Trabajo remoto y sociedad

DOI: 10.29236/sistemas.n162a7

Retos, realidades y recomendaciones de seguridad y control.

Resumen
En la actualidad se advierten diferentes reportes y análisis sobre el trabajo remoto y sus tensiones e implicaciones a nivel empresarial. Entender el trabajo remoto como una arquitectura básica compuesta por tres elementos como son las personas, los procesos organizacionales y la infraestructura tecnológica (generalmente basada en terceros), los cuales empiezan a ser enmarcados por recientes iniciativas legales y normativas, es indagar en una temática poco explorada y detallada, que propone diferentes escenarios y retos, así como oportunidades para aprender y descubrir un nuevo entorno de trabajo. En este sentido, los desafíos de seguridad y control, como parte inherente de este nuevo tejido de interconectividad y de dinámica empresarial, generan tensiones relevantes (entre sus elementos) y zonas opacas en sus interacciones que pueden (y serán) aprovechadas por los adversarios. Así las cosas, este artículo busca enmarcar este entorno laboral emergente para comprender sus interacciones, reconocer las preocupaciones de los ejecutivos de seguridad y establecer algunas recomendaciones para abordar el trabajo remoto como el nuevo normal de las empresas y la sociedad en general.

Palabras clave
Trabajo remoto, terceros de confianza, comportamientos, safety, ciberseguridad

Introducción

Mientras se escuchan voces encontradas entre el regreso progresivo a la "normalidad" y una nueva ola de contagios a nivel global, la realidad del trabajo remoto se consolida cada vez más como una opción real y concreta. Lo que antes de la emergencia sanitaria internacional era una posibilidad y se planeaba como opción para el trabajo desde diferentes sitios, hoy se hizo realidad por cuenta de una pandemia global que obligó a mantener las operaciones fuera del sitio de trabajo, confinados en casa por cuenta de un agente biológico agreste que sigue cobrando vidas a nivel internacional.

Llevarse la dinámica del trabajo a los hogares significó cambios drásticos en los modos de vida de las personas, con resultados positivos en algunos aspectos y otros no tanto por cuenta de un deterioro de la salud mental de los individuos, y la erosión del contacto físico, tan necesario en la especie humana, comoquiera que es en la interacción donde se hace evidente lo social y humano que permite el ejercicio de compartir y compartirse en múltiples esferas de la perspectiva individual (Sen et al., 2021).

El trabajo remoto se habilita como opción práctica y expedita de las organizaciones con el fin de mantener la dinámica de las organizaciones, y mantener la fuerza laboral en operaciones, para no debilitar la promesa de valor de la empresa y asegurar las "ventas" necesarias que mantengan los ingresos requeridos y así, tratar de no debilitar las finanzas, ni comprometer las garantías de sus trabajadores. Para ello, la tecnología se convierte en el aliado natural que permite "salir" a trabajar y consolidar la práctica empresarial ahora en un escenario, para algunos desconocido, para otros novedoso y para muchos totalmente inesperado (Bacon & Crawley, 2022).

En este sentido, los colaboradores organizacionales ingresaron rápidamente al mundo de la "conexión en línea" a través de una infraestructura de redes ahora habilitadas desde proveedores en la nube (pública, privada o híbrida) donde se hacía necesario recrear medidas equivalentes de seguridad y control a las disponibles dentro de la organización, lo cual implicó aprender rápidamente cómo se lograba esto ahora con terceros, y entender, qué nuevos retos y riesgos se habilitaron en este contexto de mayor dependencia, donde inicialmente sólo se tenían algunos servicios y aplicaciones, y ahora se traslada toda la organización y su fuerza de trabajo (Cano, 2021).

En consecuencia, este documento busca establecer algunos elementos o fundamentos básicos de seguridad y control para el trabajo re-

moto, comprender los retos y riesgos que se habilitan en esta nueva modalidad, y finalmente algunas recomendaciones y sugerencias que permitan a las organizaciones moverse de forma informada en una nueva realidad de operaciones que exige cambios y transformaciones a nivel individual, a nivel cultural y corporativo para mantener la dinámica de la empresa, no sólo a nivel productivo, sino cuidando sus activos más relevantes: las personas y la información.

Trabajo remoto, teletrabajo y trabajo en casa. Tres conceptos y una sola realidad

De acuerdo con la literatura actual no hay consenso sobre la conceptualización del trabajo fuera de la oficina, lo que genera algunas tensiones entre las personas y los empleadores sobre lo que significa continuar las labores en un espacio distinto al destinado por las empresas para desarrollar sus actividades. En este sentido se ha pronunciado la Organización Internacional del Trabajo (OIT) ofreciendo algunas orientaciones al respecto.

Para la OIT se establecen las siguientes definiciones: (OIT, 2020)

- *Trabajo remoto*: Es una situación en la que el trabajo se realiza total o parcialmente en un lugar de trabajo alternativo distinta de la localización que se tiene por defecto.
- *Teletrabajo*: Es una subcategoría del trabajo remoto, que incluye a los trabajadores que utilizan las tecnologías de la información y la comunicación (TIC) o los teléfonos fijos para realizar el trabajo de forma remota.
- *Trabajo en casa*: El trabajo en casa se refiere al trabajo que se realiza total o parcialmente en la propia residencia del trabajador. El lugar físico donde se realiza todo o parte del trabajo es, por tanto, el propio domicilio del trabajador.
- *Trabajo basado en el domicilio*: Es el trabajo que se realiza habitualmente en su domicilio, independientemente de que el propio domicilio pueda considerarse como el lugar de trabajo por defecto. El trabajo basado en el domicilio, por tanto, una subcategoría de la categoría de trabajo en casa.

Cualquiera que sea la definición que se adopte se tendrán algunas implicaciones concretas que afectan temas de conectividad, de ergonomía, de fatiga, de privacidad, de seguridad y control, de jornada laboral, entre otras, que comprometen a las organizaciones, sus colaboradores y condiciones laborales para la realización de sus actividades definidas en su descripción de cargo.

El trabajo remoto, como categoría superior, exige un cambio de perspectiva en términos laborales, personales y empresariales. Una lectura novedosa de lo que significa ahora la jornada de trabajo, la fatiga

por las largas horas de conectividad, el aislamiento y la condición de interacción mediada por tecnología, la fallas en la conexión, y las posibles y emergentes estrategias de fraude que se pueden alimentar bien por aumento del trabajo o por una intencionalidad malsana que puede ser usada a través de trucos con la tecnología (Barker, 2021).

El trabajo remoto establece retos a nivel cultural y social, que se traducen en una vista renovada de lo que significa confianza, sinergia y coordinación. Es un ejercicio donde la interacción deja de ser lo suficientemente cálida y amable, para privilegiar la eficiencia y la efectividad de las reuniones, afianzando la productividad de la organización y sus procesos, disminuyendo la dinámica de conexión personal y de camaradería que se potencia con la experiencia del encuentro y el contacto individual propio de la dinámica laboral habitual de la empresa: las charlas de pasillo, el café de la mañana, entre otras (Strack et al., 2021).

Características y componentes del trabajo remoto. Una vista conceptual y práctica

El trabajo remoto implica al menos tres elementos en interacción y acoplamiento permanente: la persona (y su entorno), la infraestructura tecnológica (y su contexto) y los procesos y metas corporativas (en el escenario nacional e internacional). Estos tres componentes deben estar debidamente alineados y conectados para que se haga realidad la dinámica del trabajo remoto. Si alguno de ellos, falla o presenta alguna inestabilidad existe la alta probabilidad que algo no se realice como se tiene planeado creando una zona de opacidad e incierto que termine con eventos no deseados en alguno de sus tres elementos (Strack et al., 2021)

La persona como fundamento de este modelo, es la parte más sensible de todas. Iniciando por su comportamiento y salud mental, pasando por la concentración y eficiencia en el desarrollo de su trabajo, el compromiso y sentido de logro, así como la pertenencia y el orgullo que debe caracterizar a aquel colaborador que hace parte de una empresa. Descuidar alguno de estos aspectos en el modelo de trabajo remoto implica crear una vulnerabilidad inherente que se traduce en posibles ausentismos, o bajos rendimientos y conductas no habituales que terminen deteriorando esa oportunidad de construir y lograr cosas en conjunto (Sen et al., 2021)

De otra parte, está la infraestructura tecnológica que habilita la conectividad disponible y desarrollada para soportar la interacción continua y dedicada de la organización para lograr sus metas. Esta infraestructura generalmente estará apalancada por terceros de confianza con contratos en la nube, que podrán tener elementos ya sea de condiciones privadas, públicas o

híbridas. En este modelo de operación, la organización, lo quiera o no, perderá control de muchos elementos propios de su administración y deberá confiar en que las cosas están funcionando de acuerdo con lo planeado con su proveedor de servicios. Es importante en este componente tener acuerdos concretos con el tercero para cuando la operación presenta situaciones no documentadas y eventos adversos inesperados (Deloitte, 2021).

De otra parte, los procesos y metas corporativas son el hilo conductor y la fibra que conecta a las personas para mantener el ritmo de trabajo y concretar sus fines. En el contexto del trabajo remoto, no se baja la guardia en el escenario nacional e internacional, comoquiera que es necesario mantener la facturación de la empresa y el flujo de caja. Para ello, las cadenas de suministro globales se convierten en la ruta crítica para conectar y entregar los productos y servicios claves a pesar de las condiciones adversas que se puedan presentar. Mantener la concentración y el esfuerzo en los objetivos, a pesar de las tensiones y eventualidades locales o globales, es parte de las exigencias y detalles que tanto personas como infraestructura deben coordinar para mantener la dinámica empresarial (Reeves et al., 2021).

Estos tres elementos (la persona, la infraestructura y los procesos) se configuran de forma interdependiente de tal forma que la afectación de uno de ellos puede crear un efecto dominó que termine con una posible falla generalizada que comprometa la organización como un todo.

Trabajo remoto. Retos de seguridad y control

El trabajo remoto ahora combinado con la posibilidad de una operación híbrida (parte del tiempo en remoto y en otro momento en presencial) crea condiciones distintas y retadoras para efectos de asegurar la dinámica del trabajo en las organizaciones. Los comportamientos de las personas, la protección de la infraestructura y las capacidades dinámicas de las empresas se vuelven elementos clave que combinados habilitan y fortalecen la promesa de valor de la empresa para con sus clientes.

Esta nueva modalidad, bien sea remota o híbrida, establece un entorno de múltiples distracciones no sólo físicas, sino digitales, las cuales desvían la atención de las personas bien por fatiga, por la necesidad de agilidad en su tareas o por errores que se pueden cometer muchas veces por falta de información, conocimiento o destreza. Las acciones intencionales están fuera del alcance de esta reflexión pues se estaría hablando de comportamientos irregulares asociados con violaciones de normas o estándares éticos de las empresas. Este escenario de distracciones es aprovechado por los adversarios para materializar los engaños y crear pi-

votes para generar ataques más sofisticados sobre la infraestructura tecnológica de la compañía. Un solo *click* basta para posicionar una estrategia de vulneración y permanencia de forma imperceptible en una plataforma técnica (Tessian, 2020).

La infraestructura tecnológica ahora a cargo de los terceros se vuelve verdaderamente susceptible y sensible, dado que hace parte de una red extendida de conectividad donde la organización y sus aplicaciones terminan afectadas cuando se presenta una brecha o una falla. Las tendencias recientes de ataques reportan que los agresores ya no se concentran en tratar de ingresar directamente en los sistemas propios de las empresas, sino a través de sus terceros. En este sentido, en la medida que se puedan explotar las vulnerabilidades de las infraestructuras en la nube, de las plataformas de seguridad habilitadas (*Cloud Access Security Broker*, agente de seguridad de acceso a la nube), las fallas de los protocolos de escritorio remoto, las vulnerabilidades de las aplicaciones de VPN (*Virtual Private Networks*, Redes virtuales privadas en español) y las limitaciones de seguridad de las API (*Application Program Interface*, Interfase de programas de aplicaciones) se podrán crear zonas de inestabilidad e incierto que generen la incertidumbre necesaria para que las organizaciones actúen de manera errática y no coordinada (Chernyshev et al., 2021).

Si lo anterior crea una zona de ambigüedad e incierto, se debilitan las capacidades dinámicas que las organizaciones han logrado por la implementación de tecnologías avanzadas basadas en analítica de datos y algoritmos de inteligencia artificial. Esto es, no sólo se disminuye la funcionalidad de las aplicaciones y la confianza de los clientes en ellas, sino que se compromete la promesa de valor, la experiencia y las expectativas de los consumidores, terminando por afectar la imagen de la compañía y los planes de desarrollo estratégicos de mediano y largo plazo los cuales pueden marginar a la empresa de los mercados claves (Teece et al., 2016).

Preocupaciones y recomendaciones claves para habilitar el trabajo remoto. El reto de una dinámica empresarial distinta.

Desarrollar ahora la dinámica empresarial en un entorno interconectado y de mayor flujo de información corporativa y personal a través de la infraestructura de terceros, implica reconocer los aspectos personales, de proceso y tecnológicos previamente mencionados, así como los retos de cumplimiento que aparecen por cuenta de una forma distinta de adelantar el tratamiento de los datos. En este sentido, se detallan a continuación algunas preocupaciones y sus recomendaciones claves para enfrentar las nuevas tensiones que genera el ejercicio del trabajo remoto en la

interacción digital entre múltiples actores empresariales (Gul & Slipsky, 2020):

- Aumento del flujo de datos privados y públicos en la red

Recomendación: Habilitar horarios de acceso a información sensible y monitorización de los mismos.

- Aumento de las descargas locales de información (pública y sensible)

Recomendación: Habilitar medidas de seguridad locales para el tratamiento de información sensible.

- Aumento de equipos sin parches aplicados

Recomendación: Habilitar mecanismos de verificación de instalación de parches en remoto y el uso de parches virtuales.

- Aumento de conversaciones con información propia del negocio fuera de la empresa

Recomendación: Mantener y asegurar el uso de la información empresarial sólo a las reuniones oficiales.

- Aumento de comportamientos inadecuados de las personas

Recomendación: Recuerde los procedimientos de seguridad y control establecidos a todos empleados.

- Aumento de patrones de actividad inusual en la redes

Recomendación: Monitorización, caracterización y análisis de patrones atípicos de tráfico.

- Aumento del uso de redes WIFI sin seguridad

Recomendación: Habilitar medidas mínimas de seguridad y control en redes inalámbricas.

- Aumento del uso de equipos personales

Recomendación: Uso de equipos validados y monitorizados por la empresa.

- Aumento de los engaños basados en los inciertos de la crisis

Recomendación: Validar fuente, ante las dudas preguntar y utilizar el sentido común.

- Aumento de ciberataques exitosos en los terceros de confianza

Recomendación: Realizar ejercicio de validación de controles y simulaciones de incidentes con los proveedores.

Este listado de preocupaciones y recomendaciones no pretende ser exhaustivo ni una receta a seguir, sino un conjunto de tendencias identificadas para el trabajo remoto con el fin de adelantar las acciones pertinentes de forma sistémica a nivel de las personas, los procesos, la tecnología y los retos de cumplimiento normativo.

Algunos apuntes sobre el nuevo mundo híbrido. Trabajo remoto y presencial en diferentes momentos

Afirma un reciente estudio de Mckinsey que:

En el entusiasmo por regresar del trabajo remoto, los líderes empresariales corren el riesgo de aumentar realmente la desconexión entre ellos y su gente. La idea de que cruzaremos una línea de meta y de repente habremos acabado con todo lo difícil parece existir sólo

en la mente de los altos ejecutivos (Dsmet et al., 2021, par 7), lo que implica que establecer los nuevos marcos de trabajo mixtos o híbridos, es una tarea que deberá estar asistida por una escucha atenta y activa de sus colaboradores, para construir de forma conjunta esta nueva forma de trabajar.

Las ventajas alcanzadas por muchos durante los confinamientos, entre ellas: la flexibilidad para estar en casa, ser más productivos, hacer ejercicio, liberarse del tráfico de las ciudades y ser más consciente de las realidades labores y sociales, ha hecho que las personas tengan una perspectiva distinta del trabajo y sean más críticos de la dinámica empresarial y sus exigencias. De acuerdo con Dsmet et al. (2021) desarrollar una jornada laboral en modalidad híbrida implica responder entre otras algunas preguntas como:

- ¿Qué trabajo se hace mejor en persona que virtualmente, y viceversa?
- ¿Cómo funcionan mejor las reuniones?
- ¿Cómo se puede equilibrar la influencia y la experiencia entre los que trabajan in situ y lo que no?
- ¿Cuántos días a la semana son mejores en la oficina?
- ¿Puede la comunicación de los líderes hacia los colaboradores fuera de la oficina ser tan eficaz como lo es para los trabajadores en la oficina?

Las respuestas a las preguntas previas sobre una modalidad híbrida de trabajo son aún una zona de experimentación para las empresas, por lo que se demanda un ejercicio de construcción y aprendizaje colectivo, donde colaboradores y ejecutivos elaboren sus propias aproximaciones. En este sentido, el trabajo de forma híbrida es una apuesta de reconocimiento corporativo del que "no se sabe" cuáles serán los resultados de las diferentes alternativas que se planteen al respecto y que están dispuestas a aprender junto con sus empleados para darle forma a una nueva realidad empresarial que hasta ahora avanza (Gratton, 2021).

Esta misma realidad, implica retos de seguridad y control en esta nueva modalidad, pues si en el modelo remoto las distracciones y errores son parte inherente de la dinámica empresarial de interconexión digital, una combinación de vulnerabilidades y riesgos tanto digitales como físicos, crea un entorno menos conocido y más volátil que implica atender diferentes frentes al mismo tiempo y poder correlacionar comportamientos y espacios de trabajo para dar cuenta con posibles alertas o efectos adversos generados por los adversarios (Huang et al., 2021).

En razón con lo anterior, los ejecutivos de ciberseguridad/seguridad deberán atender de forma simultánea los retos de seguridad y de *safety*, es decir aquellos impuestos

por otros en los diferentes componentes del trabajo remoto, así como los creados por los comportamientos de las personas en el tratamiento de la información respectivamente, con el fin de mantener la confianza en las interacciones digitales disponibles y motivar la confiabilidad de las acciones de los participantes de una realidad híbrida de la que poco se conoce (Martin, 2019).

Reflexiones finales

El peor riesgo que se puede materializar en la actualidad es "regresar a la normalidad". Lo anterior significa que no hubo aprendizaje, que los eventos de inestabilidad y reto que aún persisten no han generado lecciones para las personas y las organizaciones. El concepto de normalidad, asociado con el trabajo en instalaciones físicas, puede terminar siendo una limitante para romper con la inercia que tanto personas como empresas traían en el ejercicio de reconocimiento de su propio entorno.

En este sentido, abordar el trabajo remoto como un nuevo espacio de construcción de comunidad y de sociedad, es un ejercicio de reflexión personal y corporativa que debe llevar a desarrollar capacidades y habilidades inéditas para expandir el concepto de realidad que se tiene en la actualidad, y habilitar otras posibilidades para capitalizar las ventajas de estos espacios de trabajo novedosos, limitando y atendiendo al mismo tiempo las tragedias humanas que se viven por cuenta de algunas organizaciones e individuos que no han logrado conectar con esta "nueva realidad" (Dsmet et al., 2021).

El trabajo remoto, ahora combinado con la perspectiva híbrida (remoto y presencial), habilita reglas inexistentes a nivel personal, de procesos, tecnología y normatividad, que implica "sembrar respuestas parciales, humildes y pequeñas" con expectativas germinales futuras para las cuales no se tienen referentes o experiencias previas. Esto es, encontrar en la experimentación, el aprendizaje colectivo y la capitalización de experiencias, una ventana de oportunidad y aprendizaje que lleve tanto a organizaciones como a personas a ver el mundo de formas distintas (Gratton, 2021).

Así las cosas, el reto de las prácticas de seguridad y control en un entorno remoto establecen relaciones extendidas con los terceros de confianza que implican conversaciones y ejercicios más frecuentes y cercanos, que no sólo llevan una práctica estándar de cumplimiento, sino una relación de socio estratégico que entiende los retos de la empresa, y está dispuesta a desafiar sus propios estándares (más allá de lo que indican sus contratos) para desprenderse de sus mejores propuestas, arrojarlas al surco incierto de la inevitabilidad de la falla, "sin garantías de éxito", pero sí con una promesa de una relación em-

presarial más fecunda y transparente (Deloitte, 2021).

Lo anterior implica reconocer las amenazas propias de esta nueva realidad Híbrida, que llevaría a la materialización de ataques cibernéticos que pondrán a prueba la relación empresarial en mención, creando experiencias negativas y muchas veces dolorosas, las cuales deben ser parte del ejercicio de confianza digital (basado en simetría, reciprocidad y transparencia) tripartito entre los clientes, las empresas y sus terceros socios estratégicos (Sutton, 2021), y que no se deberán resolver motivando y provocando el consumo de "cajas o servicios novedosos de seguridad y control", sino desde una experiencia de crecimiento y visión de futuro. Esto es, aumentado la resiliencia digital de sus infraestructuras, o entendiendo la inevitabilidad de la falla de forma real y auténtica como parte del proceso y no como un resultado.

Referencias

Bacon, R. & Crawley, K. (2022). *IT Necessities for a Distributed World. Building a Modern IT Infrastructure for Hybrid-Remote Work*. Sebastopol, CA. O'Reilly.

Barker, J. (2021). Your big agenda just got bigger. *Deloitte Insights Magazine*. 29. https://www2.deloitte.com/us/en/insights/topics/strategy/current-business-problems-strategic-imperatives.html

Cano, J. (2021). Tecnologías habilitadoras del Smart Working. *IDC White Paper*. https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/market-research/estudio-tecnologias-habilitadoras-del-smart-working.html

Chernyshev, M., Baig, Z. & Zeadally, S. (2021). Cloud-Native Application Security: Risks, Opportunities, and Challenges in Securing the Evolving Attack Surface. *IEEE Computer*. November. 47-57. Doi: 10.1109/MC.2021.3076537

Deloitte (2021). Third-party risk management (TPRM) global survey 2021. A digital path to third-party oversight. *Report*. https://www2.deloitte.com/us/en/pages/risk/articles/extended-enterprise-risk-management-report.html

Dsmet, A., Dowling, B., Mysore, M. & Reich, A. (2021). Es hora de que los líderes sean realistas en cuanto a lo híbrido. *Mckinsey*. https://www.mckinsey.com/featured-insights/destacados/es-hora-de-que-los-lideres-sean-realistas-en-cuanto-a-lo-hibrido/es-ES

Gratton, L. (2021). How to do hybrid right. *Harvard Business Review*. https://hbr.org/2021/05/how-to-do-hybrid-right

Gul, S. & Slipsky, M. (2020). The Top 10 Employer Cybersecurity Concerns For Employees Regarding Remote Work. *Security Magazine*. https://www.securitymagazine.com/articles/91999-the-top-10-employer-cybersecurity-concerns-for-employees-regarding-remote-work

Huang, K., Pearlson, K. & Madnick, S. (2021). Is Third-party software leaving you vulnerable to cyberattacks? *Harvard Business Review*. https://hbr.org/2021/05/is-third-party-software-leaving-you-vulnerable-to-cyberattacks

Martin, P. (2019). *The rules of security. Staying safe in a risky world*. Oxford University Press.

OIT (2020). *Defining and measuring remote work, telework, work at home and home-based work. COVID-19: Guidance for labour statistics data collection*. ILO. https://www.ilo.org/global/statistics-and-databases/publications/WCMS_747075/lang--en/index.htm

Reeves, M., Shmul, Y. & Martínez, Z. (2021). How Resilient Businesses Created Advantage in Adversity During COVID-19. *Boston Consulting Group*. https://www.bcg.com/publications/2021/how-resilient-companies-created-advantages-in-adversity-during-covid

Sen, P., Deb, P. & Kumar, N. (2021). The Challenges of Work From Home for Organizational Design. Insights. *California Management Review*. https://cmr.berkeley.edu/2021/07/the-challenges-of-work-from-home-for-organizational-design/

Strack, R., Kovács-Ondrejkovic, O., Baier, J., Kotsis, Á., Antebi, P. & Kavanagh, K. (2021). Decoding the Digital Talent Challenge. *Boston Consulting Group*. https://www.bcg.com/publications/2021/what-digital-talent-expect-from-a-job

Sutton, D. (2021). *Information risk management. A practitioner's guide*. Second edition. Swindon, UK.: British Computer Society Learning and Development Ltd.

Teece, D., Peteraf, M. & Leih, S. (2016). Dynamic Capabilities and Organizational Agility: Risk, uncertainty, and strategy in the innovation economy. *California Management Review*. *58*(4). 13-35. Doi: 10.1525/cmr.2016.58.4.13

Tessian (2020). *Psychology of human error. Understand the mistakes that compromise your company's cybersecurity*. Tessian. https://www.tessian.com/research/the-psychology-of-human-error/

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*