MediaInteractive

Pontificia Universidad Católica de Chile

TrenDigital think tank

HÁBITOS Y PERCEPCIONES EN CIBERSEGURIDAD Y PRIVACIDAD DE DATOS

¿Por qué este estudio?

La transformación digital en los espacios laborales, el incremento del trabajo remoto, el uso masivo de redes sociales y las cifras crecientes de transacciones online traen una serie de nuevos desafíos.

En los últimos meses hemos visto cómo grandes empresas han sido afectadas por ataques cibernéticos, cómo colaboradores han filtrado datos y que lamentablemente hoy son recurrentes los ataques de suplantación por técnicas de phishing.

Es por ello que quisimos saber un poco más sobre los hábitos y resguardos en materia de seguridad digital que están teniendo hoy los usuarios chilenos y su percepción de seguridad en su entorno laboral pero también en el área comercial.

Además, segmentamos la muestra diferenciando entre las distintas generaciones para ver si efectivamente tienen una percepción distinta los adultos de los más jóvenes.

Es importante clarificar que este reporte no es un test ni una evaluación de los los niveles de seguridad digital de las personas, sino que su foco es identificar las preferencias, tendencias y percepción de seguridad personal, laboral y comercial.

Para ello realizamos una encuesta a 1.120 personas con acceso a Internet a nivel nacional.

ESTE REPORTE SOBRE SEGURIDAD DIGITAL SE FOCALIZA EN TRES ÁREAS

Hábitos y preferencias

Prácticas digitales, conocimiento general de ciberseguridad y privacidad de datos en Chile

Percepción como colaboradores

Percepción de los colaboradores sobre las medidas de seguridad digital aplicadas en las organizaciones

Percepción como clientes y consumidores

Percepción de los clientes y ciudadanos respecto a la gestión de las empresas en materia de ciberseguridad

1° dimensión

HÁBITOS Y PREFERENCIAS EN MATERIA DE SEGURIDAD DIGITAL

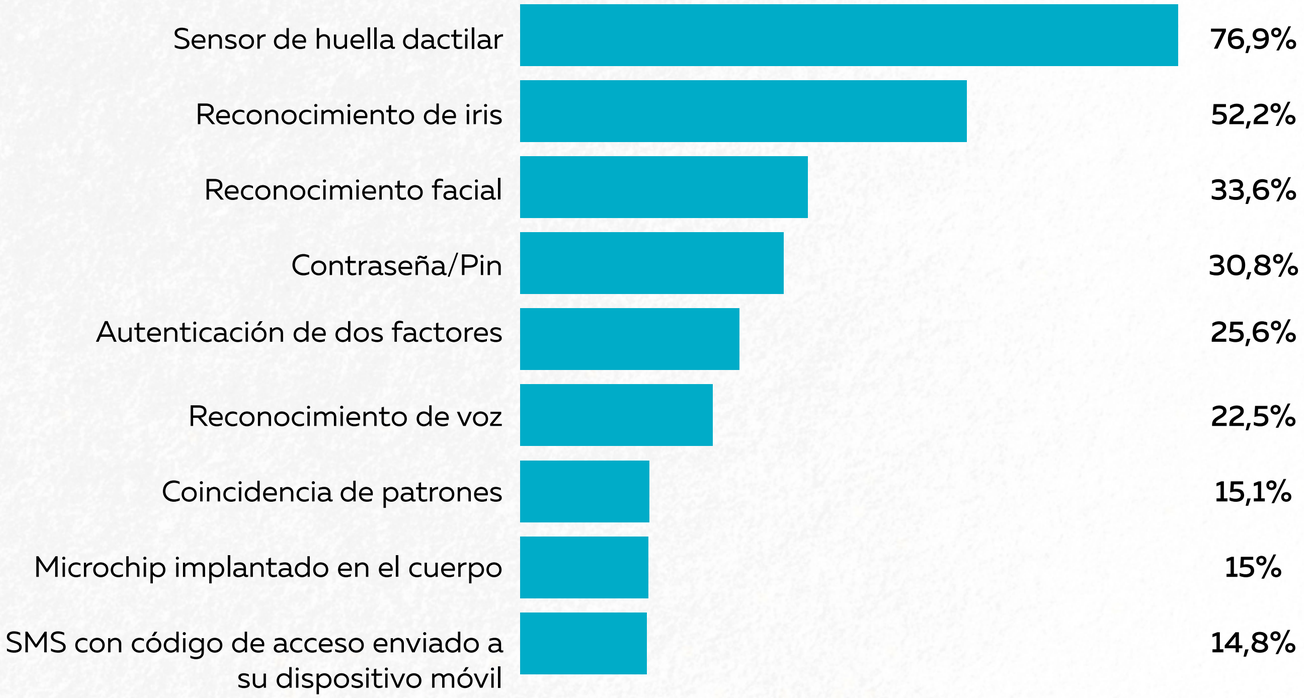
A CONTINUACIÓN SE MENCIONA UNA LISTA DE TECNOLOGÍAS DE BLOQUEO Y ACCESO PARA DISPOSITIVOS, POR FAVOR INDICA SI LAS CONOCES Y UTILIZAS

De lo anterior se observa que el uso de contraseña o pin es la tecnología de acceso y bloqueo más utilizada y conocida entre los participantes.

Un dato importante a destacar es la introducción de tecnologías como el reconocimiento de voz, facial o iris, que si bien aún no son muy utilizadas, ya son conocidas por las personas, por lo tanto no sorprendería que en los próximos años sean tecnologías que adquieran cada vez mayor relevancia para resguardar la seguridad de los dispositivos.

	NO LA CONOZCO	LA CONOZCO, PERO NO LA USO	LA USO
Contraseñas/pin	1,5%	16,3%	82,2%
SMS con código de acceso de un solo uso enviado a su dispositivo móvil	12,5%	23,4%	64,2%
Sensor de huella dactilar	1,9%	37,6%	60,5%
Autentificación de dos factores (Ej: Contraseña+código por SMS)	12,3%	31,8%	55,9%
Coincidencia de patrones	19,7%	33,2%	47,1%
Reconocimiento de voz	10,3%	76,8%	12,9%
Reconocimiento facial	10,8%	79,2%	10%
Reconocimiento de iris	17,9%	76,9%	5,2%

PENSANDO EN LOS PRÓXIMOS 5 AÑOS, INDICA LOS TRES MÉTODOS DE AUTENTIFICACIÓN/ IDENTIFICACIÓN QUE MÁS TE GUSTARÍA UTILIZAR PARA ACCEDER A TUS DISPOSITIVOS Y CUENTAS PERSONALES



Observando las tendencias para los próximos 5 años, el sensor de huella dactilar sería la tecnología preferida como método de autentificación, a lo que se suma el reconocimiento de iris y facial, tal como se advertía anteriormente. De esta manera, la contraseña y pin, tecnología actualmente más utilizada, sería desplazada, según lo indicado por los participantes del estudio.

Con respecto a las potenciales nuevas tendencias, como la tecnología de microchip implantado en el cuerpo, aún sería considerado un dispositivo lejano a hacerse realidad en la vida cotidiana de las personas.

MediaInteractive

Pontificia Universidad Católica de Chile

TrenDigital think tank

EL DESARROLLO DE TECNOLOGÍAS DE LOS ÚLTIMOS AÑOS HA GENERADO UNA SERIE DE VENTAJAS PARA LA SOCIEDAD, PERO TAMBIÉN SE HA CONVERTIDO EN UN FOCO DE VULNERABILIDADES Y RIESGOS:

¿Alguna vez te has enfrentado a las siguientes situaciones de peligro cibernético? (marque todas las opciones que consideras necesarias)

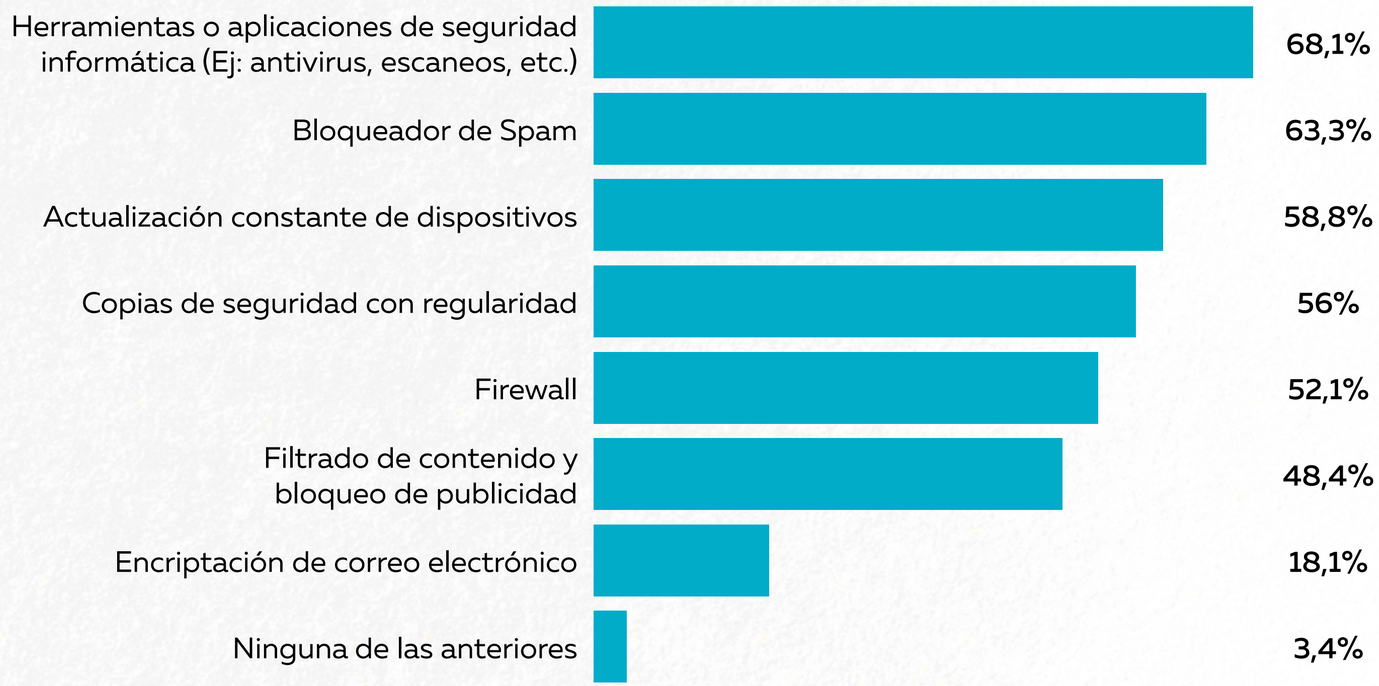
Tener un dispositivo infectado por un virus u otra amenaza a la seguridad	59,6%
Acceso no autorizado a correo electrónico o cuenta de redes sociales	33,6%
Un email, mensaje de texto u otro mensaje que haya ocasionado la descarga de malware a dispositivo	32,1%
Cargos fraudulentos en tarjetas de crédito o débito	24,4%
Víctima de robo de identidad o datos personales	15,8%
Haber sido notificado que información personal estuvo involucrada en una violación de datos	13,8%
Hacer click en un correo electrónico fraudulento o proporcionado información confidencial (personal / financiera) en respuesta a un correo electrónico fraudulento	11%
Compra en línea que resultó ser una estafa	10%
Información financiera comprometida como resultado de comprar por Internet	7,4%

La infección a dispositivos tecnológicos debido a la entrada de un virus u otro tipo de amenaza informática es reconocido como la situación más recurrente de peligro cibernético. Seguido de accesos no autorizados, principalmente a correos electrónicos y redes sociales.

Cabe destacar que situaciones en donde la información financiera en Internet se vea comprometida aún representa un peligro menos recurrente.

Por último, es importante establecer que solo un 18,6% dijo que nunca ha tenido un problema de los que se presentaron. Esto quiere decir que una gran parte de la población ha sido afectada por amenazas cibernéticas.

¿CUÁL(ES) DE LOS SIGUIENTES ELEMENTOS APLICAS ACTUALMENTE EN TUS DISPOSITIVOS PERSONALES O PROGRAMAS QUE UTILIZAS -TELÉFONO, COMPUTADOR, EMAIL, TABLET, ETC. ? (SELECCIONE TODOS LOS QUE CORRESPONDAN)

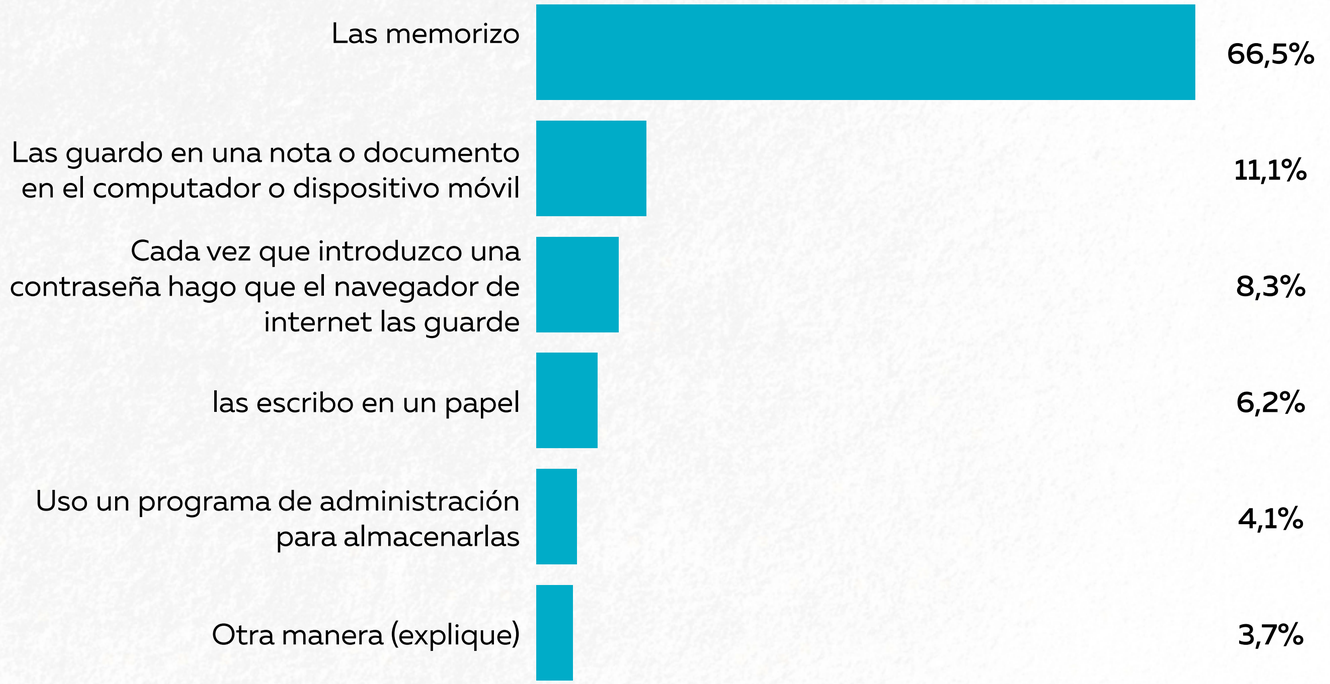


Si bien han ido emergiendo nuevas tecnologías y prácticas para resguardar la seguridad digital, las herramientas tipo anti-virus siguen siendo las más utilizadas. Esta preferencia puede explicarse por dos razones. Por una parte, destaca entre las tecnologías de resguardo a ataques cibernéticos más conocida y antigua. Pero por otra parte, también presentan una accesibilidad muy alta, ya sea porque viene ya instalada en algunos dispositivos o porque es fácil utilizar en dispositivos móviles. Es interesante que solo el 3,4% dijo no tener ninguno de los elementos de seguridad o protección.

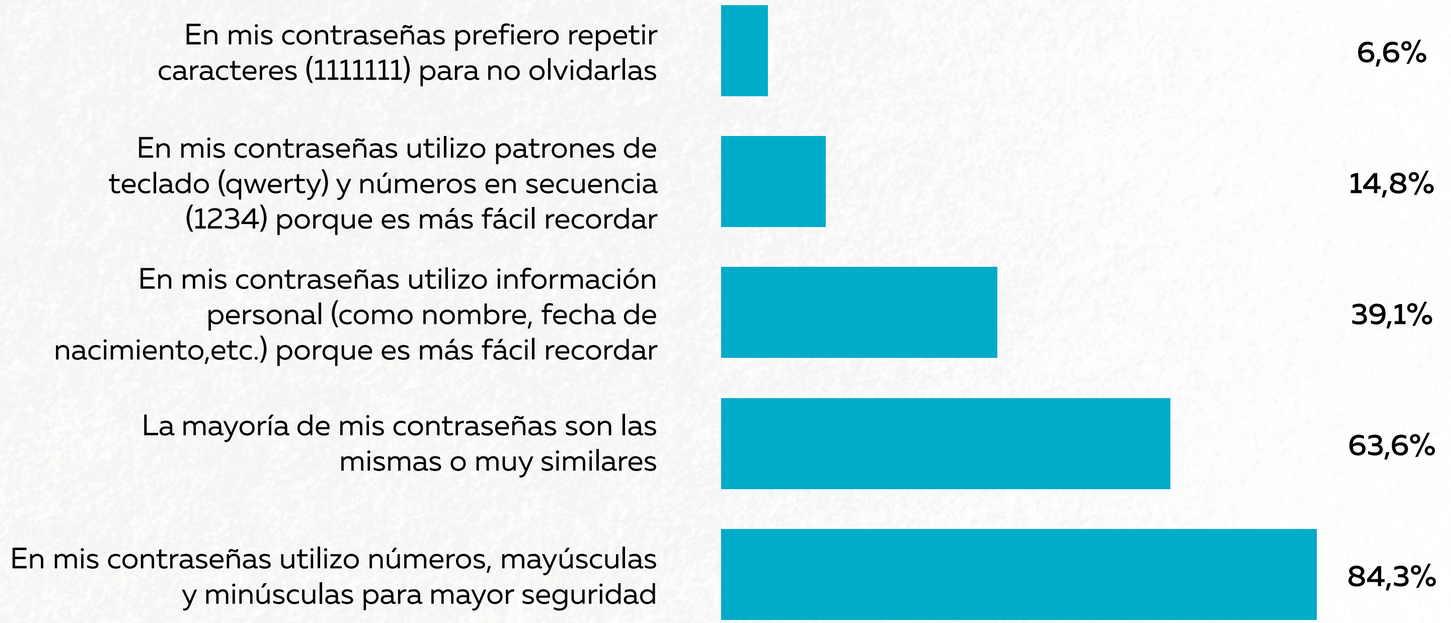
PENSANDO EN TU ACTIVIDAD EN MEDIOS DIGITALES, APLICACIONES Y SITIOS WEB, ¿CÓMO MANEJAS TUS CONTRASEÑAS? ESCOGE LA PRINCIPAL.

La memorización de las contraseñas es por lejos el método más utilizado para manejar las contraseñas en el entorno digital. Lo que en parte sería positivo debido a lo complejo de acceder a esta información por terceros.

No obstante, resulta preocupante que algunas personas guarden sus contraseñas en una nota o documento en sus dispositivos, pues frente a cualquier eventualidad, la información confidencial robada podría ser de gran magnitud.

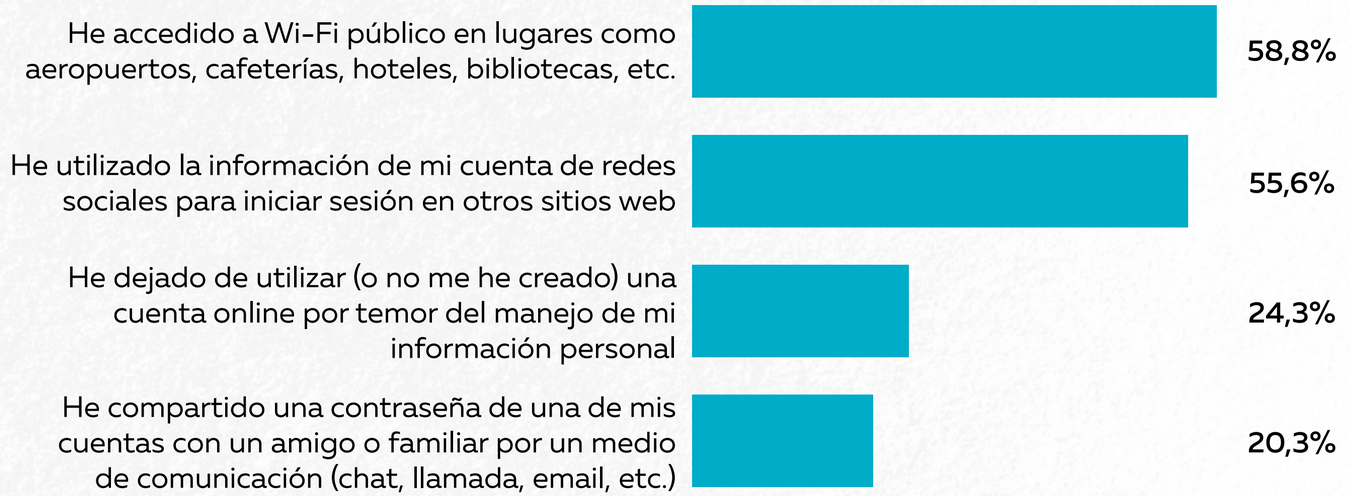


PENSANDO EN LA CONSTRUCCIÓN DE TUS CONTRASEÑAS, ¿ESTÁS DE ACUERDO CON LAS SIGUIENTES AFIRMACIONES?:



Se observan dos grandes tendencias. Por una parte es relevante el hecho que los participantes hoy estén construyendo contraseñas seguras, lo que se ve reflejado en el hecho que no se están utilizando caracteres repetidos o patrones muy similares para que no se les olvide. Sin embargo, por otra parte se ve que un porcentaje importante de usuarios utiliza contraseñas iguales o similares, lo que evidentemente podría significar un retroceso en materias de seguridad, pues el peligro ante la eventualidad de que esta única contraseña sea descifrada puede ser importante.

PENSANDO EN TU CONDUCTA DIGITAL DE LOS ÚLTIMOS 6 MESES: ¿HAS REALIZADO LAS SIGUIENTES ACCIONES?



Se puede observar que más de la mitad de los participantes se ha conectado a una red pública en los últimos meses, así como también ha utilizado información de sus cuentas de redes sociales para acceder a otros sitios.

Esta última práctica responde a una tendencia en alza en la creación de sitios web y aplicaciones, pues mediante el login de cuentas de redes sociales es posible entrar sin la necesidad de tener que registrarse o hacer una cuenta. Si bien esto en términos prácticos es una facilidad y ahorra tiempo, no tomar los resguardos necesarios, sobre todo cuando se desconoce el origen de los sitios a los cuales se accede, puede ser un peligro para la información y datos personales. Esto es aún más relevante al ver las vulneraciones de las cuentas en redes sociales durante el último tiempo.

¿CUÁN PROBABLE ES QUE CONECTADO A UNA RED PÚBLICA (AEROPUERTOS, CAFETERÍAS, HOTELES, BIBLIOTECAS) REALICES LAS SIGUIENTES ACCIONES:

	NADA PROBABLE + ALGO PROBABLE	NEUTRAL	PROBABLE + MUY PROBABLE
Acceder a redes sociales	23,9%	5,5%	70,6%
Utilizar correo electrónico	23,5%	6,1%	70,5%
Consultar cuentas bancarias	72,3%	6,6%	21,2%
Enviar archivos y documentos confidenciales	68,8%	10,3%	20,9%
Realizar transferencias bancarias	73,4%	6,7%	19,9%
Compras en línea	81,6%	6,2%	12,2%

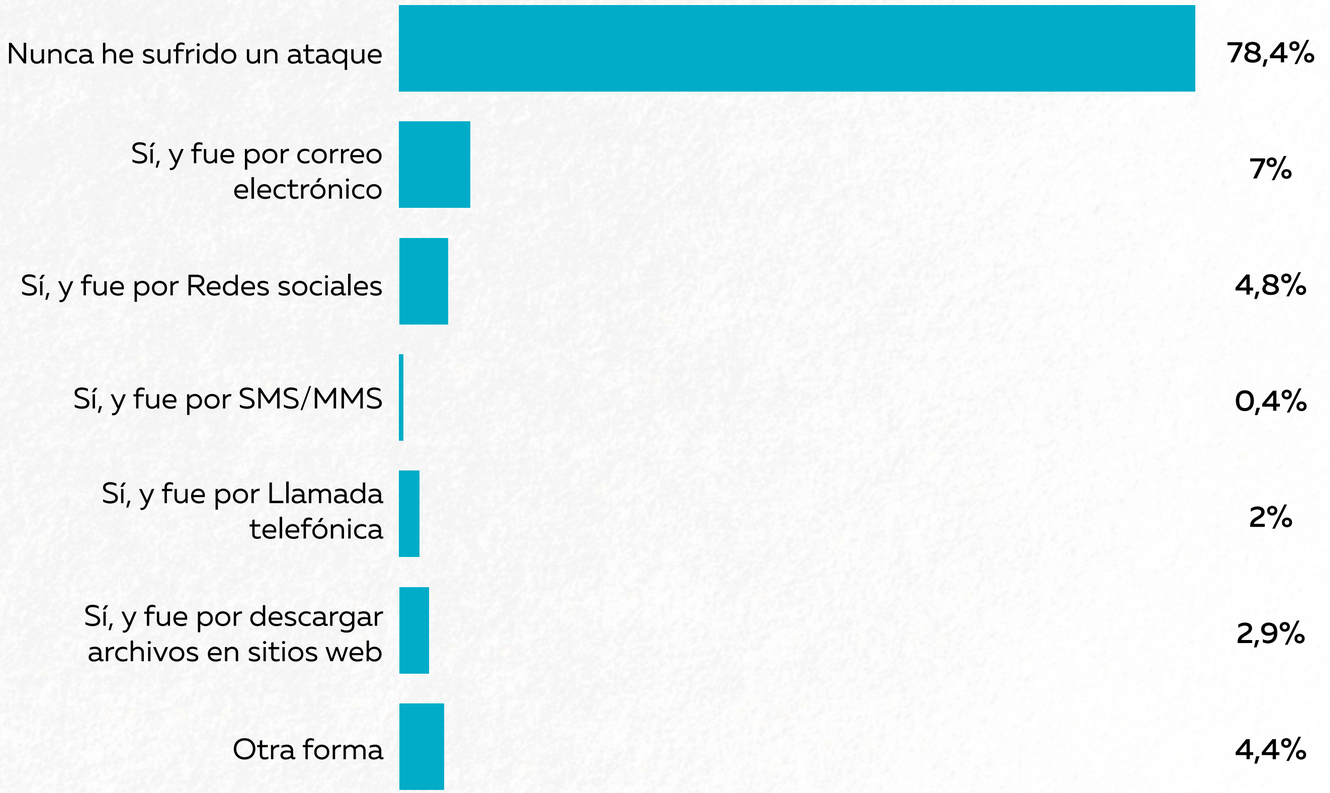
Es interesante observar que más del 80% indica que es poco probable que realice compras en línea mientras está conectado a redes públicas. Del mismo modo, realizar transferencias o consultas bancarias son acciones que aparentemente se evitarían estando bajo esta conexión, a pesar que casi el 20% ve muy probable realizar este tipo de acciones.

Contrario a lo anterior, el uso de redes sociales y correo electrónico no serían acciones limitadas al estar conectado a una red wifi pública.

Por lo tanto, se puede inferir que acciones en donde se ve involucrada información financiera se evitarían en conexiones no seguras, no obstante, la transferencia de información social o personal (no financiera) no sería percibida como un problema por los usuarios.

¿HAS SIDO VÍCTIMA DE UN ATAQUE CIBERNÉTICO O DE ROBO DE DATOS PERSONALES? DE SER ASÍ, ¿POR CUÁL MEDIO SUFRISTE EL ATAQUE?

Los datos muestran que un poco más de 20% de los encuestados declaró haber sido víctima de un ciberataque, siendo el correo electrónico como el principal medio por el cual se inició la amenaza cibernética.



2° dimensión

PERCEPCIÓN DE LOS COLABORADORES SOBRE LAS MEDIDAS DE SEGURIDAD DIGITAL APLICADAS EN LAS ORGANIZACIONES

PENSANDO EN EL LUGAR DE TU TRABAJO POR FAVOR RESPONDE LAS SIGUIENTES PREGUNTAS:

Uno de los aspectos más relevantes es la falta de conciencia que existe entre la información de tipo personal y laboral que hoy existe entre los trabajadores en el país, ya que a pesar de ser el porcentaje más alto, solo alcanza a un poco más de la mitad de los entrevistados. Esto se ve con mayor evidencia en que solo el 55,1% de las organizaciones tienen políticas de desarrollo claras en la materia.

Lo interesante es que solo un tercio de los encuestados cree que las medidas de seguridad que se han adoptado son suficientes, y lo decepcionante es que solo un 31,2% ha recibido capacitaciones para aminorar los riesgos, a pesar que el 26,1% dijo que su empresa ha sido vulnerada de alguna forma.

De lo anterior se desprende que, al parecer, las empresas están esperando que algo suceda para reaccionar en estos temas.

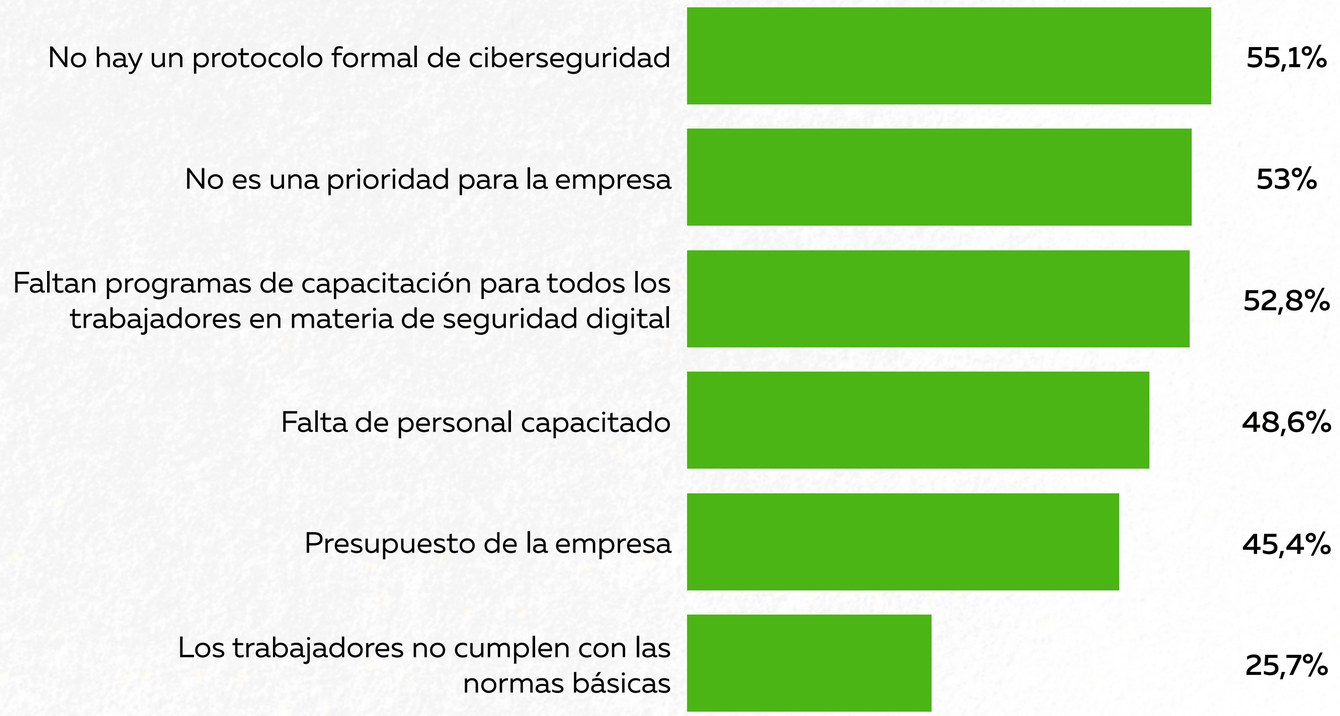
¿Se toman medidas de seguridad para separar la información y aplicaciones corporativas de los datos personales en los dispositivos de uso personal?	57,1%
¿La organización para la cual trabajas cuenta con políticas y/o medidas de seguridad digital claras?	55,1%
¿Tu organización o empresa ha tomado alguna medida de prevención en materia de seguridad digital diferente en los últimos 12 meses?	47,5%
¿Crees probable que la empresa para la cual trabajas pueda sufrir una amenaza cibernética o robo de datos en los próximos 12 meses?	46,1%
¿Consideras que las medidas de seguridad digital implementadas en tu organización son suficientes?	33,3%
¿Su empresa cuenta con un plan de educación en seguridad digital para los trabajadores, o has recibido alguna capacitación sobre conductas apropiadas para minorizar riesgos?	31,2%
¿Tu organización o empresa ha experimentado algún tipo de vulnerabilidad en seguridad digital en los últimos 12 meses?	26,1%

MediaInteractive

Pontificia Universidad Católica de Chile

TrenDigital think tank

EN MUCHAS EMPRESAS Y ORGANIZACIONES LAS MEDIDAS DE SEGURIDAD DIGITAL NO SON SUFICIENTES. AL CONSULTARLES SOBRE LAS RAZONES QUE PODRÍAN EXPLICAR ESTA BAJA PERCEPCIÓN DE SEGURIDAD, LOS DATOS MUESTRAN QUE EL FENÓMENO ES MÁS COMPLEJO DE LO QUE SE CREE.



MediaInteractive

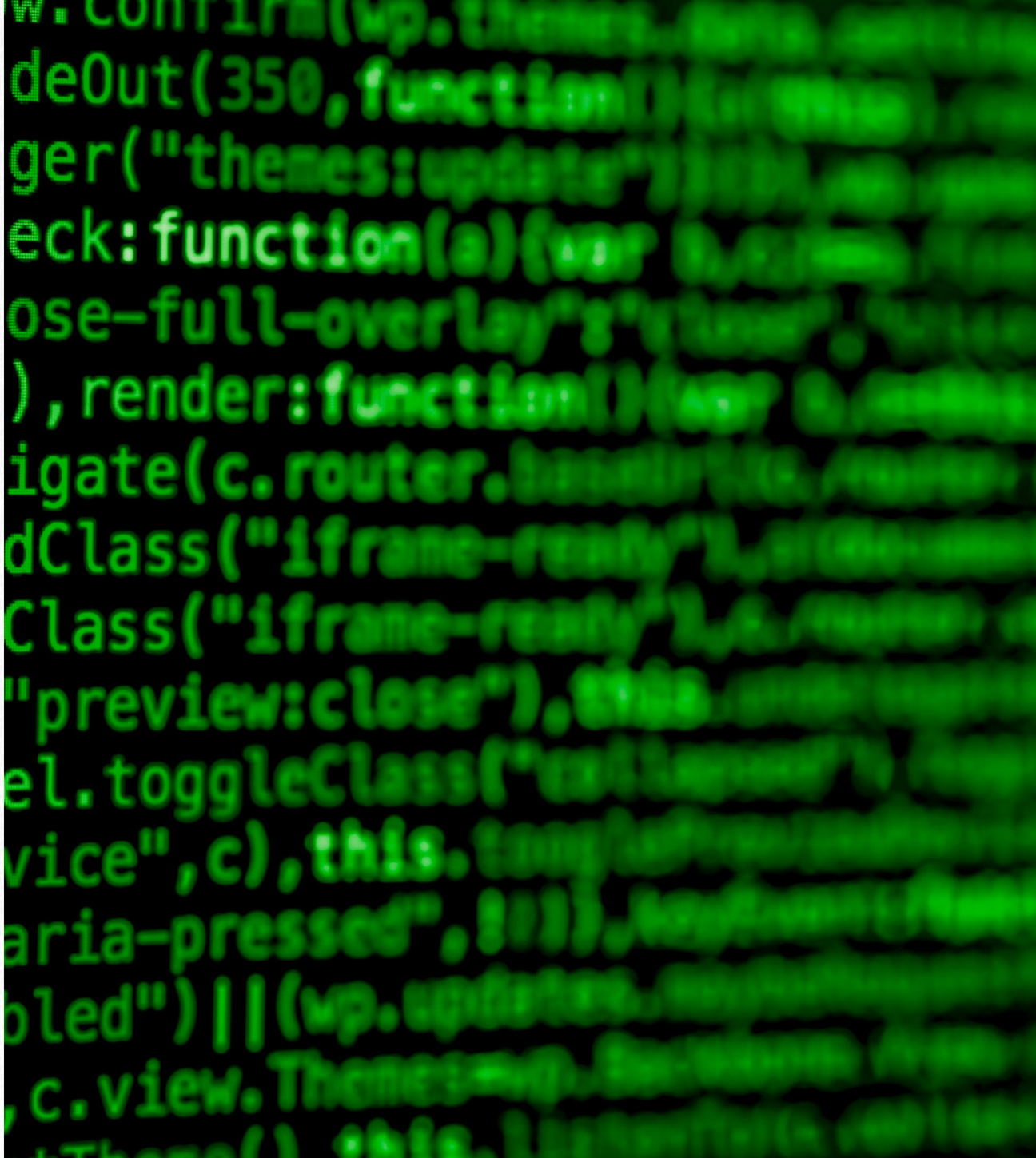
Pontificia Universidad Católica de Chile

TrenDigital think tank

A pesar que se podría pensar que el presupuesto de la empresa es el principal obstáculo para la implementación y desarrollo de seguridad digital, la falta de protocolo formal, así como la escasez de programas de capacitaciones para los trabajadores, se encuentran entre las principales razones que declaran los colaboradores para explicar la falta de seguridad digital.

Si bien ambos elementos dependen de recursos financieros, también hablan de la necesidad de trabajar las herramientas de las empresas, no sólo los aspectos tecnológicos.

Como segunda razón se menciona la baja prioridad que ocupa la seguridad digital para la empresa. Pues aparentemente, aún es un tema relativamente nuevo, a pesar de los riesgos que conlleva.



CON RESPECTO A LA PERCEPCIÓN DE LAS POLÍTICAS DE EXISTENTES, LOS DATOS TAMBIÉN MUESTRAN PROBLEMAS.

	MUY EN DESACUERDO + EN DESACUERDO	NI DE ACUERDO, NI EN DESACUERDO	DE ACUERDO + MUY DE ACUERDO
Las políticas de seguridad digital en las organizaciones son difíciles de entender	28,6%	34,6%	36,7%
Deberían existir más iniciativas de educación en seguridad digital para los trabajadores	3,1%	4,4%	92,6%
Las políticas de seguridad digital en las organizaciones permiten realizar el trabajo de forma eficiente	10,5%	28,2%	61,3%
Las políticas de seguridad digital de las organizaciones permiten ser proactivo, es decir, proponer e implementar nuevas ideas	18,6%	36,7%	44,8%
Las políticas de seguridad digital en las organizaciones son permisivas	29,4%	43,5%	27,1%
Las políticas de seguridad digital en las organizaciones son restrictivas e impiden que realice adecuadamente mi trabajo	39,5%	36,2%	24,2%

Nuevamente aparece la necesidad de más iniciativas de educación en seguridad digital para los trabajadores, estando de acuerdo y muy de acuerdo casi un 93% de la muestra.

En el desglose se puede observar que un 36,7% está de acuerdo o muy de acuerdo con que las políticas de seguridad digital en las organizaciones son difíciles de entender, sin embargo, un 61.3% indica que éstas le permiten realizar el trabajo de forma eficiente, y por tanto, no impiden que el trabajo se realice adecuadamente.

Por otra parte, se puede observar que un número importante de usuarios opta por una declaración neutra, lo que puede responder a 2 factores: temor a ser reconocido dando una crítica respecto a su trabajo (a pesar de que se advierte desde un comienzo el resguardo de identidad del estudio), y por otra, a la falta de conocimiento en la materia.

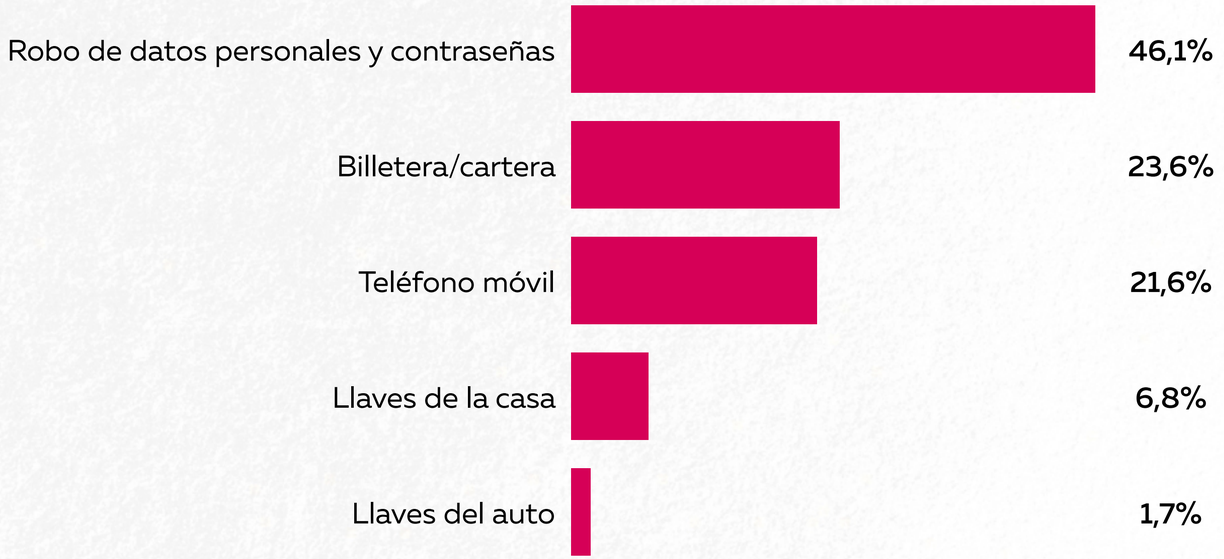
3° dimensión

CONDUCTAS Y PERCEPCIÓN EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE DATOS COMO CIUDADANOS Y CONSUMIDORES

¿CUÁL DE LOS SIGUIENTES ELEMENTOS TE PREOCUPARÍA MÁS SI TE FUERAN SUSTRAÍDOS?

Frente al caso hipotético de enfrentarse a una situación de robo, la mayor preocupación que presentan las personas hoy, es el robo de datos personales y contraseñas, mucho más que objetos físicos como las llaves del auto, el teléfono e incluso la billetera. Esto implica que las personas hoy tienen muchos de sus aspectos relevantes en sus dispositivos o cuentas.

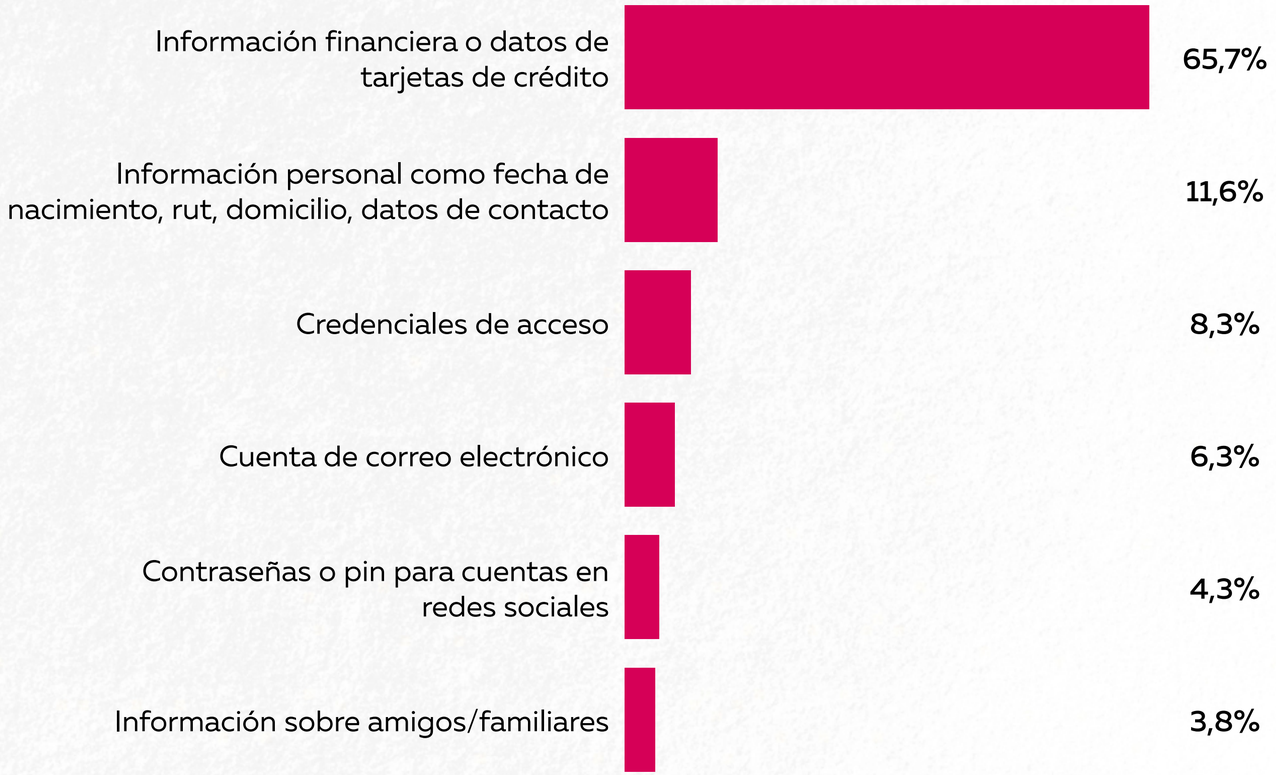
El fenómeno anterior también responde a un cambio social importante en la percepción de seguridad, que se debe en gran parte a la digitalización de la moneda y la posibilidad de las transacciones comerciales online, ante lo cual el resguardo de los datos personales y las contraseñas son clave.



ANTE UN ATAQUE CIBERNÉTICO ¿QUÉ INFORMACIÓN SERÍA LA QUE MÁS TE PREOCUPARÍA PERDER?

Frente a un ataque cibernético, las personas declaran que el robo de información financiera o de datos de la tarjeta de crédito son ampliamente la principal preocupación. Más que información personal, de familia o amigos.

La baja importancia al robo de estas últimas puede responder en gran parte, a que hoy la mayoría de las personas tiene un perfil en una cuenta de red social, por tanto, el valor de esa información ha disminuido, pues se piensa que todos tienen acceso fácilmente a aquello. Es decir, la información personal hoy es pública, en consecuencia, no hay una gran preocupación de que ésta se filtre, no así, la información financiera.



¿CUÁN SEGURO TE SIENTES AL USAR LOS SIGUIENTES SITIOS WEB Y/O APLICACIONES DE LAS SIGUIENTES ORGANIZACIONES?

	MUY INSEGURO + INSEGURO	NI SEGURO, NI INSEGURO	SEGURO + MUY SEGURO
De bancos o instituciones financieras	12,2%	18,02%	69,8%
De servicios básicos (energía, agua, gas)	11,5%	30,26%	58,3%
De organizaciones de servicios gubernamentales	17,55%	29,16%	53,3%
De grandes tiendas para compras online (Retail)	22,4%	29,18%	48,4%
Del lugar en que trabajas o estudias	14,3%	36,01%	49,6%
De redes sociales (Facebook, Instagram, Whatsapp, etc.)	37,7%	32,61%	29,7%
De tiendas online de pymes	34,4%	43,42%	22,3%

Respecto a la percepción de seguridad al utilizar ciertos sitios web o aplicaciones, las instituciones financieras son las que presentan la mejor apreciación, alcanzando casi un 70% entre la declaración de seguro y muy seguro.

Por otra parte, las redes sociales se encuentran entre las peor evaluadas en cuanto a la percepción de seguridad. Algo que sin duda pone en alerta la necesidad de educación digital, pues son los sitios web de mayor uso a nivel nacional, espacio en donde las personas comparten día a día datos, ubicaciones, información personal, información laboral, etc.

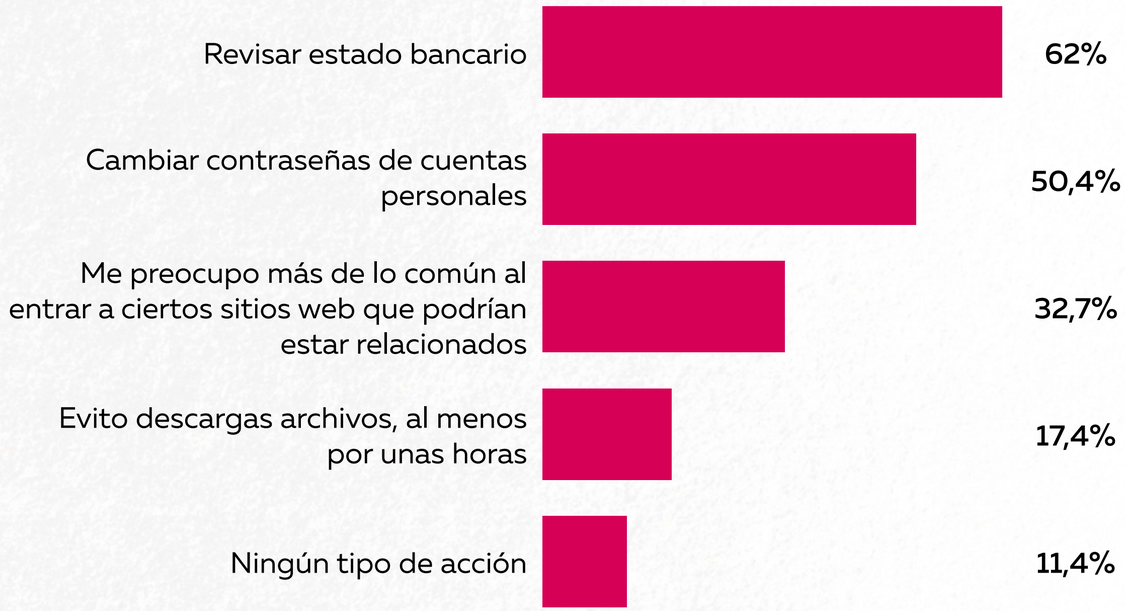
SI UNA DE LAS EMPRESAS O MARCAS DE LA QUE ERES CLIENTE SUFRIERA UNA VIOLACIÓN DE DATOS, ¿CUÁL DE LAS SIGUIENTES AFIRMACIONES REFLEJA CON MAYOR PRECISIÓN TU RELACIÓN CON ESA MARCA / NEGOCIO?

Sólo un 2,9% de los participantes declara una actitud neutra al enterarse de que la empresa de la cual es cliente sufre algún tipo de violación de datos.

Más de un cuarto afirma que reevaluaría sut relación con la empresa, mientras un 20,9% declara que dejaría de ser cliente y comprar sus servicios.

Sin duda un punto a considerar para mantener la reputación de marca, de lo contrario, la gran inversión en marketing y negocios podría verse afectada por el descuido en materia de seguridad digital.

PENSANDO EN LOS ÚLTIMOS ATAQUES CIBERNÉTICOS MASIVOS Y QUE HAN AFECTADO A ALGUNAS EMPRESAS DEL PAÍS, ¿QUÉ TIPO DE ACCIONES HAS REALIZADO, INDISTINTAMENTE SI ERES CLIENTE O NO DE LA EMPRESA AFECTADA? (MARQUE LAS QUE CREAS NECESARIO)

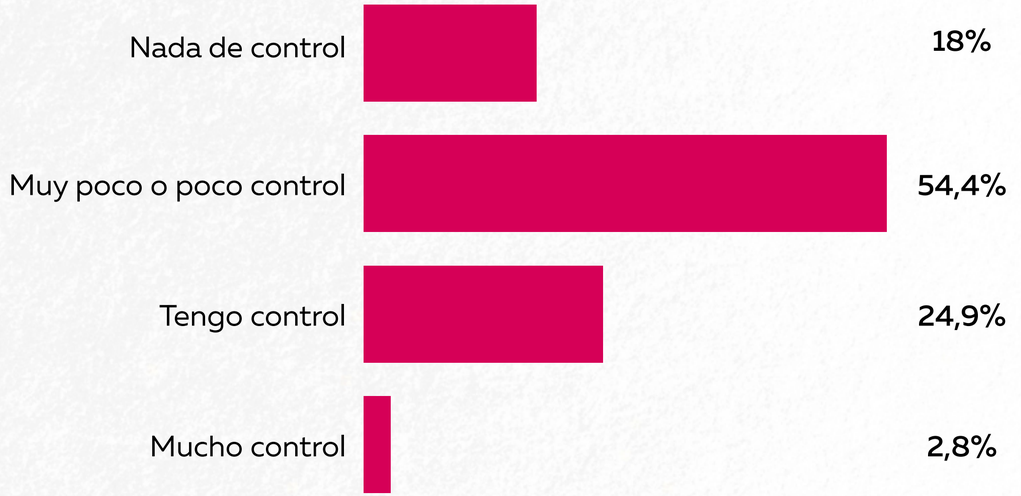


Las reacciones de los encuestados dan cuenta que, sin mencionar el tipo de ataque o amenaza en cuestión, un 62% revisó su estado bancario, indistintamente de si era o no cliente de la empresa afectada. Y sólo un 11,4% no realizó ningún tipo de acción.

Esto habla de una concepción de globalidad en los ataques cibernéticos. Es decir, se entenderían como golpes que no actúan de manera aislada, y por tanto, a pesar de estar lejano a la amenaza, surgiría cierto temor a ser afectado de alguna u otra manera, y por tanto, se reaccionaría tomando algunas acciones al respecto.

Esta concepción de globalidad y expansión de los ataques digitales, responde, quizás, a su soporte y medio digital, el cual no tiene límites tan definidos, ampliándose la concepción de los posibles daños generados.

PENSANDO AHORA COMO CONSUMIDOR DE BIENES O SERVICIOS ¿CREES QUE TIENES CONTROL SOBRE TU INFORMACIÓN PERSONAL QUE CIRCULA EN INTERNET?



Respecto a la percepción del grado de control de la información personal, más de la mitad indica la opción muy poco o poco, y sólo un 2,8% cree tener mucho control.

Estas estadísticas dan cuenta de la sensación de pérdida del manejo de la información personal que circula en Internet, concepción generada en gran parte por que la era digital se ha ido configurando como espacio privado y público. Ello también podría generarse porque los usuarios exhiben su información personal o aquella que se considera íntima en medios digitales sin grandes cuestionamientos, espacios en los cuales a pesar de sus cláusulas de privacidad, la información es fácilmente transferible y vendible.

EN RELACIÓN A LAS PRÁCTICAS Y MEDIDAS DE SEGURIDAD DIGITAL ANTE UN ATAQUE CIBERNÉTICO, INDIQUE SU GRADO DE ACUERDO CON LAS SIGUIENTES DECLARACIONES:

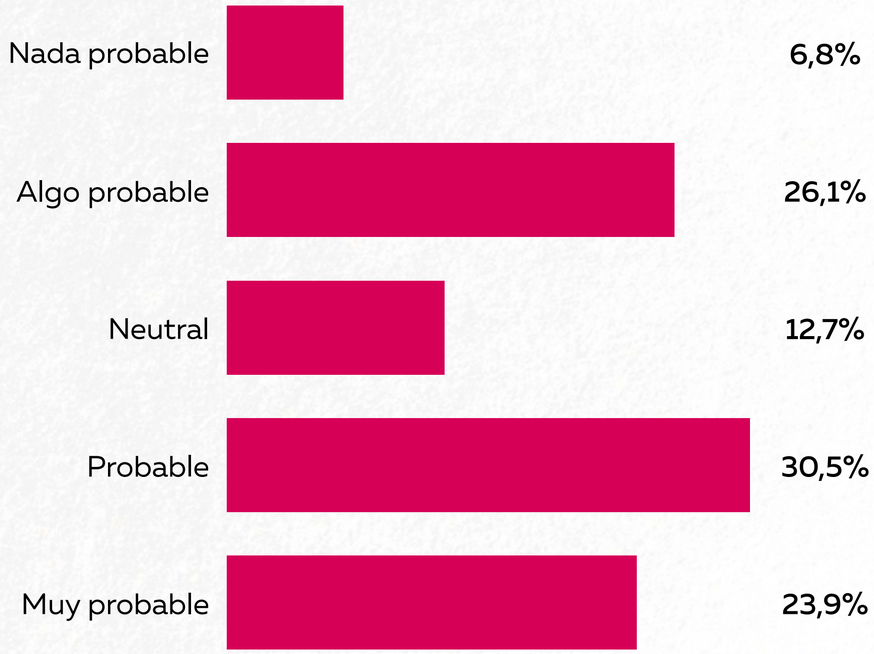
	MUY EN DESACUERDO + EN DESACUERDO	NI DE ACUERDO, NI EN DESACUERDO	DE ACUERDO + MUY DE ACUERDO
Las empresas deberían notificar a los consumidores frente a un ataque informático	1,6%	1,1%	97,4%
Las empresas deberían explicar detalladamente lo sucedido y cómo será resuelto	2%	3,5%	94,6%
Las empresas deberían explicar de manera clara y sencilla las políticas de privacidad vigentes	2,5%	4%	93,6%
Las empresas deberían compensar a sus víctimas frente a un ataque informático	2,1%	7,5%	90,4%
Las empresas deberían proporcionar pruebas de que el sistema funciona correctamente	2,4%	8%	89,6%
Lo primero que debería hacer una empresa es pedir disculpas públicas por lo sucedido	5,6%	11%	83,4%
Las empresas deberían educar en materias de seguridad a sus clientes	3,3%	9,9%	86,8%
Las empresas deberían ofrecer servicios de seguridad complementarios	11,6%	12,7%	75,7%

Respecto a las acciones que las empresas deberían tomar al ser vulnerados, un alto porcentaje de los encuestados está de acuerdo o muy de acuerdo en que deben notificar a los consumidores. Seguido de la explicación en detalle de lo sucedido y la forma en que el problema será resuelto. Es decir, los usuarios hoy quieren que las empresas les respondan y de forma directa frente a los eventos que los afectan. Es más, más del 80% de los encuestados cree que lo primero que debería hacer la empresa es pedir disculpas por lo sucedido, lo que implica que de cierta forma le asignan cuotas de responsabilidad.

Los datos muestran lo importante que es la comunicación y la transmisión de información ante eventuales amenazas. Hoy los consumidores tienen un amplio acceso a información, y muchas veces están mejor preparados que los mismos colaboradores de las empresas. Ante esto, ellos exigen una respuesta contundente en donde se les entregue una solución, o al menos, los pasos que se seguirán. Comunicación e información al cliente son clave en momentos de crisis. Por tanto, se torna fundamental tener un protocolo de acción en materia de ciberamenazas para poder responder y actuar.

¿CUÁN PROBABLE ES QUE DEJES DE ADQUIRIR PRODUCTOS Y/O SERVICIOS DE UNA EMPRESA POR MEDIO ONLINE, LUEGO DE ENTERARTE QUE FUE AFECTADA POR UN ATAQUE CIBERNÉTICO?

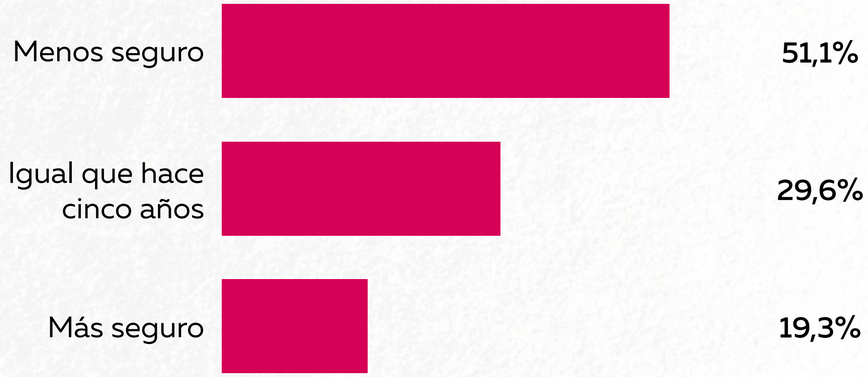
Más de la mitad de los participantes del estudio da cuenta que es probable o muy probable que deje de adquirir productos de una empresa al enterarse de que ésta fue afectada por un ataque cibernético.



¿CÓMO TE SIENTES RESPECTO A TU SEGURIDAD DE INFORMACIÓN PERSONAL COMPARADA CON LA DE HACE CINCO AÑOS?

Al comparar la sensación de seguridad de información personal actual con la de hace 5 años, más de la mitad indica sentirse menos seguro.

Esto puede ser originado no sólo por la sensación de estar expuesto a más troyanos y otras amenazas, sino que también, por la integración de lo digital a nuestras vidas. Cada vez se vuelve más difícil pensar en acciones y prácticas que no requieran de la transferencia de datos personales por medios digitales.



SEÑALA TU GRADO DE ACUERDO CON LAS SIGUIENTES DECLARACIONES:

Respecto a algunas apreciaciones en materia de seguridad digital, un número importante de participantes indicó estar de acuerdo o muy de acuerdo con que el gobierno debería desarrollar más iniciativas en materia de seguridad digital. Es interesante que las personas le asignan mayor responsabilidad al gobierno que a las empresas o que incluso a ellos mismos, por lo que se podría advertir que probablemente se instalará como un tema país desde la voz de los mismos ciudadanos.

Además, a pesar de la incriminación constante a las empresas comerciales y organizaciones por vulnerar la seguridad y privacidad de datos, reconocen una responsabilidad compartida para el resguardo de ésta.

Es más, para casi el 80% de los encuestados la seguridad cibernética y la vulneración de la privacidad de datos personales se encuentran entre los mayores riesgos que enfrenta la sociedad actual.

	MUY EN DESACUERDO + EN DESACUERDO	NI DE ACUERDO, NI EN DESACUERDO	DE ACUERDO + MUY DE ACUERDO
Es responsabilidad de los ciudadanos y consumidores resguardar sus datos personales y la información que comparten en medios digitales	17,2%	19,2%	63,5%
El gobierno/Estado debería desarrollar más iniciativas en materia de seguridad digital y uso de los datos personales de los ciudadanos	1,8%	7,6%	90,6%
Es responsabilidad compartida de las empresas y los consumidores resguardar la seguridad y privacidad de los datos	9,8%	10%	80,2%
La seguridad cibernética y la vulneración de la privacidad de datos personales se encuentran entre los mayores riesgos que enfrenta la sociedad actual	6,9%	13,6%	79,5%
Es responsabilidad exclusiva de las empresas garantizar la privacidad de los datos de los consumidores y clientes	18,4%	20,5%	61,1%
Las empresas privadas están mejor equipadas que el gobierno para proteger los datos y privacidad de las personas	22,7%	38,2%	39%

ANÁLISIS SEGÚN GENERACIONES (TRAMO DE EDAD)

MANEJO DE CONTRASEÑAS SEGÚN TRAMO DE EDAD

Si bien se podría pensar que los más jóvenes serían más precavidos en la creación de contraseñas para no utilizar información personal, patrones de secuencia o similitud entre ellas, se ve todo lo opuesto: los mayores se preocupan casi el doble de los más jóvenes.

Si bien es difícil entender este aspecto, una posible explicación es que la sensación de inseguridad aumenta con la edad o que simplemente no creen tener información comercial tan relevante.

	ENTRE 18 Y 24 AÑOS	ENTRE 25 Y 35 AÑOS	ENTRE 36 Y 54 AÑOS	ENTRE 55 Y 64 AÑOS	ENTRE 65 AÑOS Y MÁS
En mis contraseñas utilizo patrones de teclado (qwerty) y números en secuencia (1234) porque es más fácil recordar	22,7%	16%	13,1%	11,5%	8%
En mis contraseñas utilizo información personal (como nombre, fecha de nacimiento,etc.) porque es más fácil recordar	41,6%	45%	38,8%	25,4%	24%
La mayoría de mis contraseñas son las mismas o muy similares	70,8%	72,8%	61,8%	48,2%	40%

¿CUÁL DE LOS SIGUIENTES ELEMENTOS TE PREOCUPARÍA MÁS SI TE FUERAN SUSTRAÍDOS?

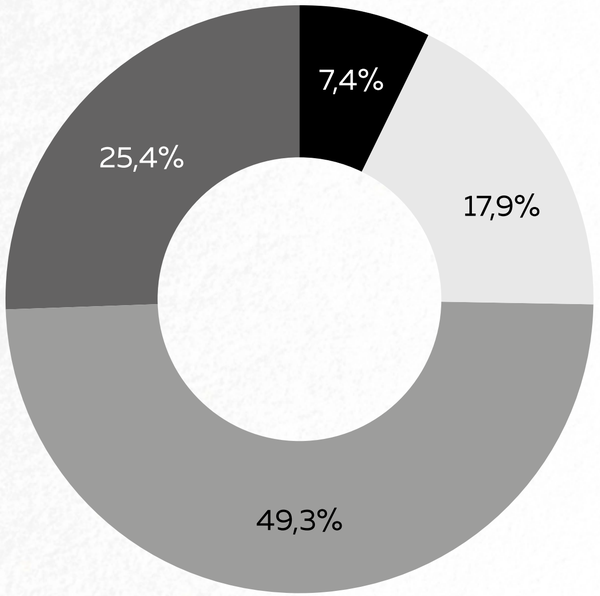
Hay dos aspectos que muestran una gran diferencia al compararse las diferentes generaciones. El primero es con respecto al teléfono: mientras que en las generaciones más jóvenes casi un tercio dice que lo que más le preocuparía perder es su celular, en los mayores de 64 años este porcentaje baja a un 7,7%. Ello muestra la mayor dependencia que hoy existe hacia el celular por parte de los centennials y millennials. Y la segunda gran diferencia es con respecto a las llaves del hogar: mientras que un 4,5% de los más jóvenes dice preocuparse por su sustracción, en el caso de los mayores este porcentaje llega al 19,2%.

	ENTRE 18 Y 24 AÑOS	ENTRE 25 Y 35 AÑOS	ENTRE 36 Y 54 AÑOS	ENTRE 55 Y 64 AÑOS	ENTRE 65 AÑOS Y MÁS
Robo de datos personales y contraseñas	41,6%	37,8%	50,5%	62,7%	50%
Billetera/cartera	22,5%	24,8%	22,9%	21,2%	19,2%
Teléfono móvil	30,3%	29,8%	17,5%	9,3%	7,7%
Llaves de la casa	4,5%	7%	7,4%	4,2%	19,2%
Llaves del auto	1,1%	1,9%	1,7%	2,5%	3,8%

METODOLOGÍA

Esta encuesta se realizó entre el 10 y el 22 de octubre del 2018 a 1.120 personas con acceso a internet. El 67,1% de los participantes fue de la Región Metropolitana. La distribución por generaciones fue la siguiente: Generación Z, de 18 a 24 años, un 7,9%. La generación de los Millennials, de 25 a 35 años, con el 37%. La Generación X, de 36 a 54 años, con un 42,3%, y los Baby Boomers, entre 55 y 64, con el 10,5% y los mayores de 65 con 2,3%. El 55% de los participantes fueron mujeres.

¿CUÁL ES SU NIVEL EDUCACIONAL?



GRACIAS