Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/5.(4).dic.2021.344-355
URL: https://recimundo.com/index.php/es/article/view/1374
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de investigación
CÓDIGO UNESCO: 5909.01 Gestión Administrativa
PAGINAS: 344-355

Seguridad de la información de los reclamos en modalidad teletrabajo

Information security of claims in telework mode

Segurança da informação de sinistros em modo de teletrabalho

Dayaner Andrés Valverde Arcos[1]; Gisella Patricia Hurel Franco[2]

RECIBIDO: 27/01/2021 **ACEPTADO:** 30/11/2021 **PUBLICADO:** 05/12/2021

1. Estudiante; Facultad de Posgrado-Administración de la Universidad Laica Vicente Rocafuerte de Guayaquil, Ecuador; dvalverdea@ulvr.edu.ec; https://orcid.org/0000-0002-6055-1053
2. Docente; Facultad de Posgrado-Administración de la Universidad Laica Vicente Rocafuerte de Guayaquil; Ecuador; ghurelf@ulvr.edu.ec; https://orcid.org/0000-0002-8313-1190

CORRESPONDENCIA
Dayaner Andrés Valverde Arcos
dvalverdea@ulvr.edu.ec

Guayaquil, Ecuador

RESUMEN

El presente trabajo pertenece al área de administración de empresas, específicamente en lo que concierne a la gestión de control de las entidades financieras, bajo el enfoque del teletrabajo para la atención de reclamos. El objetivo del estudio fue determinar el efecto que tiene la gestión de control bajo teletrabajo en las operaciones bancarias y seguridad de la información en el departamento de reclamos de una entidad financiera. Para tal fin, la metodología abordada perteneció a los estudios con un diseño descriptivo, en vista de que su intención fue describir la realidad concerniente a la atención de reclamos por parte de la entidad financiera objeto de investigación durante la emergencia sanitaria del COVID-19. Para tal fin, se realizó el levantamiento de la información con lo cual se llegó a las siguientes conclusiones principales. Existe la oportunidad de mejora del proceso de atención de reclamos bajo el sistema de teletrabajo. Se considera importante revisar y adaptar los documentos que establecen en la aludida institución la forma correcta de hacer las cosas, es decir: el Código de ética, el Manual de funciones, así como la estructura organizativa del departamento de reclamos. De este modo, se espera ofrecer un mejor servicio al cliente, garantizando de la misma manera el sigilo de la información.

Palabras clave: Teletrabajo, Operaciones Bancarias, Seguridad de la Información, Reclamos, Entidad Financiera.

ABSTRACT

The present work belongs to the area of business administration, specifically in what concerns the control management of financial institutions, under the teleworking approach for the attention of claims. The objective of the study was to determine the effect of control management under telework on banking operations and information security in the claims department of a financial institution. To this end, the methodology approached belonged to the studies with a descriptive design, since its intention was to describe the reality concerning the attention of claims by the financial institution under investigation during the health emergency of COVID-19. To this end, information was collected and the following main conclusions were reached. There is an opportunity to improve the claims attention process under the teleworking system. It is considered important to review and adapt the documents that establish in the alluded institution the correct way of doing things, that is to say: the Code of ethics, the Manual of functions, as well as the organizational structure of the department of claims. In this way, it is expected to offer a better service to the client, guaranteeing in the same way the confidentiality of the information.

Keywords: Teleworking, Banking Operations, Information Security, Claims, Financial Institution.

RESUMO

O presente trabalho insere-se na área da administração de empresas, especificamente no que diz respeito à gestão do controlo das instituições financeiras, sob a abordagem do teletrabalho para o atendimento de sinistros. O objetivo do estudo foi determinar o efeito da gestão do controlo em teletrabalho nas operações bancárias e na segurança da informação na área de sinistros de uma instituição financeira. Para tanto, a metodologia abordada pertencia aos estudos com delineamento descritivo, uma vez que se pretendia descrever a realidade no que se refere ao atendimento de sinistros da instituição financeira investigada durante a emergência sanitária do COVID-19. Para tal, foram recolhidas informações e tiradas as seguintes conclusões principais. Existe a oportunidade de melhorar o processo de atendimento de sinistros no sistema de teletrabalho. Considera-se importante rever e adaptar os documentos que estabelecem na referida instituição a forma correta de fazer, ou seja: o Código de Ética, o Manual de Funções, bem como a estrutura organizacional do departamento de reclamações. Desta forma, espera-se oferecer um melhor atendimento ao cliente, garantindo da mesma forma o sigilo das informações.

Palavras-chave: Teleworking, Banking Operations, Information Security, Claims, Financial Institution.

Introducción

La seguridad de la información es parte de la gestión de riesgos directamente vinculada con la prevención o reducción de la probabilidad de acceso, uso, divulgación, interrupción, eliminación, corrupción, modificación, inspección o grabación no autorizada. Si ocurre un incidente de seguridad, los profesionales de seguridad de la información están involucrados en la reducción del impacto negativo del incidente. La información de las notas puede ser electrónica o física, tangible o intangible. Si bien el enfoque principal de cualquier programa de seguridad de la información es proteger la confidencialidad, integridad y disponibilidad de la información, mantener la productividad organizacional es a menudo una consideración importante. Esto ha llevado a la industria de la seguridad de la información a ofrecer orientación, políticas de seguridad de la información y estándares de la industria sobre contraseñas, software antivirus, firewalls, software de cifrado, responsabilidad legal y conciencia de seguridad, para compartir las mejores prácticas.

En el caso de las transacciones fallidas en los cajeros automáticos, éstas pueden deberse a un mal funcionamiento del cajero automático o el cajero automático podría no tener efectivo. Suele no haber razones de preocupación o pánico, ya que el banco acreditará el monto en la cuenta dentro de un tiempo específico. Si la transacción en un cajero automático no se realiza correctamente y el banco no revierte el dinero adeudado de la cuenta del cliente, dentro de un período de tiempo específico, tendrá que compensarlo, según la normativa que suele regir este tipo de servicios bancarios. Sin embargo, también en este campo la seguridad de información automatizada es de vital importancia y existen diversos factores incidentes.

Dentro de la modalidad de teletrabajo es preciso también la injerencia de la seguridad de la información. Muchos empleados utilizan dispositivos informáticos de propiedad personal o propiedad de la universidad mientras trabajan en casa, otros lugares o mientras viajan. Y toda esa dinámica hace muy vulnerable este campo laboral a manipulaciones y sustracciones de información que pocas veces suele ser de alta confidencialidad.

En cada una de las áreas y actividades descritas existen realidades que aportan especificidades que requieren su análisis. Y este es el sentido primordial del presente trabajo.

La seguridad de la información

Existe una marcada diferencia entre “seguridad de la información” y “ciberseguridad” a menudo se confunden. En este sentido es preciso señalar que la “seguridad de la información es una parte crucial de la ciberseguridad, pero se refiere exclusivamente a los procesos diseñados para la seguridad de los datos. La ciberseguridad es un término más general” (Vega, Grajales, & Montoya, 2017, pág. 67).

Un “sistema de gestión de seguridad de la información” (SGSI) es un conjunto de procedimientos y lineamientos creados para que las organizaciones estén conscientes de lo que deben realizar ante una violación de datos; este grupo de pautas se convierte para las empresas en formalismos que mitigan el riesgo y que garantizan la seguridad de los datos ante un cambio de personal.

En el año 2016, el Parlamento Europeo acordó un reglamento general de protección de datos. A raíz de ese evento, lo han hecho igualmente otras instancias internacionales, lo cual se ha ido incorporando a legislaciones y reglamentaciones regionales y nacionales. Todo ese marco normativo ha ido conduciendo a que se exija a las empresas que proporcionen avisos de transgresión de datos, a nombrar delegados de protección

de datos, a requerir el consentimiento de usuarios para el procesamiento de datos y a anonimizar los datos para la privacidad (Lema & Cuenca, 2020).

En la actualidad, existen diferentes tipos de certificaciones para los trabajos de ciberseguridad; en algunas empresas el departamento de seguridad de la información, deben ser capacitados constantemente, de esta manera cuentan con conocimientos que ayudan a salvaguardar la información más vulnerable de la organización. Es así, que empresas sin fines de lucro como el "Consorcio Internacional de Certificación de Seguridad de Sistemas de Información" emite capacitaciones o certificaciones que son aceptadas ampliamente, variando sus alcances, los mismos que se adaptan a las necesidades de la empresa.

Por otra parte, está el tema de la seguridad de las aplicaciones, es una temática que conlleva al análisis de diferentes vulnerabilidades de los softwares utilizados para las aplicaciones móviles o páginas web; así como también las interfaces de programación utilizadas por algunas compañías; es importante que las empresas cuenten con mecanismos que protejan los datos de esta vulnerabilidades, las mismas que pueden encontrarse en la autentificación o autorizaciones de los usuarios, la integridad de códigos o en las configuraciones y políticas que requieren ciertos procesos maduros. "Las vulnerabilidades de las aplicaciones pueden crear puntos de entrada para infracciones importantes de seguridad de información. La seguridad de las aplicaciones es una parte importante de la defensa del perímetro de este campo tan relevante" (Cano & Almanza, 2020, pág. 477).

Adicionalmente está lo que se conoce como la "seguridad en la nube", la misma que se concentra en crear y alojar espacios seguros en entornos de nube propias y de terceros. "La nube simplemente significa que la aplicación se ejecuta en un entorno compartido, las empresas deben asegurarse de que exista un aislamiento adecuado entre los diferentes procesos en entornos compartidos" (Cano & Almanza, 2020, pág. 478). En preparación para las infracciones en seguridad de información, las organizaciones deben contar con un personal y la debida planificación para dar respuesta a incidentes para contener riesgos y amenazas.

Riesgos de la seguridad de la información

Los riesgos de la seguridad de la información comprenden los impactos para una organización y sus partes interesadas que podrían ocurrir debido a las amenazas y vulnerabilidades asociadas con la operación y uso de los sistemas de información y los entornos en los que operan esos sistemas. El medio principal de mitigar el riesgo relacionado con la seguridad de la información es a través de la selección, implementación, mantenimiento y monitoreo continuo de controles de seguridad preventivos, de detección y correctivos para proteger los activos de información contra el compromiso o para limitar el daño a la organización en caso de que ocurra un compromiso.

"El riesgo de seguridad de la información se superpone con muchos otros tipos de riesgo en términos de los tipos de impacto que podrían resultar de la ocurrencia de un incidente relacionado con la seguridad" (Observatorio de Ciberseguridad, 2020, pág. 24). También está influenciado por factores atribuidos a otras categorías de riesgo, incluidos los riesgos estratégicos, presupuestarios, de gestión de programas, de inversión, políticos, legales, de reputación, de cadena de suministro y de cumplimiento.

Seguridad de la información bancaria

El sector bancario ha sido atacado durante cientos de años. Primero, fue el robo físico de dinero. Luego fue el fraude informático. Hoy en día, no se trata solo de un fraude cibernético, sino de piratería en los servidores

para obtener la información de identificación personal de un cliente. De ahí la razón por la que la ciberseguridad en la banca es de suma importancia. "Dado que las personas y las empresas realizan la mayoría de las transacciones en línea, el riesgo de una violación de datos aumenta a diario" (Observatorio de Ciberseguridad, 2020, pág. 31). Es por eso que hay un mayor énfasis en examinar la importancia de la ciberseguridad en los procesos del sector bancario.

La razón obvia de la importancia de la ciberseguridad en las transacciones del sector bancario es proteger los activos de los clientes. A medida que más personas se quedan sin efectivo, las actividades se realizan a través de páginas de pago en línea y escáneres de crédito físicos. En ambas situaciones, la información confidencial puede redirigirse a otras ubicaciones y utilizarse para actividades maliciosas. Esto no solo afecta al cliente. También daña enormemente al banco mientras intentan recuperar los datos. Cuando lo toman como rehén, es posible que el banco deba pagar cientos de miles de dólares para divulgar la información. A su vez, pierden la confianza de sus clientes y otras instituciones financieras.

Eso no es lo único que sucede cuando no se implementan los pasos para la seguridad cibernética de la banca. El cliente debe cancelar todas sus tarjetas y abrir nuevas cuentas, posiblemente en otro banco. Y aunque sus fondos están protegidos, no impide que los delincuentes intenten utilizar información importante y confidencial. Se requieren soluciones de software bancario para evitar actividades maliciosas (Cano & Almanza, 2020). A medida que los bancos han mejorado su seguridad cibernética, los piratas informáticos han recurrido a sistemas bancarios compartidos y redes de terceros para obtener acceso. Si estos no están tan protegidos como el banco, los atacantes pueden pasar con facilidad. Dado que el sector no está seguro de cómo implementar software de seguridad cibernética para la banca en este mercado en constante cambio, "la capacidad de los atacantes para apoderarse de grandes cantidades es mayor y más sofisticada" (Lema & Cuenca, 2020, pág. 70). Una auditoría absoluta es imperativa antes de que la empresa implemente un software nuevo para la seguridad cibernética, revisar las fortalezas y debilidades en la configuración del mismo es primordial para evitar las fugas de información, también es preciso que los informes de auditoría ofrezcan recomendaciones que permitan el ahorro de recursos y dinero, por lo que las entidades financieras requieren de aplicaciones que bloquean los ataques a los programas utilizados para controlar los datos de los clientes; sin embargo, es importante que las empresas incluyan firewall que impidan en acceso de actividades maliciosas en la red utilizada.

Los reclamos

Los reclamos en relación con los servicios de los cajeros automáticos ocurren cuando el titular de la tarjeta solicita dinero de su cajero automático y afirma que el cajero automático no entregó el dinero, a pesar de que la cantidad aún se debite de la cuenta del titular de la tarjeta y se acreditó en la cuenta de caja del cajero automático. "Cuando esto sucede, el procesador del cajero automático abrirá una investigación y, por lo general, tiene tres días para proporcionar el diario del cajero automático" (Sierra & Murillo, 2020, pág. 39).

Los cajeros automáticos pueden cometer errores, y cuando lo hacen, puede costarles tiempo y dinero limpiarlos. "Pueden contabilizar un monto de depósito incorrectamente, dispensar muy poco o demasiado efectivo, no entregar un recibo y quedarse con la tarjeta bancaria del cliente" (Jácome, 2020, pág. 19). Los errores más espectaculares ocurren cuando los cajeros automáticos dispensan efectivo a cualquiera que pase, incluidos aquellos sin dinero en sus cuentas o incluso sin cuentas.

La modalidad teletrabajo

El teletrabajo como actividad, se representa como un acuerdo de empleo en el que el empleado trabaja fuera de la oficina del empleador. "A menudo, esto significa trabajar desde casa o en un lugar cercano, como una cafetería, una biblioteca o un espacio de trabajo conjunto. Muchas industrias, incluidas las de ventas, publicaciones, servicio al cliente y marketing, ofrecen trabajos de teletrabajo" (García, 2020, pág. 315). Es así que muchos trabajos, incluido la programación de computadoras y software se pueden realizar a través del teletrabajo; algunos profesionales médicos, analistas de reclamos de salud y radiólogos, han comenzado a trabajar desde casa.

El teletrabajo permite que, en vez de viajar a la oficina, el colaborador utilice la tecnología de la información y comunicación (Tic) para mantener contacto constante con la oficina central y sus compañeros. De esta manera puede utilizar dispositivos móviles como un teléfono, computadores portátiles, chat en línea, videoconferencias o correo electrónicos para llevar a cabo sus funciones; así, la tecnología facilita en gran medida el desarrollo del trabajo desde casa, por lo que el acceso a internet a través de una red inalámbrica eficiente es vital para una práctica comunicativa fluida.

Sin embargo, la práctica de teletrabajo, no exime al trabajador de asistir ocasionalmente a la oficina a reuniones, convocatorias o para comunicarse con su emperador, de esta manera este tipo de trabajo se los puede realizar de tiempo completo, parcialmente o realizar combinaciones de asistencia remota ciertos días de la semana.

. En la práctica, el teletrabajo es una práctica que permite que el empleado realice un "trabajo desde cualquier parte, en un lugar de trabajo alternativo aprobado. Esta definición de teletrabajo incluye lo que generalmente se denomina trabajo a distancia, pero no incluye ninguna parte del trabajo realizado durante un viaje oficial o trabajo móvil" (Páez, Chávez, Apunte, & Rosales, 2020, pág. 9). También se puede estar familiarizado con el término lugar de trabajo flexible. Si bien el trabajo remoto y móvil son términos que a veces se utilizan como sinónimos de teletrabajo, tienden a funcionar de manera diferente al teletrabajo.

Los ambientalistas consideran que esta es una forma eficaz y probada de reducir la contaminación en grandes ciudades. No cabe duda de que el desplazamiento de los empleados a su lugar de trabajo exige un gran volumen de combustible fósil, y está claro que la emisión de un número tan elevado de vehículos constituye una gran parte de la contaminación atmosférica en las grandes ciudades. Por un lado, tenemos una fuerte tendencia positiva de inmigración de mano de obra a las grandes ciudades, y por otro lado un ritmo suave en la construcción de infraestructura de transporte como nuevas carreteras, puentes y medios de transporte dentro de las ciudades en general, "entonces se puede concluir que la única forma probada de controlar la contaminación del aire en estas ciudades es el teletrabajo" (Vargas, 2020, pág. 7).

Ventajas y desventajas de la modalidad teletrabajo

En relación con las ventajas y desventajas de la modalidad del teletrabajo vale la pena focalizar aspectos de mayor especificidad y amplitud. Para autores como Castro, Galarza y Sánchez (2017), el teletrabajo tiene diferentes beneficios tanto para los empleados como para la empresa. "Algunos de estos beneficios incluyen el hecho de que los empleados tienen un horario de trabajo más flexible, ya que pueden trabajar a su propio ritmo sin presión" (pág. 37). Asimismo, es posible que los trabajadores deban no combatir aquellas distracciones típicas de las oficinas o lugares de trabajo; pero si deben organizar sus actividades laborales.

Así, un colaborador que deba trasladarse menos ahorra dinero y tiempo de desplazamiento, por lo que puede concentrarse para ser más productivo.

Con un horario más flexible, menos distracciones en el lugar de trabajo y sin tener que lidiar con el transporte, los trabajadores a distancia pueden ser más productivos. Esta modalidad puede brindar un cierto aumento en la autonomía e incluso en la lealtad de los empleados. Además de un mejor equilibrio entre el trabajo y la vida de los empleados. "Puede ahorrarle dinero a una organización, considerando los bienes raíces y otros gastos generales. En líneas generales puede decirse que el teletrabajo también beneficia al planeta" (Castro, Galarza, & Sánchez, 2017, pág. 29). Menos trabajadores que necesiten viajar significa menos emisiones de dióxido de carbono. Si bien el teletrabajo puede presumir de muchos beneficios, también puede ser la fuente de algunos desafíos para los cuales también deben prepararse empleados y organizaciones.

Metodología

Diseño de investigación

El diseño de investigación es propio de las investigaciones descriptivas, en los casos en que se desea describir una determinada realidad mediante sus componentes principales. Asimismo, el enfoque investigativo es de tipo mixto, en donde intervienen los paradigmas cuantitativos y cualitativos (Valverde , 2021).

Métodos y técnicas

Se utilizó también el método analítico el cual representa una serie de medios para confirmar la verdad; así como fue preciso la aplicación de técnicas como la revisión bibliográfica para la fundamentación teórica de la investigación, la encuesta, la entrevista y la observación para el levantamiento de datos de las variables (Valverde , 2021).

Instrumentos y procesamientos de datos

Finalmente, los instrumentos utilizados se encuentran las fuentes primarias, el cuestionario y la ficha de observación; además, el procesamiento de la información se realizó mediante la aplicación de la estadística descriptiva con la cual se construyeron las gráficas respectivas, a partir de las cuales se desarrolló el análisis de los hallazgos. (Valverde , 2021).

Población y Muestra

La población se encuentra conformada por 200 trabajadores de la entidad financiera. De este modo, la muestra es de tipo no probabilística y estuvo compuesta por el total del personal que labora en el departamento de reclamos la cual asciende a 33 individuos consultados (Valverde , 2021).

Resultados y discusión

De acuerdo al análisis de los resultados, y según se observa en la figura 1, el 75,8% de los entrevistados señalan que recibieron capacitación en la atención de reclamos según la modalidad de teletrabajo, por lado contrario un 21,2% indica que no hubo capacitación sobre este aspecto y por último el 3% restante demuestra inseguridad de respuesta ante dicho planteamiento al escoger la alternativa de respuesta tal vez. De esta manera, es posible inferir que no se realizó a su totalidad la formación en atención de reclamos en modalidad de teletrabajo, observándose necesidades de adiestramiento en cierta cantidad de personal (Valverde , 2021).

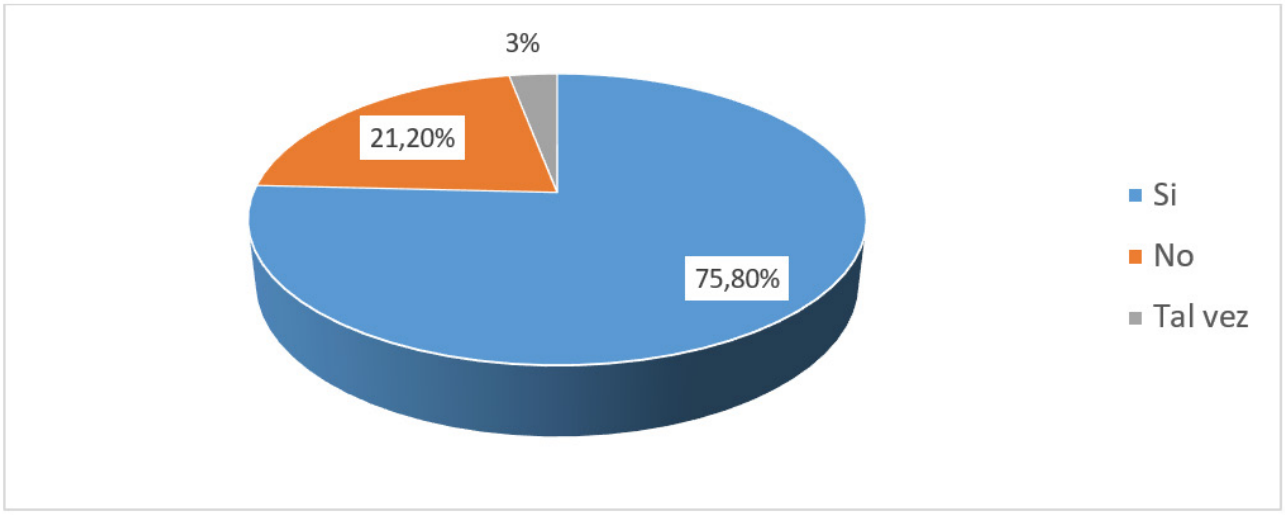

Figura 1. Capacitación en atención de reclamos en modalidad de teletrabajo.

Fuente: Valverde, 2021

Del mismo modo, en la figura 2, se muestra como la mayor parte de los sujetos consultados el 75,8%, en concordancia con los datos de la pregunta anterior, indica que sí se establecieron con claridad los procesos para la gestión de reclamos durante la emergencia sanitaria. Por otro lado, el 15,2% estableció la opción de tal vez y por último el 9% señaló que no hubo precisión en dicha materia. En este sentido, se observa la necesidad de mejorar los procedimientos e instructivos en esta área de la organización (Valverde, 2021).

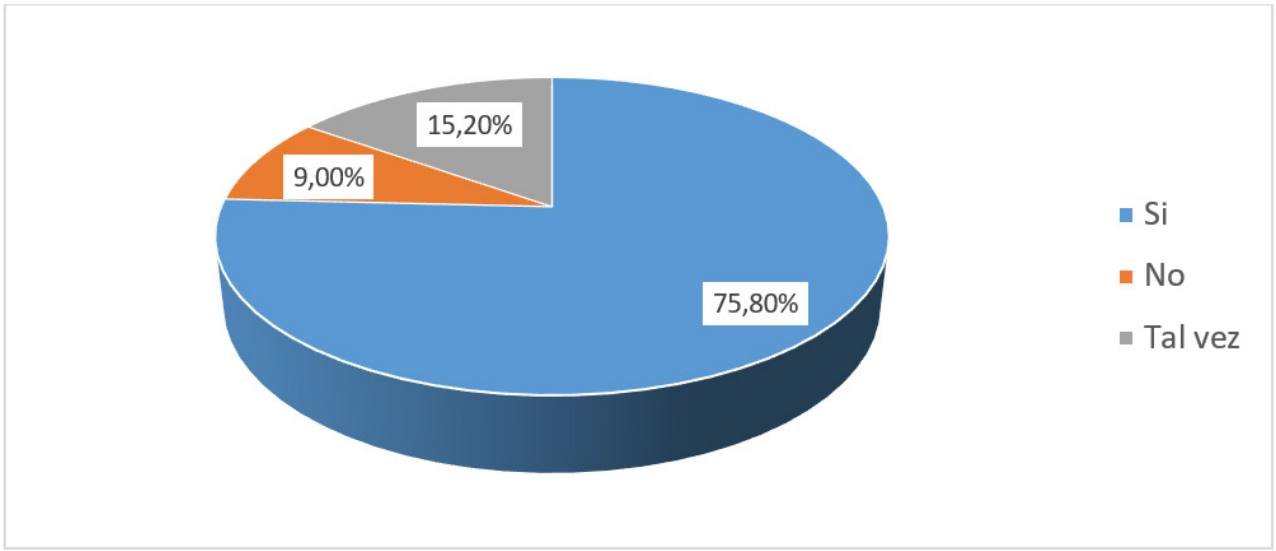

Figura 2. Claridad en la gestión de reclamos durante la emergencia sanitaria

Fuente: Valverde, 2021

En este orden de ideas, de acuerdo a lo que se observa en la figura 3, la mayor parte de los sujetos encuestados, el 90,9% indica que la entidad financiera sí ejecutó el control de sus actividades en modalidad de teletrabajo. Solamente el resto de la muestra consultada, el 9,1% señaló con inseguridad que tal vez. De esta manera, es posible evidenciar la necesidad de mejora en los procedimientos y funciones de esta área de trabajo, así como en lo que concierne al código de ética de la organización (Valverde , 2021).

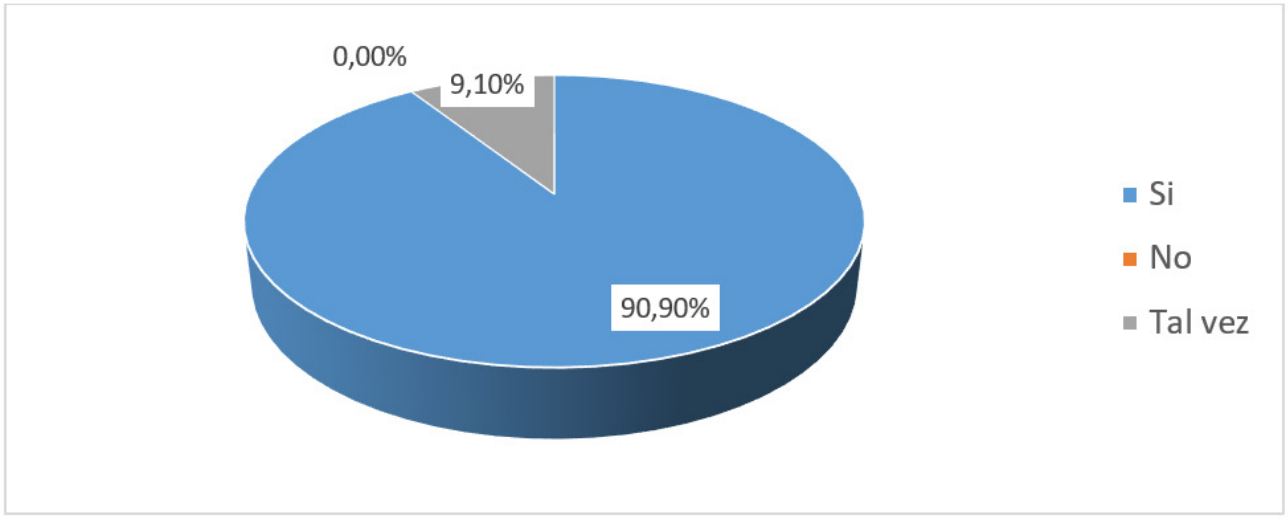

Figura 3. Control en modalidad de teletrabajo.

Fuente: Valverde, 2021

Ahora bien, de acuerdo a lo que evidencia la figura 4, la mayor parte de los encuestados el 90,9% indica que se generaron más reclamos durante la emergencia sanitaria. De forma contraria, solamente el resto de los entrevistados el 9,1% responde tal vez a dicha interrogante. De lo anterior es posible inferir el aumento en la cantidad de reclamos durante el inicio de la emergencia sanitaria resultando por ende la necesidad de establecer procedimientos e instructivos orientados a atender este tipo de atención al cliente bajo la modalidad virtual de teletrabajo (Valverde, 2021).

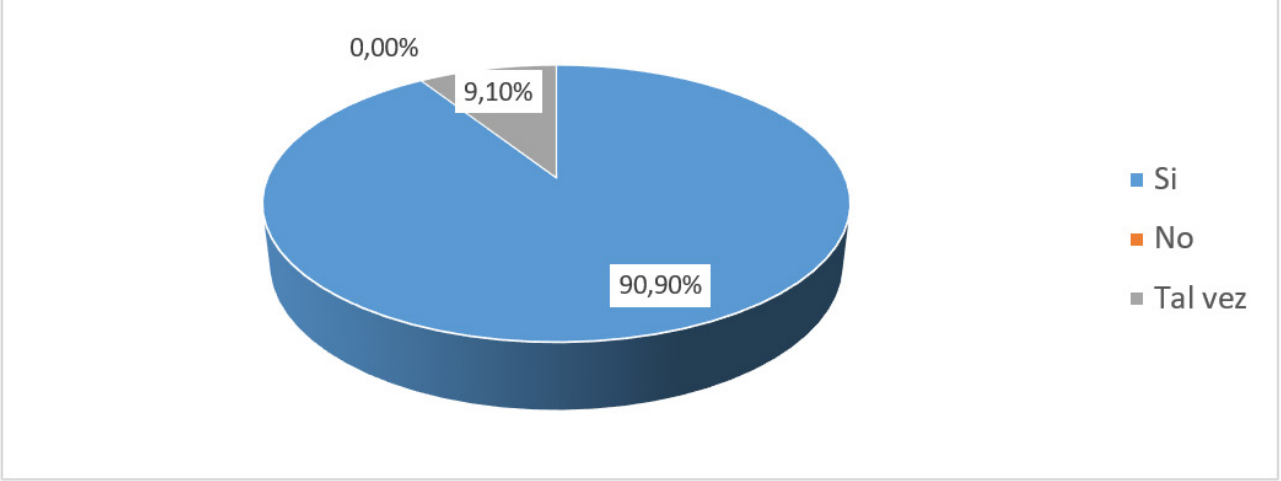

Figura 4. Aumento de reclamos durante la emergencia sanitaria.

Fuente: Valverde, 2021

Ahora bien, de acuerdo a lo que evidencia la figura 4, la mayor parte de los encuestados el 90,9% indica que se generaron más reclamos durante la emergencia sanitaria. De forma contraria, solamente el resto de los entrevistados el 9,1% responde tal vez a dicha interrogante. De lo anterior es posible inferir el aumento en la cantidad de reclamos durante el inicio de la emergencia sanitaria resultando por ende la necesidad de establecer procedimientos e instructivos orientados a atender este tipo de atención al cliente bajo la modalidad virtual de teletrabajo (Valverde, 2021).

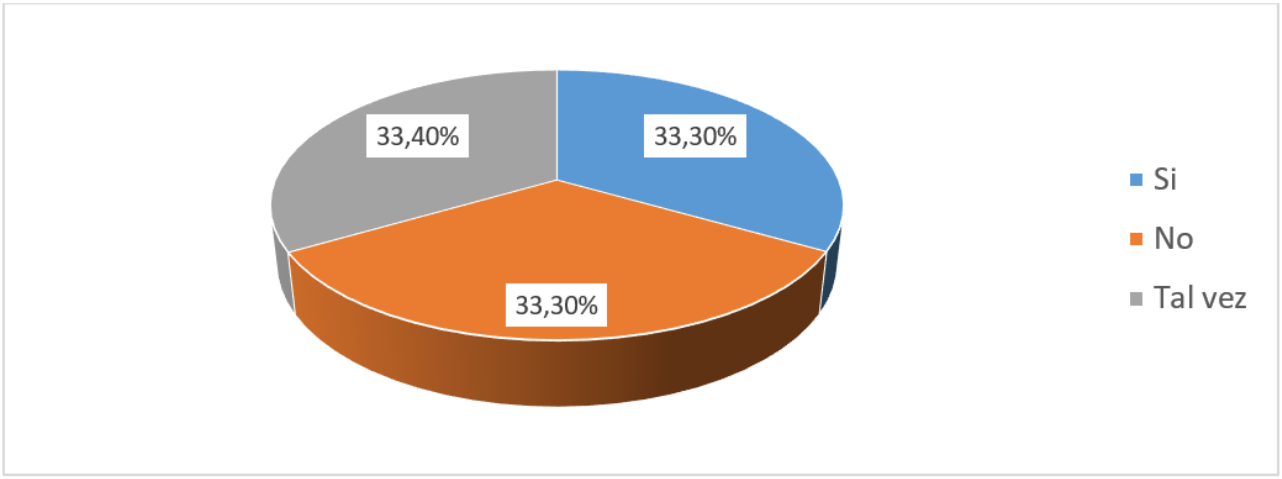

Figura 5. Falencias en la gestión de control.

Fuente: Valverde, 2021

Al respecto del análisis de los datos anteriores, la figura 6 muestra que la mayor parte de los entrevistados, el 78,8% señala que la gestión de control protegió el flujo de información durante la atención en modalidad de teletrabajo, mientras que, por el contrario, el 21,2% de los sujetos consultados opinó que tal vez, demostrando inseguridad ante tal planteamiento. De ello es posible inferir que existe la oportunidad de mejora en los procesos de control para preservar el sigilo de la información concerniente al cliente y a la organización durante la atención de los reclamos bajo la modalidad de teletrabajo (Valverde , 2021).

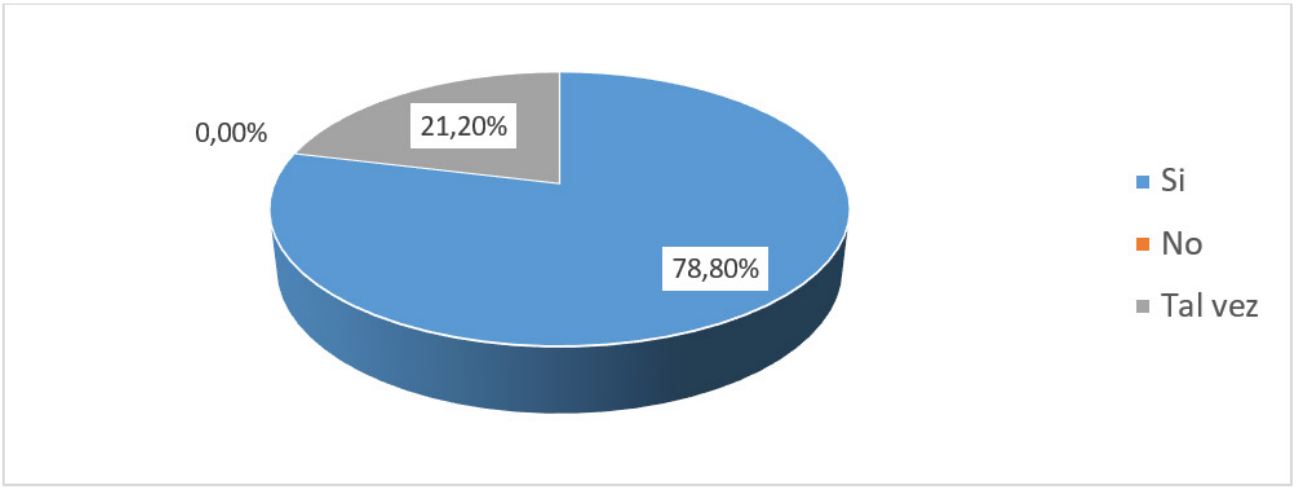

Figura 6. Flujo de información.

Fuente: Valverde, 2021

De acuerdo con los datos anteriormente analizados, se puede evidenciar la conveniencia de la gestión de control durante la atención de los reclamos mediante la modalidad de teletrabajo. Así de acuerdo a lo expuesto por García (2020) implica proveer soporte permanente al proceso decisorio en los niveles de gerenciamiento estratégico, táctico y operativo, por medio de la revisión de datos que conciernen los intereses del negocio.

Del mismo modo, a través de los resultados se evidencia la conveniente aplicación de

la modalidad de teletrabajo en los procesos de atención al cliente en el manejo de reclamos específicamente. En relación con ello, Páez et al. (2020) el teletrabajo es una alternativa laboral a distancia que emplea las tecnologías de la información y las comunicaciones.

Es una opción aplicada con mayor frecuencia como medida de prevención ante la nueva realidad luego de la pandemia. Según los resultados, el teletrabajo representa una opción de atención oportuna de los reclamos hechos por los clientes. Las instituciones financieras representan una pieza importante para la recuperación de la sociedad por lo que se amerita una idónea participación de su parte en la ayuda de los clientes.

Conclusiones

Una vez concluida la investigación se llega a las siguientes conclusiones principales. La nueva realidad impuesta en los diferentes sectores de la sociedad por la emergencia generada a causa del COVID-19, trajo consigo la necesidad de realizar cambios importantes en la manera de organizar la mayoría de los procesos y actividades. De acuerdo con esto, la atención al cliente en las entidades financieras fue una de las áreas con mayor impacto en este sentido. Particularmente, la atención de los reclamos fue una de las áreas con más necesidad de reformulación y adaptación según las nuevas exigencias del entorno y exigencias de los clientes.

Específicamente, para el caso del presente estudio el departamento de reclamos bajo la modalidad de teletrabajo, presenta falencias en cuanto al cumplimiento de su razón de ser, así como en el resguardo de la información durante la emergencia sanitaria. De acuerdo al análisis de los datos, se observa necesidad de capacitación del personal para la atención del cliente en telecommuting. Ciertamente, existe la oportunidad de redefinir las formas de trabajo, así como mejorar los controles para el resguardo de la información y mayor capacidad de respuesta ante las demandas de los usuarios. De esta manera, según los resultados recogidos se evidencia la necesidad de revisar y modificar los documentos en los cuales se establece el qué y el cómo de los procedimientos para la atención de reclamos bajo la modalidad de teletrabajo. Específicamente, merecen ser adaptados a la nueva realidad, el Código de ética, el manual de funciones y la estructura organizacional del departamento de reclamos de la entidad financiera. Atendiendo a las nuevas necesidades que presentan los clientes de la institución bancaria, cobra valor la modalidad de teletrabajo para la atención de reclamos de una manera eficiente y mediante el resguardo imprescindible de la información.

En este sentido, entre las consideraciones finales se puede mencionar que de acuerdo al nuevo contexto social que presentan las entidades financieras, en el cual es imprescindible reducir al mínimo posible la atención presencial en las diferentes sucursales; sumado además al objetivo de mantener la fidelidad del cliente; resulta preciso mantener la creación de entornos virtuales para la atención al cliente. Es así como, es de gran importancia el mejoramiento de respuesta a los reclamos de los usuarios, así como la preservación de la información de datos de los mismos durante dichos procesos. Siendo así la modalidad de teletrabajo oportuna y objeto de mejora continua, según la política de calidad de la institución.

Bibliografía

Cano, J., & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018. RISTI. Revista Ibérica de Sistemas y Tecnologías de Información, N° E27, 470-483.

Castro, P., Galarza, I., & Sánchez, S. (2017). Ventajas y desventajas del teletrabajo a nivel psicosocial. Tesis de Grado . Bogotá: Universidad Cooperativa de Colombia.

García, E. (2020). Desempeño del teletrabajador en el sector construcción en tiempos de Covid – 19 . CEIT, 5(5-1), 312-324.

Jácome, H. (2020). Análisis de la transformación digital de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno de la ciudad de Quito. Tesis de Grado. Quito: Universidad Politécnica Salesiana.

Lema, C., & Cuenca, J. (2020). Plan de gestión de seguridad de la información, caso de estudio: gobierno provincial del Cañar . Journal of Science and Research, 62-75.

Observatorio de Ciberseguridad. (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington, D.C.: Banco Interamericano de Desarrollo.

Páez, M., Chávez, M., Apunte, R., & Rosales, R. (2020). El teletrabajo en el Distrito Metropolitano de Quito (Ecuador): Normativa y características sustanciales. Revista Espacios, Vol. 41 (Nº 17), 7-15.

Sierra, S., & Murillo, J. (2020). Análisis del nivel de satisfacción por el uso de cajeros inteligentes de entidades bancarias en la ciudad de Guayaquil. Tesis de Grado. Guayaquil: Universidad Católica de Santiago de Guayaquil.

Valverde , D. (2021). Gestión de control bajo teletrabajo en las operaciones bancarias y seguridad de la información en el departamento de reclamos de una entidad finciera. Guayaquil: Universidad Laica Vicente Rocafuerte de Guayaquil.

Vargas, J. (2020). El teletrabajo: nueva modalidad laboral y una opción digital para las empresas y la sociedad . Revista ODIGOS, Vol. 1, Núm. 1, 1-12.

Vega, C., Grajales, H., & Montoya, L. (2017). Sistemas de información: definiciones, usos y limitantes . Orinoquia, vol. 21, núm. 1, 64-72.

CITAR ESTE ARTICULO:

Valverde Arcos, D. A., & Hurel Franco, G. P. (2021). Seguridad de la información de los reclamos en modalidad teletrabajo. RECIMUNDO, 5(4), 344-355. https://doi.org/10.26820/recimundo/5.(4).dic.2021.344-355