USAC TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DE OCCIDENTE -CUNOC-

CUNOC
Dirección del Sistema de Investigación
José Baldomero Arriaga Jerez

Boletín informativo
Actualidad

DIRECCIÓN GENERAL DE INVESTIGACIÓN (DICUNOC)
"José Baldomero Arriaga Jerez"
CENTRO UNIVERSITARIO DE OCCIDENTE

BOLETÍN NO 17. AÑO XXIX Julio 2026

JUAN FRANCISCO BERTHET
PROFESOR INVESTIGADOR

Problemática de compartir datos en línea en Guatemala y sus riesgos frente a las extorsiones digitales

Introducción

Hoy en día, la tecnología ha cambiado muchísimo la forma en que vivimos y nos relacionamos con los demás. Tener acceso a internet ya no es un lujo, sino algo básico que usamos prácticamente todos los días.

Lo utilizamos para hablar con amigos y familiares, hacer tareas, trabajar o simplemente divertirnos. En Guatemala, cada vez más personas se conectan a través de sus celulares, lo que ha hecho que el internet esté presente en casi todos los aspectos de la vida diaria. Las redes sociales se han vuelto muy populares y forman parte de la rutina de muchas personas.

"El intercambio de datos en línea en Guatemala ha dejado de ser un asunto meramente tecnológico, convirtiéndose en un complejo problema social y legal que alimenta directamente las redes de extorsión digital".

Además, aplicaciones móviles y diferentes plataformas digitales facilitan muchas actividades, desde aprender algo nuevo hasta hacer compras o trámites. Todo esto ha permitido que la comunicación sea más rápida y sencilla. Sin embargo, también ha cambiado la forma en que interactuamos y compartimos información. Muchas personas pasan gran parte de su tiempo conectadas sin darse cuenta. En general, el internet se ha vuelto una herramienta imprescindible en la vida moderna, especialmente en países como Guatemala donde su uso sigue creciendo.

Sin embargo, este crecimiento también ha generado nuevos desafíos, especialmente en el ámbito de la seguridad digital. Uno de los principales problemas es la falta de control sobre la información personal que los usuarios comparten en línea. Las personas publican datos personales sin considerar los riesgos asociados, lo que crea oportunidades para que los ciberdelincuentes utilicen esa información con fines ilícitos.

En este contexto, los delitos digitales han aumentado de forma significativa en Guatemala, destacando el robo de datos, el fraude electrónico y las extorsiones digitales. Estos delitos no solo afectan el patrimonio económico de las víctimas, sino que también generan consecuencias psicológicas y sociales, como el miedo, la ansiedad y la pérdida de confianza en las instituciones.

¿Qué son los datos personales y por qué son importantes?

Los datos personales son toda aquella información que permite identificar a una persona, ya sea de forma directa o indirecta. Entre estos datos se encuentran el nombre, número de identificación, dirección, correo electrónico, número telefónico, historial laboral y hasta hábitos de consumo.

En el entorno digital, los datos personales adquieren un valor especialmente alto, ya que pueden ser utilizados para múltiples propósitos positivos, como mejorar servicios o facilitar transacciones. Sin embargo, también pueden ser utilizados de forma incorrecta o ilegal, especialmente por delincuentes.

El acceso a esta información permite a los ciberdelincuentes construir perfiles detallados de sus víctimas, lo que aumenta la efectividad de delitos como el fraude y la extorsión.
La cultura digital en Guatemala presenta importantes deficiencias, siendo uno de los principales problemas el uso del internet sin conocimientos básicos sobre seguridad informática, lo que expone a la población a riesgos constantes.

Muchas personas utilizan redes sociales, aplicaciones y páginas web sin comprender plenamente las consecuencias de sus acciones en línea, lo que se refleja en errores frecuentes como compartir información personal sin restricciones, incluyendo datos sensibles que pueden ser utilizados con fines maliciosos.

También es común que los usuarios acepten solicitudes de amistad o contacto de personas desconocidas, lo que incrementa la probabilidad de caer en engaños o fraudes. A esto se suma el uso de contraseñas débiles o repetidas, que facilitan el acceso no autorizado a cuentas personales, así como el ingreso de datos en páginas no seguras que no cuentan con protocolos de protección adecuados. Otro aspecto preocupante es la falta de actualización de dispositivos y aplicaciones, lo que deja vulnerabilidades abiertas que pueden ser explotadas por ciberdelincuentes. En conjunto, esta falta de conocimiento y conciencia digital facilita el trabajo de los delincuentes, quienes aprovechan la ingenuidad o el desconocimiento de los usuarios para obtener información, cometer fraudes o realizar actividades ilícitas que afectan tanto la seguridad individual como la colectiva.

El internet ha transformado de manera significativa la forma en que se cometen los delitos, permitiendo que los delincuentes operen con mayor facilidad sin necesidad de estar físicamente cerca de sus víctimas.

A través de medios digitales, pueden obtener información personal mediante engaños o accesos no autorizados, contactar a las víctimas por redes sociales, mensajes o llamadas, realizar fraudes electrónicos y ejecutar extorsiones utilizando datos previamente recopilados, lo que hace que estos delitos sean cada vez más sofisticados.

Esta evolución ha provocado que los crímenes se vuelvan más rápidos, efectivos y difíciles de rastrear, ya que los responsables pueden ocultar su identidad y actuar desde diferentes lugares.

En este contexto, la percepción de inseguridad digital en Guatemala ha ido en aumento, ya que diversos estudios evidencian que la población muestra una creciente preocupación por la protección de su información en línea, especialmente frente a problemas como el robo de datos, las estafas y los fraudes electrónicos. Sin embargo, este interés por la ciberseguridad suele intensificarse únicamente cuando ocurren incidentes relevantes, lo que refleja una reacción tardía en lugar de una cultura preventiva constante.

Además, se han identificado amenazas frecuentes como el phishing, la ingeniería social y el fraude digital, prácticas que diariamente afectan a los usuarios al aprovechar su confianza, desconocimiento o falta de medidas de seguridad, lo que evidencia la necesidad urgente de fortalecer la educación digital y la prevención para reducir estos riesgos.

Hackeo al Ministerio de Trabajo

El hackeo al portal “Tu Empleo” del Ministerio de Trabajo representa uno de los incidentes más importantes en Guatemala en materia de ciberseguridad. Este ataque expuso datos de aproximadamente 200,000 ciudadanos, incluyendo información personal y laboral.

Este tipo de incidentes demuestra que la información digital no está completamente protegida, incluso cuando se encuentra en plataformas oficiales del gobierno.

Ataques a instituciones públicas y crisis digital del Estado

El caso del Ministerio de Educación, donde se filtraron 178 GB de información, pone en evidencia la fragilidad de los sistemas digitales del Estado guatemalteco.

Asimismo, otras instituciones también han sido afectadas por ataques informáticos, lo que demuestra que el problema no es aislado, sino sistémico.

Estos hechos reflejan una realidad preocupante en Guatemala, donde la falta de inversión en ciberseguridad limita la capacidad de prevenir y enfrentar los delitos digitales de manera efectiva. Muchas instituciones, tanto públicas como privadas, operan con sistemas tecnológicos obsoletos que no cuentan con las actualizaciones necesarias para enfrentar las amenazas actuales.

A esto se suma la escasa capacitación técnica del personal encargado de manejar información sensible, lo que incrementa los errores humanos y las vulnerabilidades. Asimismo, la ausencia de protocolos adecuados dificulta la respuesta ante incidentes, lo que provoca reacciones tardías y poco eficientes cuando ocurre un ataque o una filtración de datos. Esta combinación de factores crea un entorno frágil que puede ser fácilmente aprovechado por los ciberdelincuentes.

La extorsión digital es uno de los delitos más frecuentes y preocupantes dentro de este contexto, y consiste en el uso de medios tecnológicos para amenazar, intimidar o presionar a una persona con el fin de obtener dinero u otros beneficios.

Este tipo de delito ha evolucionado con el uso de herramientas digitales, lo que permite a los delincuentes operar de forma más rápida y con menor riesgo de ser identificados. A través de redes sociales, llamadas telefónicas, correos electrónicos o aplicaciones de mensajería, los extorsionistas logran establecer contacto directo con sus víctimas, generando un ambiente de presión y miedo que facilita el cumplimiento de sus demandas.

Para llevar a cabo estas acciones, los delincuentes utilizan la información obtenida previamente para crear escenarios creíbles y altamente convincentes. Entre las estrategias más comunes se encuentran los falsos secuestros, donde simulan tener retenido a un familiar de la víctima, así como amenazas directas a seres queridos para generar pánico inmediato.

También recurren a la suplantación de autoridades, haciéndose pasar por miembros de instituciones oficiales para exigir pagos bajo supuestas investigaciones o sanciones. Estas tácticas buscan manipular emocionalmente a las víctimas, reduciendo su capacidad de análisis y llevándolas a actuar de manera impulsiva sin verificar la veracidad de la información.

El impacto de la extorsión digital es profundo y se manifiesta en distintos niveles. En el ámbito económico, muchas personas pierden dinero al ceder ante las amenazas, e incluso algunos negocios se ven obligados a cerrar debido a las constantes presiones.

A nivel psicológico, las víctimas experimentan ansiedad, miedo, estrés y una sensación permanente de inseguridad que afecta su bienestar emocional y su vida cotidiana. En el plano social, este tipo de delitos genera desconfianza hacia los demás, provocando aislamiento y debilitando las relaciones interpersonales. Además, a nivel institucional, se produce una pérdida de confianza en el Estado y en las autoridades encargadas de brindar seguridad y justicia.

Existen diversos factores que favorecen el crecimiento de los delitos digitales en Guatemala, siendo uno de los principales la falta de educación digital en la población. Muchas personas desconocen los riesgos del entorno en línea y no cuentan con las herramientas necesarias para proteger su información personal. El uso excesivo de redes sociales también contribuye a este problema, ya que facilita la exposición de datos que pueden ser utilizados por delincuentes. A esto se suma la debilidad institucional y la falta de leyes claras y actualizadas que permitan una regulación efectiva del entorno digital.

Dicho esto, la impunidad juega un papel clave en la expansión de estos delitos, ya que la falta de consecuencias para los responsables incentiva a otros a cometer actos similares. La combinación de todos estos factores crea un entorno propicio para la delincuencia digital, donde las víctimas son cada vez más vulnerables y los delincuentes encuentran menos barreras para operar. Por ello, es fundamental fortalecer la educación, mejorar las leyes, invertir en tecnología y promover una cultura de prevención que permita reducir los riesgos y proteger a la población frente a estas amenazas.

El marco legal en Guatemala en materia digital presenta importantes desafíos que limitan la protección efectiva de los ciudadanos en el entorno en línea. Aunque en los últimos años han surgido algunas iniciativas orientadas a regular la ciberseguridad y el uso de datos personales, todavía no existe un sistema jurídico sólido, actualizado y completamente articulado que garantice la protección integral de la información personal. Esta situación dificulta la persecución de los delitos informáticos, ya que muchas conductas no están claramente tipificadas o carecen de mecanismos adecuados de investigación y sanción.

Asimismo, la falta de regulación adecuada afecta la protección de los ciudadanos, quienes quedan expuestos a riesgos como el robo de identidad, la extorsión y el fraude digital, sin contar siempre con recursos legales efectivos. Además, la regulación de las plataformas digitales sigue siendo limitada, lo que impide establecer responsabilidades claras sobre el manejo de datos y la seguridad de los usuarios.

En contraste, en otros países la ciberseguridad se ha convertido en una prioridad nacional, especialmente en varias naciones de América Latina donde se han desarrollado políticas públicas, estrategias nacionales de ciberseguridad y marcos legales más robustos para proteger la información de la población.

Estos países han invertido en infraestructura tecnológica, han modernizado sus leyes y han fortalecido sus instituciones encargadas de responder a incidentes digitales. En comparación, Guatemala presenta rezagos significativos en aspectos clave como la infraestructura tecnológica, que aún es limitada en cobertura y capacidad; la regulación legal, que necesita mayor actualización y alcance; y la capacidad de respuesta institucional ante amenazas cibernéticas.

Esta brecha evidencia la necesidad urgente de adoptar modelos internacionales exitosos, adaptándolos al contexto nacional, con el fin de fortalecer la protección digital, mejorar la confianza en el uso de las tecnologías y garantizar la seguridad de la población en el entorno digital.

Las medidas de prevención para reducir los riesgos asociados al uso de internet deben abordarse tanto a nivel individual como institucional, ya que la seguridad digital depende de la actuación conjunta de todos los actores involucrados.

A nivel personal, es fundamental que los usuarios adopten hábitos responsables como evitar compartir datos sensibles, tales como contraseñas, información bancaria, direcciones o documentos personales en plataformas digitales o con personas desconocidas. Asimismo, es importante configurar adecuadamente la privacidad en redes sociales, limitando quién puede ver la información y las publicaciones personales.

El uso de contraseñas seguras, que combinen letras, números y símbolos, contribuye a dificultar el acceso no autorizado a las cuentas, al igual que la activación de la autenticación en dos pasos, que añade una capa adicional de protección frente a posibles ataques. Por otro lado, a nivel institucional, es necesario que organizaciones públicas y privadas mantengan sus sistemas tecnológicos actualizados para corregir vulnerabilidades y prevenir ciberataques. También deben implementar protocolos de seguridad claros, que permitan responder de manera eficiente ante incidentes digitales, y capacitar constantemente a su personal en buenas prácticas de ciberseguridad, ya que el factor humano es uno de los puntos más vulnerables en la protección de la información.

En este contexto, la educación digital adquiere un papel clave para fortalecer la seguridad en línea. Es indispensable que forme parte del sistema educativo en Guatemala, de modo que desde temprana edad los estudiantes aprendan sobre el uso responsable de internet, la protección de datos personales y los riesgos digitales a los que pueden estar expuestos.

Esta formación permitirá desarrollar habilidades críticas para identificar amenazas, tomar decisiones informadas y actuar de manera preventiva. De esta forma, se contribuirá a la formación de ciudadanos más conscientes, responsables y preparados para desenvolverse de manera segura en el entorno digital.

La problemática de compartir datos en línea en Guatemala es un fenómeno complejo que involucra factores tecnológicos, sociales y legales que interactúan entre sí. En el ámbito tecnológico, muchas personas acceden a internet a través de dispositivos móviles sin contar con herramientas adecuadas de protección, como antivirus o configuraciones de privacidad actualizadas. Esto incrementa la vulnerabilidad frente a ciberataques, robo de identidad y accesos no autorizados a información personal.

Desde el punto de vista social, la falta de educación digital juega un papel determinante. Gran parte de la población no posee conocimientos suficientes sobre los riesgos asociados al uso de redes sociales, aplicaciones de mensajería y otras plataformas digitales. Esto se traduce en prácticas peligrosas, como compartir información sensible (números de teléfono, direcciones, fotografías privadas o datos financieros) sin considerar las posibles consecuencias. Además, existe una baja cultura de prevención, lo que facilita que los delincuentes aprovechen estas debilidades.

En el ámbito legal e institucional, se observa una falta de normativas actualizadas y de mecanismos efectivos para prevenir y sancionar los delitos informáticos. Aunque se han dado algunos avances, el crecimiento acelerado del entorno digital ha superado la capacidad de respuesta de las instituciones. Esto ha permitido el aumento de delitos como la extorsión, el fraude en línea y el acoso digital, afectando tanto a individuos como a empresas.

Los casos analizados evidencian que la seguridad digital debe convertirse en una prioridad tanto para el Estado como para la sociedad en general. Es fundamental fortalecer las políticas públicas mediante la creación de leyes más robustas y actualizadas que regulen el uso de datos personales y castiguen los delitos cibernéticos de forma efectiva.

Asimismo, es necesario invertir en infraestructura tecnológica que permita una mejor protección de la información y el desarrollo de sistemas de monitoreo y respuesta ante incidentes digitales.

Por otro lado, resulta imprescindible fomentar una cultura de prevención a través de la educación digital. Esto implica implementar programas educativos desde edades tempranas que enseñen a utilizar internet de manera responsable y segura. También es importante promover campañas de concientización dirigidas a toda la población, que brinden herramientas prácticas para identificar riesgos, proteger la privacidad y actuar ante posibles amenazas.

En conclusión, proteger la información personal en el entorno digital no solo es una necesidad, sino una responsabilidad compartida entre el Estado, las instituciones y la ciudadanía. Solo mediante un esfuerzo conjunto que combine educación, regulación y tecnología será posible garantizar la seguridad y el bienestar de la población en Guatemala frente a los desafíos del mundo digital.

REFERENCIAS BIBLIOGRAFICAS

https://www.prensalibre.com/guatemala/guatemala-no-se-detiene/informe-sobre-ciberestafas-que-tan-seguros-se-sienten-los-guatemaltecos-en-linea/

https://guate365.org/noticias/nacionales/2026-04-27-hackean-ministerio-trabajo-guatemala-200-mil-datos-robados/

https://www.infobae.com/guatemala/2026/04/30/continuan-las-alertas-los-ciberataques-simultaneos-vulneran-plataformas-oficiales-y-exponen-credenciales-administrativas-en-guatemala/

https://dialogos.org.gt/wp-content/uploads/2025/09/Informe-Extorsiones-1.pdf

https://www.prensalibre.com/guatemala/justicia/extorsiones-en-guatemala-50-denuncias-diarias-en-el-ultimo-ano-de-gobierno-de-alejandro-giammattei/

https://nuevomundo.gt/blog/2025/09/30/extorsiones-en-guatemala/

DIRECTORIO

Director Dicunoc: Raúl Bethancourt

Autor: Juan Francisco Berthet (Profesor Investigador)

Diseño y Estilo : Fred Rivera (Profesor Investigador)

La Dirección General de Investigación del Centro Universitario de Occidente (Dicunoc) "José Baldomero Arriaga Jerez", es una dependencia del Centro Universitario de Occidente, cuya misión es el desarrollo de la Investigación Científica en todos los campos del conocimiento. Se interesa especialmente en impulsar la investigación científica y tecnológica vinculada al desarrollo regional y local en el área de influencia del CUNOC que comprende los Departamentos del Sur-Nor-Occidente del país.