Retos de las auditorías remotas basadas en riesgos

Sandra Azucena Blanco Granados

Facultad de Ciencias Económicas, Universidad Militar Nueva Granada

Especialización en Control Interno, II semestre

Iván Cortes Clopatofsky, director

22 de septiembre de 2021

Nota autor

Este trabajo de investigación formativa fue elaborado de la asignatura de Investigación que hace parte del programa.

Tabla de Contenido

Índice de ilustraciones

Resumen

Considerando que la tecnología tiene un papel muy importante en el crecimiento y desarrollo de los países, más aún cuando las economías requieren seguir avante ante pruebas tan trascendentales como la vivida a nivel mundial en el año 2020 con la pandemia COVID-19, se hace clave pensar y actuar en pro de mantener identificados, analizados, monitoreados y controlados los riesgos tecnológicos, para evitar su materialización. Es en este momento en el que esta investigación toma relevancia, ya que involucra el análisis de riesgos tecnológicos en la operación y en la ejecución de las auditorias, así como las estrategias para controlarlos y para mitigarlos.

Palabras clave: Ciberataque, ciberseguridad, auditoria remota, home office, riesgos, controles.

Abstract

Considering the transcendental tests as the one experienced in 2020 with the COVID-19 pandemic, it becomes a key factor to act in favor of keeping technological risks identified, analyzed, monitored, and controlled to avoid their materialization. It is currently that this research becomes relevant, since it involves the analysis of technological risks in the operation, and in the execution of audits. This research serves as well to develop strategies to control and mitigate future problems.

Keywords: Cyber attack, cybersecurity, remote audit, home office, risks, controls.

Teniendo en cuenta la crisis que se está viviendo a nivel mundial a causa de la pandemia Covid 19, la necesidad del trabajo en el modelo de virtualidad ha sido un reto tanto para las empresas como para sus funcionarios. Los países, especialmente los tercermundistas, no estaban preparados para afrontar este reto, la tecnología, la contingencia, las comunicaciones no se encontraban afinadas y el impacto de abrir las puertas al exterior de las empresas, dejo abiertas muchas "puertas traseras", permitiendo que los hackers tuvieran la posibilidad de ingresar y alojar en los sistemas de información de las instalaciones, virus que pueden ocasionar pérdidas importantes para las organizaciones.

Los trabajos no volverán a su curso normal, anteriormente la mayor parte de estos se realizaban en las instalaciones físicas de las empresas. Ahora el trabajo remoto es una necesidad y las empresas que quieran mantenerse en el mercado, deben estar preparadas para asumir esta nueva forma de operar.

Las organizaciones están reaccionando ante esta nueva realidad analizando los pros y los contras del trabajo remoto, así mismo, han venido realizando ajustes en todos los aspectos, para promover el trabajo en casa, ya que con ella se obtienen beneficios representados en la optimización de tiempo, costos y recursos.

Definición del problema

El antes, durante y después de la pandemia han traído consigo, riesgos que no habían sido considerados previamente por las organizaciones y que ahora se presentan debido a la virtualidad. Por otro lado, realizar auditorías remotas involucran en sí, riesgos tecnológicos, propios de las auditorias, que tampoco estaban considerados.

Por estas razones es importante que las empresas consideren los riesgos tecnológicos empresariales tanto para realizar el trabajo de manera remota, como para la ejecución de las auditorías, de otra forma las organizaciones podrían llegar a ser atacadas desde sus sistemas de información, permitiendo a los cibercriminales generar interrupciones en las operaciones, recopilar información y/o debilitar los sistemas tecnológicos afectando la estabilidad de las empresas, robando datos críticos y en ultimas podrían generar hasta la quiebra de las organizaciones.

Pregunta de investigación

¿Qué riesgos tecnológicos deberían contemplar las organizaciones a través del trabajo en la virtualidad?

Objetivos

Objetivo General

Identificar los riesgos tecnológicos que se deberían analizar y gestionar, para poder garantizar la realización segura del trabajo remoto, tanto para las operaciones de las organizaciones como para la ejecución de las auditorías y proponer controles para una adecuada gestión del riesgo.

Objetivos Específicos

Identificar las particularidades del teletrabajo y el home office.

Establecer las características y buenas prácticas en el desarrollo de auditorías remotas

Proponer controles para la mitigación de riesgos tecnológicos a los que se exponen las organizaciones por la ejecución del trabajo en la virtualidad y en las auditorías remotas.

Marco Teórico

Home Office (Trabajo en casa)

El trabajo en casa es una modalidad de trabajo regulada en la Ley 2088 del 12 de mayo de 2021, que " es a través de la cual el Congreso de la República, define el trabajo en casa como la posibilidad de ejercer las actividades laborales fuera de donde normalmente se realizan y cuando fuere necesario, con el uso de tecnologías de la información y las comunicaciones.

Para el cumplimiento de la labor, el trabajador puede hacer uso de los equipos de cómputo de su propiedad o de otra forma, será el empleador quien debe entregar a sus funcionarios los equipos requeridos para poder cumplir con la labor encomendada. Por otro lado. se hace inminente la necesidad que las organizaciones capaciten a sus colabores en temas digitales. (Congreso de la República, 2021).

Estadísticas en pandemia

Antes de la pandemia, en Colombia la cantidad de personas que trabajaban desde lugares remotos a los sitios definidos por el empleador, eran aproximadamente 200.000, Fasecolda estima que, durante la pandemia, aproximadamente de 2 a 3 millones de personas, trabajaron desde sitios remotos. Por otro lado según estudios realizados por la “Federación Colombiana de Gestión Humana” el 76.2% de las empresas desean continuar con esta modalidad de trabajo durante uno o dos días de la semana y en gran medida las empresas no han implementado políticas para la realización del trabajo remoto, ya que sin la aplicación de las mismas, las empresas se exponen a riesgos que podrían resultar muy costosos en cuanto al manejo de privacidad de la información. (Manchego, 2020).

Una de las desventajas tecnológicas más relevantes del teletrabajo es la relacionada con la “Seguridad de la información de la organización”, los ciberataques, están creciendo

exponencialmente, los hackers pretenden acceder a los recursos informáticos de las organizaciones con fines fraudulentos y los accesos remotos a los aplicativos y/o información de las organizaciones, se ven cada vez más expuestos. (Velásquez & Vera, 2010).

Es a través del ciberespacio donde millones de cibernautas navegan, entre estos cibernautas se pueden encontrar ciberdelincuentes.

Los ciberataques continúan

Entre los ciberataques que impactaron a grandes compañías en los 10 últimos años, encontramos:

- En noviembre de 2010, Wikileaks filtró la información que se intercambiaba entre las diferentes embajadas de los Estados Unidos. La noticia indicaba "In 2010, Julian Assange became a household name after his website Wikileaks began publishing top secret information about government departments around the world. Assange, a highly intelligent man, was able to hack numerous governmental databases, and he used his site to release the information periodically. Controversial information" (Malfere, 2012).
- Durante una semana el servicio de Sony Playstation Network quedaron sin funcionamiento, la información de 77 millones de personas quedó comprometida.
- "Ha aparecido en Internet una serie de documentos con 68 millones de cuentas y contraseñas de Dropbox, que se han demostrado reales. Fueron hackeadas en 2012" (Pascual Estapé, 2016).
- En diciembre de 2013, la compañía Target fue atacada a través de un programa maligno, generando impacto en 70 millones de clientes a quienes se les robaron la información personal y la información bancaria, esta información fue reportada así "In November and December of 2013, cybercriminals breached the data security of

Target, one of the largest U.S. retail chains, stealing the personal and financial information of millions of customer" (Weiss & Miller, 2015).

- Ebay fue atacada en mayo de 2014, a través de las contraseñas de los empleados, permitiendo la vulneración de los datos personales de sus clientes, afectando a 145 millones de usuarios.
- En el año 2015 las elecciones de EEUU fueron atacadas por ciberdelincuentes y la información de 191 millones de votantes quedó accesible en internet.
- En noviembre de 2016, más de 142 millones de cuentas, fueron puestas en venta en el mercado negro de internet. Esta información correspondía a datos de correos y contraseñas de los clientes de la empresa de pornografía Adult FriendFinder.
- Uber en octubre de 2016 fue atacada y los datos de 57 millones de sus clientes quedaron expuestos, Uber canceló varios miles de dólares para que la información no fuese publicada
- En marzo de 2018, la empresa Cambridge Analytica, utilizó datos robados para influir en las elecciones presidenciales en los Estados Unidos
- En marzo de 2019, Facebook almacenó 419 millones de teléfonos en un servidor que no estaba protegido.
- A raíz de la pandemia, la empresa CyberEdgeGroup, identificó que el 81% de las organizaciones en el año 2020, fueron atacadas por ciberdelincuentes.
- Al corte de noviembre de 2020 se identificaron 113 millones de amenazas informáticas y 350,000 diariamente por otro lado la Universidad de Maryland afirma que los hackers están realizando ataques a los sistemas informáticos a razón de uno cada 39 segundos."

- La modalidad de los ataques ha venido evolucionando, el Ransomware (secuestro de nformación), DDoS (ataques de denegación de servicio), Pshising (uso de información confidencial para fines delictivos), son los ciberataques que están utilizando los ciberdelincuentes para estafar, robar, vender información y hacer declinar los sistemas de información de las organizaciones objetivo (https://www.nsit.com.co/ciberataques-mas-famosos-del-2020/, s.f.).

Algunas Compañías Comprometidas en los últimos 8 años

Compañía	Fecha	Consecuencia
Heartland Payment Systems	2008	134 millones de tarjetas de créditos expuestas
MySpace	2013	360 millones de cuentas de usuarios comprometidas
Adobe	2013	153 millones de cuentas comprometidas
Yahoo	2013 2014	3 billones de cuentas de usuarios comprometidas
eBay	2014	Información de 145 millones de usuarios expuestos
NetEase	2015	235 millones de cuentas de usuarios comprometidas
Adult FriendFinder	2016	412.2 millones de cuentas de usuarios comprometidas
LinkedIn	2012 2016	165 millones de cuentas de usuarios comprometidas
Equifax	2017	147.9 millones de cuentas consumidores comprometidas
Marriot International	2014 2018	500 millones de cuentas de clientes comprometidas
Dubsmash	2018	162 millones de cuentas de usuarios comprometidas
My Fitness Pal	2018	150 millones de cuentas de usuarios comprometidas
Zynga	2019	218 millones de cuentas comprometidas
Canva	2019	137 millones de cuentas comprometidas
Sina Weibo	2020	538 millones de cuentas comprometidas

Ilustración 1. Algunas compañías comprometidas en los últimos 8 años.

Nota. Tomado Importancia de la Inteligencia Artificial en la Seguridad Cibernética. (Martinez, 2020).

La materialización de estos riesgos se evidencia en la lentitud de los equipos, disminución en la capacidad de almacenamiento y/o presencia de mensajes emergentes. Estos virus pretenden identificar las vulnerabilidades y robar o bloquear información vital de las organizaciones generando daños que en muchas oportunidades son irreparables, pudiendo llegar hasta hacer desaparecer a las compañías del mercado y se presentan a través de diferentes modalidades como:

1. Malware, que es un software maligno que se infiltra en los sistemas informáticos, con el fin de robar la información infiltrándose en los equipos de las organizaciones. El porcentaje de dispersión del programa maligno entre los años 2019 y 2020 fue del 63% a través de correos, el 32% a través de redireccionamiento a sitios web y el 5% por descarga de aplicaciones maliciosas.

   Existen diferentes tipos del programa maligno, así:

   - "Ransomware es un virus que afecta distintos Sistemas Operativos principalmente a Android y a Windows, este se encarga de encriptar información para luego extorsionar a la víctima" (Pedraza Moreno & Rojas Henao, 2018). Es el secuestro de la información, a través de este programa maligno, los ciber atacantes bloquean o cifran la información de tal forma que es imposible acceder a ella y solo hasta que se pague un rescate, se desbloqueará la misma. "En el país los ataques por Malware en lo corrido del año crecieron en un 612%, el monto pagado por rescate de información está entre los 32 millones y los 160 millones de pesos" (Cámara Colombiana de Informática y Telecomunicaciones, 2019).
   - troyanos: "Virus Caballo de Troya (Trojan Horse) Son los más peligrosos desde el punto de vista de la seguridad, porque una vez instalado el virus en la computadora,

los teleoperadores del sistema denominados Crakers, son capaces de manejarla a distancia" (Ficarra, 2002).

- spyware: "Es considerado spyware aquella aplicación que envía información sobre los hábitos de navegación y uso de software de un usuario al sitio web de su creador" (Burgos, 2009), este virus es el que captura información que viaja por la red, con la que posteriormente se materializan robos como el retiro de dinero con datos de tarjetas crédito
- adware: Son programas cuyo objetivo consiste en mostrar de manera continua, ventanas de publicidad (Ruiz Larrocha, 2019).
- botnets: "Los botnets son un conjunto de computadores que sirven para atacar una red y usar sus recursos a distancia" (Ávila, 2019)

2. Inyección SQL: A través de líneas de código, toma el control de la información y roba los datos de las bases de datos organizacionales
3. Phising: "Se llama phishing al uso de emails fraudulento diseñados para el robo de identidad e información privada valiosa" (Gobierno USA, 2012)
4. Suplantación de correos de empresas, con direcciones URL muy parecidas a las legítimas de las empresas, con el fin de robar información comercial
5. Man in the middle: Robo de información a través de ataques a las redes de comunicaciones

La forma de propagación de estos virus es a través de la navegación por sitios desconocidos o inseguros, a través del correo electrónico, con la utilización de USB's que contengan archivos infectados. Los virus pueden tener características tales como:

- polimorfismo: Son programas de computador que van mutando, estos son más difíciles detectar y así mismo difíciles de erradicar
- residentes en memoria o no residentes en memoria: Los no residentes en memoria solo se ejecutan cuando existe un archivo contaminado
- virus sigilosos: son los que se adhieren a los archivos existentes
- virus que se unen con otros virus y hacen más potente el daño sobre los ordenadores
- resistentes al formateo y llegan hasta dañar físicamente los equipos
- retrovirus, que anulan el efecto de los antivirus

De acuerdo con lo informado por la revista Portafolio el 5de septiembre de 2021, “Los ataques cibernéticos en Latinoamérica han aumentado un 24 % en lo que va de año en comparación con los primeros 8 meses de 2020, según un informe presentado este martes, en el que se advierte de la creciente amenaza de programas maliciosos para espiar a la pareja y de "apps" de intrusión de acceso remoto.” (Portafolio, 2021). Lo que prende las alertas, más aún cuando la virtualidad llegó para quedarse y gran cantidad de empresas están manejando una parte importante de sus funcionarios en modalidad de trabajo en casa o en teletrabajo.

Identificar las particularidades del teletrabajo y el home office

La implementación de diferentes modalidades de trabajo, la profesionalización de las actividades y el boom tecnológico, ocasionaron un devenir de modificaciones, ajustes y desarrollo legal y reglamentario. Es así, como respuesta a este continuo cambio, surgen nuevas alternativas de trabajo en países industrializados, las cuales están basadas en la confianza hacia el trabajador y el rendimiento mediante la medición del cumplimiento de objetivos, la Organización Internacional del Trabajo definió el teletrabajo como “el teletrabajo conlleva un trabajo realizado con la ayuda

de las TIC, fuera de las instalaciones del empleador" (Organización Internacional del Trabajo, 2020).

En Colombia, el desarrollo ha sido un poco más demorado a pesar que en el artículo 23 del Código Sustantivo establece los elementos del contrato de trabajo es hasta el 2008 donde surge la Ley 1221 que "tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC)" (Congreso de Colombia, 2008), posteriormente el Decreto 884 de 2012, mediante el cual decreta "Aspectos laborales del teletrabajo" (Colombia, 2012). y más adelante, posterior a la emergencia sanitaria derivada del Covid-19 surge la ley 2121 del 5 de agosto 2021 mediante la cual se regula "por medio de la cual se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones" (El Congreso de Colombia, 2021).

La crisis económica subyacente a la pandemia, ocasionó el cierre de muchas empresas y la disminución de puestos de trabajo, por lo que las empresas tomaron como alternativa para el manejo de los trabajos administrativos o susceptibles de trabajo remoto, el trabajo desde casa, sin embargo y para la fecha de la ocurrencia de la emergencia sanitaria, no se tenía ninguna disposición en el ordenamiento jurídico colombiano que cubriera esta situación sui generis aparte del teletrabajo, por lo que los empleadores públicos y privados optaron por continuar sus operaciones con la singularidad "desde casa o en home office".

Viéndolo desde una perspectiva objetiva, se realizó un análisis de riesgos y una decisión en pro de un bienestar general, se continuaron las operaciones bajo un modelo, para la fecha inexistente en nuestro país el "home office".

A los ojos de la ciudadanía, no fueron evidentes las diferencias abismales entre el "home office" y el modelo de teletrabajo, muy pocas empresas desde el 2008 se animaron a cumplir los requisitos para la implementación de este modelo, que más allá de ser difícil su ejecución, no contaba con una cultura en pro del trabajo desde casa, sin embargo, estas empresas frente a la emergencia sanitaria fueron las que de alguna manera aseguraron su supervivencia, al tener planes de contingencia y plataformas dedicadas para el manejo de estas eventualidades en un primer escenario. En un segundo escenario, se encontraban las empresas que luchaban por asegurar su existencia y que a la luz de un cierre inminente optaron por enviar a sus trabajadores a "home office" e improvisar una serie de herramientas para migrar hacia esta forma de trabajo.

Teletrabajo

En el primer caso, el "teletrabajo" surge como una de las tendencias de la flexibilización laboral y establece unas características específicas como la realización de una actividad laboral fuera de las instalaciones de la organización, en modalidades como el "teletrabajo autónomo" que permite la realización de las labores desde el lugar que prefiera el trabajador, el "teletrabajo suplementario" que permite una alternancia entre las labores dentro de la compañía y el domicilio del trabajador y el "teletrabajo móvil" el cual no tiene un lugar definido para la realización de las tareas y así mismo le permite ausentarse de la oficina frecuentemente.

Esta modalidad está expresamente desarrollada por la legislación nacional y se establecen una serie de obligaciones por parte del empleador y del trabajador, por parte del empleador como la afiliación a la ARL, el suministro de los equipos informáticos, cubrir el costo de la energía o conexiones necesarias por parte del trabajador, la verificación de las condiciones de trabajo de acuerdo al SGSST. Así mismo, por parte del trabajador adicional obligaciones establecidas en el contrato de trabajo y la ley, establece que en cualquier momento se puede cambiar la modalidad

de trabajo “La continuada subordinación o dependencia del trabajador respecto del empleador, que faculta a éste para exigirle el cumplimiento de órdenes, en cualquier momento, en cuanto al modo, tiempo o cantidad de trabajo” (Congreso de la República, 1990).

Beneficios Económicos

La realización de actividades mediante este tipo de modalidades permite, la reducción de costos del trabajador en gastos de transporte, vestuario y alimentación, el surgimiento de iniciativas de organización laboral en pro de un aumento de la productividad y eficiencia optimizando el tiempo, así mismo se requiere una responsabilidad muy alta por parte del trabajador para el desarrollo de los objetivos o metas planteadas.

Por parte del empleador también hay un beneficio económico, ya que hay una disminución en los espacios de trabajo a ocupar dentro de la compañía, así como en insumos, papelería y gastos propios de la operación (arriendos, servicios públicos, gastos en personal de aseo)

Beneficios Sociales

Este tipo de metodologías, permite beneficios sociales a los trabajadores como la erradicación del tiempo de los trayectos hacia el lugar de trabajo teniendo como consecuencia una disminución del estrés que causa estos desplazamientos, así mismo permite compartir espacios familiares con la permanencia en casa, y este tipo de modalidades permite la integración social a las personas que usualmente tendrían dificultades en la obtención de un empleo por temas discriminatorios o con pérdida de capacidad laboral.

Beneficios al Medio ambiente

Existe un beneficio general por la disminución de trabajadores que se trasladan a sus lugares de trabajo diariamente en cuanto a la huella de carbono, y así mismo se establecen políticas como la disminución del uso del papel, las cuales vienen apalancadas desde las entidades públicas.

“Home Office”

En el segundo caso, el home office es un nuevo desarrollo legal y reglamentario, a través de la circular 0041 del 2 de junio de 2020, “por medio del cual el Ministerio del Trabajo imparte lineamientos respecto al trabajo en casa” (Ministerio del Trabajo, 2020). Diseñada como una forma de proteger el empleo durante la emergencia sanitaria, los lineamientos básicos que se establecieron para este tipo de empleados señalaban entre otros, que no se podía disminuir el salario, se debía respetar el horario laboral, se debía notificar a la ARL la condición de trabajo temporal entre otras. Es así como en ese tipo de trabajo, las actividades del trabajador se establecían muchas veces en sus computadores personales, y sin cumplirse los protocolos de seguridad establecidos por las organizaciones.

Es solo hasta el 2021, donde mediante la ley 2121 promulgada por el gobierno "por medio de la cual, se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones” (Congreso de la República, 2021), se establecen nuevos lineamientos para este tipo de trabajo, teniendo un tratamiento diferencial y especial para esta modalidad, siendo totalmente diferente al teletrabajo y destinado únicamente a situaciones fortuitas o de fuerza mayor, por lo que por iniciativas del gobierno nacional se pretende que muchas de las empresas que optaron por el “home office” durante la emergencia sanitaria migren al modelo de “teletrabajo”.

La conclusión después de verificar las diferencias de ambas modalidades de trabajo flexible, desde la perspectiva de un auditor, se puede establecer fácilmente como las organizaciones que estuvieron expuestas a más altos riesgos corresponden al modelo de “home office”, siendo un modelo útil pero inseguro, estableciendo que en el caso de deficientes o inexistentes controles y protocolos de seguridad por parte de las organizaciones, es una puerta

abierta frente a ataques cibernéticos que pueden ocasionar problemas serios con un impacto económico y reputacional.

Establecer las características y buenas prácticas en el desarrollo de auditorías remotas

La evolución de la tecnología, generó la implementación de nuevas herramientas que permiten la ejecución virtual de funciones que generalmente se realizarían físicamente, es así como en la última década tenemos grandes avances tecnológicos que nos han puesto a prueba en diferentes flancos, pero es hasta la pandemia del Coronavirus COVID-19, donde se evidencia la necesidad de acelerar la articulación de conocimientos previos con la nueva tecnología, teniendo como principal protagonista profesiones como la ingeniera, la cibernética y la tecnología que permiten el acercamiento virtual entre trabajadores, clientes y entidades.

Es así como desde la perspectiva de la auditoria tenemos a la mano diferentes herramientas tecnológicas, que, aunadas con el conocimiento, la experiencia y los valores propios del auditor permiten seguir desarrollando con una "nueva normalidad" las funciones que realizamos, afrontando nuevos retos.

Uno de los pilares de la auditoria es el análisis de la información, por lo que la calidad, fiabilidad, veracidad y disponibilidad de la misma son de vital importancia, independientemente de la forma en la que se tengan las evidencias de los procesos auditados.

Aspectos para tener en cuenta

Cobra relevancia las actividades en la ejecución de las auditorias remotas ya que, aunque son similares a las presenciales, se deben tener en cuenta las recomendaciones contempladas en la Norma Técnica Colombiana 19011:2018, en donde se:

> …proporciona orientación sobre los sistemas de gestión de auditoría, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y realizar las auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas que intervienen en el proceso de auditoría. Estas actividades incluyen el individuo (s) la gestión del programa de auditoría, los auditores y los equipos de auditoría. Es aplicable a todas las organizaciones que necesitan para planificar y realizar auditorías internas o externas de los sistemas de gestión o gestionar un programa de auditoría. La aplicación de este documento a otros tipos de auditorías es posible, siempre que se preste especial atención a la competencia específica necesaria. (ISO, 2018).

Durante la ejecución de la auditoria remota, se pueden establecer las siguientes buenas prácticas.

Estudio de viabilidad

La auditoría se debe desarrollar basada en un estudio de viabilidad donde a través de sus resultados se pueda garantizar el acceso a las evidencias a través de las herramientas con la que se cuenta para la ejecución de la auditoria. Es importante establecer que el requisito sine qua non para el desarrollo de este tipo de auditoria es el acceso a internet por parte del auditor y auditado, y derivado de este surgen riesgos en la virtualidad para el acceso a la información de la organización.

Protocolo y planificación

El desarrollo de la auditoria remota, tiene matices diferentes a los de la auditoria presencial, pero mantiene su estructura, planificación y ejecución, simplemente estos protocolos se ajustan a la virtualidad. En el caso de las auditorias remotas, es necesario evaluar los riesgos y se requiere determinar la viabilidad de esta, delimitar su alcance y posteriormente realizar una selección de herramientas tecnológicas para su desarrollo.

Elección de herramienta tecnológicas

Durante el desarrollo de las actividades propias de la organización dependiendo la modalidad de trabajo virtual elegido, bien sea bajo el modelo de teletrabajo o bajo el modelo de homeoffice, surge la necesidad del conocimiento técnico para establecer riesgos potenciales y sobe todo para garantizar la ejecución de las auditorias bajo una comunicación fluida con el acceso a la información requerida la cual es necesaria para su desarrollo.

Definición de tareas y agenda para su desarrollo

- se deben definir las tareas y actividades que se pueden incrementar con relación a las de una auditoria in situ, lo cual permite una ejecución separada o en conjunto que requiere un mayor nivel de detalle de los procesos auditados derivado de un nivel de conocimiento más profundo de dichos procesos de la organización.
- así mismo se debe solicitar a la organización el agendamiento que garantice la disponibilidad de los auditados en las fechas definidas en la etapa de planeación.
- es necesaria la verificación del acceso a los sistemas, hardware, software, conectividad, acceso a internet y capacitación para el manejo de las herramientas tecnológicas a utilizar, por parte de la organización.
- se deben establecer las fechas y entregables que harán parte de las evidencias de la auditoria.

Durante el desarrollo de una auditoria

Revisión documental

Se requiere una preparación previa por parte de la organización, en donde se permita acceder de manera segura a las evidencias solicitadas por el auditor, garantizando el acceso y visibilidad de la información, utilizando herramientas como el almacenamiento en la Nube,

servidor de almacenamiento, SharePoint u otros. Esta información debe ser revisada por el auditor, es así como su acceso debe garantizarse durante el desarrollo de la auditoria.

Estrategias para el desarrollo de entrevistas

Es necesario implementar una prueba técnica de la plataforma de videoconferencias manteniendo una planeación ambiental que garantice que el auditado esté libre de distracciones, estableciendo un protocolo para el desarrollo de la entrevista que contenga limitaciones en el acceso a notificaciones laborales o personales y el acceso o interacción no requerido con terceros. Se requiere establecer como prelación de comunicación la vía videollamada sobre la conexión por voz, realizando una preparación previa de preguntas hito para el desarrollo de la auditoria e implementación de grabación de la entrevista como evidencia de lo manifestado por el auditor.

Así mismo en el desarrollo de la entrevista se deben garantizar estrategias para la manifestación de la escucha activa implementando la retroalimentación a través del contacto visual o pausas intencionales, físicamente se recomienda el vestuario de acuerdo al roll de auditor con colores o accesorios que no distraigan la finalidad de la reunión, realizando un encuadre a la cámara que establezca el enfoque sobre el rostro y finalmente se debe cuidar el lenguaje corporal y el tono de voz en el desarrollo de la auditoria.

Cierre de la Auditoria

En el informe de la auditoria, se debe establecer que procesos no fueron susceptibles de auditar y que requieren una intervención presencial, así mismo se debe determinar la idoneidad y calidad de la herramienta tecnológica utilizada en el proceso.

Esta reunión de cierre es la misma que en las auditorias presenciales, la cual deberá realizarse pocos días después de finalizadas las entrevistas. Previa esta reunión es viable una

reunión de análisis de resultados del equipo de auditores estableciendo las conclusiones, entregables y cierre.

Ventajas de las auditorías remotas

Al realizar la auditoria sincrónica a través de medios tecnológicos, se establecen como beneficios: la reducción de costos derivados de la eliminación de gastos de desplazamiento, digitalización de la información física que permite su fácil acceso, fortalecimiento de plataformas informáticas, recopilación sincrónica de videos y fotografías, implementación de sistemas de seguridad de la información, realización de auditorías remotas simultaneas en diferentes sucursales de la organización, ampliación del tiempo efectivo de la auditoria y dedicación exclusiva.

Limitaciones de las auditorías remotas

Algunas de las limitaciones que se presentan derivadas de las auditorias remotas son: intermitencia en las comunicaciones, software obsoleto o con limitación, hardware por debajo de los requerimientos planeados en la auditoria, falta de experticia en el uso de herramientas tecnológicas, costos de implementación de plataformas de comunicación, implementación de programas de gestión documental, aumento de posibilidades de fraude al intentar modificar las evidencias digitales presentes o pasadas, aumento del tiempo designado al desarrollo de la auditoria al no tener disponibilidad de las evidencias a auditar, limitaciones en la percepción de comunicación no verbal y riesgo de pérdida de información confidencial.

Finalmente, previo a determinar las ventajas y desventajas al realizar este tipo de auditorías es importante señalar que algunos principios básicos se ven impactados por la realización mediante esta metodología, como son : la afectación en la imparcialidad en la generación de hallazgos por los obstáculos en la realización en tiempo real; la fiabilidad y reproducción de los hallazgos de la auditoria dependen de los medios tecnológicos y herramientas para capturar las evidencias durante

el desarrollo de la misma; respecto a los riesgos asociados a la planificación, estos pueden variar con relación a los verificados en el análisis de viabilidad; los canales de comunicación puedes ser ineficaces; falta de acceso o control de la información documental; se puede afectar la disponibilidad y cooperación del auditado al utilizar esta metodología remota.

Propuesta de controles para la mitigación de riesgos tecnológicos

El trabajo desde instalaciones físicas diferentes a las corporativas genera una falsa sensación de tranquilidad, lo que redunda en minimización de los controles que pueden ser trascendentales en épocas en las que los ciberataques están al acecho de cualquier oportunidad de acceso a los sistemas de información, con fines delictivos. Por este motivo es clave estar alerta en poder identificar y controlar estas potenciales amenazas, así como contar con el monitoreo permanente de los nuevos eventos de riesgo que día a día se vienen incrementando exponencialmente.

Los controles deben estar enfocados en dos vías, tanto a nivel corporativo, como a nivel de usuarios final, solo si existe la verdadera conciencia en estos dos aspectos, se creará un fuerte vínculo que ayudará a proteger a las empresas y a minimizar las vulnerabilidades ante ciberataques.

Control de contraseñas y configuración multifactor

Uno de los eventos más predominantes durante la pandemia fue el “ataque de fuerza bruta”, este es uno de los métodos utilizados por los hackers para acceder a las cuentas de usuario o sistemas de información. Según la definición de la compañía internacional de seguridad informática Karspersky, los ataques de fuerza bruta, son intentos de descifrar contraseñas a través de la búsqueda en páginas web o identificación de llaves de cifrado de los mensajes, hasta lograr encontrar la contraseña correcta, una vez que los ciberdelincuentes logran identificar la contraseña,

acceden a los equipos de la red y se mueven transversalmente dentro de los sistemas de información hasta lograr encontrar información sensible que utilizan posteriormente para sus fines delictivos. Así lo refiere la Revista Nexos Científicos, "Un ataque de fuerza bruta es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso" (Larenas & Rosero, 2020).

Entre las formas de minimizar el riesgo ante los ataques de fuerza bruta, están el uso de contraseñas robustas, manejadas tanto a nivel de aplicación como a nivel de usuario.

Las aplicaciones tienen la posibilidad de controlar las características de las contraseñas de usuario, exigiendo parámetros mínimos en la construcción de la mismas, tales como longitud, caracteres que debe incluir, uso de letras mayúsculas o minúsculas, control de números o letras consecutivas, comparaciones en contraseñas utilizadas con anterioridad, tiempo de expiración de contraseña, cambio de contraseña en la primera conexión, estos controles son automáticos y ayudan a prevenir en parte el acceso no autorizado a los sistemas de información. Como complemento a estos controles, los sistemas de información tienen la posibilidad de realizar el control de acceso a través de diferentes factores de autenticación como son "algo que sabe" éste es un factor que solo lo debe conocer el usuario como por ejemplo la contraseña, "algo que se tiene" por ejemplo un token, un teléfono o una tarjeta, "algo que se es" hace referencia a controles biométricos.

Sin embargo el otro 50% lo constituye el usuario final y es allí en donde se deben implementar los controles complementarios, que prevengan accesos no deseados a los sistemas de información, para esto es clave mantener capacitados a los usuarios en temas relacionados con los ataques cibernéticos, con el fin de concientizarlos acerca de la necesidad del autocuidado y proponer en controles tales como evitar utilizar contraseñas que relacionen personalmente al

individuo, ya que la ingeniería social permite que se conozca la información de las personas y se pueda concluir con facilidad, la contraseña diseñada por el usuario, el uso de palabras duplicadas, secuencias del teclado, uso de fechas, así mismo las preguntas para restauración de contraseñas, son claves para facilitar o entorpecer la identificación de las contraseñas.

Canales de comunicación seguros

El teletrabajo y/o trabajo remoto, exige la realización de conexiones entre los computadores de los funcionarios con las redes de las organizaciones. Estas conexiones se deben realizar con la seguridad que en el transporte la información no va a ser vulnerada ni conocida por entes diferentes al emisor y receptor de la misma. Ante la emergencia de la pandemia, muchas empresas decidieron hacer uso de herramientas de acceso remoto, tales como TeamViewer, exponiendo sus compañías a graves vulnerabilidades como la CVE-2020-13699, "TeamViewer presenta una vulnerabilidad de seguridad peligrosa rastreada en el aviso CVE-2020-13699. Permite a los usuarios malintencionados explotar las instancias en ejecución instaladas.. Por el momento, la versión de Windows de la aplicación está afectada" (Beltov, 2020). Hecho que pudo haber sido aprovechado por los hackers para realizar diferentes tipos de ataques.

La forma de controlar la seguridad de la información que fluye a través de internet es la utilización de VPN´s que sirven para conectar computadores, sin embargo para garantizar la disponibilidad e integridad de la información que fluye a través de las VPN´s se cuenta con protocolos de cifrado que encriptan la información de punta a punta e identifican si hubo modificación en los paquetes de datos en el transporte de los mismos.

Los controles a nivel de usuario final, como complemento al uso de las VPN´s, van dirigidos a evitar utilizar redes abiertas, para la ejecución del trabajo remoto y al cambio frecuente de las claves de Wifi.

Actualización de parches de seguridad

Dentro del software que manejan en los computadores, se encuentra el sistema operativo, que es una serie de programas a través de los cuales se puede realizar el manejo de la memoria, disco duro, medios de almacenamiento y manejo de los periféricos de los equipos de cómputo, permitiendo que funcionen los programas que se instalan en los computadores. A través de las actualizaciones del sistema operativo, se incluyen nuevas funcionalidades, se actualizan los controladores, se eliminan errores y se solucionan las vulnerabilidades identificadas. Así mismo sucede con el software instalado en equipos de los clientes, la falta de aplicación de actualizaciones puede provocar que los hackers aprovechen estas vulnerabilidades para instalar virus informáticos que encriptan o dañan los archivos e instalan programas espía, por otra parte los cibercriminales podrían acceder al historial de navegación web y con esto se les facilitaría llegar a apoderarse de información de la organización.

> El sistema operativo (a veces también citado mediante su forma abreviada OS en inglés) se encarga de crear el vínculo entre los recursos materiales, el usuario y las aplicaciones (procesador de texto, vídeojuegos, etcétera). Cuando un programa desea acceder a un recurso material, no necesita enviar información específica a los dispositivos periféricos; simplemente envía la información al sistema operativo, el cual la transmite a los periféricos correspondientes a través de su driver (controlador). Si no existe ningún driver, cada programa debe reconocer y tener presente la comunicación con cada tipo de periférico (López Jurado., 2021).

Es por esta razón que las organizaciones deben estar pendientes de las actualizaciones de software generadas por los fabricantes, en la que están informando el avance de las nuevas versiones, así como la adquisición y aplicación de los últimos parches de seguridad generados por

el fabricante de software, no sin antes evaluar el impacto de su instalación. Estas actualizaciones hacen parte de las medidas preventivas para garantizar la seguridad en internet.

Uno de los controles a nivel de usuario es evitar seleccionar la opción de guardar contraseña de los aplicativos, pues es a través de esta opción que los sistemas almacenan localmente las contraseñas. Esta situación se presta para facilitar el acceso a las contraseñas almacenadas y al historial de inicio de sesión, cuando no se ha actualizado la versión del sistema operativo.

Por otra parte, los funcionarios también deben mantener actualizado el sistema operativo y software de los computadores utilizados en trabajo remoto, evitando realizar instalaciones de fuentes desconocidas para evitar se infectados con software malicioso

Implementación de almacenamiento en la nube

El almacenamiento de la información localmente conlleva riesgos que normalmente no son calculados, más aún cuando el trabajo es realizado remotamente. Entre los riesgos identificados con este tipo de almacenamiento están la dificultad en acceder a la información, el costo de almacenamiento, la pérdida de la información en caso de fallas en los equipos de cómputo. Para evitar la materialización de esos riesgos, es conveniente mantener la información controlada, disponible, segura, con copias de respaldo y que puede generar ventajas en cuanto a la disponibilidad del espacio de almacenamiento, bajo costo, control de acceso a la información de acuerdo a la segregación de funciones, este modelo es el que corresponde al almacenamiento en la nube, este tipo de almacenamiento adicionalmente tiene la ventaja que son los proveedores de la nube los que se encargan de garantizar la seguridad, integridad y disponibilidad de los archivos.

Los usuarios remotos deben tener la claridad y el compromiso de evitar la transferencia de archivos a través de wetransfer, dropbox, whatsapp y otros medios de transferencia que no garantizan el cumplimiento de las políticas de seguridad de la organización.

Establecer medidas de protección de equipos extraviados

Es importante identificar los controles necesarios para evitar las pérdidas de información de la organización, cuando alguno de sus equipos de cómputo se pierde, estas medidas deberían incluir el control de localización, seguimiento de utilización del software de la organización desde el equipo extraviado, bloqueo de la pantalla con pin y/o autenticación biométrica, bloqueo de los datos remotamente.

Programar y capacitar a los funcionarios de la organización

Estas capacitaciones van dirigidas al correcto uso de los medios tecnológicos para el trabajo remoto, explicando sus beneficios, cuidados, controles, políticas de seguridad, consecuencias de su incumplimiento, realizando el acompañamiento y asesoría necesario para lograr una adecuada asimilación del conocimiento.

Generación de backups

Los backups, son las copias de respaldo de la información, que garantizan reducir el tiempo de reacción ante problemas, existen varios tipos de backups, los completos contienen la totalidad de la base de datos respaldada; los progresivos o incrementales, almacenan los cambios que han sucedido a partir del último respaldo realizado; y los diferenciales contienen la información que ha cambiado a partir del backups completo. La generación de backups es parte de la estrategia de seguridad organizacional realizarse periódicamente, entre los controles que se deben implementar para garantizar contar con los backups están:

- garantizar la generación del backup y la funcionalidad de la restauración de la información, con la garantía que se han superado las pruebas que evidencien el correcto funcionamiento

- Ubicar la copia de seguridad en un equipo diferente al que contiene los archivos originales
- Tomar los backups, de acuerdo con las periodicidades establecidas

Es importante que el usuario final apoye las pruebas de las restauraciones, garantizando que la información es consistente y completa.

Conclusiones

Las empresas que deseen mantenerse vigentes en el mercado, ante situaciones inesperadas tales como la pandemia, deben permanentemente explorar nuevas opciones tecnológicas y ser innovadoras en los modelos de operación, sin dejar de lado el análisis de los controles necesarios para garantizar que la organización trabaje de manera segura y cuente con la capacidad de reacción que le brinde ventajas competitivas, convirtiendo los retos en oportunidades de crecimiento.

Garantizar la continuidad de los procesos de auditoría, cuando la forma de atender la operación de las compañías ha cambiado a causa del trabajo remoto, resulta ser uno de los eslabones más importantes para tener en cuenta, ya que es allí donde se pueden generar eventos de riesgo no contemplados, que podrían ser determinantes para que las empresas perduren en el tiempo.

Una de las ventajas de realizar auditorías remotas, es poder aprovechar las bondades de la tecnología, tales como el uso de drones, teléfonos y videoconferencias, que proporcionan la posibilidad de recolectar evidencias en tiempo real, así como la optimización de tiempos muertos, lo que redunda en un mayor cubrimiento de auditorías de los procesos y por consiguiente un trabajo de apoyo a la organización en pro del mejoramiento continuo.

Es trascendental que antes de habilitar el modelo de teletrabajo y/o trabajo remoto, las organizaciones realicen una evaluación exhaustiva del estado de la seguridad de los componentes tecnológicos, de tal forma que se determine si hay necesidad de realizar inversiones en seguridad tecnológica que las protegerán de eventuales ataques cibernéticos.

Para identificar si las auditorias se pueden realizar en sitio o remotamente, es importante considerar aspectos tales como el estudio de viabilidad, la planificación, las herramientas

tecnológicas con las que se cuenta y el modelo para la revisión documental. La evaluación de estas variables, permiten determinar si las auditorias se pueden realizar remotamente.

Recomendaciones

Se recomienda a las organizaciones:

Utilizar el teletrabajo como pilar para el desarrollo de la virtualidad, ya que a diferencia del home office, este permite mantener el control de los dispositivos, así como el acceso a la información con las seguridades definidas e implementadas por las organizaciones, minimizado la posibilidad de riesgos generados por ciberataques, debido a las debilidades en la seguridad del uso de equipos externos a las organizaciones.

En el caso de estricta necesidad del manejo del modelo de trabajo "Home Office", blindar los equipos, escritorios remotos y/o redes virtuales de tal forma que manejen la seguridad de las comunicaciones incluyendo privacidad, autenticación e integridad, para evitar que sean foco de ciberdelincuencia, poniendo en peligro la información y/o los sistemas tecnológicos de la organización.

Capacitar a los funcionarios, para la ejecución de su trabajo y/o atención de las auditorias remotas, de tal forma que los actividades no se vean interrumpidas por efecto de desconocimiento de las herramientas de trabajo remoto, que apalancan la continuidad de las operación de las empresas, aun en situaciones de contingencia, en las cuales no es posible el trabajo presencial.

Es importante que las organizaciones se mantengan a la vanguardia de los avances tecnológicos en temas relacionados con la ciberseguridad y capaciten a todas sus partes interesadas, de tal forma que se realice un frente común en prevención de riesgos de acceso indebido a los sistemas tecnológicos, con el fin de poder mantener seguras las instalaciones y la información, aun cuando se esté operando remotamente.

Se recomienda que, dentro del plan de continuidad de negocio, se consideren los procesos, procedimientos, conectividades, capacitaciones e instalaciones, relacionadas con los

accesos implementados para la ejecución del trabajo remoto, así como estar preparados para prevenir la materialización de ataques cibernéticos, blindando los sistemas y activos de información del negocio a través del uso de la tecnología y el fomento de la cultura de control.

Bibliografía

Ávila, R. (2019). *Del bit a las redes sociales: Seleccionario de voces de las TIC.* Ciudad de México: Pixelee.

Beltov, M. (2020). CVE-2020-13699: La falla crítica de TeamViewer permite a los hackers explotar los dispositivos de los usuarios. *Sensors Tech Forum*.

Burgos, A. (2009). *Seguridad PC.*

Cámara Colombiana de Informática y Telecomunicaciones. (2019). *Tendencias del cibercrimen en Colombia 2019-220.*

Código sustantivo del trabajo. (s.f.).

Colombia, P. d. (2012). *Decreto 884.*

Congreso de Colombia. (2008). *Ley 1221.*

Congreso de la República. (12 de 05 de 2021). *ley 2088 del 12 de mayo de 2021*. Recuperado el 05 de 10 de 2021, de https://dapre.presidencia.gov.co/normativa/normativa/LEY%202088%20DEL%2012%20DE%20MAYO%20DE%202021.pdf

EL Congreso de Colombia. (2021). *Ley 2121.*

Ficarra, F. (2002). *Virus informáticos: Entre el negocio y el temor.* Quito, Ecuador.

Gobierno USA. (2012). *Guia del consumidor.*

https://www.nsit.com.co/ciberataques-mas-famosos-del-2020/. (s.f.).

Malfere, L. (2012). *Julian Assange: Biography of the Wikileaks Mastermind.* Hyperink.

Manchego, M. (15 de 06 de 2020). Teletrabajo y trabajo en casa ¿cuál es la diferencia? *Portafolio*.

Martinez, Y. R. (2020). *La Importancia de la Inteligencia Artificial en la Seguridad Cibernética.*

Ministerio del Trabajo. (2020). *Circular 0041* .

Organización Internacional del Trabajo. (2020). *El teletrabajo durante la pandemia COVID-19 y después de ella - Guía práctica.* Ginebra.

Pascual Estapé, J. A. (31 de 08 de 2016). Se confirma el hackeo de Dropbox, 68 millones de cuentas afectadas. *Computer Hoy*. Obtenido de https://computerhoy.com/noticias/internet/confirma-hackeo-dropbox-68-millones-cuentas-afectadas-50344

Pedraza Moreno, V. M., & Rojas Henao, N. (2018). *Ransomware en Android.*

Portafolio. (2021). Ciberataques en Latinoamérica han aumentado un 24 % este año. *Portafolio*.

Ruiz Larrocha, E. (2019). *Nuevas tendencias en los sistemas de información.* Madrid: Centro de Estudios Ramón Areces S.A.

Velásquez, M., & Vera, M. (2010). Teletrabajo: Una Revisión Teórica sobre sus Ventajas y Desventajas. *Investigatio*.

Weiss, N. E., & Miller, R. S. (2015). The Target and Other Financial Data Breaches:. *Congressional Research Service*, 38.