Seguridad Digital

Fraudes, suplantación de identidad y hábitos digitales inseguros en un contexto de retorno a la rutina laboral.

Marzo y la reactivación laboral y digital, siendo la seguridad digital uno de los pilares de la protección social. Tras los periodos vacacionales, marzo marca el regreso pleno a la actividad laboral, académica y administrativa en Costa Rica. Este retorno intensifica el uso de plataformas digitales, correos electrónicos y servicios bancarios en línea, creando un escenario propicio para el fraude, la suplantación de identidad y otros delitos informáticos. Desde la criminología preventiva, la seguridad digital se consolida como una dimensión esencial de la seguridad humana y familiar.

Sin embargo, este aumento en la conectividad no siempre va acompañado de prácticas adecuadas de seguridad digital, lo que expone a la población a fraudes electrónicos, suplantación de identidad y delitos informáticos cada vez más sofisticados. Desde una perspectiva criminológica preventiva, marzo se convierte en un mes crítico donde la falta de cultura de autoprotección digital amplifica las oportunidades delictivas y evidencia la necesidad urgente de integrar la seguridad digital como un componente esencial de la seguridad humana, familiar y social.

Un país hiperconectado, pero sin protección

Costa Rica ha experimentado un crecimiento acelerado en la digitalización de servicios públicos, privados y financieros. Sin embargo, este avance tecnológico no siempre ha sido acompañado por una cultura sólida de seguridad digital. El mes de marzo, caracterizado por la reactivación laboral y el aumento del intercambio de información digital, evidencia una brecha crítica entre conectividad y protección.

Datos del Organismo de Investigación Judicial (OIJ) indican que, posterior a vacaciones, se incrementan las denuncias por estafas digitales, principalmente mediante correos falsos, mensajes engañosos y suplantación de identidad. La urgencia, la sobrecarga laboral y la confianza excesiva se convierten en factores de riesgo que los delincuentes digitales explotan de manera sistemática.

Marzo como escenario de riesgo digital estructural

Desde la criminología de las oportunidades, el delito digital se fortalece cuando convergen tres elementos: acceso a la víctima, motivación del infractor y ausencia de barreras preventivas. Marzo reúne estas condiciones: usuarios activos, rutinas aceleradas y hábitos digitales descuidados.

Cuadro 1. Semana 1 – Revisión y fortalecimiento de la seguridad digital

Enfoque preventivo	Tips y recomendaciones
Contraseñas	Cambiar contraseñas periódicamente reduce el acceso no autorizado.
Sesiones abiertas	Cerrar sesiones evita usos indebidos de cuentas activas.
Accesos	Revisar dispositivos conectados permite detectar intrusiones.

La primera semana enfatiza que la seguridad digital no es una acción puntual, sino un hábito continuo. Estudios del MICITT señalan que una gran proporción de fraudes digitales se producen por contraseñas débiles o reutilizadas. Cambiar credenciales, activar

autenticación de doble factor y revisar accesos no autorizados constituye una barrera preventiva básica que reduce significativamente la vulnerabilidad personal y laboral.

Por esta razon marzo se convierte en un punto de partida estratégico para la prevención del delito digital, ya que coincide con la reactivación total de rutinas laborales y administrativas. Desde la criminología de la oportunidad, el delincuente digital se beneficia de sistemas descuidados, contraseñas antiguas y sesiones abiertas en múltiples dispositivos. La falta de actualización de credenciales genera un entorno de bajo riesgo para el infractor y alta exposición para la víctima.

Cambiar contraseñas, revisar accesos activos y cerrar sesiones abiertas no debe interpretarse como una acción técnica aislada, sino como un ejercicio de autocontrol preventivo. Estudios internacionales indican que una proporción significativa de accesos no autorizados ocurre semanas o meses después de la filtración inicial de datos, lo que convierte a marzo en un momento clave para cerrar brechas acumuladas. Esta práctica reduce la probabilidad de victimización secundaria y fortalece la resiliencia digital tanto individual como institucional.

Cuadro 2. Semana 2 – Correos, mensajes y manipulación emocional

Enfoque preventivo	Tips y recomendaciones
Urgencia	Desconfiar de mensajes que generan presión inmediata.
Verificación	Confirmar información por canales oficiales.
Atención	No hacer clic sin revisar el remitente.

Los delincuentes digitales utilizan estrategias de ingeniería social basadas en el miedo, la urgencia o la promesa de beneficios inmediatos. El OIJ reporta que la mayoría de víctimas realiza la acción fraudulenta en menos de cinco minutos tras recibir el mensaje. Detenerse, analizar y verificar rompe la cadena del delito y devuelve el control a la persona usuaria.

Durante la segunda semana, el foco se traslada a uno de los mecanismos más utilizados en el fraude digital: la ingeniería social. Los delincuentes no atacan directamente los

sistemas tecnológicos, sino el comportamiento humano. Mensajes que apelan a la urgencia, el miedo o la autoridad institucional buscan anular el pensamiento crítico y provocar respuestas inmediatas.

Desde la criminología cognitiva, este fenómeno evidencia cómo la presión emocional reduce la capacidad de evaluación del riesgo. Marzo, al ser un mes de alta carga laboral, aumenta la vulnerabilidad psicológica de las personas usuarias. Detenerse, verificar y desconfiar de mensajes inesperados se convierte en una barrera conductual que interrumpe la cadena del delito. La prevención, en este caso, no depende del software, sino de la capacidad de la persona para reconocer la manipulación y ejercer control consciente sobre su respuesta.

Cuadro 3. Semana 3 – Protección de datos personales y financieros

Enfoque preventivo	Tips y recomendaciones
Datos sensibles	No compartir información bancaria o personal.
Identidad	Proteger datos es proteger estabilidad financiera.
Desconfianza saludable	Ninguna institución solicita datos por llamadas o mensajes.

La suplantación de identidad constituye uno de los delitos digitales con mayor impacto emocional y económico. Desde la criminología financiera, la información personal es un activo que, una vez expuesto, puede ser utilizado repetidamente. Proteger los datos no solo evita pérdidas inmediatas, sino daños prolongados a la reputación y estabilidad económica.

La tercera semana aborda uno de los activos más valiosos en el ecosistema criminal digital: la información personal. Datos como números de identificación, claves bancarias o accesos a plataformas financieras permiten al delincuente operar incluso sin contacto directo con la víctima. Desde la criminología financiera, la suplantación de identidad no es un delito aislado, sino una puerta de entrada a múltiples formas de fraude.

La normalización del intercambio de datos en entornos digitales ha reducido la percepción de riesgo, lo que incrementa la exposición. Marzo es un mes especialmente sensible, ya que muchas personas realizan trámites bancarios, pagos y gestiones administrativas. Proteger la información personal implica reconocer que ninguna institución legítima solicita datos sensibles por medios informales. La prevención efectiva requiere adoptar una postura de desconfianza informada, entendida no como paranoia, sino como autocuidado racional frente al riesgo digital.

Cuadro 4. Semana 4 – Actualizaciones y vulnerabilidades tecnológicas

Enfoque preventivo	Tips y recomendaciones
Actualizaciones	Corrigen fallas de seguridad.
Vulnerabilidades	Ignorar avisos deja puertas abiertas al delito.
Responsabilidad digital	Mantener dispositivos al día es autoprotección.

Las actualizaciones de software no son opcionales: corrigen fallas que los delincuentes explotan activamente. Informes internacionales indican que una alta proporción de ataques exitosos ocurre en dispositivos desactualizados. La prevención tecnológica requiere disciplina y comprensión del riesgo digital cotidiano.

La cuarta semana enfatiza un aspecto frecuentemente subestimado: las vulnerabilidades tecnológicas. Las actualizaciones de software corrigen fallas de seguridad que, una vez detectadas, son rápidamente explotadas por actores delictivos. Ignorar estas actualizaciones convierte al dispositivo en un objetivo fácil, ya que el delincuente conoce de antemano la debilidad del sistema.

Desde la criminología situacional, mantener dispositivos actualizados actúa como una forma de “endurecimiento del objetivo”, aumentando el esfuerzo requerido para cometer el delito y reduciendo su atractivo. En marzo, cuando se incrementa el uso de dispositivos para trabajo remoto, estudio y trámites, esta práctica adquiere un valor preventivo colectivo. La responsabilidad digital deja de ser individual y se transforma en una acción de protección compartida que reduce riesgos en redes familiares y laborales.

Cuadro 5. Semana 5 – Seguridad digital como seguridad familiar

Enfoque preventivo	Tips y recomendaciones
Impacto social	Un fraude afecta a todo el entorno familiar.
Hábitos	Crear rutinas digitales seguras protege a todos.
Educación	Compartir prácticas preventivas fortalece la red familiar.

La seguridad digital trasciende lo individual. Un fraude puede comprometer recursos familiares, generar estrés emocional y afectar relaciones personales. Construir hábitos digitales seguros en familia amplía la prevención y reduce el impacto colectivo del delito.

La quinta semana amplía el enfoque desde lo individual hacia lo colectivo. Un incidente de fraude digital no afecta únicamente a la persona directa, sino que genera consecuencias económicas, emocionales y relacionales en todo su entorno familiar. La criminología social reconoce que la victimización digital puede provocar estrés, pérdida de confianza y deterioro de la estabilidad doméstica.

Promover hábitos digitales seguros en el núcleo familiar fortalece la prevención primaria y genera una red de protección informal. Compartir experiencias, advertir sobre intentos de fraude y educar a personas adultas mayores o jóvenes reduce la probabilidad de victimización múltiple. Marzo, como mes de reorganización y planificación, ofrece una oportunidad estratégica para incorporar la seguridad digital como un valor familiar y comunitario, consolidando una cultura preventiva sostenible.

Discusión crítica

La seguridad digital continúa ocupando un lugar secundario en la agenda pública y en la percepción social del riesgo, a pesar de su impacto creciente en la vida cotidiana. A diferencia de los delitos

tradicionales, el delito digital carece de visibilidad física inmediata, lo que contribuye a su normalización y subestimación. Esta invisibilidad no implica menor daño; por el contrario, el fraude digital y la suplantación de identidad generan consecuencias económicas, psicológicas y sociales que suelen extenderse en el tiempo y afectar a múltiples niveles del entorno de la víctima.

Desde una perspectiva criminológica estructural, el aumento de la digitalización sin una alfabetización preventiva adecuada ha creado un desequilibrio entre oportunidad delictiva y capacidad de autoprotección ciudadana. Marzo, como mes de reactivación laboral y administrativa, intensifica este desequilibrio: el incremento de transacciones, trámites y comunicaciones digitales amplía el “espacio de contacto” entre potenciales víctimas y ofensores. La falta de pausas cognitivas, producto de la presión laboral, facilita la toma de decisiones impulsivas, condición que los delincuentes explotan mediante estrategias de ingeniería social cuidadosamente diseñadas.

Asimismo, la discusión sobre seguridad digital suele centrarse en soluciones tecnológicas, relegando el análisis del comportamiento humano. Sin embargo, la evidencia criminológica demuestra que la mayoría de los fraudes digitales exitosos no se deben a fallas técnicas, sino a errores conductuales inducidos. Esto plantea un desafío crítico: la prevención no puede limitarse a software, firewalls o sistemas automatizados, sino que debe incorporar procesos educativos que fortalezcan la percepción del riesgo, el autocontrol y la toma de decisiones informadas.

Otro aspecto relevante es la desigualdad en la exposición al delito digital. Personas adultas mayores, jóvenes y usuarios con menor alfabetización tecnológica presentan mayor vulnerabilidad, lo que convierte al fraude digital en un fenómeno con implicaciones de exclusión social. La victimización digital puede traducirse en pérdida de ahorros, endeudamiento, deterioro de la salud mental y ruptura de vínculos de confianza, profundizando brechas sociales preexistentes. En este sentido, la seguridad digital debe entenderse como un componente de la seguridad humana, y no únicamente como un problema técnico o individual.

Finalmente, la ausencia de una cultura preventiva sólida refleja una brecha institucional y comunitaria. Si bien existen campañas informativas, estas suelen ser reactivas, fragmentadas y poco contextualizadas en los momentos de mayor riesgo. Marzo evidencia la necesidad de estrategias sostenidas, interinstitucionales y comunitarias que integren la seguridad digital en la rutina diaria de las personas. Solo a través de un enfoque preventivo integral, que combine educación, corresponsabilidad social y políticas públicas coherentes, será posible reducir la incidencia y el impacto del delito digital en la sociedad costarricense.

Conclusión

El análisis desarrollado a lo largo del mes de marzo evidencia que la seguridad digital no puede seguir siendo tratada como un aspecto accesorio de la vida moderna, sino como un componente esencial de la seguridad humana, económica y social. En un país cada vez más digitalizado, donde las gestiones laborales, financieras y educativas dependen de plataformas virtuales, la ausencia de hábitos preventivos adecuados amplifica las oportunidades delictivas y expone a amplios sectores de la población a fraudes y suplantaciones de identidad con consecuencias profundas y duraderas.

La revisión semanal de los tips de seguridad demuestra que pequeñas acciones cotidianas como: cambiar contraseñas, verificar mensajes, proteger datos personales y mantener dispositivos actualizados, tienen un impacto preventivo significativo. Estas prácticas, lejos de ser complejas o inaccesibles, representan mecanismos de autoprotección al alcance de cualquier persona y constituyen la primera línea de defensa frente al delito digital. La prevención, en este contexto, se construye desde la rutina, la atención consciente y el ejercicio del autocontrol.

Asimismo, este artículo pone en evidencia que la seguridad digital no es una responsabilidad exclusivamente individual. Un incidente de fraude afecta al núcleo familiar, al entorno laboral y, en muchos casos, a la confianza colectiva en los sistemas digitales. Promover una cultura de seguridad digital compartida, donde se dialoguen riesgos, se compartan alertas y se eduque a las personas más vulnerables, fortalece la prevención comunitaria y reduce la victimización múltiple. La seguridad digital, por tanto, debe entenderse como un bien social que se construye de manera colaborativa.

Finalmente, marzo se presenta como una oportunidad estratégica para transformar la percepción del riesgo digital en acción preventiva sostenida. Incorporar la seguridad digital en la planificación familiar, en las dinámicas laborales y en las políticas públicas no solo reduce la incidencia del delito, sino que fortalece la resiliencia social frente a un fenómeno criminal en constante evolución. Apostar por la educación preventiva, la corresponsabilidad y la vigilancia consciente permitirá avanzar hacia una sociedad más informada, protegida y capaz de enfrentar los desafíos de la criminalidad digital con criterio, responsabilidad y solidaridad.

Fuentes Bibliográficas

Clarke, R. V., & Felson, M. (1993). Routine activity and rational choice. New Brunswick, NJ: Transaction Publishers.

Consejo Nacional de Supervisión del Sistema Financiero. (2024). Recomendaciones de seguridad para usuarios de servicios financieros digitales. San José, Costa Rica.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. Londres: Home Office Research, Development and Statistics Directorate.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2024). Guía nacional de buenas prácticas en seguridad digital. San José, Costa Rica.

Ministerio de Seguridad Pública. (2023). Informe anual de prevención del delito y seguridad ciudadana. San José, Costa Rica.

Organismo de Investigación Judicial. (2023). Delitos informáticos y fraude electrónico en Costa Rica: análisis estadístico. San José, Costa Rica.

Organización Mundial de la Salud. (2023). Violence prevention and digital environments. Ginebra: OMS.

Programa de las Naciones Unidas para el Desarrollo. (2022). Informe sobre desarrollo humano y seguridad humana en América Latina. Nueva York: PNUD.

United Nations Office on Drugs and Crime. (2021). Handbook on cybercrime and crime prevention. Viena: UNODC.