad de la Información, año 2020.