Alfonso VICENTE
Universidad de la República, Uruguay
avicente@fing.edu.uy
ORCID iD: https://orcid.org/0000-0003-3575-5326

Ariel SABIGUERO
Universidad de la República, Uruguay
asabigue@fing.edu.uy
ORCID iD: https://orcid.org/0009-0008-6759-0865

Gonzalo ESNAL
Investigador independiente, Uruguay
esnalbornes@hotmail.com
ORCID iD: https://orcid.org/0009-0006-3256-7169

Recibido: 28/04/2025 - Aceptado: 06/02/2026

Para citar este artículo / To reference this article / Para citar este artigo:
Vicente, A., Sabiguero, A. y Esnal, G. (2026). Alcance del derecho a la protección de datos personales en organizaciones que realizan inspección de HTTPS no informada. *Revista de Derecho, 25*(49), e493. https://doi.org/10.47274/DERUM/49.3

Alcance del derecho a la protección de datos personales en organizaciones que realizan inspección de HTTPS no informada

Resumen: En el contexto del acceso a Internet, surge una tensión entre el derecho de las organizaciones a proteger sus activos y el derecho a la privacidad de las personas. Esta tensión se agudiza cuando las organizaciones inspeccionan el tráfico HTTPS sin informar ni obtener consentimiento. Muchas personas utilizan dispositivos provistos por una organización para conectarse a Internet y transmitir información personal de cuya privacidad se preocupan, con la expectativa de que esta transmisión sea privada y no pueda ser inspeccionada por terceras partes. En algunos casos, las organizaciones que proveen estos dispositivos, en un intento legítimo de proteger sus activos frente a amenazas existentes en Internet, utilizan técnicas para inspeccionar esta información, pero lo hacen sin aviso, sin solicitud de consentimiento y de una forma que es muy difícil de percibir para un usuario no especializado. En este trabajo se elabora un argumento en contra de esta práctica cuando se realiza sin conocimiento y sin consentimiento de los titulares de los datos personales. Asimismo, comentamos el Dictamen N° 22/022 de la Unidad Reguladora y de Control de Datos Personales que se redactó a instancias de nuestra consulta, y las implicancias de la reciente Ley 20.327 sobre ciberdelincuencia.

Palabras clave: privacidad, datos personales, derechos digitales

Universidad de Montevideo, Uruguay - Este es un artículo de acceso abierto distribuido bajo los términos de una licencia de uso y distribución CC BY-NC 4.0.
Para ver una copia de esta licencia visite http://creativecommons.org/licenses/by-nc/4.0/

Scope of the right to personal data protection in organizations that carry out uninformed HTTPS inspection

Abstract: In the context of Internet access, a tension arises between the right of organizations to protect their assets and the right to privacy of individuals. This tension is exacerbated when organizations inspect HTTPS traffic without informing or obtaining consent. Many individuals use devices provided by an organization to connect to the Internet and transmit personal information about whose privacy they are concerned, with the expectation that this transmission is private and cannot be inspected by third parties. In some cases, organizations that provide these devices, in a legitimate attempt to protect their assets from threats on the Internet, use techniques to inspect this information, but they do so without notice, without requesting consent, and in a way that is very difficult for a non-specialized user to perceive. In this paper we elaborate an argument against this practice when it is carried out without the knowledge and consent of the owners of the personal data. We also comment on the Opinion No. 22/022 of the Regulatory and Personal Data Control Unit, which was drafted at the request of our consultation, and the implications of the recent Law 20.327 on cybercrime.

Keywords: privacy, personal data, digital rights

Escopo do direito à proteção de dados pessoais em organizações que realizam inspeção HTTPS desinformada

Resumo: No contexto do acesso à Internet, surge uma tensão entre o direito das organizações de proteger seus ativos e o direito à privacidade dos indivíduos. Essa tensão é exacerbada quando as organizações inspecionam o tráfego HTTPS sem informar ou obter consentimento. Muitos indivíduos usam dispositivos fornecidos por uma organização para se conectar à Internet e transmitir informações pessoais sobre as quais estão preocupados com a privacidade, com a expectativa de que essa transmissão seja privada e não possa ser inspecionada por terceiros. Em alguns casos, as organizações que fornecem esses dispositivos, em uma tentativa legítima de proteger seus ativos contra ameaças na Internet, usam técnicas para inspecionar essas informações, mas o fazem sem aviso prévio, sem solicitar consentimento e de uma forma que é muito difícil de ser percebida por um usuário não especializado. Este documento elabora um argumento contra essa prática quando ela é feita sem o conhecimento e o consentimento dos titulares dos dados. Também comentamos o Parecer N° 22/022 da Unidade de Regulamentação e Controle de Dados Pessoais, que foi elaborado após nossa consulta, e as implicações da recente Lei 20.327 sobre crimes cibernéticos.

Palavras-chave: privacidade, dados pessoais, direitos digitais

Introducción

Este trabajo, enmarcado en la Ley 18.331 –que consagra el derecho a la protección de datos personales como derecho humano en el sentido dado por el artículo 72° de la Constitución de la República– se centra en la privacidad de los trabajadores que utilizan dispositivos provistos por su empleador. A raíz de este vínculo, el trabajador se expone al escrutinio de actividades privadas más allá del principio de razonabilidad.

Muchos trabajadores suelen utilizar dispositivos –como celulares, tabletas o computadoras personales– suministrados y administrados por su empleador para transmitir información personal. Pueden por ejemplo utilizar su cuenta de correo electrónico, acceder a su cuenta bancaria o a los resultados de un examen médico. Cuando se realizan estas actividades existe una expectativa fundada –en atención a la existencia de protocolos de transporte cifrado– de que la transmisión de la información personal sea privada, en el sentido de que ningún tercero podrá interceptarla e inspeccionarla.

1. Planteo general: alcance de la "conexión segura"

Los navegadores de Internet indican al usuario de alguna manera que la conexión es segura. Hasta hace poco los navegadores más populares utilizaban un ícono de un candado para indicar esto, y los usuarios han sido instruidos para interpretar esta señal como condición suficiente de seguridad en la transmisión de los datos. Sin embargo, este supuesto no siempre se cumple, sea por el accionar de la organización que provee los dispositivos o de terceros.

Las organizaciones, por su parte, tienen derecho a proteger sus activos, en el entendido de que existen amenazas derivadas de la navegación en Internet. Sin embargo, en el contexto laboral al que particularmente nos referimos –pero que podría extrapolarse a otros contextos como centros educativos, centros de salud, etc.–, se ha sostenido que "los poderes de vigilancia y control derivados del derecho de propiedad, tienen como límite la dignidad humana del trabajador y la intimidad", por lo cual la propiedad de los servidores y el equipamiento informático no justifica la invasión de la privacidad del trabajador (Raso Delgue, 2014, p. 4).

En esta misma línea, debemos tener en cuenta que "para lograr el equilibrio entre los diferentes derechos e intereses, es fundamental el principio de proporcionalidad", según el cual "es esencial que el trabajador esté informado sobre la vigilancia a la que está siendo sometido, sobre los datos que se han recolectado y con qué objetivo se mantienen" (Viega, 2010, p. 32).

Para el usuario común no es posible detectar y bloquear amenazas informáticas cuando la transmisión de la información se realiza cifrada de extremo a extremo. A estos efectos, los propietarios de los medios informáticos, pueden utilizar técnicas para interponerse literalmente "en el medio" de la transmisión, con la finalidad de descifrarla, inspeccionarla, y volverla a cifrar.

Sin embargo, cuando se lleva a cabo esta acción, el navegador de Internet es capaz de detectar que el sitio al que se está accediendo no es aquel que cifró la información

originalmente e indica que se ha roto el cifrado de extremo a extremo, notificando al usuario a través de mensajes tales como: "conexión insegura" o "sitio no seguro". Para evitar estas advertencias, algunas organizaciones modifican además el comportamiento del navegador, de forma que este indique que se está utilizando una "conexión segura". Esto pueden realizarlo en la medida en que tienen privilegios de administrador en sus dispositivos, y para el usuario no especializado esta indicación de "conexión segura" podría ser garantía suficiente de la privacidad de sus datos personales. Se puede afirmar que mediante esta técnica la organización ha inducido al usuario a creer que la transmisión de sus datos está cifrada de extremo a extremo, cuando de hecho no lo está.

Cabe suponer que, en la mayoría de los casos, las organizaciones que utilizan estas técnicas se limiten a realizar inspecciones en busca de virus o malware, lo que normalmente se realiza en un componente tecnológico de forma autónoma. Sin embargo, desde el punto de vista del usuario, no hay forma de saber cómo se procesa la información cuando se ha roto el cifrado de extremo a extremo. Eventualmente, se podrían estar inspeccionando, recolectando y/o modificando datos personales, incluso aquellos especialmente protegidos –según los artículos 18º y 19º de la Ley 18.331– o credenciales de acceso a sistemas que los manejan. En otros lugares alertamos sobre la relevancia de proteger frente a este tipo de ataques a los Prestadores de Servicios de Confianza (Sabiguero, Vicente y Esnal, 2024), y tratamos de generar consciencia sobre los riesgos de autenticarse solamente por HTTPS sin segundo factor de autenticación en este tipo de servicios tan críticos (Vicente, Sabiguero y Esnal, 2024).

Dentro de los límites de la razonabilidad y proporcionalidad, no se cuestiona el derecho de las organizaciones a protegerse de las amenazas de Internet, y a implementar las medidas de seguridad que consideren pertinentes en el marco de su derecho de propiedad amparado en el artículo 7º de la Constitución de la República. Lo que sí se cuestiona, es la práctica de interceptar las comunicaciones de forma inadvertida para el usuario. La única forma de conciliar los derechos de ambas partes es advertir del tratamiento que se realiza sobre la transmisión de la información, y solicitar el consentimiento en los términos de los artículos 9 y 13 de la Ley 18.331. El conocimiento previo e informado del trabajador –o en general del usuario– en relación a las técnicas que implementa el empleador –o en general la organización que le provee dispositivos– le permitirá optar por utilizar o no los dispositivos para transmitir su información personal.

A modo de ejemplo, en cuanto al uso del correo electrónico, se ha sostenido que: "Cuando se trata de una dirección electrónica cuyo titular es el trabajador, obviamente no existe posibilidad lícita alguna de que el empleador fiscalice o controle el tráfico que sale o ingresa de la misma, aún cuando el trabajador utilice el ordenador de la empresa y la red de telecomunicaciones para utilizar la misma. En cambio, cuando se trata de una dirección electrónica otorgada por el empleador al trabajador con fines exclusivamente laborales, se presenta el debate sobre si existe potestad de monitorear la misma o no. El derecho al secreto de las comunicaciones y el derecho a la intimidad ponen un freno a los poderes empresariales de control, restringiendo o limitando los casos en que se admite tal posibilidad" (Castello, 2010, pp. 35-68).

2. Marco normativo hasta la Ley 20.327

Entendemos de rigor comenzar señalando la preocupación del constituyente por la protección del derecho al honor, libertad y seguridad entre otros, cimiento del orden jurídico sobre el cual se apoya los derechos fundamentales bajo estudio. En esta línea, el artículo 28º de la Constitución consagra la reserva y privacidad de los papeles, correspondencia epistolar, telegráfica y de cualquier otra especie, manifestando que: "son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

Cabe también referirse a la Declaración Universal de Derechos Humanos de 1948. Su artículo 12º dispone: "Nadie será objeto de injerencias en su vida privada […] o su correspondencia […]" y que "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". En el mismo sentido, la Convención Americana sobre Derechos Humanos de 1969 o Pacto de San José de Costa Rica, ratificada por la Ley 15.737 de 08/03/1985, en su artículo 11º numeral 2 dispone que: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". Estos textos internacionales abordan desde un contexto general la protección de la vida privada como una dimensión de la dignidad humana. Aquí hallamos el punto de conexión con la más reciente legislación de protección a los datos personales.

La fórmula abierta del artículo 72º de la Carta que reconoce la existencia de otros derechos, deberes y garantías inherentes a la personalidad humana o que se deriven de la forma republicana de gobierno, será la base sobre la cual se edificará el derecho a la protección de los datos personales como derecho humano fundamental que comprende el derecho a la privacidad, a la intimidad, a la imagen propia y a la autodeterminación informativa, entre otros, enlazado por el artículo 1º de la Ley 18.331 (Durán Martínez, 2009, pp. 42-43).

Dicha Ley de Protección de Datos Personales en su Artículo 9º consagra el principio del previo consentimiento informado indicando que: "El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse…", estableciendo en el literal D como excepción que este no será necesario cuando: "Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento".

En el ámbito del trabajo, el artículo 84º de la Ley 19.355, declara que: "los registros y documentos destinados a la protección y contralor del trabajo, […], se encuentran comprendidos en lo dispuesto" en el literal D del artículo 9º.

De acuerdo al Repertorio de recomendaciones prácticas de la OIT (1997) para el ámbito laboral, "Los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que la gobiernan y de sus derechos".

Según el artículo 3º de la Ley 18.331, el ámbito objetivo de aplicación refiere a: "los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado". Asimismo, el literal M del artículo 4º define el tratamiento de datos como:

"operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias". En mérito a estos dos artículos, la interceptación de la comunicación por la organización o empleador encuadra en la definición de procesamiento de datos personales. Cabe dilucidar si es de aplicación alguna de las excepciones expuestas.

El Protocolo de enmienda del Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales, suscrito en Estrasburgo, el 10 de octubre de 2018, y aprobado en Uruguay mediante la Ley 19.948, establece en el artículo 1º que su objetivo es "proteger a todos los individuos [...] con respecto al tratamiento de sus datos personales", y el artículo 2º establece que por tratamiento se entiende "cualquier operación o conjunto de operaciones llevadas a cabo sobre los datos personales", entendemos que al hacer referencia a "cualquier operación o conjunto de operaciones" se está protegiendo los datos personales del individuo también en el contexto de la transmisión de los mismos.

La Unidad Reguladora y de Control de Datos Personales (URCDP) también ha sancionado normas relevantes. El Dictamen Nº 10/010 de la URCDP, establece que la normativa vigente —refiriéndose a la Ley 18.331— "resulta de aplicación a la *transmisión* de imágenes y sonidos por medio de la videovigilancia" (el énfasis es nuestro). Sin embargo, considerando que la videovigilancia tiene como finalidades intereses legítimos, la URCDP dictamina que "resulta pertinente que todos los responsables que establezcan sistemas de videovigilancia adopten un distintivo". Este distintivo "deberá especificar ante quién se podrán ejercer los derechos consagrados en la Ley Nº 18.331". Si bien no está explícito en el Dictamen, puede comprenderse que la función del distintivo es hacer más detectable la situación de estar videovigilado.

Quizá el antecedente más relevante para este trabajo podría ser la Resolución Nº 79/2014 de la URCDP. En el Considerando II establece que "se debe realizar un balance entre el derecho de la empresa a proteger sus bienes e instalaciones, y el derecho a la intimidad y a la protección de datos personales de los trabajadores, a la luz de los principios que inspiran la Ley, sobre todo los de consentimiento, finalidad y proporcionalidad". Y el Considerando IV de la misma Resolución establece que "en principio, *siempre que los trabajadores sean informados debidamente* y se consideren los límites, es legítimo instalar cámaras para controlar la actividad e instalaciones dentro de la empresa sin solicitar el consentimiento expreso de los trabajadores" (el énfasis es nuestro).

Si bien el alcance de este trabajo aplica a la navegación por Internet en términos generales, consideración aparte puede merecer aquella navegación en Internet cuyo objetivo sea el correo electrónico o alguna forma de correspondencia entre personas.

En este sentido, el Anexo II del Decreto Nº 92/2014 establece los "Lineamientos para la implementación y uso de servicios de correo electrónico seguro", con el fin de garantizar un adecuado nivel de confidencialidad de los mismos. El alcance son los dominios gubernamentales, las comunicaciones realizadas por éstos hacia servidores de terceros y todos los correos electrónicos recibidos o enviados por los mismos. Allí se establece que: "Los correos electrónicos deben ser protegidos tanto en su generación, almacenamiento, como así también durante su transmisión y recepción, de manera que se garantice su confidencialidad durante toda su vida." Es claro que el correo electrónico

debe ser protegido durante su transmisión. Más adelante el artículo detalla que "se debe garantizar que los correos electrónicos en tránsito entre dos MTAs[1], o entre un MUA[2] y un MTA no comprometa la confidencialidad de la comunicación cuando sea posible". El Decreto es claro respecto a la seguridad que debe existir cuando se envían correos entre servidores gubernamentales, indicando que: "La implementación de canales de comunicación cifrados entre MUAs y MTAs de dominios gubernamentales es mandatorio, y deberá implementarse utilizando SSL v3, TLS 1.0[3], STARTTLS[4] o superior. Los MTAs de dominios gubernamentales no deberán aceptar la descarga o entrega de correos por parte de MUAs si este canal cifrado no se puede negociar". Es claro que se prioriza la confidencialidad sobre la capacidad de comunicación al expresarse claramente que de no poder negociarse un canal seguro, se deberá "interrumpir el intento de entrega o recepción" ya que "Los MTA no deberán aceptar la descarga o consulta de correos electrónicos sobre canales en texto claro".

La protección de la privacidad se espera ocurra de extremo a extremo. También se atiende el fenómeno del acceso a correo electrónico a través de técnicas conocidas como "webmail", tecnología que también debe ser considerada, pues indica: "De implementar servicios de webmail estos deben ser implementados sobre el protocolo HTTPS utilizando un certificado de seguridad válido, y deberán estar alojados dentro del territorio nacional". El Decreto no solamente aborda la comunicación de los correos utilizando protocolos específicos para su transmisión, como su eventual visualización mediante navegadores. Se amplía además a que: "Los titulares de cuentas de correo de dominios gubernamentales no podrán acceder a sus cuentas desde servicios webmail que no sean el provisto por el organismo". Este punto refuerza además el carácter de confidencialidad, pues, si bien al usuario le puede resultar cómodo leer sus correos en otros sistemas de uso común como GMail, el decreto prioriza la confidencialidad, pues, configurar la descarga del correo en cualquier servicio de terceros, habilita a éstos a acceder a la información allí contenida.

En base a lo anterior, podemos afirmar que en este conflicto, entre el derecho a la privacidad de las personas y el derecho a la protección de sus activos de las organizaciones, encontramos un sustento normativo claro y explícito, que defiende y enmarca en varios aspectos el derecho a la privacidad y a la no interceptación o inspección de documentos. La posibilidad técnica que tienen las organizaciones de interceptar e inspeccionar datos personales de forma difícilmente perceptible, es una cuestión de hecho y no de derecho.

Por último, debemos destacar la reciente aprobación de la Ley 20.327 de fecha 25 de setiembre de 2024, que incorpora normas específicas para la prevención y represión de la ciberdelincuencia. A través de esta norma se agregan una serie de artículos al Código Penal Uruguayo. Estos delitos cubren una amplia gama de circunstancias, a saber: el Acoso telemático (art. 288 BIS), el Fraude informático (art. 347 BIS), el Daño informático (art. 358 QUATER), el Acceso ilícito a datos informáticos (art. 297 BIS), la Interceptación ilícita (art. 297 TER), la Vulneración de datos (art. 297 QUATER), la Suplantación de

1 MTA (Mail Transfer Agent) es el servidor que realiza el envío y la recepción de correo electrónico.

2 MUA (Mail User Agent), es el sistema que se encarga de recibir y enviar mensajes de correo electrónico a través de los protocolos para el envío (STMP) y para la recepción (POP3 o IMAP).

3 SSL y TLS son protocolos utilizados para cifrar información entre dos puntos.

4 STARTTLS es un método para convertir una conexión insegura preexistente a segura utilizando SSL o TLS.

identidad (art. 347 TER), y el Abuso de los dispositivos (art. 358 QUINQUIES). Asimismo, la norma incorpora varios agravantes para los delitos enumerados y establece la necesidad de promover una serie de medidas educativas.

Nos interesa destacar en particular los siguientes delitos que se incorporan al artículo 297º del Código Penal: 1) Acceso ilícito a datos informáticos, 2) Interceptación ilícita y 3) Vulneración de datos:

> "ARTÍCULO 297 BIS. (Acceso ilícito a datos informáticos).- El que mediante medios informáticos o telemáticos, sin autorización y sin justa causa acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital, será castigado con seis a veinticuatro meses de prisión."
>
> "ARTÍCULO 297 TER. (Interceptación ilícita).- El que sin autorización y sin justa causa intercepte, interrumpa o interfiera por medios técnicos, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, sean originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte los mismos, será castigado con seis a veinticuatro meses de prisión."
>
> "ARTÍCULO 297 QUATER. (Vulneración de datos).- El que mediante la utilización de cualquier medio telemático acceda, se apodere, utilice, o modifique datos confidenciales de terceros, registrados en soportes digitales, o cualquier otro tipo de archivo o registro público o privado, sin autorización de su titular, será castigado con seis a veinticuatro meses de prisión. El que, habiendo formado parte o no de su descubrimiento, difunda, revele o ceda a terceras personas los datos, hechos o imágenes registrados en soportes digitales será castigado con un año de prisión a cuatro años de penitenciaría."

Estos tres delitos se relacionan directamente con el objeto del presente análisis, y en particular el de interceptación ilícita, definido como la captación no autorizada de datos informáticos en tránsito. La norma tipifica esta conducta como delito cuando se realiza sin autorización ni justa causa. En este contexto, la cuestión central radica en determinar, en cada caso concreto, si la conducta efectivamente configura alguno de los tipos penales previstos, atendiendo a elementos como la existencia o no de consentimiento informado por parte del titular de los datos, la naturaleza del acceso, y las circunstancias que rodean la transmisión y tratamiento de la información.

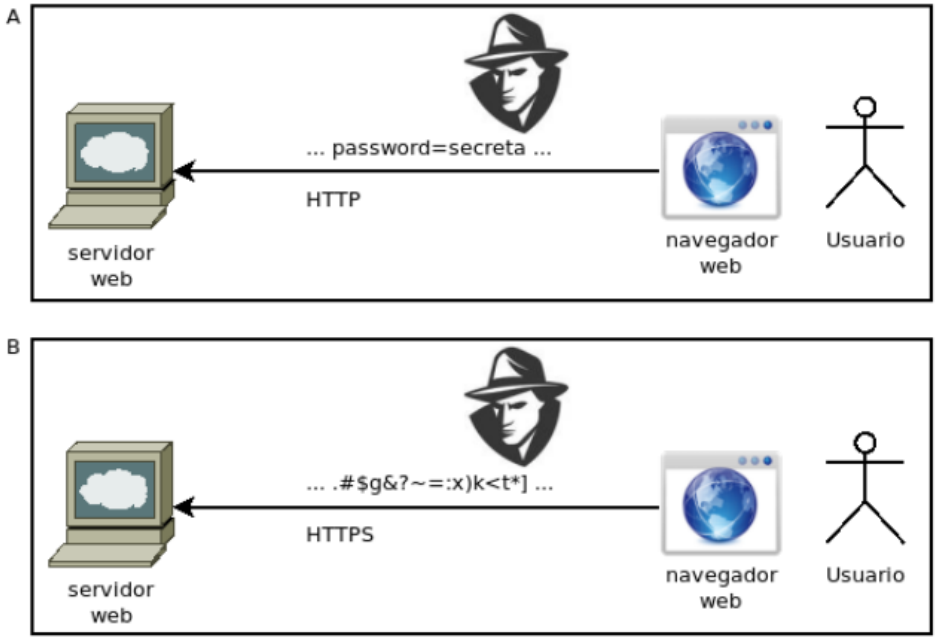
3. Conceptos técnicos fundamentales de la "navegación segura"

La navegación en Internet se realiza a través del protocolo cliente-servidor llamado Hypertext Transfer Protocol (HTTP). Éste es un protocolo considerado inseguro, en el sentido que la información que se transmite no está cifrada, y en caso de que alguien la intercepte podrá inspeccionarla.

En 1994 la empresa Netscape Communications creó HTTPS, donde la "S" puede leerse como "Seguro". En HTTPS la información se transmite cifrada "de extremo a

extremo", donde un extremo es el servidor y el otro extremo es el cliente. En la actualidad, virtualmente todos los sitios Web que ofrecen aplicaciones por medio de las cuales se accede a información personal, utilizan HTTPS de forma exclusiva. La Figura 1 ejemplifica la diferencia entre la navegación por HTTP (caso A) y HTTPS (caso B). El servidor web podría ser de un banco, de un sitio de compra en línea, de un centro de salud o de un proveedor de correo electrónico para uso personal.

Figura 1. Navegación por HTTP y HTTPS



La popularidad de HTTPS ha aumentado significativamente en los últimos años, impulsada por una creciente preocupación por la privacidad y la seguridad en la web. Esta tendencia hacia el uso preferente de conexiones cifradas ha sido documentada desde hace años (Google, 2022). Más recientemente, Google ha avanzado en la adopción de políticas orientadas a establecer HTTPS no solo como la opción recomendada, sino como la única disponible en muchos de sus servicios. Así, el enfoque actual es avanzar hacia una navegación HTTPS por defecto, bloqueando activamente conexiones en texto claro cuando sea posible (Google, 2023b).

La forma en que las aplicaciones protegen la privacidad de sus usuarios por medio de HTTPS está basada en el cifrado criptográfico. El usuario —cliente— confía en un certificado digital de sitio que asegura la identidad de la organización —servidor— que ofrece un servicio por Internet. Estos certificados de sitio son firmados por Autoridades de Certificación o en inglés "Certificate Authorities" (CAs), que a su vez son firmados por Autoridades de Certificación Raíz o en inglés "Root CAs". La confianza en los certificados tiene la propiedad de herencia: si se confía en una CA, se confía en los certificados de sitio que ella firma. De la misma forma, cuando se confía en una Root CA, se confía en las CAs que ella firma. El término "confianza" aquí describe el comportamiento del software, que puede no reflejar una confianza real del usuario sobre la privacidad de su

información. Existen trabajos que describen cómo algunos gobiernos pueden forzar a algunas CAs para que generen certificados de sitio y cómo los fabricantes de navegadores web y sistemas operativos incluyen certificados de CAs de múltiples gobiernos en los cuales los usuarios "confían" sin saberlo (Soghoian y Stamm, 2011). En cualquier caso, estos son conceptos fundamentales de lo que se conoce como Infraestructura de Clave Pública o en inglés "Public Key Infrastructure" (PKI), y constituyen las bases de la navegación segura.

En la práctica, los sistemas operativos y/o navegadores web vienen "de fábrica" con los certificados de las principales Autoridades de Certificación Raíz, con lo cual los usuarios no deben realizar ninguna acción especial para que su navegador web confíe en los sitios de Internet más comunes. Sin embargo, si un usuario quisiera confiar en una Autoridad de Certificación o una Autoridad de Certificación Raíz no incluida en las "de fábrica", podría importar los certificados de aquellas en las que decida confiar. Según el navegador web y el sistema operativo, esto podría hacerse en el propio navegador, o bien, en un almacén de certificados centralizado en el sistema operativo. Por este motivo, quien administra un dispositivo, puede definir y modificar en qué certificados confía el navegador o el dispositivo en su totalidad.

Varios manuales de usuario insisten en que una forma de saber si se está realizando una "navegación segura" es verificar que se utilice protocolo HTTPS y que el navegador web muestre un candado verde. En particular, esto es lo que hace una guía de AGESIC destinada a instruir en seguridad de la información a docentes, educadores y público en general (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento [AGESIC], 2018).

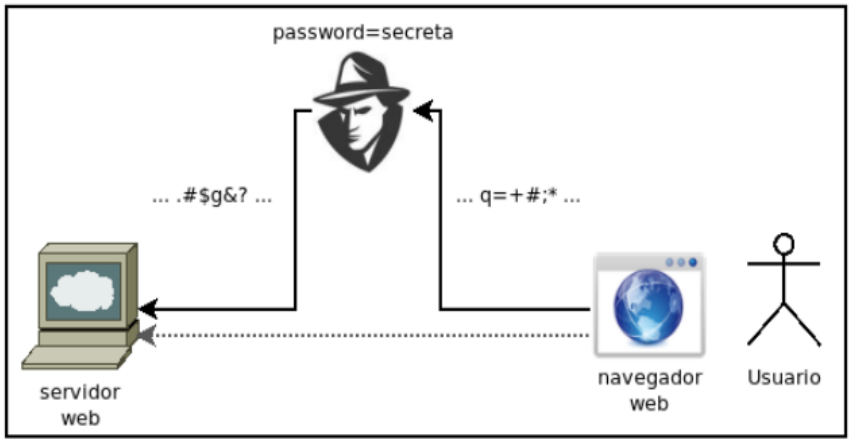
Es probable que la mayor parte de los usuarios no especializados piensen que por el solo hecho de utilizar HTTPS y ver un candado su conexión está cifrada de extremo a extremo, y no puede haber nadie "en el medio" de la conexión que pueda inspeccionar su tráfico. Muchas veces se ha educado a los usuarios para verificar que aparezca el candado; no para abrirlo, ver la entidad que firmó el certificado del sitio, y distinguir entre autoridades de certificación confiables y no confiables. Vale comentar que actualmente los navegadores están abandonando la práctica de mostrar un candado para indicar que una conexión es segura, debido a que el ícono se podía malinterpretar —los usuarios podían interpretar que el sitio en sí mismo era seguro y confiable— y a que con la adopción generalizada de HTTPS podía resultar innecesario mostrar un indicador para algo que era común. En esta línea, en setiembre de 2023 Google Chrome reemplazó el ícono del candado por un símbolo más neutral, similar a un sintonizador, para evitar malentendidos y animar a los usuarios a interactuar con el ícono para obtener más información sobre la seguridad del sitio (Google, 2023a).

Todo el avance de HTTPS tendiente a mantener una Internet más segura justifica el esfuerzo de las compañías por ofrecer HTTPS como única vía de acceso, pero es importante reconocer que las formas en que se educa a los usuarios determinan sus expectativas de confianza.

4. Técnica “Man In The Middle”

Mantendremos la expresión en inglés “Man In The Middle” —literalmente, hombre en el medio— o MITM, para denotar tanto la técnica de ataque como el agente que se pone “en el medio” entre un usuario —cliente— y un sitio web —servidor. La técnica, ilustrada en la Figura 2, consiste en interceptar la transmisión de la información, descifrar la información que llega del cliente, procesarla, y volverla a cifrar para enviarla al servidor. En sentido inverso, descifra las respuestas del servidor, las procesa, y las vuelve a cifrar antes de enviárselas al cliente. El cliente piensa que el MITM es el servidor, y el servidor piensa que el MITM es el cliente. El MITM tiene acceso a toda la información descifrada, que puede incluir contraseñas, registros médicos, cuentas bancarias, tarjetas de crédito o cualquier otro tipo de información sensible.

Figura 2. Técnica “Man In The Middle”



Para que el usuario no se de cuenta, además de interceptar la transmisión, el MITM debe modificar el dispositivo del usuario para que confíe en un certificado emitido por el MITM. De esta forma, el usuario puede creer que tiene una “conexión segura” con cifrado de extremo a extremo entre él y el servidor web al que accede, cuando en realidad no es así. Lo que sí tiene es una conexión cifrada entre él y el MITM, quien a su vez tiene una conexión cifrada con el servidor web al que el usuario accede. Lo cual implica que en realidad tiene una conexión insegura, en el sentido de que el MITM puede inspeccionar toda la información que se transmite.

5. Necesidad de seguridad en las organizaciones

Las organizaciones tienen un interés legítimo en proteger su propiedad, y en particular, de protegerse frente a las múltiples amenazas existentes en Internet. Muchas organizaciones, como organismos del Estado, empresas, centros educativos o prestadores de salud, cuentan con dispositivos dentro de una red interna, a través de los cuales algunos usuarios —funcionarios, empleados, estudiantes o pacientes— acceden a Internet. Esto

representa un riesgo, ya que como resultado de esta navegación, los dispositivos podrían infectarse con algún tipo de software malicioso.

Una de las formas en que las organizaciones se protegen de esta amenaza es inspeccionando toda la información que se transmite. Esto se conoce como inspección profunda, o en inglés, "deep inspection" o "packet inspection". Incluso hay trabajos que proponen sistemas de inspección profunda que puedan proporcionar tanto seguridad como privacidad (Parekh, Wang y Stolfo, 2006) en un claro intento de reconciliar la necesidad de la inspección con el derecho a la privacidad, y recomendaciones de autoridades de seguridad que incluyen aspectos de privacidad (National Security Agency, 2019).

En este contexto, la navegación por HTTPS representa un desafío técnico adicional, ya que la organización no puede inspeccionar información que está cifrada de extremo a extremo. Sin embargo, una organización que administra sus dispositivos está en condiciones ideales para aplicar la técnica MITM, no necesariamente para espiar o interferir en la transmisión de información de los usuarios, sino con el fin legítimo de detectar y eventualmente bloquear amenazas de seguridad. La organización ya tiene infraestructura de red "en el medio" entre sus dispositivos e Internet, y como administra sus dispositivos puede decidir que éstos confíen en un certificado emitido por ella. De esta forma, cuando un usuario utiliza un dispositivo de la organización para acceder a Internet, y accede a un sitio por HTTPS, ve un certificado que no es el del servidor al que está accediendo, pero su navegador web le dice que está accediendo a una "conexión segura". El usuario no experimenta ningún cambio evidente al navegar por sus sitios de confianza, y la organización puede protegerse al realizar la inspección de la información que se transmite por HTTPS. A esta técnica se la conoce con varios nombres, como inspección de HTTPS, o en inglés, "HTTPS inspection", "SSL inspection", "TLS inspection", "TLS break and inspect", o "HTTPS interception".

Vale decir que en la mayoría de los casos probablemente no existe intención de engañar a los usuarios, y no se los espía ni se interfiere en la transmisión de información. Incluso muchas organizaciones que utilizan esta técnica excluyen de la inspección de HTTPS algunos sitios que consideran seguros, o donde la privacidad es extremadamente importante, como los sitios de banca electrónica o los de correo personal.

6. Expectativas y normas jurídicas

Debido a la forma en que han sido instruidos sobre la "navegación segura", los usuarios tienen una expectativa legítima de que sus conexiones por HTTPS sean privadas. Cuando una organización utiliza una técnica de inspección de HTTPS frustra esta expectativa, pero además, si lo hace sin informar a los usuarios que no pueden contar con ella, lleva a los usuarios a confiar en un mecanismo de seguridad que se ha roto. Las normas jurídicas podrían tener que adaptarse a las expectativas. Como dice Hayek:

> "La protección contra la frustración de las expectativas que el derecho puede ofrecer en una sociedad en continuo cambio será siempre la protección de algunas expectativas, pero no de todas. [...] la función de las reglas de conducta sólo puede consistir en

> indicar a la gente con qué expectativas puede contar y con cuáles no. El desarrollo de tales reglas implica evidentemente una continua interacción entre normas jurídicas y expectativas [...]" (Hayek, 1985).

Como dejamos en claro, toda organización tiene el derecho de protegerse, y en la enorme mayoría de los casos podría esperarse que la inspección de HTTPS se utilice únicamente con fines legítimos de protección. Pero es un hecho que si esta técnica no ha sido informada, para la mayor parte de los usuarios es muy difícil advertirla, y que aún después de informada los usuarios no tienen forma de saber qué tipo de tratamiento recibe la inspección de la transmisión de sus datos.

Existen referencias a nivel internacional que expresan esta preocupación sobre la legalidad de estas técnicas (Brookman, 2015). A nivel nacional, los autores hemos realizado una consulta sobre el conflicto de derechos existente a la URCDP que tuvo una respuesta favorable. El espíritu de la consulta fue aclarar con qué expectativas pueden contar las personas en Uruguay en lo que concierne a su privacidad cuando utilizan dispositivos de las organizaciones a las que están vinculados, y sobre todo, que las organizaciones tengan un mandato claro sobre si deben informar y/o solicitar consentimiento a sus usuarios cuando realizan una inspección de HTTPS.

El Dictamen Nº 22/022 de la URCDP reconoce este conflicto de derechos. En el numeral 1 reconoce el derecho del empleador de utilizar la técnica de MITM, sujeto a que, como se establece en el numeral 2: "*En todos los casos deberá informarse previamente a los empleados de los alcances de la técnica referida*, en el marco de lo dispuesto en el artículo 13º de la Ley [18.331]" (el énfasis es nuestro).

Por tanto existe claramente una regulación que protege a los ciudadanos ante la frustración de sus expectativas sobre la seguridad de sus conexiones a Internet. Sin embargo, la cuestión que resaltamos es en relación al cumplimiento de este Dictamen, ya que más de un año después de su promulgación muchas organizaciones seguían realizando una inspección de HTTPS no informada, incluyendo algunas del Estado.

Realizamos más de treinta solicitudes de acceso a la información pública, habiendo obtenido respuesta en veinticuatro casos. De los organismos que respondieron, declararon no realizar la técnica de inspección de HTTPS los siguientes quince organismos:

1. ADMINISTRACIÓN DE SERVICIOS DE SALUD DEL ESTADO
2. ADMINISTRACIÓN NACIONAL DE CORREOS
3. LABORATORIO TECNOLÓGICO DEL URUGUAY
4. MINISTERIO DE AMBIENTE
5. MINISTERIO DE DESARROLLO SOCIAL
6. MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL
7. MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL
8. PODER LEGISLATIVO - CÁMARA DE REPRESENTANTES
9. PRESIDENCIA DE LA REPÚBLICA - AGESIC
10. PRESIDENCIA DE LA REPÚBLICA - ONSC

11. PRESIDENCIA DE LA REPÚBLICA - PRESIDENCIA
12. PRESIDENCIA DE LA REPÚBLICA - URCDP
13. UNIDAD REGULADORA DE SERVICIOS DE COMUNICACIONES
14. UNIDAD REGULADORA DE SERVICIOS DE ENERGÍA Y AGUA
15. UNIVERSIDAD TECNOLÓGICA

Declara realizar inspección de HTTPS y haber comunicado la INTENDENCIA DE MONTEVIDEO, aunque es de destacar que su forma de haber comunicado es mediante la publicación de una nota en el estatuto del funcionario.

Por otro lado, declaran realizar inspección de HTTPS y no haber comunicado, los siguientes seis organismos:

1. JUNTA DE TRANSPARENCIA Y ÉTICA PÚBLICA
2. PODER LEGISLATIVO - CÁMARA DE SENADORES
3. PODER LEGISLATIVO - COMISIÓN ADMINISTRATIVA
4. BANCO HIPOTECARIO DEL URUGUAY
5. MINISTERIO DE INDUSTRIA ENERGÍA Y MINERÍA
6. MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS

Por conocimiento directo de los autores, sabemos que otros dos organismos están en las condiciones de realizar inspección de HTTPS sin haber realizado comunicación alguna:

1. BANCO DE SEGUROS DEL ESTADO
2. BANCO DE PREVISIÓN SOCIAL

En resumen, de veinticuatro organismos públicos relevados, ocho (uno de cada tres) están incumpliendo la directiva Nº 22/022 de la URCDP.

Esto sin considerar la respuesta del MINISTERIO DEL INTERIOR, que declaró la información reservada por motivos de seguridad nacional, pero de la lectura del expediente que adjuntaron en la respuesta puede deducirse que también están en la situación de realizar inspección de HTTPS sin haber realizado comunicación alguna.

El conjunto de datos que apoya los resultados de este estudio no se encuentran disponibles.

7. Conclusión

El presente trabajo ha puesto de manifiesto el conflicto entre el derecho legítimo de las organizaciones a proteger sus activos frente a amenazas digitales y el derecho fundamental de los individuos a la privacidad y a la protección de sus datos personales. Este conflicto adquiere particular relevancia cuando las organizaciones aplican técnicas de inspección de HTTPS sin conocimiento ni consentimiento de los titulares de los datos, frustrando así una expectativa razonable de confidencialidad en las comunicaciones.

Si bien el ordenamiento jurídico uruguayo no presenta un vacío normativo en esta materia —como lo demuestran la Ley 18.331, el Dictamen N.º 22/022 de la URCDP y la reciente Ley 20.327 sobre ciberdelincuencia—, estamos de acuerdo con Raso Delgue

en que: "las reglas no son suficientes para resolver los casos puntuales" (Raso Delgue, 2010). Además, persiste una brecha entre lo normativamente exigido y lo efectivamente cumplido. Esta brecha se ve reflejada en el hecho de que múltiples organismos públicos continúan realizando inspección de HTTPS sin haber comunicado tal práctica a los usuarios, en contravención directa de las obligaciones legales.

A fin de conciliar la necesidad de seguridad organizacional con el respeto por los derechos fundamentales de los usuarios en general, y los trabajadores en particular, consideramos indispensable reforzar los mecanismos de transparencia y consentimiento. Proponemos, en este sentido, que se exija la incorporación explícita de cláusulas de consentimiento informado en los contratos de trabajo, así como la implementación de alertas visibles en los dispositivos gestionados por las organizaciones, que adviertan sobre la posibilidad de inspección de las comunicaciones. Sólo una regulación clara, acompañada de prácticas institucionales respetuosas y auditables, permitirá preservar la confianza de los ciudadanos en el entorno digital y asegurar que las organizaciones persigan sus fines legítimos sin transgredir los límites impuestos por la dignidad humana.

Referencias

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2018). Guía Didáctica de Seguridad de la Información. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/guia-didactica-de-seguridad-de-la-informacion

Brookman, J. (2015) Is Breaking Web Encryption Legal? En *Center for Democracy and Technology*. https://cdt.org/insights/is-breaking-web-encryption-legal

Castello, Alejandro. (2010). Límites del control tecnológico del empleador. En *El trabajo ante las nuevas tecnologías*, pp. 35-68. FCU.

Consejo de Europa. (2018). Protocolo de enmienda al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108+), suscrito en Estrasburgo el 10 de octubre de 2018. https://rm.coe.int/16808ac918

Constitución de la República Oriental del Uruguay. (1997). Constitución de 1967 con las reformas de 1989, 1994 y 1997. Montevideo: IMPO – Centro de Información Oficial. https://www.impo.com.uy/bases/constitucion

Felt, A. P., Barnes, R., King, A., Palmer, C., Bentzel, C., y Tabriz, P. (2017). Measuring HTTPS adoption on the web. En *26th USENIX Security Symposium* (USENIX Security 17) (pp. 1323-1338).

Google. (2022). Cifrado HTTPS en la Web – Informe de transparencia de Google [Versión archivada]. Wayback Machine. https://web.archive.org/web/20220610000000/https://transparencyreport.google.com/https/overview

Google. (2023a). An update on the lock icon. Chromium Blog. https://blog.chromium.org/2023/05/an-update-on-lock-icon.html

Google. (2023b). Towards HTTPS by default. Chromium Blog. https://blog.chromium.org/2023/08/towards-https-by-default.html

Hayek, F. A. (1985). *Derecho, legislación y libertad*. Unión Editorial.

Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. https://www.un.org/es/universal-declaration-human-rights/

National Security Agency. (2019). Managing Risk from Transport Layer Security Inspection. NSA. https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2002225460/

Organización de los Estados Americanos. (1969). Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica). https://www.oas.org/es/cidh/mandato/Basicos/convencion.asp

Organización Internacional del Trabajo. (1997). Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores. Ginebra: Oficina Internacional del Trabajo. https://www.ilo.org/global/publications/WCMS_160878/lang--es/index.htm

Parekh, J. J., Wang, K., y Stolfo, S. J. (2006). Privacy-preserving payload-based correlation for accurate malicious traffic detection. En *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense* (pp. 99-106).

Raso Delgue, J. (2010). Privacidad del trabajador, en *El trabajo ante las nuevas tecnologías*, pp. 19-24. FCU.

Raso Delgue, J. (2014). Nuevas tecnologías: conflictos entre el interés de la empresa y la vida privada del trabajador. En *Relaciones Laborales y Derecho del Empleo*.

Sabiguero, A., Vicente, A. y Esnal, G. (2024). Let There Be Trust. En *2024 IEEE URUCON* (pp. 1-5). IEEE.

Soghoian, C., y Stamm, S. (2011). Certified lies: Detecting and defeating government interception attacks against SSL (short paper). En *International Conference on Financial Cryptography and Data Security* (pp. 250-259). Springer, Berlin, Heidelberg.

Unidad Reguladora y de Control de Datos Personales. (2010). Dictamen N.º 10/010. URCDP. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/dictamen-no-10010

Unidad Reguladora y de Control de Datos Personales. (2014). Resolución N.º 79/014. Reglas para la aplicación del artículo 23 del Decreto N.º 414/009 sobre cesión y comunicación de datos personales entre organismos públicos. URCDP. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/resolucion-no-79014

Unidad Reguladora y de Control de Datos Personales. (2022). Dictamen N.º 22/022. URCDP. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/dictamen-no-22022

Uruguay. (1985). Ley N.º 15.737. Régimen de protección de la información y de los actos administrativos. IMPO. https://www.impo.com.uy/bases/leyes/15737-1985

Uruguay. (2008). Ley N.º 18.331. Protección de datos personales y acción de habeas data. IMPO. https://www.impo.com.uy/bases/leyes/18331-2008

Uruguay. (2014). Decreto N.º 92/014. Reglamentación de la Ley N.º 18.331 sobre protección de datos personales. IMPO. https://www.impo.com.uy/bases/decretos/92-2014

Uruguay. (2015). Ley N.º 19.355. Rendición de Cuentas y Balance de Ejecución Presupuestal. Ejercicio 2014. IMPO. https://www.impo.com.uy/bases/leyes/19355-2015

Uruguay. (2021). Ley N.º 19.948. Modificación de la Ley N.º 18.331 sobre protección de datos personales. IMPO. https://www.impo.com.uy/bases/leyes/19948-2021

Uruguay. (2023). Ley N.º 20.327. Protección de datos personales. Derogación de la Ley N.º 18.331. IMPO. https://www.impo.com.uy/bases/leyes/20327-2023

Vicente, A., Sabiguero, A. y Esnal, G. (2024). Firmar con prestadores de servicios de confianza: riesgos y precauciones a tener en cuenta. En *Revista de la Asociación de Ingenieros del Uruguay*, 100(1), 55-61.

Viega, María José. (2010). Protección de los datos personales relacionados con el trabajo, en *El trabajo ante las nuevas tecnologías*, pp. 25-34. FCU.

Contribución de los autores (Taxonomía CRediT): 1. Conceptualización, 2. Curación de datos, 3. Análisis formal, 4. Adquisición de fondos, 5. Investigación, 6. Metodología, 7. Administración de proyecto, 8. Recursos, 9. Software, 10. Supervisión, 11. Validación, 12. Visualización, 13. Redacción - borrador original, 14. Redacción - revisión y edición. A.V. ha contribuido en: 1, 2, 3, 5, 6, 10, 11, 12, 13,14, A.S en: 1, 2, 3, 5, 6, 10, 11, 12, 13, 14 y G.E. en: 1, 2, 3, 5, 6, 10, 11, 12, 13, 14.

Disponibilidad de datos: El conjunto de datos que apoya los resultados de este estudio no se encuentra disponible.

Editor responsable Miguel Casanova: mjcasanova@um.edu.uy