

LA NUEVA FORMA DE VIVIR CON

# SEGURIDAD

POSTPANDEMIA

*Cómo vivir seguro y sin miedo  
en un mundo hiperconectado*

*La seguridad ya no es una opción... es una habilidad*

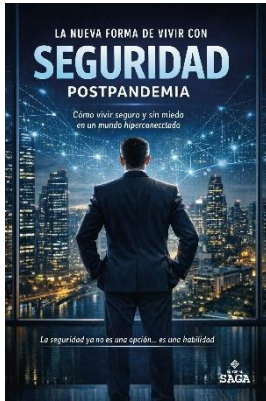
# La nueva forma de vivir con seguridad postpandemia

*Cómo vivir seguro y sin miedo  
en un mundo hiperconectado*

  
EDITORIAL  
**SAGA**

**Autores:**

*Freddy Gerardo Sarzosa Mendez  
Galo Alberto Villacres Zumarraga  
José Leonardo Aguiar Muñoz*



## Datos bibliográficos

<b>ISBN:</b>	<b>978-9907-803-32-7</b>
<b>Título del libro:</b>	La nueva forma de vivir con seguridad postpandemia Cómo vivir seguro y sin miedo en un mundo hiperconectado
<b>Autores:</b>	Sarzosa Mendez, Freddy Gerardo Villacres Zumarraga, Galo Alberto Aguar Muñoz, José Leonardo
<b>Editorial:</b>	SAGA
<b>Materia:</b>	301 - Sociología y antropología
<b>Público objetivo:</b>	Profesional / académico
<b>Publicado:</b>	2026-04-27
<b>Número de edición:</b>	1
<b>Tamaño:</b>	5Mb
<b>Soporte:</b>	Libro digital descargable
<b>Formato:</b>	Pdf (.pdf)
<b>Idioma:</b>	Español
<b>DOI:</b>	<a href="https://doi.org/10.63415/saga.2026.89">https://doi.org/10.63415/saga.2026.89</a>

Hecho en Ecuador / Made in Ecuador

## Autores

**Sarzosa Mendez, Freddy Gerardo**

Policia Nacional del Ecuador

✉ fgsm777@hotmail.com

id <https://orcid.org/0009-0001-6333-1398>

Quito, Ecuador



Soy Freddy Gerardo Sarzosa Méndez, profesional ecuatoriano con más de dos décadas de experiencia en seguridad pública y privada, inteligencia estratégica y gestión operativa. Mi trayectoria se ha desarrollado principalmente en la Policía Nacional del Ecuador, donde he asumido funciones de alto nivel en análisis de información, ciberdelitos, seguridad bancaria, control y liderazgo operativo.

Actualmente me desempeño como Jefe de Seguridad del Director del Centro Nacional de Inteligencia, responsabilidad que consolida mi experiencia en protección de dignatarios, manejo de crisis y toma de decisiones en entornos complejos. A lo largo de mi carrera, he liderado equipos multidisciplinarios, coordinado operaciones estratégicas y contribuido al fortalecimiento del sistema de seguridad nacional.

Mi formación académica incluye dos Maestrías en Estudios Avanzados de Terrorismo, y Gestión de Riesgos, además dos licenciaturas en Ciencias Policiales y Seguridad, estudios de Postgrado especializados en seguridad pública y privada, seguridad a Entidades Financieras, Seguridad de la Información TICs, complementados con capacitación internacional en gestión de riesgos, prevención del delito y seguridad industrial. Asimismo, he ejercido como docente e instructor, aportando a la formación de nuevos profesionales en el ámbito policial.

Me caracterizo por mi enfoque estratégico, disciplina operativa y compromiso con la excelencia, orientando mi labor hacia la innovación en seguridad, la protección integral y el desarrollo de soluciones efectivas para el sector público y corporativo.

## Villacres Zumarraga, Galo Alberto

Policia Nacional del Ecuador

✉ albertvillacres@live.com

 <https://orcid.org/0009-0002-1881-6916>

Quito, Ecuador



Soy un profesional en constante evolución, con una trayectoria consolidada en el ámbito de la seguridad, la tecnología y la protección integral de personas y entornos. Mi formación y experiencia dentro del servicio policial me han permitido desarrollar competencias en inteligencia, contrainteligencia y seguridad estratégica, aplicadas tanto en escenarios operativos como en

entornos institucionales de alto nivel.

Actualmente, continúo fortaleciendo mis capacidades en áreas clave como lenguajes de programación, ciencia de datos y ciberseguridad, entendiendo que el mundo moderno exige profesionales híbridos, capaces de integrar el conocimiento técnico con la toma de decisiones estratégicas. Este proceso de preparación constante se orienta también al análisis del terrorismo, el cibercrimen y las nuevas amenazas emergentes, donde la información y la anticipación marcan la diferencia.

Mi enfoque se basa en la seguridad prospectiva: no solo reaccionar ante los riesgos, sino anticiparlos, modelarlos y neutralizarlos antes de que se materialicen. Esto implica el uso de herramientas OSINT, análisis de datos y tecnologías emergentes para generar entornos seguros, tanto en el ámbito público como privado.

Además, participó activamente en el desarrollo de soluciones tecnológicas orientadas a la seguridad y la optimización de procesos, combinando mi experiencia operativa con la innovación digital. Creo firmemente en la preparación continua como pilar del éxito, y en la capacidad de adaptación como la mejor defensa ante un mundo en constante cambio.

Mi propósito es claro: evolucionar, proteger y liderar desde el conocimiento.

**Aguiar Muñoz, José Leonardo**

Policia Nacional del Ecuador

✉ jose\_leonardo233@hotmail.com

 <https://orcid.org/0009-0003-3003-7226>

Montalvo, Ecuador



Soy José Leonardo Aguiar Muñoz, sirviendo a mi País con 21 años de experiencia en diferentes ámbitos en el campo de seguridad ciudadana, estrategias y prevención de delitos.

En mi trayectoria profesional en su mayoría la he dedicado en la Policía Nacional, los primeros 11 años en el Grupo Especial Móvil Antinarcóticos GEMA, en las áreas operativas táctica: Toma de objetivos, rescate y operaciones

Fluviales, operaciones Subacuáticas.

Así mismo, en el GEMA en varios años Instructor de armas y tiro, Primeros Auxilios de combate, Operaciones Rivereñas, Inspecciones Subacuáticas en buques Mercantes “BUCEO “, formando líderes actores de soluciones en momentos adversos.

Seguido en mi profesión 9 años en seguridad a personas en Riesgo autoridades como: Ministro de Producción Comercio Exterior Inversiones y Pesca, Jefe de seguridad del Primer Vicepresidente de la Asamblea Nacional y del señor Director General del Centro Nacional de Inteligencia.

Me defino siempre trabajar con responsabilidad, honestidad, disciplina, actor de soluciones en la tarea o misión encomendada en el sector privado y público.



El contenido y las ideas expuestas en esta obra se encuentran protegidos por la normativa vigente en materia de propiedad intelectual y constituyen derechos exclusivos de su(s) autor(es)

Todos los derechos reservados © 2026

## Sinopsis

Este libro presenta una guía integral para transitar la vida después de la pandemia desde una perspectiva de seguridad cotidiana, emocional y digital. Parte del cambio radical que transformó rutinas, percepciones de riesgo y relaciones sociales, mostrando que la protección dejó de limitarse al espacio físico para extenderse a pantallas, datos personales y decisiones diarias. A lo largo de sus capítulos se describe la ilusión de tranquilidad previa al COVID-19, el impacto del confinamiento en hábitos y miedos, y la expansión de la hiperconexión que expone información, emociones y vínculos. La obra propone reemplazar la reacción impulsiva por atención consciente, con estrategias prácticas para reconocer fraudes, reducir vulnerabilidades domésticas, proteger dispositivos y fortalecer la resiliencia emocional. También destaca el valor de la comunidad, la cooperación y la alfabetización digital como pilares para recuperar la sensación de control sin caer en paranoia. Con lenguaje accesible y enfoque aplicado, el texto acompaña al lector en la construcción de hábitos sostenibles que integran prevención, bienestar y pensamiento crítico, ofreciendo herramientas para moverse con equilibrio en una realidad incierta y tecnológica. Cada página refuerza la idea de que la seguridad es práctica diaria, flexible, compartida y orientada a vivir con calma informada y sostenible.

**Palabras clave:** seguridad; ciberseguridad; hábitos; resiliencia; hiperconexión; prevención

## Synopsis

This book presents a comprehensive guide to navigating life after the pandemic from a perspective of everyday, emotional, and digital safety. It starts from the radical change that transformed routines, risk perception, and social relationships, showing that protection is no longer limited to physical space and now extends to screens, personal data, and daily decisions. Throughout its chapters, it describes the illusion of calm before COVID-19, the impact of confinement on habits and fears, and the expansion of hyperconnection that exposes information, emotions, and relationships. The work proposes replacing impulsive reaction with mindful attention, offering practical strategies to recognize scams, reduce household vulnerabilities, protect devices, and strengthen emotional resilience. It also highlights the value of community, cooperation, and digital literacy as pillars for recovering a sense of control without falling into paranoia. With accessible language and an applied approach, the text accompanies readers in building sustainable habits that integrate prevention, wellbeing, and critical thinking, providing tools to move with balance in an uncertain and technological reality. Every page reinforces the idea that safety is a daily, flexible, shared, and sustainable practice oriented toward living with informed calm.

**Keywords:** safety; cybersecurity; habits; resilience; hyperconnection; prevention

## Índice General

<b>Sinopsis.....</b>	<b>vii</b>
<b>Índice General .....</b>	<b>9</b>
<b>Introducción .....</b>	<b>13</b>
<b>Capítulo 1: Antes del Covid-19: la ilusión de la seguridad .....</b>	<b>19</b>
1.1 Rutinas y vulnerabilidades ocultas .....	20
1.1.1 Lo que tu día a día revelaba sobre tu seguridad.....	20
1.1.2 Señales que ignoramos y nos hacían vulnerables .....	21
1.1.3. Rutinas en casa, en la calle y en lo digital: capas de riesgo .....	23
1.2. Problemas que ignorábamos.....	26
1.2.1 Seguridad ciudadana antes de la pandemia: problemas latentes.....	26
1.2.2 Ejemplo real: cómo un descuido común pone en riesgo a todos .....	28
1.3 El enemigo invisible: la brecha digital .....	30
1.3.1 Acceso desigual, riesgos desiguales.....	31
1.3.2 Tus datos y privacidad sin protección.....	32
1.3.3 Cómo hackers y actores maliciosos aprovechan la desinformación.....	34
1.4. Vivir sin miedo... ¿realmente?.....	35
1.5. Despertar a la realidad .....	38
1.5.1 Qué aprendimos sobre la seguridad que creíamos tener .....	39
1.5.2 Claves para no repetir errores del pasado .....	40
<b>Capítulo 2: El impacto de la pandemia: vulnerabilidades al descubierto.....</b>	<b>43</b>

2.1. El confinamiento global y la cultura del miedo .....	44
2.1.1. Un mundo en pausa: confinamiento y restricciones históricas .....	44
2.1.2. Impacto emocional y mental del encierro .....	45
2.1.3. Cultura del miedo e inseguridad cotidiana .....	46
2.2. La digitalización forzada: dependencia tecnológica y exposición .....	48
2.2.1. Teletrabajo y educación virtual: continuidad a cualquier precio .....	48
2.2.2. Consumo digital y plataformas: de la comodidad a la sobreexposición .....	51
2.3. Auge de la violencia doméstica y comunitaria.....	52
2.3.1. El hogar como lugar de riesgo ampliado .....	53
2.3.2. Tensiones, género y comunidad: cuando el conflicto se desborda.....	54
2.3.3. Mini-guía para actuar sin ponerse en riesgo .....	55
2.4. Cibercrimitos en expansión .....	56
2.4.1. Un crecimiento silencioso durante el confinamiento.....	57
2.4.2. Modalidades de ataque más frecuentes durante la pandemia .....	58
2.5. La desinformación y el caos informativo.....	59
2.5.1. El ruido informativo: demasiada información, poca claridad .....	60
2.5.2. Cómo se viraliza una mentira: el lado emocional del contenido.....	61
2.5.3. De la confusión al riesgo: cuando la desinformación afecta tu seguridad.....	62
<b>Capítulo 3: Vivir en el mundo postpandemia: nuevas amenazas y desafíos.....</b>	<b>65</b>

3.1. La nueva normalidad y los efectos duraderos .....	66
3.1.1 Cambios en la rutina diaria: cuando lo normal dejó de serlo .....	66
3.1.2 Huellas emocionales: miedo, cansancio y desconfianza sutil .....	67
3.1.3 Nuevas formas de relacionarse, trabajar y cuidarse .....	68
3.2 La hiperconexión permanente .....	70
3.2.1. Del “estar conectados” al “estar siempre en línea” .....	70
3.2.2. Trabajo, estudio y vida gestionados por pantallas .....	71
3.2.3. Costes invisibles: fatiga digital y pérdida de privacidad....	73
3.3. El poder de los datos: entre utilidad y control.....	74
3.3.1. Los datos como nuevo recurso estratégico.....	75
3.3.2. Modelos de negocio basados en datos y asimetrías de poder .....	77
3.4. Ingeniería social y manipulación emocional .....	78
3.4.1. Qué es la ingeniería social: cuando el objetivo eres tú .....	79
3.4.2. Emociones como vector de ataque: miedo, urgencia, confianza .....	80
3.5. Salud mental y gestión emocional en la era digital .....	82
3.5.1. Cicatrices emocionales de una crisis prolongada.....	83
3.5.2. Sobrecarga digital, ansiedad y cansancio invisible .....	84
3.5.3. Estrategias de autocuidado emocional en la era hiperconectada.....	85
3.6. Hacia una cultura de conciencia y responsabilidad.....	86
3.6.1. De la reacción a la prevención: hábitos conscientes en lo cotidiano.....	87
3.6.2 Alfabetización mediática e informacional: una “vacuna” contra la desinformación.....	88

<b>Capítulo 4: Estrategias para vivir seguro y sin miedo .....</b>	<b>91</b>
4.1 Hacia una seguridad integral: física, emocional y digital .....	92
4.1.1 Tres dimensiones de la seguridad en la vida cotidiana .....	92
4.1.2 Seguridad consciente: pasar del piloto automático a la atención plena .....	93
4.1.3 De la preocupación a la acción: redefinir qué significa “vivir sin miedo” .....	94
4.2. Autoprotección cotidiana sin complicaciones .....	96
4.2.1 Hogar y entorno cercano: tu primer espacio seguro .....	96
4.2.2 Calle, transporte y espacios públicos: moverse con atención, no con pánico .....	97
4.2.3 Trabajo y estudio: seguridad en entornos compartidos .....	98
4.3 Seguridad digital accesible para todos .....	100
4.3.1 Lo mínimo indispensable: claves, 2FA y dispositivos .....	100
4.3.2 Higiene digital mensual: limpiar, actualizar, respaldar .....	101
4.3.3 Reconocer fraudes y engaños en línea .....	102
4.4 Manejo del miedo y resiliencia emocional .....	104
4.4.1 Entender el miedo como aliado, no solo como amenaza ..	104
4.4.2 Técnicas breves para bajar la ansiedad en el día a día .....	105
4.4.3 Construir resiliencia: recuperar el equilibrio después de un susto .....	107
4.5. Comunidad y cooperación .....	108
4.5.1 Redes de apoyo cercanas: familia, vecinos, amistades .....	108
4.5.2 Seguridad en entornos laborales y educativos .....	110
4.5.3 Proyectos colaborativos de seguridad y bienestar .....	111
<b>Referencias Bibliográficas.....</b>	<b>113</b>

## Introducción

La pandemia no solo cambió nuestras rutinas: cambió la forma en que entendemos el riesgo. Antes del COVID-19, la seguridad era, para muchos, una sensación cómoda y casi invisible. Íbamos y veníamos sin pensar demasiado, confiábamos en la “normalidad” y asumíamos que lo peligroso les ocurría a otros o en contextos lejanos. Pero un evento global bastó para recordarnos una verdad incómoda: **la seguridad no es un estado permanente, es una construcción diaria.**

Desde entonces, vivimos en un escenario distinto. Trabajamos, estudiamos, compramos, nos informamos y nos relacionamos a través de pantallas. Nuestros datos circulan más que nunca. Las emociones (miedo, urgencia, ansiedad, confianza) se han vuelto un terreno fértil para la manipulación. Y, al mismo tiempo, enfrentamos una paradoja: **necesitamos sentirnos seguros, pero no queremos vivir con paranoia.** Queremos protegernos sin encerrarnos, cuidarnos sin desconfiar de todo, usar la tecnología sin convertirnos en víctimas de ella.

Este libro nace precisamente para acompañarte en esa transición: de la seguridad por costumbre a la seguridad por conciencia. “La nueva forma de vivir con seguridad postpandemia: cómo vivir seguro y sin miedo” es una guía práctica y reflexiva para comprender el mundo que quedó después del COVID-19 y, sobre todo, para recuperar control sobre lo que hoy determina tu bienestar: tus hábitos, tu atención, tu información, tu criterio y tu entorno.

Aquí no encontrarás discursos alarmistas ni promesas mágicas. Encontrarás algo más valioso: una mirada clara y aplicable para reconocer riesgos reales (físicos, emocionales y digitales) y convertir esa comprensión en acciones simples, sostenibles y eficaces.

## **¿Por qué hoy se habla de seguridad de otra manera?**

Porque la seguridad ya no se limita a “evitar un robo” o “cerrar bien la puerta”. Hoy, la vulnerabilidad puede entrar por múltiples vías: una rutina repetida que te expone sin que lo notes, una decisión impulsiva tomada por miedo, un mensaje engañoso que explota tu urgencia, un enlace falso que roba tu información, una sobrecarga digital que deteriora tu salud mental, o una desinformación viral que te hace actuar contra tus propios intereses.

En el mundo postpandemia, la seguridad se volvió integral. Y eso implica comprender algo esencial: la protección no se logra solo con herramientas, se logra con hábitos. Por eso este libro combina análisis con estrategias prácticas, pensamiento crítico con acciones concretas, y bienestar emocional con autoprotección digital.

## **¿A quién está dirigido este libro?**

A profesionales y jóvenes universitarios que quieren entender lo que cambió y lo que sigue cambiando sin quedarse atrapados en el miedo. A quienes desean vivir con mayor tranquilidad, mejorar su autoprotección, fortalecer su bienestar emocional y moverse con criterio en una realidad tecnológica, compleja y globalizada.

Si alguna vez te preguntaste:

- “¿Por qué siento más inseguridad aunque la pandemia pasó?”
- “¿Cómo me protejo en internet sin volverme paranoico?”
- “¿Cómo identifico fraudes, manipulación o desinformación?”
- “¿Cómo manejo el miedo y la ansiedad sin ignorar los riesgos?”
- “¿Qué hábitos simples realmente funcionan para vivir más seguro?”

...este libro es para ti.

## **Un recorrido coherente: de la ilusión a la acción**

La estructura del libro está pensada como un camino progresivo. No se trata de darte listas sueltas de consejos, sino de ayudarte a construir un mapa mental completo: entender el origen del cambio, reconocer los riesgos actuales y aplicar soluciones prácticas.

### **Capítulo 1. Antes del COVID-19: La ilusión de la seguridad**

Comenzamos observando el “antes”. No para idealizarlo, sino para entender por qué nos sentíamos seguros. Aquí analizamos cómo las rutinas —en casa, en la calle y en lo digital— ocultaban capas de riesgo que ignorábamos: señales que pasaban desapercibidas, problemas latentes de seguridad ciudadana, y una brecha digital que ya estaba presente, pero que no se veía con claridad. Este capítulo te ayuda a identificar algo fundamental: muchas vulnerabilidades existían, solo que no las mirábamos.

### **Capítulo 2. El impacto de la pandemia: vulnerabilidades al descubierto**

Luego entramos en el momento que lo cambió todo. El confinamiento global amplificó el miedo y modificó la convivencia; la digitalización forzada nos volvió dependientes de plataformas; el hogar dejó de ser solo refugio y, en muchos casos, se convirtió en un espacio de riesgo; y los ciberdelitos crecieron en silencio mientras millones aprendían a vivir en línea “a cualquier precio”. Además, el caos informativo y la desinformación mostraron cómo una mentira viral puede ser tan peligrosa como un problema físico. Este capítulo te permite comprender por qué, desde entonces, el riesgo se siente más cercano y difícil de controlar.

### **Capítulo 3. Vivir en el mundo postpandemia: nuevas amenazas y desafíos**

Aquí nos ubicamos en el presente. Exploramos la nueva normalidad: cambios duraderos en la rutina, huellas emocionales como cansancio y desconfianza sutil, hiperconexión permanente y sus costos invisibles. Analizamos el poder de los datos (entre utilidad y control) y explicamos cómo funciona la ingeniería social: cuando el objetivo no es tu dispositivo, sino tu mente y tus emociones. Cerramos con un enfoque clave: salud mental y gestión emocional en la era digital, y el paso hacia una cultura de conciencia y responsabilidad. Este capítulo responde a una pregunta central: ¿cómo se vive seguro cuando el riesgo no siempre es visible?

### **Capítulo 4. Estrategias para vivir seguro y sin miedo**

Finalmente, llegamos a lo más práctico: un plan integral y accesible para fortalecer tu seguridad física, emocional y digital. Aquí aterrizamos lo aprendido en acciones simples: autoprotección cotidiana sin complicaciones, seguridad digital mínima indispensable (claves, 2FA, dispositivos), higiene digital mensual, reconocimiento de fraudes, técnicas breves para bajar la ansiedad y construir resiliencia después de un susto. Además, incorporamos un elemento que muchas guías olvidan: la seguridad también se construye con otros. Por eso trabajamos comunidad, redes de apoyo y cooperación en entornos laborales y educativos. Este capítulo tiene un objetivo claro: que termines el libro con herramientas reales para actuar desde hoy.

### **Lo que te llevas al terminar este libro**

Al cerrar estas páginas, no solo habrás entendido por qué el mundo se siente distinto. Habrás desarrollado:

- Una forma más clara de identificar riesgos sin caer en el alarmismo.

- Hábitos concretos para protegerte en casa, en la calle y en espacios compartidos.
- Una base sólida de seguridad digital aplicable sin ser experto en tecnología.
- Estrategias sencillas para regular miedo, ansiedad y sobrecarga informativa.
- Una mirada preventiva y consciente, centrada en el bienestar y no en la paranoia.

Porque vivir seguro hoy no significa vivir con miedo. Significa vivir con atención, criterio y equilibrio. Significa saber cuándo actuar, qué hábitos sostener y cómo recuperar la calma sin bajar la guardia.

La seguridad postpandemia no es un regreso a lo anterior. Es una nueva forma de estar en el mundo. Y este libro está escrito para ayudarte a recorrerla con claridad... y sin perder tu tranquilidad.



## **Capítulo 1:**

### **Antes del Covid-19: la ilusión de la seguridad**

## 1.1 Rutinas y vulnerabilidades ocultas

Antes de 2020, la mayoría de las personas en América Latina comenzaba el día de forma casi automática: apagar la alarma del celular, revisar mensajes, abrir la puerta de casa, tomar el mismo bus o la misma ruta al trabajo, saludar a los mismos rostros conocidos. Esa repetición cotidiana generaba una sensación de tranquilidad. Lo que se repite se siente seguro. Sin embargo, muchas de esas rutinas escondían riesgos que no veíamos, o que preferíamos no ver.

En términos objetivos, la región ya era una de las más violentas del mundo, con tasas de homicidio cercanas a 23–25 por cada 100.000 habitantes, aproximadamente cuatro veces el promedio global, que rondaba los 6 por cada 100.000 habitantes (Vilalta et al., 2016b). A pesar de esas cifras, la mayoría de personas seguía organizando su vida como si la violencia fuera un problema ajeno, concentrado en “otras zonas” o “otra gente”. Esta desconexión entre los datos y la experiencia subjetiva es el punto de partida para comprender las vulnerabilidades ocultas de la vida diaria.

### 1.1.1 *Lo que tu día a día revelaba sobre tu seguridad*

Imagina un día típico antes de la pandemia:

- Te levantas, desbloqueas el celular sin pensar y dejas abiertas notificaciones, ubicación y acceso a tus redes sociales.
- Sales de casa, cierras la puerta con llave, pero dejas las ventanas entreabiertas “para que corra el aire”.
- Tomas siempre la misma ruta al trabajo, a la misma hora, por las mismas calles, porque “ya las conoces”.
- Publicas una historia de Instagram con tu café de la mañana, etiquetando el lugar exacto donde estás.

En apariencia, todo esto es normal (Ver Figura 1). Pero, visto desde la seguridad, cada uno de esos pasos deja un rastro:

patrones predecibles, información visible y puntos débiles físicos y digitales.

Los estudios sobre criminalidad urbana muestran que los victimarios suelen aprovechar precisamente esos patrones: horarios repetidos, recorridos fijos, distracciones en el transporte público o zonas de baja vigilancia (Vilalta et al., 2016b). No es casualidad que muchas víctimas, al relatar un robo o una agresión, digan frases como: “Yo siempre hacía lo mismo, nunca me había pasado nada”. La rutina se vuelve una especie de “coartada psicológica” para no pensar en el riesgo.

### Figura 1

*Un día típico antes de 2020*



#### 1.1.2 Señales que ignoramos y nos hacían vulnerables

A nivel subjetivo, muchas personas eran conscientes de que algo no estaba bien: escuchar de robos frecuentes en el barrio, enterarse de un secuestro exprés en otra ciudad, o ver en las noticias que la delincuencia y la corrupción seguían siendo temas centrales

en la agenda pública. Encuestas como Latinobarómetro y otros estudios regionales muestran que crimen, violencia e inseguridad eran percibidos como uno de los principales problemas sociales de América Latina, incluso antes de la pandemia (OECD, 2020).

Sin embargo, que un problema sea percibido como grave no significa que se traduzca en cambios de conducta. De hecho, había una especie de “contradicción” cotidiana:

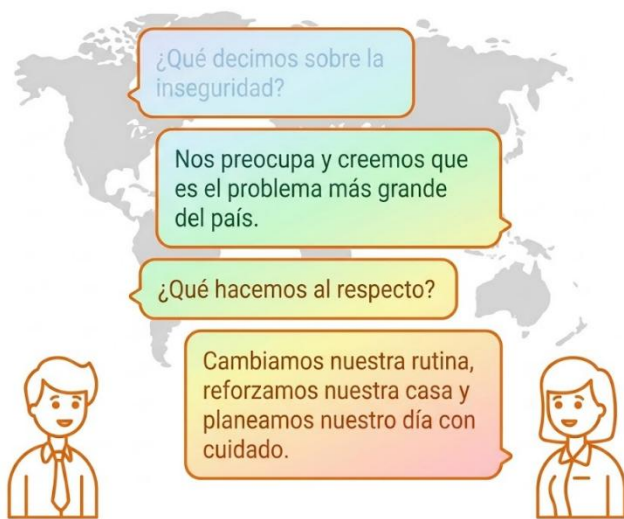
- Se reconocía la inseguridad en términos generales (“el país está peligroso”).
- Pero se minimizaba el riesgo personal (“a mí no me va a pasar”).

Esta paradoja ha sido estudiada por la psicología como sesgo de optimismo y sesgo de normalidad. El primero se refiere a la tendencia a pensar que los eventos negativos son menos probables para uno mismo que para los demás (Sharot, 2011). El segundo, el sesgo de normalidad, implica subestimar la posibilidad de una crisis porque el cerebro asume que “todo seguirá como siempre”. Ambos sesgos estaban presentes en la vida previa al COVID-19: escuchábamos historias de asaltos, pero seguíamos usando el celular en la calle; veíamos noticias de corrupción, pero confiábamos en que “al final no afectaría tanto nuestra vida” (ver Figura 2).

Desde la seguridad ciudadana esto tiene una consecuencia directa: si la mente normaliza el riesgo, la persona no se prepara. No revisa salidas de emergencia, no toma rutas alternativas, no conversa en familia sobre qué hacer ante un incidente, no revisa la configuración de privacidad de sus redes sociales. Es decir, las señales estaban ahí, pero el sistema mental y social prefería mirarlas de reojo.

## Figura 2

### Conversación típica antes de 2020



#### 1.1.3. Rutinas en casa, en la calle y en lo digital: capas de riesgo

Las vulnerabilidades ocultas no aparecían solo en un momento del día, sino en capas (Vilalta et al., 2016b):

1. En el hogar: En muchos barrios de la región, las casas tenían rejas, candados y puertas metálicas. Esa imagen transmitía fortaleza, pero no siempre se acompañaba de hábitos consistentes: dejar las llaves “escondidas” bajo la alfombra, compartir en redes sociales que la familia estaba de viaje, o confiar en que “el barrio se cuida solo”. Al mismo tiempo, las estadísticas mostraban que gran parte de los delitos violentos se concentraban en contextos urbanos, con una fuerte presencia de violencia interpersonal y organizada (Vilalta et al., 2016a).
2. En el traslado y el espacio público: Usar siempre la misma parada de bus, caminar por la misma calle poco iluminada o distraerse con el teléfono en la mano eran conductas ubicuas.

El espacio público, ya marcado por desigualdades urbanas, se convertía en escenario donde la rutina hacía predecible a la víctima. De acuerdo con la ONU (2021) estudios sobre crimen urbano han resaltado que la combinación de patrones repetidos, baja vigilancia y entornos socialmente excluidos facilita la acción delictiva.

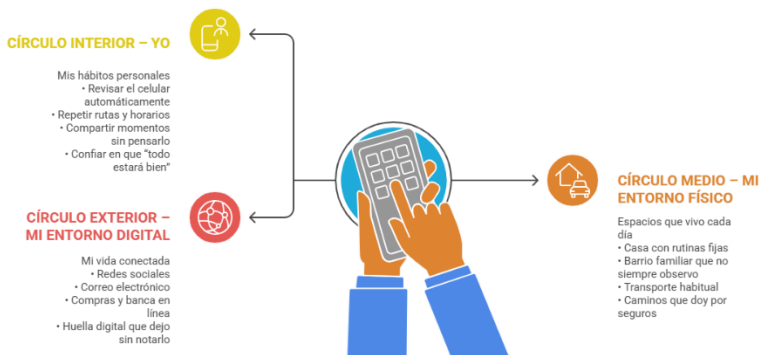
3. En la vida digital: Incluso antes de la pandemia, el uso de Internet y dispositivos móviles crecía aceleradamente en América Latina. La penetración de banda ancha móvil en la región pasó, en promedio, de 8,27 % en 2011 a 44 % en 2015, lo que muestra una rápida adopción de tecnologías móviles (Alderete, 2019). A nivel global, la Unión Internacional de Telecomunicaciones (2019) señalaba que solo algo más de la mitad de la población mundial estaba conectada, a pesar de que el 97 % estaba bajo cobertura móvil. Esto significa que, en pocos años, millones de personas de la región integraron el celular a su rutina diaria... pero sin una educación proporcional en ciberseguridad y protección de datos.

En este contexto, acciones aparentemente inocentes como compartir fotos de la familia, publicar tickets de viaje, etiquetar la ubicación en tiempo real o aceptar solicitudes de amistad de desconocidos configuraban un mapa muy detallado de la vida del usuario. Para un delincuente, esa información puede ser tan valiosa como una llave física. A continuación, se presentan las capas de vulnerabilidad habituales de las personas (ver Figura 3).

Las rutinas nos daban la sensación de que el mundo era manejable. Ir de un punto A a un punto B, repetir horarios, ver las mismas caras... todo ello construía una narrativa de control. Sin embargo, los datos sobre violencia, la expansión tecnológica sin acompañamiento educativo y los sesgos psicológicos en la percepción del riesgo muestran que esa seguridad era, en gran parte, una ilusión. Este apartado ha querido hacer visible lo

invisible: las pequeñas decisiones que, acumuladas, pueden aumentar o disminuir nuestra vulnerabilidad.

**Figura 3**  
*Capas de vulnerabilidad*



## Ejercicio 1

### Mini-tip Práctico

#### 3 Riesgos Ocultos en tu Rutina

El objetivo es generar *consciencia activa, no miedo*.



#### Paso 1: Contexto

Piensa en tu mañana típica, desde que te levantas hasta que llegas a tu lugar de trabajo o estudio.



#### Paso 2: Identifica

Haz una lista rápida de **tres acciones** que realizas siempre igual.

- Revisar el celular en la calle.
- Dejar la laptop visible en el auto.
- Publicar una historia desde el mismo lugar.



#### Paso 3: Analiza y Ajusta



¿Qué información estoy mostrando sin querer?



¿Quién podría aprovechar esta información o este hábito?



¿Qué mínimo ajuste podría hacer mañana para reducir ese riesgo?

Este tipo de ejercicios ayuda a romper el sesgo de normalidad, porque obliga a mirar la rutina con otros ojos. Como señalan los estudios sobre percepción del riesgo, el primer paso para cambiar un comportamiento es reconocer que el peligro existe y puede afectarnos personalmente.

## **1.2. Problemas que ignorábamos**

Antes del COVID-19, en buena parte de América Latina ya convivíamos con una realidad marcada por la violencia y el delito, pero de una forma normalizada. Las noticias sobre robos, asesinatos, extorsiones o corrupción formaban parte del paisaje informativo cotidiano, y sin embargo, muchas personas sentían que esos problemas estaban “lejos” de su vida diaria. La sensación era paradójica: por un lado, se reconocía que la región era insegura; por otro, se actuaba como si nada grave fuera a ocurrirnos personalmente.

Diversos informes muestran que, incluso antes de la pandemia, América Latina y el Caribe concentraban algunas de las tasas de homicidio más altas del mundo, con niveles aproximadamente tres veces superiores al promedio global (18 frente a 5,6 homicidios por cada 100.000 habitantes (UNODC, 2022). Aun así, para muchas personas estos números eran “estadísticas lejanas” que no se traducían en cambios de conducta preventiva. La violencia se percibía como un problema estructural de los Estados, de los barrios “peligrosos” o de los grupos criminales, pero rara vez como un riesgo que exigiera revisar nuestros hábitos cotidianos de seguridad.

### ***1.2.1 Seguridad ciudadana antes de la pandemia: problemas latentes***

Detrás de la aparente normalidad pre-pandemia, existían tres grandes problemas que permanecían, en gran medida, invisibles o subestimados (ver Figura 4):

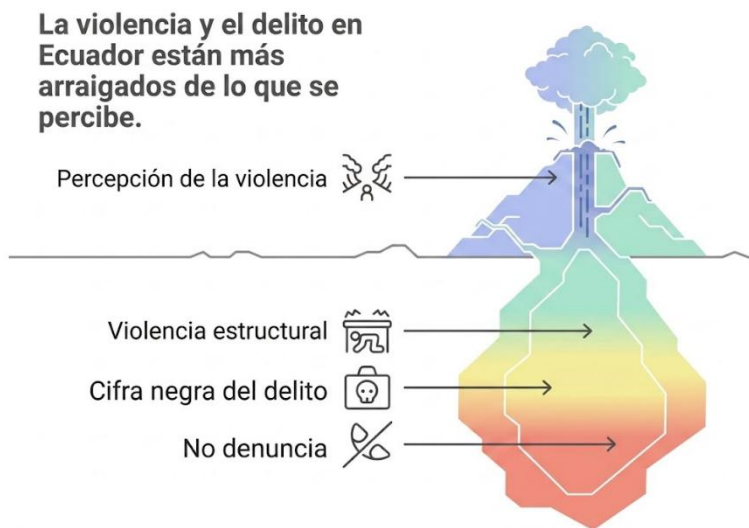
1. Altos niveles de violencia y delito crónico: Informes del Banco Mundial y de UNODC han señalado de forma consistente que América Latina y el Caribe se mantienen, desde hace años, entre las subregiones con mayor tasa de homicidios a nivel global (Wepy, 2021). Lejos de ser un fenómeno coyuntural, la violencia letal y la criminalidad urbana se habían consolidado como rasgos estructurales, asociados a desigualdad, presencia de crimen organizado y debilidad institucional.
2. La “cifra negra”: delitos que nunca se denuncian: Uno de los problemas más graves y menos visibles es la enorme cantidad de delitos que nunca llegan a registrarse. Estudios sobre la llamada “cifra negra del delito” muestran que en América Latina existe una brecha significativa entre los delitos que la población declara haber sufrido en encuestas de victimización y los que efectivamente constan en los registros policiales. Para ciertos tipos de violencia, especialmente la violencia de género, esta cifra negra puede alcanzar entre el 92 % y el 95 %, es decir, solo una pequeña fracción de los hechos llega a ser denunciada o registrada (Augustín et al., 2022).
3. Altísima no denuncia en países específicos, como Ecuador: Investigaciones recientes señalan que Latinoamérica registra algunas de las tasas más altas de no denuncia del mundo, y que en países como Ecuador alrededor del 80 % de los hechos delictivos no se reportan a las autoridades (Arévalo, 2021). Esto significa que, antes de la pandemia, ya existía una gran brecha entre la inseguridad real que vivían las personas y la inseguridad “oficial” que reflejaban las estadísticas. Muchas víctimas optaban por el silencio por desconfianza institucional, miedo a represalias o la percepción de que “no sirve de nada denunciar”.

Desde el punto de vista psicológico, esta situación generó una especie de equilibrio falso: la gente sentía miedo, pero no lo suficiente como para transformar sus pautas de comportamiento. Investigaciones sobre victimización y miedo al delito en

Latinoamérica muestran que haber sido víctima directa o temer serlo se asocia con menor satisfacción con la vida y menor bienestar subjetivo (Reyes-Martínez, 2021). Sin embargo, ese malestar muchas veces se gestionaba con resignación, más que con estrategias de protección consciente.

#### Figura 4

*Problemas latentes de seguridad antes del COVID-19*



#### **1.2.2 Ejemplo real: cómo un descuido común pone en riesgo a todos**

Para entender estos problemas de manera más cercana, imaginemos una escena cotidiana antes de 2020:

Un vecino sale de casa a trabajar apurado. Deja la puerta sin asegurar completamente porque “solo se va un momento”. En la vereda, un desconocido observa la rutina: sabe a qué hora sale, cuánto tarda y quién queda dentro de la vivienda. Ese mismo día, alguien entra sin forzar cerraduras, se lleva un computador portátil y algunos objetos pequeños. El vecino duda en denunciar: piensa

que “no van a recuperar nada” y teme que los trámites sean una pérdida de tiempo. Al final, no acude a la policía.

Lo que, a simple vista, parece “un robo más”, en realidad revela varios de los problemas que ignorábamos:

- Un hábito débil de seguridad (no asegurar bien la puerta, repetir la misma rutina todos los días).
- La observación silenciosa de terceros sobre nuestros movimientos y vulnerabilidades.
- La normalización del delito menor, que se asume como “parte de la vida urbana”.
- La decisión de no denunciar, que alimenta la cifra negra y envía un mensaje implícito de impunidad.

Si multiplicamos ese mismo patrón por miles de hogares, tenemos una imagen clara de por qué buena parte de la inseguridad en la región permanecía oculta o subestimada. Las estadísticas oficiales captaban solo una parte del problema, mientras que el resto (miedo, resignación, desconfianza) quedaba encerrado en los relatos personales.

## Ejercicio 2

**¿En cuántas ocasiones has salido de casa confiando en que 'no va a pasar nada'?**

(Este recuadro ayuda a que el lector se identifique con la situación).

### La Inercia de la Rutina

Cada mañana, nuestra rutina nos envuelve en una inercia cómoda. Ejecutamos hábitos confiando ciegamente en que "siempre ha sido seguro".



#### Revisar el Celular

Justo al salir de la puerta, mostrando distracción y vulnerabilidad.



#### Mochila sin Supervisión

Por solo un minuto, tiempo suficiente para un oportunista.



#### Compartir Ubicación

Creando un patrón diario predecible para un observador.

Este tipo de recuadro ayuda a que el lector se identifique con la situación y conecte su propia experiencia con los datos que se presentan en el capítulo.

### 1.3 El enemigo invisible: la brecha digital

Antes de la pandemia, la mayoría de las conversaciones sobre seguridad se centraban en lo visible: la calle, el barrio, el transporte público, la vivienda. Sin embargo, ya se venía gestando un enemigo silencioso e invisible: la brecha digital. Esta no solo se refería a quién tenía o no tenía conexión a internet, sino también a cómo se usaba esa conexión, con qué nivel de conocimiento y bajo qué condiciones de protección o vulnerabilidad.

En América Latina, diversos organismos advertían que el acceso a las tecnologías de la información y la comunicación avanzaba de forma desigual. El Índice de Desarrollo de la Banda Ancha (IDBA) del Banco Interamericano de Desarrollo mostraba, ya en 2020, que la región mantenía brechas persistentes en infraestructura, capacidades y uso avanzado de internet, con diferencias notables entre zonas urbanas y rurales, y entre grupos de altos y bajos ingresos (BID, 2020). Es decir, mientras algunos sectores urbanos comenzaban a disfrutar de digitales, otros seguían desconectados o con conexiones de muy baja calidad.

En el caso de Ecuador, la Encuesta TIC 2019 del Instituto Nacional de Estadística y Censos reportó que solo el 45,5 % de los hogares tenía acceso a internet a nivel nacional antes de la pandemia, lo que implica que más de la mitad de las familias seguía excluida de la conectividad básica (INEC, 2019). Esta cifra revela que la promesa de un mundo digital accesible para todos era, en la práctica, una realidad parcial y profundamente desigual.

### ***1.3.1 Acceso desigual, riesgos desiguales***

La brecha digital no solo separaba a quienes estaban conectados de quienes no lo estaban; también ampliaba las desigualdades en educación, empleo, información y protección. Estudios en la región muestran que, a nivel de hogares, alrededor del 59 % de los residentes urbanos y apenas el 20 % de los residentes rurales utilizaban algún tipo de servicio de internet antes del COVID-19, reflejando una distancia importante entre ciudad y campo (Palacios, 2021).

Esta desigualdad tenía consecuencias directas sobre la seguridad. Quien no estaba conectado perdía acceso a información relevante, a servicios en línea, a oportunidades educativas y laborales, e incluso a sistemas de alerta temprana. En cambio, quien sí estaba conectado, muchas veces lo hacía sin formación ni conciencia de riesgo, exponiendo datos personales, opiniones y

rutinas a un entorno digital poco regulado. En otras palabras, la brecha digital producía dos tipos de vulnerabilidad (ver Figura 5):

- Vulnerabilidad por exclusión (no tengo internet, quedo fuera).
- Vulnerabilidad por exposición sin protección (tengo internet, pero no sé cuidarme en línea).

A nivel regional, la Comisión Económica para América Latina y el Caribe (CEPAL) ya alertaba, antes de la pandemia, que el 81 % de los hogares de mayores ingresos tenía conexión a internet, frente a solo el 38 % de los hogares de menores ingresos, creando una distancia estructural entre quienes podían aprovechar los beneficios de la digitalización y quienes quedaban rezagados (CEPAL, 2023). Esta brecha no solo era tecnológica, sino también social y de seguridad.

### Figura 5

*Dos vulnerabilidades en un mismo mundo digital*



#### 1.3.2 Tus datos y privacidad sin protección

Para quienes sí estaban conectados, el problema no era solo el acceso: era el uso ingenuo de la tecnología. Antes de 2020, millones de personas crearon perfiles en redes sociales, compartieron fotografías, ubicaciones en tiempo real, opiniones políticas y hasta datos familiares sin preguntarse quién podía ver, guardar o explotar esa información.

## Figura 6

### *Ciclo básico de los datos personales en plataformas digitales*



Esta figura ayudaría a que el lector comprenda visualmente que cada acción digital genera un rastro, y que ese rastro tiene valor e impacto en su seguridad.

Las plataformas digitales se consolidaron como espacios de interacción masiva, pero también como mecanismos de recolección de datos sumamente detallados. Empresas y anunciantes empezaron a operar con modelos de negocio basados en el seguimiento de la actividad del usuario lo que consulta, lo que compra, lo que “likea”, sin que la mayoría tuviera una idea clara de la magnitud de esa vigilancia comercial (BID, 2021).

Al mismo tiempo, la ausencia de una cultura de ciberseguridad básica hacía que muchas personas reutilizaran contraseñas, ignoraran la autenticación de dos factores o descargaran archivos de procedencia dudosa. El World Bank reportó que el costo global del cibercrimen alcanzó alrededor de 600 mil millones de dólares en 2018, mostrando que los ataques

digitales ya eran un fenómeno masivo y rentable para los delincuentes incluso antes del COVID-19 (World Bank, 2018).

En este escenario, tus datos personales y tu privacidad estaban, en la práctica, poco protegidos. No se trataba solo de “si alguien hackea mi cuenta”, sino de una exposición sistemática de hábitos, preferencias y relaciones que podía ser utilizada para fines comerciales, políticos o delictivos sin que el usuario lo percibiera.

### ***1.3.3 Cómo hackers y actores maliciosos aprovechan la desinformación***

La misma estructura digital que permitía compartir información útil se convirtió también en una vía para diseminar desinformación, engaños y estafas. Antes de la pandemia, el Latin American Communication Monitor 2018–2019 identificaba el fenómeno de las fake news como uno de los principales desafíos para la comunicación estratégica en la región, señalando que los profesionales ya percibían la desinformación como un riesgo creciente para las instituciones y la ciudadanía (Moreno et al., 2019).

Los ciberdelincuentes aprendieron rápidamente a explotar esta mezcla de brecha digital, baja alfabetización mediática y exposición de datos. Correos falsos de bancos, supuestos premios, ofertas irreales y mensajes alarmistas se convirtieron en herramientas para obtener contraseñas, números de tarjetas o información sensible (Paspuel et al., 2024). En contextos de alta desigualdad, estas estrategias eran especialmente efectivas entre personas con menos formación digital, reforzando la vulnerabilidad de quienes ya enfrentaban dificultades económicas y educativas.

En términos de seguridad, la brecha digital se traducía así en una paradoja:

- Quienes estaban fuera de la red carecían de información y servicios clave.

- Quienes estaban dentro, pero sin formación, se convertían en blanco fácil de manipulación y fraude.

Ambos grupos, por razones distintas, estaban expuestos a un enemigo que no se veía en la calle, pero que operaba de manera constante desde pantallas, servidores y algoritmos.

#### **1.4. Vivir sin miedo... ¿realmente?**

Durante muchos años, en gran parte de América Latina se instaló la idea de que “hay inseguridad, pero uno aprende a vivir con eso”. La rutina, la costumbre y la necesidad de seguir adelante hicieron que muchas personas afirmaran que “no viven con miedo”, aunque sus decisiones diarias estuvieran marcadas por la preocupación y la desconfianza. Antes de la pandemia, esta aparente tranquilidad se sostenía en una mezcla de normalización del riesgo, falta de información y varios sesgos psicológicos que nos llevaban a minimizar los peligros reales.

Los datos muestran que esa sensación de control era, en buena medida, una ilusión. Informes recientes señalan que alrededor del 50 % de los residentes de América Latina y el Caribe declaran sentirse inseguros, frente a un promedio cercano al 20 % a nivel mundial (Rodríguez et al., 2024).

Al mismo tiempo, en algunos estudios de victimización se observa que aproximadamente un tercio de la población ha sufrido al menos un delito en los últimos años, y aun así muchas personas consideran que “exagerar” las precauciones no es necesario (Reyes, 2021).

Es decir, objetivamente el entorno es riesgoso, pero subjetivamente una parte importante de la población insiste en que “no tiene miedo” o que “no le va a pasar”.

Esta aparente contradicción se explica, en parte, por el llamado optimismo irrealista. La psicología social ha mostrado que

tendemos a creer que los eventos negativos son menos probables en nuestra propia vida que en la de los demás. Neil Weinstein, en un estudio clásico, demostró que muchas personas juzgan su riesgo personal frente a enfermedades o accidentes como menor que el de sus pares, incluso cuando los datos objetivos no respaldan esa percepción (Weinstein, 1980). Este fenómeno, conocido como *optimism bias*, lleva a frases como “sí hay robos, pero a mí no me va a pasar”, o “esa estafa le ocurre a gente descuidada, yo me fijo”. La consecuencia práctica es clara: si siento que el riesgo es “para otros”, no cambio mi conducta.

A este sesgo se suma el llamado sesgo de normalidad o *normalcy bias*. Este sesgo describe la tendencia a subestimar la posibilidad y el impacto de un desastre o crisis, asumiendo que la vida seguirá siendo normal, incluso ante señales claras de peligro (Ginés, 2021).

Se ha observado en eventos tan diversos como desastres naturales, guerras o colapsos económicos: muchas personas retrasan su reacción, dudan de las advertencias o permanecen en lugares de riesgo porque “siempre ha estado todo bien”. En términos cotidianos, el sesgo de normalidad se traduce en pensamientos como “siempre he hecho esto así y nunca pasó nada” (ver Figura 7).

Desde el punto de vista emocional, decir “no tengo miedo” no siempre significa ausencia de miedo, sino a veces miedo encapsulado. Muchas personas prefieren no hablar de sus temores porque creen que hacerlo es signo de debilidad, o porque sienten que nada cambiará. Otros transforman el miedo en cinismo o en bromas, como una manera de lidiar con la ansiedad. Sin embargo, la investigación reciente indica que la percepción de inseguridad y la exposición a delitos se asocian con mayores niveles de malestar psicológico, síntomas de ansiedad y deterioro en la salud mental. Es decir, aunque el discurso público insista en “vivir sin miedo”, el cuerpo y la mente registran el impacto.

En la práctica, esta ilusión de vivir sin miedo tiene efectos concretos en la forma en que organizamos nuestra vida. Cuando pensamos que tenemos todo bajo control:

- Postergamos decisiones importantes de prevención (asegurar la vivienda, revisar contraseñas, hablar en familia de qué hacer ante una emergencia).
- Naturalizamos conductas de riesgo, como compartir información personal en redes, desplazarnos por zonas peligrosas sin avisar a nadie o confiar en enlaces y mensajes dudosos.
- Evitamos informarnos en profundidad, porque hacerlo nos obligaría a cambiar hábitos que consideramos cómodos.

La pandemia de COVID-19 fue, en este sentido, un golpe frontal a esa ilusión de seguridad. Mostró que la vida podía cambiar radicalmente en cuestión de semanas, que los sistemas de salud y de seguridad no estaban preparados y que nuestras vidas digitales y físicas estaban mucho más conectadas de lo que pensábamos. Muchos experimentaron, por primera vez, la sensación de que “nadie tiene el control absoluto”, y que el miedo puede ser también una señal útil para reorganizar prioridades y conductas.

### Figura 7

*Tipos de sesgo presentes en ante eventos inesperados*



#### Optimismo Irrealista

Crea una falsa sensación de invulnerabilidad



#### Sesgo de Normalidad

Fomenta la complacencia y la falta de preparación

## 1.5. Despertar a la realidad

La pandemia de COVID-19 funcionó como un espejo brutal: nos obligó a ver que la seguridad que creíamos tener era, en gran medida, una construcción frágil. Lo que se pensaba como “normalidad” a rutinas estables, contacto social cercano, uso cotidiano de la tecnología sin mayor reflexión; se quebró de un día para otro. Millones de personas experimentaron, quizá por primera vez, la sensación simultánea de vulnerabilidad física, emocional y digital.

En el plano emocional, la evidencia muestra que el impacto no fue menor. La Organización Mundial de la Salud (OMS) estimó que, solo en el primer año de la pandemia, la prevalencia global de ansiedad y depresión aumentó alrededor de un 25 %, asociada al miedo al contagio, el aislamiento y la incertidumbre económica (OMS, 2022a). Es decir, no solo estábamos expuestos a un virus, sino también a una crisis de salud mental que alteró la forma en que las personas perciben su seguridad y su futuro (Kupcova et al., 2023).

En paralelo, en regiones como América Latina, la pandemia se superpuso a una realidad ya complicada en términos de violencia, desigualdad y crimen organizado. Informes recientes recuerdan que la región continúa siendo una de las más violentas del mundo, con tasas de criminalidad que se mantienen por encima de niveles considerados “epidémicos” y donde la falta de seguridad ciudadana es un obstáculo central para el desarrollo (UNODC, 2023). Aun cuando algunos delitos disminuyeron durante los confinamientos estrictos, nuevas formas de violencia, extorsión y criminalidad se adaptaron rápidamente al contexto pandémico, especialmente en entornos digitales y en economías ilícitas ligadas a la crisis.

Desde la teoría social, autores como Ulrich Beck ya advertían que vivimos en una “sociedad del riesgo”, es decir, un tipo

de modernidad que se organiza alrededor de la gestión de peligros producidos por nuestras propias formas de vida: tecnología, consumo, globalización, sistemas financieros, entre otros (Leiss et al., 1994). El COVID-19 no creó la vulnerabilidad, pero sí la visibilizó: nos mostró que no basta con tener cerraduras y alarmas; también necesitamos sistemas de protección emocional, redes de apoyo y mínimos de seguridad digital.

### ***1.5.1 Qué aprendimos sobre la seguridad que creíamos tener***

El primer aprendizaje es que la seguridad no puede reducirse a la idea de “estar a salvo mientras nada cambie”. La pandemia demostró que:

1. La estabilidad era más frágil de lo que pensábamos. Un virus invisible paralizó sistemas de salud, escuelas, empresas y gobiernos. La vida cotidiana se alteró en cuestión de semanas, y muchos de los supuestos de “normalidad” dejaron de ser válidos.
2. El bienestar emocional es parte de la seguridad. El aumento de trastornos de ansiedad y depresión muestra que no basta con evitar el delito o la enfermedad física; necesitamos cultivar recursos internos para afrontar la incertidumbre (OMS, 2022a)
3. Lo digital dejó de ser accesorio para volverse estructural. Teletrabajo, educación virtual, banca electrónica y redes sociales pasaron a ser infraestructuras críticas. Esto vino acompañado de un aumento documentado de ataques informáticos y ciberamenazas vinculadas al contexto del COVID-19 (Saleous et al., 2022).
4. La inseguridad no es solo objetiva, también es subjetiva. Estudios recientes sobre percepción de inseguridad muestran que, en América Latina, una parte importante de la población identifica el crimen y la violencia como el principal problema de sus países (Bisca et al., 2024)

5. La sensación de inseguridad no depende solo de las cifras de delito, sino también de la experiencia emocional de miedo, desconfianza y vulnerabilidad (Hernández & Zurita, 2022)

En conjunto, el “despertar” consiste en reconocer que la seguridad es multidimensional: incluye lo físico, lo emocional, lo social y lo digital. Seguir pensando en seguridad solo como “no me asaltan en la calle” es, hoy, quedarse peligrosamente corto.

### ***1.5.2 Claves para no repetir errores del pasado***

A partir de estas lecciones, el reto es no volver a caer en la misma ilusión de control. Algunas claves son:

- Pasar de la reacción a la prevención. La pandemia evidenció que muchos sistemas, desde la salud hasta la protección social estaban diseñados para responder tarde (Castillo et al., 2022). A nivel individual, esto se traduce en dejar de “esperar a que pase algo” para recién actuar: planificar, anticipar escenarios y construir hábitos de cuidado es esencial.
- Aceptar el riesgo como parte de la vida moderna. En lugar de negar el riesgo, la propuesta es relacionarnos de forma más adulta con él, reconociendo que siempre existirán amenazas, pero que podemos desarrollar estrategias de reducción de daño, resiliencia y aprendizaje continuo (Leiss et al., 1994).
- Desarrollar pensamiento crítico frente a la información. El caos informativo durante la pandemia mostró lo fácil que es manipular emociones y decisiones a través de noticias falsas o mensajes alarmistas (Saleous et al., 2022)
- Educarse para verificar fuentes, contrastar datos y no compartir contenido sin revisar se convierte en una forma de autoprotección y cuidado colectivo.

Entender la seguridad como un derecho y un proyecto compartido.

Organismos como el PNUD plantean la seguridad ciudadana como un bien público y un metaderecho humano: no depende solo de la policía o del Estado, sino también de la comunidad y de las redes de apoyo (R. González, 2024)

Para que este “despertar” no se quede solo en una reflexión teórica, puedes trabajar con una base de seguridad personal en cinco pasos. Este checklist (ver Figura 8) se presenta a continuación:

**Figura 8**  
*Checklist para tu seguridad personal*

**1. Revisa tu Entorno Físico**

- Identifica 3 riesgos concretos (zonas oscuras, puertas sin seguro, trayectos solitarios).
- Prioriza qué puedes corregir con un cambio pequeño esta semana.

**2. Cuida tu Mente y Cuerpo**

- Observa tus niveles de estrés, miedo o ansiedad.
- Si notas síntomas persistentes, considera buscar apoyo profesional (OMS, 2022).

**3. Establece Higiene Digital**

- Cambia contraseñas débiles. Activa la autenticación de dos pasos (2FA).
- Desconfía de enlaces o mensajes que usen miedo o urgencia (Saleous et al., 2022).

**4. Construye tu Red Mínima de Apoyo**

- Haz una lista de 3 a 5 personas clave con quienes contar en momentos de crisis.
- Acuerden canales de comunicación de emergencia y puntos de encuentro.

**5. Actualiza tu Visión (Cada 6 Meses)**

- Repite este checklist y pregúntate: ¿Qué cambió en mi entorno (físico, digital, emocional)?
- Ajusta tus hábitos según nuevas amenazas, experiencias o aprendizajes.



## **Capítulo 2:**

### **El impacto de la pandemia: vulnerabilidades al descubierto**

## **2.1. El confinamiento global y la cultura del miedo**

Cuando la Organización Mundial de la Salud (OMS) declaró la pandemia de COVID-19 en marzo de 2020, el mundo entró en una fase de restricciones sin precedentes. En pocos días, más de 180 países impusieron cierres de escuelas, límites a la movilidad, suspensiones de actividades presenciales y órdenes de confinamiento. El Oxford COVID-19 Government Response Tracker (OxCGRT) documentó sistemáticamente estas medidas desde el cierre de centros educativos hasta restricciones de viaje, toques de queda y confinamientos; y construyó un índice de “rigidez” que mostró niveles extremos de severidad en la mayoría de los países durante 2020 y 2021 (Hale et al., 2021).

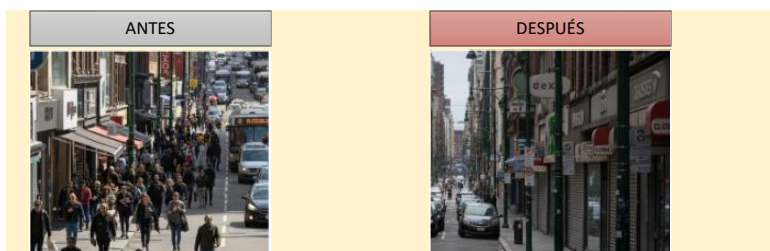
### ***2.1.1. Un mundo en pausa: confinamiento y restricciones históricas***

Para millones de personas, la vida cotidiana se redujo a unos pocos espacios: la casa, la pantalla del ordenador y el teléfono móvil. Las calles se vaciaron, las interacciones presenciales se interrumpieron y muchas actividades esenciales se trasladaron a lo digital. UNICEF (2021) estimó que al menos 1 de cada 7 niños y jóvenes (unos 332 millones en todo el mundo) vivió bajo políticas de “quedarse en casa” (stay-at-home) durante la mayor parte del primer año de la pandemia, con impactos directos en su bienestar emocional y su salud mental.

Aunque el confinamiento fue una de las herramientas más efectivas para frenar la transmisión del virus en la comunidad, las revisiones señalan que las medidas de distanciamiento y los cierres redujeron de forma significativa la propagación de la COVID-19 (Murphy et al., 2023). De un día para otro, se interrumpieron los trayectos habituales, los encuentros informales, las pausas en el trabajo o en la universidad, y los espacios públicos que funcionaban como amortiguadores del estrés (ver Figura 9).

## Figura 9

*Espacio público antes y después del confinamiento por COVID-19.*



### ***2.1.2. Impacto emocional y mental del encierro***

El confinamiento no solo modificó los espacios; también impactó de forma profunda en la salud mental. Revisiones amplias sobre la pandemia y la salud mental señalan que la COVID-19 se asoció con un aumento de síntomas de ansiedad, depresión, estrés postraumático, insomnio y soledad, tanto en población general como en grupos específicos (Clemente-Suárez et al., 2021).

En el caso de América Latina, donde la pandemia se superpuso a contextos de desigualdad, informalidad laboral y sistemas de salud frágiles, el impacto psicosocial fue especialmente intenso. Gallegos et al. (2021), en una revisión sobre la región, destacan que la pandemia generó “consecuencias psicosociales y de salud mental significativas” y visibilizó problemas preexistentes como el acceso desigual a servicios, la precariedad económica y la exposición a múltiples formas de violencia.

Asimismo, estudios empíricos con muestras de la región muestran cifras preocupantes: Caycho-Rodríguez et al. (2021) evaluaron a 4.881 personas de siete países latinoamericanos (Argentina, Ecuador, México, Paraguay, Uruguay, Colombia y El Salvador) y encontraron niveles moderados y severos de ansiedad y depresión en una parte importante de la muestra, además de un miedo elevado a la COVID-19. Con lo cual, el modelo estadístico del

estudio muestra que el miedo al contagio predijo de forma significativa los síntomas de ansiedad y depresión

En otras palabras, el confinamiento no fue solo “quedarse en casa”: fue convivir durante meses con el miedo al contagio, la pérdida de ingresos, la inestabilidad laboral o académica y la sobrecarga de cuidados.

La Figura 10 presenta una mini-guía que resume los principales indicadores de saturación emocional, útil para identificar la necesidad de descanso o apoyo profesional.

### Figura 10

#### *Señales de sobrecarga emocional durante un encierro*

Si en un periodo de confinamiento notas que:

 <b>Concentración:</b> <ul style="list-style-type: none"><li>• Te cuesta concentrarte o completar tareas sencillas.</li></ul>	 <b>Sueño:</b> <ul style="list-style-type: none"><li>• Duermes mucho menos o mucho más de lo habitual.</li></ul>	
 <b>Ánimo:</b> <ul style="list-style-type: none"><li>• Sientes irritabilidad, tristeza o miedo la mayor parte del día.</li></ul>	 <b>Información:</b> <ul style="list-style-type: none"><li>• Evitas hablar del tema, consumes muchas noticias sobre él.</li></ul>	 <b>Intereses:</b> <ul style="list-style-type: none"><li>• Has dejado de hacer actividades que antes te daban alegría.</li></ul>

 Si te identificas con varias de estas señales, considera tomar un descanso y buscar apoyo.

### 2.1.3. Cultura del miedo e inseguridad cotidiana

El confinamiento también instaló una cultura del miedo que iba más allá del riesgo sanitario. El virus estaba en todas partes: en las superficies, en la respiración de otros, en los objetos que llegaban a la casa. La consigna de “protégete del otro” alteró la forma de mirar a desconocidos, vecinos e incluso familiares. La proximidad que antes era sinónimo de confianza y afecto comenzó a percibirse como potencial amenaza.

En América Latina, donde la inseguridad ya formaba parte del paisaje cotidiano, esta cultura del miedo se superpuso a temores

preexistentes: miedo al delito, a la pérdida del empleo, al colapso del sistema sanitario. Estudios sobre la región señalan que la pandemia “agravó el malestar psicosocial” y se sumó a un contexto de altos niveles de ansiedad, estrés y miedo en la población (Clemente-Suárez et al., 2021).

La sensación de inseguridad ya no se limitaba a “la calle” o a ciertos barrios, sino que entraba en la casa a través de la pantalla: cifras de fallecidos, imágenes de hospitales, rumores en redes sociales, cadenas de WhatsApp con información alarmante (Clemente-Suárez et al., 2021). Una parte importante de la población comenzó a tomar decisiones principalmente desde el miedo: acumular productos, aislarse en exceso, evitar cualquier gestión presencial, aunque fuera necesaria o, en el extremo contrario, negar la gravedad de la situación como mecanismo de defensa.

### Ejercicio 3

**Ejercicio práctico – “Mi línea del tiempo del confinamiento”**

Dibuja una línea del tiempo del periodo de confinamiento más estricto que viviste. Marca tres momentos: inicio, punto de mayor miedo, y un momento en que empezaste a adaptarte.

El diagrama muestra una línea del tiempo horizontal que avanza de izquierda a derecha. Se dividen en tres secciones principales:

- INICIO (Confinamiento estricto):** Representado por un ícono de una casa con una cerradura y un calendario. Debajo hay un cuadro con tres preguntas: "¿Qué sentías?", "¿Qué información consumías?" y "¿Qué decisiones tomabas para 'sentirte seguro/a'?".
- PUNTO DE MAYOR MIEDO:** Representado por un ícono de una persona con una nube de pensamientos y un ícono de noticias con un signo de exclamación. Debajo hay un cuadro con las mismas tres preguntas.
- ADAPTACIÓN (Punto de inflexión):** Representado por un ícono de una planta creciendo y un ícono de una persona en una casa. Debajo hay un cuadro con las mismas tres preguntas.

Este ejercicio permite conectar la experiencia personal con la idea de cultura del miedo, y sirve como puente hacia las secciones siguientes del capítulo.

## **2.2. La digitalización forzada: dependencia tecnológica y exposición**

Cuando el mundo “se cerró” físicamente, muchas de las puertas que quedaron abiertas fueron pantallas. En cuestión de semanas, actividades que antes se repartían entre la casa, la oficina, la universidad, el banco, el supermercado o los espacios de ocio se concentraron en el mismo lugar: la conexión a Internet del hogar.

La Organización Internacional del Trabajo (OIT) describe este periodo como “el experimento de teletrabajo masivo más extenso de la historia”, señalando que millones de trabajadores fueron enviados a casa sin tiempo para preparar políticas claras, equipamiento adecuado o límites saludables entre vida personal y laboral (International Labour Organization, 2020). A la vez, el sistema educativo vivió la mayor disrupción de su historia reciente: la UNESCO estima que, en el momento más crítico, más de 1.6 mil millones de estudiantes en más de 190 países se quedaron fuera de las aulas físicas y dependieron de soluciones de aprendizaje a distancia (CEPAL, 2020).

Con lo cual, esta digitalización acelerada permitió sostener parte de la vida económica y social, pero también multiplicó los puntos de exposición: más cuentas, más contraseñas, más datos personales circulando, más tiempo frente a la pantalla y, muchas veces, menos conciencia de riesgo.

### ***2.2.1 Teletrabajo y educación virtual: continuidad a cualquier precio***

El teletrabajo se presentó inicialmente como una solución “salvadora”: permitía mantener empleos, reducir contagios y sostener cierta normalidad económica. Sin embargo, la OIT (2020) advierte que el paso abrupto a jornadas completas desde casa, sin experiencia previa ni apoyos claros, generó riesgos importantes: aislamiento, jornadas más largas, difuminación de límites entre

trabajo y descanso, y aumento de la carga mental, especialmente para quienes además asumían tareas de cuidado.

Antes de la pandemia, solo una fracción de la fuerza laboral trabajaba desde casa; en algunos países, menos del 5 % lo hacía de forma regular. Con las órdenes de confinamiento entre enero y marzo de 2020, en Europa casi 4 de cada 10 empleados pasaron a teletrabajar, y en países como Finlandia, más de la mitad de los trabajadores se trasladaron súbitamente al hogar (International Labour Organization, 2020). Este cambio masivo se replicó, con matices, en otras regiones.

La consecuencia fue una sensación de “siempre disponible”: reuniones que se extendían más allá del horario, correos contestados de noche, trabajo intercalado con tareas domésticas. Estudios recopilados por la OIT muestran que una proporción importante de personas que trabajaban desde casa durante la pandemia reportaba jornadas más largas, trabajo en tiempo libre y más reuniones uno a uno para compensar la falta de contacto físico.

En paralelo, la educación se volcó a entornos digitales. La UNESCO (2021) reporta que el cierre de escuelas afectó a más de 1.6 mil millones de estudiantes y a más de 100 millones de docentes, obligados a improvisar clases en línea con recursos y capacitación desiguales. Muchos hogares tuvieron que convertir cocinas y dormitorios en aulas, compartiendo un solo dispositivo entre varios integrantes de la familia. Para docentes, estudiantes y trabajadores, el hogar dejó de ser un lugar de descanso y se convirtió en oficina, aula, sala de reuniones y espacio de cuidados al mismo tiempo.

Desde la perspectiva de la seguridad personal, esta continuidad “a cualquier precio” tuvo efectos claros:

- Más datos laborales y académicos circulando por redes domésticas poco protegidas.

- Uso intensivo de plataformas de videoconferencia y almacenamiento en la nube, muchas veces sin revisar sus configuraciones de privacidad.
- Fatiga digital, que reduce nuestra capacidad de identificar correos sospechosos, enlaces falsos o solicitudes de información innecesaria.

La Figura 11 presenta un checklist de ciber-bienestar orientado a promover una pausa digital consciente, útil para equilibrar el teletrabajo y el estudio mediante prácticas seguras y saludables.

### Figura 11

#### *Pausa digital consciente en teletrabajo y estudio*



Este tipo de prácticas no elimina el riesgo, pero ayuda a recuperar algo que la digitalización forzada nos arrebató: la sensación de que podemos poner límites saludables a la tecnología, en lugar de que la tecnología marque la totalidad de nuestro día.

## ***2.2.2 Consumo digital y plataformas: de la comodidad a la sobreexposición***

Mientras el trabajo y el estudio se trasladaban a la red, también lo hicieron compras, pagos y trámites. Plataformas de comercio electrónico, delivery, banca en línea y aplicaciones de movilidad se convirtieron en aliados cotidianos para reducir la exposición física al virus. La Comisión Económica para América Latina y el Caribe (CEPAL) (2020) destaca que, durante la pandemia, las tecnologías digitales jugaron un papel clave para atenuar los efectos de las cuarentenas, pero que las brechas de acceso, asequibilidad y calidad de conexión profundizaron las desigualdades existentes.

Cada nueva cuenta creada en una app de compras o entregas a domicilio implicaba proporcionar nombre, teléfono, dirección, método de pago y, en muchos casos, permisos de geolocalización en tiempo real. Lo que para el usuario se vivía como “comodidad” (la compra llega a la puerta de casa, el taxi aparece en minutos, la comida se rastrea en el mapa) significaba, desde la perspectiva de la seguridad, la creación de un rastro detallado de hábitos:

- Dónde vives y a qué horas sueles estar en casa.
- Qué rutas utilizas con mayor frecuencia.
- Cuándo sueles pedir comida, medicamentos o productos específicos.

Si estos datos se almacenan sin medidas adecuadas de protección, o se comparten con terceros sin transparencia, se convierten en una nueva capa de vulnerabilidad. Informes de CEPAL subrayan que, además de la brecha de acceso, la pandemia aceleró la discusión sobre protección de datos y privacidad, precisamente porque las soluciones digitales se expandieron sin que siempre existieran marcos regulatorios claros o prácticas robustas de seguridad.

La Figura 12 ilustra cómo, a lo largo del día, las actividades digitales cotidianas implican el uso y exposición de distintos tipos de datos personales.

**Figura 12**  
*Tu ruta diaria en la nube*



### 2.3. Auge de la violencia doméstica y comunitaria

El confinamiento no solo detuvo la movilidad y vació las calles: también cerró puertas y obligó a millones de personas a permanecer en casas que no siempre eran seguras. Mientras el discurso público hablaba de “quédate en casa”, para muchas mujeres, niñas, niños y personas mayores, el hogar se transformó en el lugar donde el riesgo era cotidiano.

Organismos internacionales comenzaron a hablar de una “pandemia en la sombra” para referirse al aumento de la violencia contra las mujeres y las niñas durante el COVID-19 (ONU Mujeres, 2020).

En América Latina, un informe del Banco Interamericano de Desarrollo (BID) mostró que, durante los primeros meses de la pandemia, las llamadas a líneas especializadas de atención por violencia doméstica aumentaron entre 16 % y 127 % en ciudades como Buenos Aires, Bogotá o Lima, mientras caían las llamadas al 911 y las denuncias policiales formales, especialmente en países como Ecuador, Colombia o Uruguay (Perez-Vincent & Carreras,

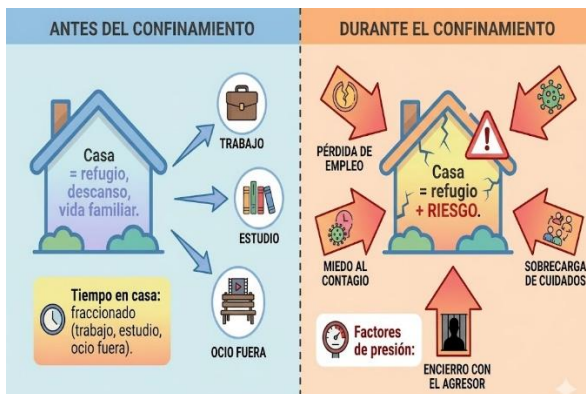
2021). Esto sugiere una realidad incómoda: más violencia, pero menos capacidad de pedir ayuda por los canales tradicionales.

### 2.3.1. El hogar como lugar de riesgo ampliado

Antes de la pandemia, era común pensar en la casa como el espacio más seguro. Sin embargo, el confinamiento reveló que, para muchas personas, el peligro estaba justamente puertas adentro. El cierre de escuelas, la pérdida de empleo, la convivencia forzada con el agresor y el estrés económico crearon una mezcla explosiva de factores de riesgo dentro del hogar.

Desde la psicología social y la salud pública, diversos estudios han mostrado que el confinamiento incrementó factores como el estrés, la ansiedad, la irritabilidad, el abuso de sustancias y la incertidumbre económica, todos asociados a mayor riesgo de violencia intrafamiliar. La casa siguió siendo hogar, pero también se convirtió en una especie de “cámara de presión” donde los conflictos se intensificaban y las salidas eran cada vez más limitadas (ver Figura 13).

**Figura 13**  
Cuando el hogar deja de ser refugio



## Ejercicio 4

### Mini-ejercicio: Mapea tu casa con otros jos



1. Dibuja un plano simple de tu casa.

2. Marca con un color los espacios de calma (ej. dormitorio, balcón).

3. Marca con otro color los espacios de tensión (ej. cocina, sala).

4. Pregúntate: ¿Qué puedes cambiar para reducir tensiones?

Este ejercicio no busca culpabilizar a nadie, sino visibilizar cómo el entorno físico puede amplificar o aliviar el conflicto.

#### **2.3.2. Tensiones, género y comunidad: cuando el conflicto se desborda**

El aumento de la violencia durante la pandemia no fue solo un fenómeno “de puertas adentro”: también se manifestó en los vínculos comunitarios, en los edificios, barrios y espacios donde la convivencia se hizo más intensa. Sin embargo, el impacto no fue neutral: afectó de forma desproporcionada a mujeres, niñas y niños.

La CEPAL (2020) y ONU Mujeres (2020) han señalado que la pandemia profundizó desigualdades ya existentes: la sobrecarga de cuidados no remunerados, la pérdida de empleo femenino y la dependencia económica frente a parejas agresoras incrementaron el riesgo de violencia de género. En América Latina, la violencia feminicida se mantuvo en niveles alarmantes durante 2020, pese al

confinamiento, lo que llevó a hablar de una verdadera “pandemia en la sombra” en la región (CEPAL, 2021).

Al mismo tiempo, un análisis global sobre 26 estudios en países de ingresos bajos y medios halló que 12 de 15 investigaciones (80 %) reportaban incrementos de violencia contra mujeres y niñas durante el COVID-19, especialmente en contextos de fuerte restricción de movilidad y caída de ingresos (Bourgault et al., 2021).

No solo las mujeres adultas estuvieron en riesgo. Informes de OPS/OMS y CEPAL advierten que, durante el confinamiento, las niñas y los niños quedaron más expuestos a la violencia física, psicológica y al abuso, al pasar más tiempo en hogares tensos, con adultos sometidos a estrés, ansiedad y pérdida de ingresos (UNICEF, 2020).

### ***2.3.3. Mini-guía para actuar sin ponerse en riesgo***

Ante la sospecha o la vivencia directa de violencia doméstica, el miedo y la confusión son comprensibles. Durante la pandemia, muchas personas no sabían si podían salir, adónde acudir, o si sería peor “meterse en problemas”. Organismos como ONU Mujeres y la ONU han insistido en que responder a esta “pandemia en la sombra” exige combinar prevención, atención segura y redes de apoyo cercanas (CEPAL, 2020; ONU Mujeres, 2020).

A continuación, la Figura 14 presenta cuatro acciones clave para actuar frente a situaciones de violencia, incluyendo nombrar lo ocurrido, buscar un canal seguro, documentar de forma discreta y proteger a los dependientes.

## Figura 14

### Acciones clave para actuar frente a situaciones de violencia



## 2.4. Cibercrimitos en expansión

Durante la pandemia, mientras gran parte del mundo permanecía encerrado en casa, una parte del delito se movió decididamente al terreno digital. Las mismas condiciones que buscaban proteger la salud física como: teletrabajo, educación virtual, banca y compras en línea; y crearon un escenario ideal para que los ciberdelincuentes ampliaran su campo de acción. Organismos internacionales advirtieron muy pronto que el crimen digital estaba creciendo a un ritmo mucho más rápido que la capacidad de respuesta institucional y ciudadana (Lallie et al., 2021).

En cuestión de meses, el correo electrónico, las redes sociales y las aplicaciones de mensajería se convirtieron en canales privilegiados para fraudes, robos de identidad, extorsiones y ataques a organizaciones públicas y privadas. La región latinoamericana, ya golpeada por desigualdades estructurales, llegó a registrar algunos de los niveles más altos de ciberataques del mundo durante la primera mitad de 2020, especialmente a través de navegadores móviles (Interpol, 2022).

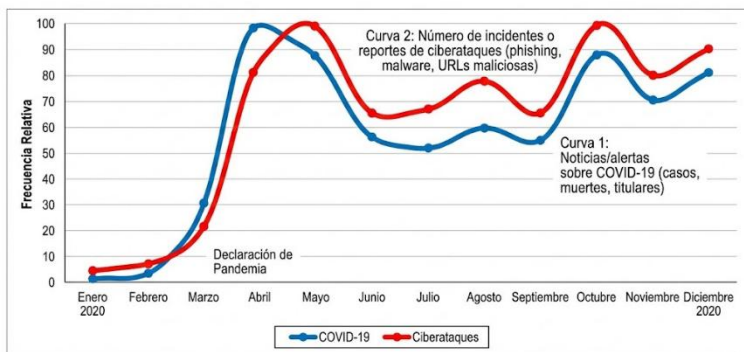
### 2.4.1. Un crecimiento silencioso durante el confinamiento

Mientras la atención pública se centraba en las curvas de contagios, otra curva crecía en paralelo: la de los ciberataques. Desde los primeros meses de 2020, la ONU alertó sobre un aumento del 350 % en sitios web de phishing relacionados con la COVID-19 solo en el primer trimestre del año, muchos de ellos dirigidos a hospitales y sistemas de salud (Lederer, 2020).

En la misma línea, INTERPOL (2022) informó que, entre enero y abril de 2020, uno de sus socios privados detectó 907.000 mensajes de spam, 737 incidentes de malware y 48.000 URLs maliciosas vinculadas específicamente a la COVID-19. La Organización Mundial de la Salud (OMS) (2020) también reportó un incremento de cinco veces en los ciberataques dirigidos a su personal y a la ciudadanía desde que inició la pandemia (ver Figura 15).

**Figura 15**

*La otra curva que crecía*



*Mientras mirábamos una curva, casi no vimos la otra*

En América Latina, este fenómeno fue especialmente intenso. Interpol (2022) señala que, en el primer semestre de 2020, la región registró las tasas de ciberataques más altas del mundo, con

casi tres veces más ataques vía navegadores móviles que el promedio global.

#### ***2.4.2. Modalidades de ataque más frecuentes durante la pandemia***

El crecimiento del ciberdelito no fue solo cuantitativo, sino también cualitativo. Los atacantes adaptaron sus tácticas al lenguaje de la crisis sanitaria: mensajes sobre vacunas, bonos de ayuda, resultados de pruebas o actualizaciones bancarias se convirtieron en señuelos habituales.

Entre las modalidades más frecuentes durante la pandemia se destacan:

- Phishing y fraudes en línea: correos, SMS o mensajes de WhatsApp que imitaban a bancos, instituciones públicas o servicios de entrega. INTERPOL reportó que alrededor de dos tercios de los países encuestados observaron un uso significativo de temas COVID-19 en campañas de phishing y fraude (Interpol, 2022)
- Malware y ransomware: Europol documentó el uso de campañas de ransomware dirigidas a hospitales y servicios críticos, aprovechando su alta dependencia digital y su urgencia por continuar operando (Europol, 2020).
- Suplantación de identidad y robo de credenciales: desde portales falsos de banca electrónica hasta webs que simulaban ser organismos de salud, se multiplicaron las páginas diseñadas para capturar usuarios y contraseñas.

En América Latina, estas tendencias globales se tradujeron en casos concretos. En Ecuador, por ejemplo, se ha documentado el uso de chats y correos falsos que aparentan ser de bancos para robar datos de cuentas y de banca electrónica. Medios nacionales reportan que las denuncias de ciberdelitos aumentaron un 5,4 % en

2020 con respecto al año previo, en parte por este tipo de engaños (Primicias, 2021).

Investigaciones académicas también confirman que países como Brasil y México concentraron buena parte de los ataques en la región, con fuerte presencia de ingeniería social, phishing y malware (Flor-Unda et al., 2023).

La Figura 16 ofrece una mini-guía práctica para identificar mensajes sospechosos, destacando señales como la presión emocional, solicitudes inusuales de datos y la verificación de la identidad del remitente.

**Figura 16**

*Identificación de mensajes sospechosos*

Tres preguntas antes de hacer clic

The infographic is titled "Tres preguntas antes de hacer clic" and is presented in a light gray rounded rectangle. It contains four panels, each with an icon, a bold question, and a short paragraph of text.

- Panel 1 (top-left):** Icon of a magnifying glass over an envelope. Question: **¿Quién me escribe realmente?** Text: "¿El correo, número o enlace coincide exactamente con el oficial del banco, institución o servicio?"
- Panel 2 (top-right):** Icon of a clock with an exclamation mark. Question: **¿Me meten presión o miedo?** Text: "“Último aviso”, “se bloqueará su cuenta”, “pierde el bono si no responde ahora”. El miedo es la herramienta clásica de la ingeniería social."
- Panel 3 (bottom-left):** Icon of a padlock and a key. Question: **¿Me piden datos que normalmente nadie pide por este canal?** Text: "Ningún banco serio pide por correo o chat tu clave completa, token o PIN."
- Panel 4 (bottom-right):** Icon of a shield with a checkmark. Question: **Regla de Oro** Text: "Ante la duda, contacta directamente por los los canales oficiales de la institución."

## 2.5. La desinformación y el caos informativo

Si algo caracterizó los primeros meses de la pandemia fue la sensación de que la información cambiaba cada hora. Lo que un

día era una recomendación oficial, al siguiente quedaba obsoleto. Asimismo, esta inestabilidad informativa agravada por redes sociales, rumores y canales no verificados llevó a la OMS a declarar una “infodemia”, definida como un exceso de información (correcta y falsa) que dificulta que la población encuentre fuentes fiables y tome decisiones adecuadas (OMS, 2020).

Esta mezcla de miedo, incertidumbre y mensajes contradictorios tuvo efectos directos en la seguridad personal: desde personas que rechazaron medidas sanitarias hasta quienes tomaron decisiones riesgosas por seguir recomendaciones no verificadas.

### ***2.5.1. El ruido informativo: demasiada información, poca claridad***

Durante la pandemia, las redes sociales se convirtieron en un campo donde se mezclaban noticias reales, rumores, interpretaciones personales, teorías conspirativas y contenidos manipulados. Según un análisis de Naciones Unidas (2020) la desinformación relacionada con la COVID-19 se extendió a través de miles de publicaciones que incluían curas falsas, negacionismo, mentiras sobre vacunas y contenido diseñado para provocar miedo o confusión.

En América Latina este fenómeno se intensificó, ya que WhatsApp y Facebook son canales dominantes de información cotidiana. UNICEF y la OPS alertaron que cadenas falsas sobre tratamientos, síntomas y vacunas circularon ampliamente por WhatsApp desde marzo de 2020, generando confusión y decisiones de riesgo (ver Figura 17).

**Figura 17**  
*El ruido dentro del ruido*



### **2.5.2. *Cómo se viraliza una mentira: el lado emocional del contenido***

Una característica crucial de la desinformación es que no se difunde por ser creíble, sino por ser emocional. Contenidos que provocan miedo, sorpresa, indignación o urgencia se comparten más rápido, antes de que el lector se detenga a verificar.

Un estudio de MIT concluyó que las noticias falsas tienen un 70 % más de probabilidades de ser compartidas en redes sociales que las noticias verdaderas, principalmente porque provocan emociones más intensas (Vosoughi et al., 2018).

Durante la pandemia, esto se manifestó en tres tipos de contenidos:

1. Mensajes alarmistas
  - Ejemplo: “Mañana cerrarán supermercados, compra hoy todo lo que puedas”.
2. Promesas mágicas

- Ejemplo: remedios caseros “milagrosos” para evitar contagios.
3. Explicaciones conspirativas
- Ejemplo: “la pandemia fue creada para controlar a la población”.

Por otra parte, la UNESCO (2020) advirtió que la propagación de estos contenidos tuvo consecuencias reales en la salud pública, generando resistencia a medidas preventivas o promoviendo prácticas peligrosas.

La Figura 18 presenta una mini-guía con tres filtros rápidos para detectar desinformación, enfocada en verificar el origen, identificar emociones intensas y aplicar el principio de las diez palabras.

**Figura 18**

*3 filtros rápidos para no caer en desinformación*



### **2.5.3. De la confusión al riesgo: cuando la desinformación afecta tu seguridad**

La desinformación no es un problema abstracto: afecta directamente la seguridad física y emocional de las personas.

Según un informe del PNUD (2022), señala que la confusión masiva durante la pandemia llevó a decisiones de riesgo como:

- automedicación peligrosa,
- rechazar atención médica por miedo,
- evitar acudir a hospitales aun con síntomas graves,
- compartir datos personales en enlaces falsos sobre “ayudas económicas”,
- comprar productos fraudulentos relacionados con COVID-19.

Asimismo, un reporte de INTERPOL (2022) documentó miles de fraudes digitales que explotaron la desinformación sanitaria: sitios falsos de venta de mascarillas, vacunas o pruebas de COVID-19; páginas que capturaban datos bancarios; víctimas que perdieron dinero creyendo en bonos inexistentes.

En otras palabras, la desinformación no solo altera opiniones; altera conductas, y esas conductas pueden dejar a personas, familias y comunidades en situaciones reales de vulnerabilidad.



## **Capítulo 3:**

### **Vivir en el mundo postpandemia: nuevas amenazas y desafíos**

### **3.1. La nueva normalidad y los efectos duraderos**

La pandemia de COVID-19 no solo interrumpió la vida cotidiana durante unos meses: alteró de forma profunda la manera en que trabajamos, estudiamos, nos relacionamos y entendemos la seguridad. Aunque muchas restricciones se levantaron, la sensación de “volver a lo de antes” nunca fue completa. Millones de personas arrastran todavía huellas emocionales como ansiedad, cansancio, hipervigilancia y cambios en sus rutinas que se convirtieron en parte de una “nueva normalidad” (American Psychological Association, 2023). Estudios longitudinales han mostrado que, incluso años después de las primeras olas de contagio, los niveles de malestar psicológico (síntomas de ansiedad, depresión o estrés postraumático) se mantuvieron por encima de los niveles pre-pandemia en varios países, indicando que el impacto fue duradero y no solo un episodio pasajero (OMS, 2022b).

En este contexto, la seguridad ya no se experimenta únicamente como “no me asaltan” o “no me enfermo”, sino como un equilibrio frágil entre salud mental, estabilidad económica, vínculos sociales de calidad y sensación de control sobre la propia vida.

#### ***3.1.1 Cambios en la rutina diaria: cuando lo normal dejó de serlo***

Uno de los efectos más visibles de la pandemia fue la ruptura de la rutina. Sin embargo, lo más importante no fue solo el paréntesis del confinamiento, sino lo que vino después: horarios híbridos, reuniones virtuales permanentes, menor contacto físico espontáneo y una nueva forma de “medir” la seguridad en cada salida o encuentro.

La Figura 19 muestra un mini-tip para gestionar la nueva rutina mediante un diario que permite clasificar acciones,

distinguir entre protección real y ansiedad acumulada, y reducir el desgaste emocional.

**Figura 19**  
*Diario de la nueva rutina*



La “nueva normalidad” supuso un ajuste continuo de microdecisiones, que aumentó la carga mental y la sensación de vigilancia sobre uno mismo y los demás. Investigaciones realizadas en Europa y América Latina describen cómo esta reconfiguración de la vida cotidiana se tradujo en agotamiento emocional y sensación de incertidumbre sostenida, incluso cuando bajaron las restricciones sanitarias, especialmente entre personas que combinan trabajo remoto, tareas de cuidado y responsabilidades domésticas.

### **3.1.2 Huellas emocionales: miedo, cansancio y desconfianza sutil**

La pandemia fue, al mismo tiempo, una experiencia sanitaria y una experiencia emocional colectiva. Millones de personas perdieron familiares, trabajo o proyectos de vida. Incluso quienes no sufrieron pérdidas directas vivieron meses de incertidumbre, noticias alarmantes y cambios bruscos en sus vínculos. No es extraño que, en la etapa postpandemia, persistan sentimientos de hipervigilancia, irritabilidad, cansancio crónico o tristeza difícil de nombrar.

Metaanálisis recientes han encontrado incrementos significativos en síntomas de ansiedad y depresión en la población general durante y después de la pandemia, con mayor impacto en jóvenes, mujeres y personas con menor seguridad económica (OMS, 2022b). Estos estudios señalan que el estrés relacionado con el confinamiento, la sobrecarga de cuidados y la inestabilidad laboral contribuyó a un “segundo impacto” de la pandemia: una crisis de salud mental que continúa más allá de los contagios.

La Figura 20 presenta una mini-guía con tres preguntas reflexivas orientadas a identificar hábitos que brindan seguridad, conductas mantenidas por miedo y pequeños cambios para mejorar el bienestar en la “nueva normalidad”.

**Figura 20**  
*Hábitos de seguridad*



### **3.1.3 Nuevas formas de relacionarse, trabajar y cuidarse**

La nueva normalidad también trajo cambios que pueden convertirse en oportunidades si se gestionan conscientemente. El teletrabajo y la educación en línea, por ejemplo, abrieron posibilidades de flexibilizar horarios y reducir desplazamientos, pero exigieron aprender a poner límites entre la vida personal y la pantalla. Las relaciones sociales se trasladaron parcialmente al entorno digital, lo que permitió mantener contacto a distancia,

pero también incrementó el riesgo de aislamiento silencioso y malentendidos.

En términos de seguridad, esto significa que hoy una persona puede sentirse “protegida” en su casa, pero al mismo tiempo estar expuesta a riesgos digitales o al desgaste emocional por hiperconectividad. Cuidarse ya no es solo cerrar la puerta o elegir un camino iluminado: es también silenciar notificaciones, filtrar contenidos, diversificar fuentes de información y sostener vínculos que aporten calma en lugar de más ruido.

La Figura 21 muestra la transición entre el “antes”, “durante” y “después” de la pandemia, destacando cómo las rutinas presenciales dieron paso al confinamiento y, posteriormente, a modelos híbridos y prácticas de seguridad consciente.

**Figura 21**

*Del confinamiento a la nueva normalidad*



La Figura 22 resume los principales cambios emocionales, sociales y laborales observados tras la pandemia, incluyendo ansiedad, vínculos digitales y la consolidación del teletrabajo y los modelos híbridos.

**Figura 22**

*Tres dimensiones de la nueva normalidad*



### 3.2 La hiperconexión permanente

La pandemia aceleró un proceso que ya venía en marcha: pasamos de “usar internet” en ciertos momentos del día a vivir prácticamente siempre conectados. Informes globales de uso digital muestran que, solo entre 2019 y 2020, el tiempo medio diario en línea aumentó alrededor de 16 minutos, lo que supuso un incremento cercano al 4 % en cuestión de meses (Kemp, 2021). Este aumento puede parecer modesto, pero refleja una tendencia estructural: el trabajo, el estudio, el ocio y las relaciones personales comenzaron a pasar, casi por completo, por una pantalla.

#### 3.2.1. Del “estar conectados” al “estar siempre en línea”

La Unión Internacional de Telecomunicaciones (UIT) (ITU, 2020) ya advertía que, antes y durante la pandemia, más de la mitad de la población mundial utilizaba internet, cifra que se elevaba a casi el 70 % entre jóvenes de 15 a 24 años. Es decir, la generación joven entró a la crisis sanitaria con una vida digital más intensa, lo que hizo que el salto hacia la hiperconexión fuera aún más marcado en este grupo.

Al mismo tiempo, muchas personas empezaron a notar los efectos de esta vida “siempre en línea”. Una encuesta del Pew Research Center en Estados Unidos mostró que un tercio de los adultos intentó reducir el tiempo que pasaba con su smartphone o en internet durante la pandemia, y que el 72 % de los padres percibió que sus hijos en edad escolar pasaban significativamente más tiempo frente a pantallas que antes del COVID-19 (McClain et al., 2021).

Esta hiperconexión no solo multiplicó las oportunidades (teletrabajo, educación en línea, acceso a servicios), sino que también abrió una puerta a nuevas formas de cansancio, distracción y vulnerabilidad. La conexión permanente se convirtió, a la vez, en herramienta y riesgo. La Figura 23 presenta un “mapa de pantallas” que permite registrar el uso de dispositivos a lo largo del día, con el fin de tomar conciencia del tiempo dedicado al trabajo, estudio, ocio, redes y noticias.

**Figura 23**  
*Mapa de pantallas*

Toma un día típico y anota tu uso de pantallas.  
¡No es para juzgar, es para tomar conciencia!

MAÑANA	TARDE	NOCHE
Horas: _____	Horas: _____	Horas: _____
Uso: <input type="checkbox"/> Trabajo <input type="checkbox"/> Estudio <input type="checkbox"/> Ocio <input type="checkbox"/> Redes <input type="checkbox"/> Noticias	Uso: <input type="checkbox"/> Trabajo <input type="checkbox"/> Estudio <input type="checkbox"/> Ocio <input type="checkbox"/> Redes <input type="checkbox"/> Noticias	Uso: <input type="checkbox"/> Trabajo <input type="checkbox"/> Estudio <input type="checkbox"/> Ocio <input type="checkbox"/> Redes <input type="checkbox"/> Noticias

El objetivo no es juzgar, sino tomar conciencia de cuán “siempre en línea” está su vida cotidiana.

### 3.2.2. Trabajo, estudio y vida gestionados por pantallas

Uno de los cambios más profundos fue el traslado masivo del trabajo y el estudio al hogar. Antes de la pandemia, el teletrabajo era una práctica minoritaria: en Europa, por ejemplo, alrededor del 11 % de los empleados trabajaba desde casa con cierta regularidad.

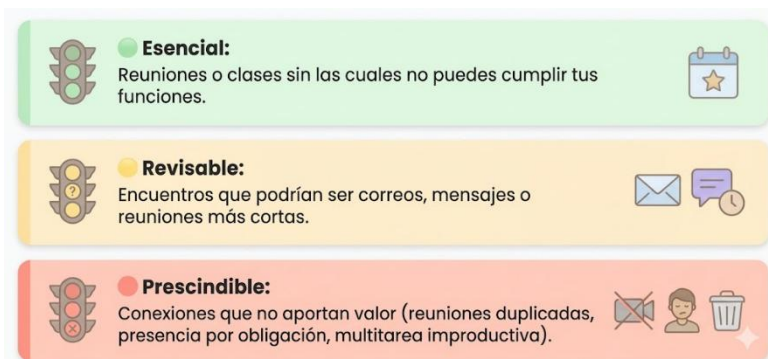
En 2021, tras los confinamientos, ese porcentaje se duplicó hasta alcanzar aproximadamente el 22 % de los trabajadores que teletrabajaban al menos parte del tiempo (Vargas et al., 2022).

Otras estimaciones señalan que, en el punto álgido de la crisis, cerca del 70 % de los trabajadores a tiempo completo llegó a trabajar desde casa, y que las reuniones por videollamada aumentaron en torno a un 50 % respecto a la etapa previa (Owl labs, 2025). A la par, plataformas como Zoom pasaron de 10 millones de participantes diarios en diciembre de 2019 a unos 300 millones en abril de 2020, lo que supuso un crecimiento explosivo en cuestión de semanas (Curry, 2025).

En el ámbito educativo, escuelas y universidades migraron de forma acelerada hacia plataformas de videoconferencia y aulas virtuales, generando una experiencia híbrida entre hogar y escuela. Varios estudios describen cómo la utilización intensiva de estas herramientas trajo consigo nuevos desafíos: “fatiga de Zoom”, sobrecarga de tareas en línea, dificultades para separar la vida laboral o académica de la vida privada y sensación de estar “siempre disponible” (Riedl, 2021).

La Figura 24 muestra el “semáforo de reuniones y pantallas”, una herramienta que clasifica las actividades digitales en esenciales, revisables y prescindibles para optimizar el tiempo y la productividad.

**Figura 24**  
*Semáforo de reuniones y pantallas*



### **3.2.3. Costes invisibles: fatiga digital y pérdida de privacidad**

La hiperconexión tuvo también un precio menos visible: el desgaste físico, emocional y cognitivo. La literatura científica ha empezado a describir el fenómeno de la “fatiga por videoconferencia” o “Zoom fatigue” como una forma de agotamiento somático y mental asociada al uso intensivo de plataformas de videollamada (Riedl, 2021). Investigaciones posteriores como la de Stanford Report (2021) han señalado que factores como verse a uno mismo constantemente en la pantalla, la falta de lenguaje corporal completo y la sobrecarga de estímulos visuales incrementan la carga cognitiva y el cansancio.

Otros estudios han relacionado el uso excesivo de pantallas durante la pandemia con consecuencias como problemas de sueño, aumento del sedentarismo, cambios en la alimentación y deterioro del bienestar mental, especialmente en niños, adolescentes y adultos jóvenes (Resende et al., 2023). Estas “heridas digitales” no siempre son visibles, pero afectan la concentración, el ánimo y la capacidad de recuperación emocional.

A esto se suma la pérdida de privacidad. Cada conexión, clic y búsqueda genera datos que se convierten en insumos para

sistemas de publicidad segmentada, perfiles de consumo o incluso mecanismos de vigilancia. Informes sobre economía de datos muestran cómo los modelos de negocio basados en plataformas dependen precisamente de esta recopilación masiva de información personal, que muchas veces el usuario acepta sin leer a través de políticas de privacidad extensas y poco comprensibles (Kemp, 2021).

En este contexto, la hiperconexión permanente configura un escenario paradójico: nunca habíamos tenido tanto poder para informarnos, comunicarnos y trabajar a distancia, pero tampoco habíamos estado tan expuestos a la fatiga, la sobrecarga y la pérdida de control sobre nuestros propios datos. La Figura 25 presenta una mini-guía con tres límites saludables (de tiempo, espacio y datos) orientados a promover una relación más equilibrada con la tecnología y proteger el bienestar digital.

**Figura 25**

*Tres límites sanos para una mente conectada*



### 3.3. El poder de los datos: entre utilidad y control

En la etapa posterior a la pandemia, hablar de seguridad sin hablar de datos es prácticamente imposible. Cada interacción digital como un mensaje, una búsqueda, un pago, una historia en redes sociales, deja un rastro que puede ser almacenado, analizado y utilizado. Diversos informes muestran que el volumen de datos

creados en el mundo está creciendo de forma exponencial: por ejemplo, un estudio de IDC, citado por Seagate, estimó que la “Global Datasphere” pasaría de 33 zettabytes en 2018 a 175 zettabytes en 2025, es decir, más de cinco veces en apenas siete años (Reinsel et al., 2018).

Este crecimiento ha llevado a organismos como la OCDE (2023) y la UNCTAD a considerar los datos como un recurso estratégico para la economía digital, comparable a la energía o al capital financiero, pero con características propias: se pueden copiar, combinar y reutilizar casi sin costo, y su valor depende del contexto y del análisis que se haga de ellos.

El problema es que este “nuevo petróleo” de la era digital no está distribuido de forma equitativa: una parte importante de los datos queda concentrada en grandes plataformas y empresas con enorme capacidad tecnológica, mientras que las personas, e incluso muchos Estados, apenas tienen una comprensión parcial de qué se recoge, cómo se usa y con qué fines. Eso coloca al ciudadano en una posición ambivalente: se beneficia de servicios personalizados, pero al mismo tiempo cede control sobre su información personal y su comportamiento futuro.

### ***3.3.1. Los datos como nuevo recurso estratégico***

La idea de que los datos se han convertido en un activo económico central está ampliamente documentada. La OCDE (2025) habla de “data-driven innovation” para referirse a la forma en que los datos y la analítica impulsan la productividad, la creación de nuevos modelos de negocio y la mejora de servicios públicos y privados.

Desde esta perspectiva, los datos no son solo un subproducto de nuestras actividades, sino un insumo que permite desarrollar algoritmos de recomendación, sistemas de crédito, plataformas de transporte, aplicaciones de salud y herramientas de

seguridad. UNCTAD, en sus informes sobre economía digital, subraya que los datos son un activo clave para generar valor privado y social, siempre que existan marcos adecuados de gobernanza y protección de derechos (Kemp, 2021)

Sin embargo, el ciudadano común rara vez se percibe a sí mismo como “productor” de un recurso valioso. Usar una app de transporte, pagar con tarjeta o aceptar las cookies de un sitio web parece una acción neutra, cuando en realidad está alimentando bases de datos que, posteriormente, pueden utilizarse para segmentar mercados, estimar riesgos, anticipar comportamientos o incluso influir en decisiones futuras. Además, el medir el valor económico de los datos es complejo, precisamente porque su importancia se multiplica cuando se combinan y se analizan a gran escala (OECD, 2021).

La Figura 26 muestra una mini-guía para que el lector identifique los datos que genera en un día.

**Figura 26**  
*¿Qué datos genero en un día?*



Este ejercicio permite que el lector entienda que los datos no “aparecen” en las bases de datos por arte de magia: somos nosotros quienes los generamos continuamente, a menudo sin darnos cuenta.

### **3.3.2. Modelos de negocio basados en datos y asimetrías de poder**

El crecimiento de la economía digital ha dado lugar a empresas cuyo modelo de negocio depende casi por completo del análisis de grandes volúmenes de datos. Plataformas de comercio electrónico, redes sociales, servicios de streaming y aplicaciones financieras personalizan precios, contenidos y recomendaciones a partir de lo que saben de cada usuario. La OCDE (2021) ha mostrado que los modelos de negocio basados en datos permiten a las empresas innovar y ganar eficiencia, pero también pueden reforzar posiciones dominantes y generar fuertes asimetrías frente a consumidores y pequeñas empresas.

En este contexto, el usuario se convierte simultáneamente en cliente y materia prima: utiliza un servicio “gratis” o de bajo costo, pero paga con sus datos, su atención y su tiempo. La información recopilada se emplea para segmentar audiencias, orientar publicidad o determinar qué contenidos tienen más probabilidades de captar su interés. A menudo, el usuario desconoce la lógica exacta de los algoritmos que deciden qué ve primero, qué ofertas recibe o qué oportunidades se le presentan.

En el sector financiero, por ejemplo, la OCDE (2025) advierte que el uso intensivo de datos personales y técnicas de minería puede mejorar la inclusión financiera, pero también generar riesgos de discriminación algorítmica, fraude y prácticas opacas si no hay regulaciones claras ni educación del consumidor.

La Figura 27 explica el ciclo del dato en una plataforma digital, mostrando cómo las acciones del usuario se transforman en registros, perfiles y modelos predictivos que luego determinan los contenidos que recibe.

**Figura 27**  
*El ciclo del dato en una plataforma*



Esta figura ayuda al lector a visualizar que, detrás de una interacción aparentemente simple, existe un ciclo completo de extracción y uso de datos donde la empresa suele saber mucho más del usuario que a la inversa.

### 3.4. Ingeniería social y manipulación emocional

Después de ver cómo los datos se han convertido en materia prima del nuevo mundo digital, queda una pregunta clave: ¿cómo logran algunos actores que seamos nosotros mismos quienes abramos la puerta al riesgo? La respuesta está en la ingeniería social: un tipo de ataque que no empieza en el computador, sino en las emociones.

La ingeniería social no se basa en vulnerabilidades técnicas, sino en vulnerabilidades humanas: confianza, miedo, urgencia, curiosidad. Grandes informes de ciberseguridad señalan que en más de dos tercios de las brechas de seguridad interviene, de algún modo, el “factor humano”, ya sea por error, descuido o manipulación directa mediante tácticas como el phishing o el engaño personalizado (Campos et al., 2025).

En esta sección veremos qué es la ingeniería social, cómo utiliza nuestras emociones y qué podemos hacer para recuperar el control.

### **3.4.1. Qué es la ingeniería social: cuando el objetivo eres tú**

Las principales organizaciones de ciberseguridad coinciden en una idea:

la ingeniería social es una técnica de ataque que utiliza la manipulación psicológica para que una persona realice acciones que comprometen su seguridad o la de su organización.

IBM (2020), por ejemplo, define la ingeniería social como un conjunto de ataques que manipulan a las personas para que compartan información que no deberían compartir, descarguen software que no deberían instalar o envíen dinero a criminales, aprovechando errores humanos y no fallas técnicas.

De forma similar, Prado (2021).describe la ingeniería social como una técnica que explota rasgos como la confianza, el miedo, la curiosidad y la urgencia, manipulando a las personas para que revelen información confidencial o realicen acciones que ponen en riesgo sus sistemas y datos.

En otras palabras, el atacante no necesita “romper” el sistema:

- te convence a ti de que le abras la puerta,
- te empuja a hacer clic en un enlace,
- a entregar una clave “solo por esta vez”,
- o a compartir un dato “para verificar tu identidad”.

Lo hace vistiéndose de confianza: se parece a tu banco, a una institución pública, a un jefe, a un profesor, a un servicio de mensajería, o incluso a un familiar. Y lo hace activando emociones: miedo a perder algo, urgencia por responder, curiosidad ante un mensaje inesperado, deseo de ayudar.

### **3.4.2. Emociones como vector de ataque: miedo, urgencia, confianza**

La ingeniería social funciona porque entiende algo muy humano: cuando estamos asustados, apurados o ilusionados, pensamos peor.

Además, se considera a los atacantes “aprovechan aspectos clave de la psicología humana, como la confianza, el miedo, la curiosidad y la urgencia”, y crean situaciones que nublan el juicio racional para lograr que la víctima actúe sin verificar (M. González & Quevedo, 2025).

Algunas tácticas frecuentes son:

- Miedo y urgencia
  - “Tu cuenta será bloqueada en 24 horas si no confirmas tus datos”.
- Confianza y autoridad
  - Correos que aparentan venir de un jefe, un profesor, una institución del Estado o un banco.
  - Solicitudes “internas” de cambio de contraseña o de compartir documentos.
- Curiosidad y recompensa
  - Mensajes del tipo “mira este video tuyo”, “tienes un paquete retenido” o “tienes un premio pendiente”.

Esta lógica no se limita al correo o a los mensajes de texto. La desinformación y las noticias falsas también explotan nuestras emociones para influir en lo que creemos y compartimos. Un informe reciente sobre fake news y salud mental documenta que las noticias falsas usan lenguaje exagerado y contenido emocional (miedo, ira, excitación) para aumentar la probabilidad de que la gente crea y comparta esa información, y que este tipo de contenido se distribuye incluso seis veces más rápido que la información verificada (Bartolomé, 2021).

Durante la pandemia, este tipo de desinformación emocional contribuyó a aumentar la ansiedad, la confusión y la sensación de peligro constante, dificultando que las personas pudieran distinguir entre riesgos reales y riesgos exagerados. La Figura 28 representa la cadena de manipulación emocional, donde un disparo emocional desencadena reacciones impulsivas que pueden culminar en pérdidas de datos, dinero o confianza.

**Figura 28**  
*Cadena de la manipulación emocional*



La buena noticia es que, igual que se puede aprender a reconocer un semáforo en la calle, también podemos aprender a detectar señales de manipulación emocional en el entorno digital. Ningún método es infalible, pero pequeñas prácticas constantes cambian mucho el nivel de riesgo. La Figura 29 presenta la mini-guía “PAUSA”, una regla práctica que invita a detenerse, analizar la emoción, ubicar la fuente, sospechar de la urgencia y verificar por un canal alterno antes de hacer clic.

**Figura 29**  
Método “PAUSA”

**P - Para físicamente**  
No respondas ni hagas clic de inmediato. Respira tres veces profundo. Esa micro-pausa reduce la probabilidad de actuar solo por impulso emocional.

**A - Analiza la emoción**  
Pregúntate: ¿qué me quiere hacer sentir este mensaje? ¿Miedo, urgencia, culpa, ilusión? Si la emoción es muy intensa, es una bandera roja.

**U - Ubica la fuente**  
Revisa el remitente real, la dirección de correo, la URL o el número. ¿Es exactamente el mismo de siempre? Las guías de IBM y otros proveedores recomiendan verificar siempre el origen antes de compartir cualquier dato, justamente porque muchos ataques se basan en suplantar identidades confiables.

**S - Sospecha de la urgencia**  
Si el mensaje insiste en que “debes actuar ya”, sin darte tiempo para verificar, es muy probable que sea ingeniería social. Verizon recuerda que en la mayoría de brechas con “elemento humano”, el problema no es la tecnología sino la respuesta apresurada ante un mensaje engañoso.

**A - Asegúrate por un canal alterno**  
Antes de hacer algo, confirma por otro medio: llama al banco al número oficial, escribe directamente a la persona por un canal que ya conozcas, entra por tu app habitual en lugar de tocar el enlace del mensaje.

### Ejercicio 5

### Ejercicio práctico: Tu propio museo de trampas

Durante una semana, crea una carpeta de capturas de pantalla con:

- Correos sospechosos
- Mensajes de WhatsApp extraños
- Publicaciones que te hayan generado miedo o urgencia

Al final de la semana, revisalos con calma y marca:

- qué emoción intentaban activar
  - Miedo
  - Urgencia
  - Curiosidad
  - Culpa
  - Ilusión
- qué dato te estaban pidiendo
  - Contraseña
  - Datos bancarios
  - Información personal
  - Ubicación
  - Contactos
- qué habrías hecho si hubieras reaccionado sin pensar
  - Hacer clic en el enlace
  - Descargar archivo
  - Responder al mensaje
  - Compartir la información
  - Enviar dinero

Este pequeño ejercicio de observación convierte la manipulación en algo visible y nombrable, y eso ya es una forma de protección: aquello que puedes nombrar, puedes empezar a gestionar.

### 3.5. Salud mental y gestión emocional en la era digital

La pandemia no solo dejó huellas en los sistemas sanitarios y económicos, sino también en la mente de millones de personas. De acuerdo con la Organización Mundial de la Salud (2022),

durante el primer año del COVID-19 la prevalencia global de ansiedad y depresión aumentó aproximadamente un 25 %, lo que llevó a la OMS a calificar la situación como una “llamada de atención a todos los países” sobre la necesidad de priorizar la salud mental.

Ese incremento no se explica solo por el miedo al contagio o las pérdidas económicas, sino también por la combinación de aislamiento, incertidumbre, duelos no resueltos y exposición constante a información alarmante. Informes posteriores han confirmado que muchas personas continúan arrastrando síntomas de ansiedad, depresión, fatiga y dificultades cognitivas meses o incluso años después de la infección, lo que sugiere que la recuperación mental suele ser más lenta que la física (Kupcova et al., 2023b).

En este contexto, la era digital ha cumplido un doble papel: por un lado, ha permitido sostener vínculos, trabajo y acceso a servicios; por otro, ha intensificado la sobrecarga informativa, el tiempo de pantalla y la comparación social constante. La gestión emocional en la postpandemia ya no puede pensarse sin considerar este entorno hiperconectado.

### ***3.5.1. Cicatrices emocionales de una crisis prolongada***

Aunque las restricciones más duras quedaron atrás, muchas personas siguen experimentando lo que algunos psicólogos denominan una forma de “trauma colectivo”. La American Psychological Association (2023), a través de la serie de informes Stress in America, ha descrito cómo la pandemia, junto con crisis económicas, conflictos y polarización social, ha dejado a la población “en proceso de recuperación de un trauma colectivo”, con niveles sostenidos de preocupación por el futuro y agotamiento emocional.

A esa carga se suman los efectos de la incertidumbre prolongada: planes pospuestos, duelos sin rituales tradicionales, cambios laborales abruptos y la sensación de que “todo puede cambiar de un día para otro”. Estudios recientes muestran que, incluso tras superar la fase aguda de la enfermedad, una proporción significativa de personas mantiene síntomas de ansiedad, depresión y fatiga hasta nueve meses después, lo que indica una recuperación mental mucho más lenta que la física (Vaziri, 2025).

En este escenario, cuidar la salud mental ya no es un lujo ni un tema “secundario”, sino una necesidad básica. Reconocer el impacto emocional de lo vivido y de lo que seguimos viviendo, es el primer paso para dejar de minimizar el malestar (“no es para tanto”) y empezar a construir estrategias reales de cuidado.

### Ejercicio 6

Tómate 5 minutos para responder, por escrito:

	¿Qué cambios emocionales noto en mí desde la pandemia?		¿Qué de eso estoy normalizando como si fuera “parte de la vida adulta” pero en realidad me pesa?
	sueño		
	irritabilidad		
	apatía		
	preocupación constante		

Este pequeño ejercicio abre la puerta a una mirada más honesta sobre tu propio estado emocional.

#### 3.5.2. Sobrecarga digital, ansiedad y cansancio invisible

La otra cara de la postpandemia es la hiperconexión. El mundo no solo volvió “a la calle”: también se quedó, de forma estable, en las pantallas. El informe global Digital 2024 estima que el usuario típico de redes sociales pasa alrededor de 2 horas y 23

minutos al día en estas plataformas, en un contexto en el que ya existen más de 5.000 millones de usuarios activos en redes (Kemp, 2021).

Aunque el tiempo de pantalla no es “bueno” o “malo” por sí mismo, diferentes estudios vienen mostrando que ciertos patrones de uso (particularmente el consumo pasivo, la comparación constante y la exposición a contenidos hostiles) se asocian con mayores síntomas de ansiedad, depresión y peor calidad de sueño. Una revisión reciente de Nagata et al. (2024) sobre uso de pantallas y salud mental señala que, aun cuando los efectos promedio son modestos, el impacto puede ser significativo en personas con vulnerabilidades previas o bajo alto estrés.

### ***3.5.3. Estrategias de autocuidado emocional en la era hiperconectada***

La buena noticia es que pequeñas decisiones diarias pueden tener un efecto poderoso en la salud mental. El autocuidado emocional en la era digital no implica “vivir sin tecnología”, sino aprender a usarla con límites claros y complementar su presencia con espacios de descanso, conexión real y silencio.

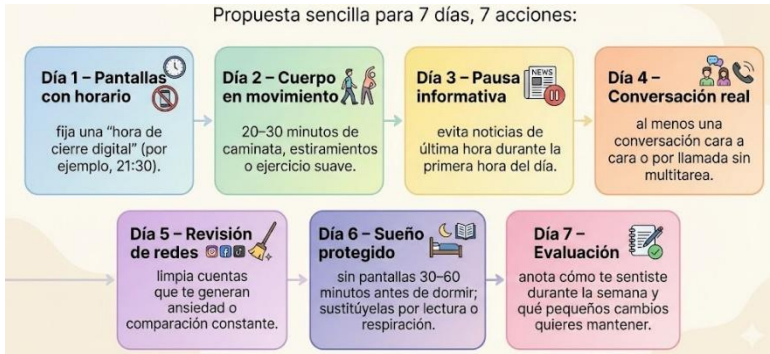
Diversas guías clínicas y revisiones sobre salud mental recomiendan combinar el apoyo profesional con hábitos protectores como la actividad física regular, el sueño reparador, la regulación del tiempo de pantalla y el fortalecimiento de redes de apoyo (American Psychological Association, 2023).

A la luz de la evidencia reciente sobre reducción de pantalla y bienestar, una estrategia realista puede ser plantearse “micro-cambios” medibles: disminuir 30 minutos al día el uso del teléfono, establecer una “hora sin pantallas” antes de dormir o definir un día a la semana con notificaciones desactivadas para redes sociales (Pieh et al., 2025). La Figura 30 presenta una propuesta de siete días con siete acciones concretas para promover hábitos digitales y

emocionales más saludables, desde regular horarios de pantalla hasta evaluar el bienestar semanal.

### Figura 30

#### Plan de autocuidado emocional 7x7



### 3.6. Hacia una cultura de conciencia y responsabilidad

La etapa postpandemia no solo nos dejó más cansados y conectados, también nos puso frente a una pregunta incómoda: ¿qué hacemos con todo lo que ya sabemos sobre riesgo, datos, emociones y vulnerabilidades? Pasar del miedo a la responsabilidad implica construir una cultura donde la seguridad deje de ser un asunto puramente técnico o policial y se convierta en una práctica cotidiana basada en la conciencia, el pensamiento crítico y la corresponsabilidad.

Organismos internacionales han insistido en que la gestión del riesgo digital y de la información no puede limitarse a instalar antivirus o actualizar contraseñas; requiere cambios en la forma en que personas, organizaciones y Estados entienden su papel en el ecosistema digital. La OCDE (2022), por ejemplo, propone tratar la seguridad digital como un riesgo económico y social, no solo técnico, y pide políticas públicas que fomenten que individuos y empresas integren la gestión del riesgo en sus decisiones diarias.

Al mismo tiempo, la UNESCO (2025) ha desarrollado el enfoque de alfabetización mediática e informacional (MIL) como un conjunto de competencias clave para enfrentar la desinformación, el discurso de odio y los efectos de las plataformas digitales sobre nuestras creencias y decisiones.

Sobre esta base, este apartado plantea tres dimensiones para avanzar hacia una cultura de conciencia y responsabilidad: los hábitos individuales, las competencias críticas y la corresponsabilidad institucional y social.

### ***3.6.1. De la reacción a la prevención: hábitos conscientes en lo cotidiano***

Durante la pandemia, muchas personas descubrieron la seguridad “a golpes”: cambiaron rutinas solo después de vivir un contagio cercano, un robo, una estafa o una crisis emocional. La lógica reactiva (“cambio cuando algo malo me pasa”) es comprensible, pero insostenible. Construir una cultura de conciencia implica moverse de la reacción a la prevención: anticiparse, observar patrones y tomar decisiones antes de que el riesgo se materialice.

La gestión del riesgo, en términos simples, consiste en reconocer que no existe la seguridad absoluta, pero sí es posible reducir la probabilidad y el impacto de ciertos daños. La OCDE (2025) señala que las amenazas digitales se han multiplicado y sus consecuencias pueden ser económicas, reputacionales, psicológicas y sociales, por lo que la gestión del riesgo debe integrarse en la vida diaria de personas y organizaciones. En la práctica, esto significa adoptar pequeños hábitos conscientes: revisar la configuración de privacidad, diversificar contraseñas, desconfiar de correos urgentes con enlaces, contar con contactos de emergencia verificados, hablar de planes de respuesta en familia o en el trabajo. No se trata de vivir paranoicos, sino de vivir atentos.

La Figura 31 presenta una mini-guía de chequeo de conciencia con cinco preguntas clave orientadas a fortalecer la seguridad y el bienestar digital mediante la reflexión personal.

**Figura 31**  
*Chequeo de conciencia en 5 preguntas*



La idea es que el lector comprenda que la conciencia no es un estado abstracto, sino una serie de microdecisiones diarias que, sumadas, reducen la vulnerabilidad.

### **3.6.2 Alfabetización mediática e informacional: una “vacuna” contra la desinformación**

La experiencia del COVID-19 mostró de forma dramática que la desinformación puede costar vidas, erosionar la confianza en las instituciones y fragmentar comunidades. Frente a este panorama, la UNESCO (2025) ha promovido la Semana Mundial de la Alfabetización Mediática e Informacional (Global Media and Information Literacy Week), subrayando que estas competencias son “para el bien público” porque permiten a las personas evaluar fuentes, contrastar datos y participar de forma más responsable en el espacio digital.

La alfabetización mediática e informacional no se limita a saber usar una aplicación; implica comprender cómo se produce la información, quién la financia, qué intereses pueden estar detrás y

cómo influyen los sesgos en nuestra propia interpretación (The Guardian, 2025). En contextos polarizados, contar con estas competencias se vuelve una forma de protección frente a narrativas manipuladoras y campañas de desinformación.

Investigaciones recientes muestran que incluso quienes se consideran “nativos digitales” pueden tener dificultades para evaluar la credibilidad de fuentes y contenidos. Iniciativas educativas en distintos países han demostrado que programas estructurados de alfabetización mediática mejoran la capacidad de las personas para identificar noticias falsas y reducir la difusión de contenidos engañosos.

La Figura 32 representa un modelo escalonado para el pensamiento crítico digital, avanzando desde el consumo pasivo de información hasta la acción responsable basada en contraste y contextualización.

**Figura 32**  
*Escalera de la alfabetización crítica*



Esta figura refuerza la idea de que la responsabilidad informacional no es innata, se aprende y se entrena, igual que cualquier otra habilidad.



## **Capítulo 4:**

### **Estrategias para vivir seguro y sin miedo**

## **4.1 Hacia una seguridad integral: física, emocional y digital**

Los capítulos anteriores mostraron cómo, antes de la pandemia, muchas personas confiaban en rutinas y costumbres que daban una sensación de seguridad casi automática; cómo durante el confinamiento se hicieron visibles nuevas vulnerabilidades desde la dependencia de la tecnología hasta el impacto emocional del aislamiento; y cómo, en el presente postpandemia, convivimos con una realidad híbrida donde lo físico, lo emocional y lo digital se entrelazan a cada momento. Asumir esta visión “3D” de la seguridad no busca generar miedo, sino ofrecer un mapa más completo desde el cual tomar decisiones. Cuando el lector reconoce que su bienestar depende de este triángulo (cuerpo, mente y datos), puede empezar a introducir pequeños cambios en cada dimensión que, sumados, aumentan tanto la protección objetiva como la sensación de control subjetivo sobre la propia vida.

### ***4.1.1 Tres dimensiones de la seguridad en la vida cotidiana***

En la vida cotidiana, muchas personas siguen asociando la palabra “seguridad” casi exclusivamente con el riesgo de sufrir un robo, una agresión física o un incidente en la calle o en casa. Sin embargo, después de la pandemia de COVID-19, esa visión se quedó corta. Hoy, sentirse seguro implica también cómo se experimenta el bienestar emocional y cómo se habita el mundo digital: desde las redes sociales hasta las cuentas bancarias en línea. Estudios recientes muestran que la percepción de bienestar personal tras la pandemia integra de forma inseparable dimensiones como la seguridad física, la estabilidad emocional y la sensación de control frente a riesgos tecnológicos y sociales, más aún en entornos urbanos densos y complejos (Guo et al., 2024). Por eso, al entender la seguridad integral como un sistema de tres dimensiones interconectadas: cuerpo (seguridad física), mente (seguridad emocional) y datos (seguridad digital) (ver Figura 33).

**Figura 33**

*El triángulo de la seguridad integral*



La seguridad física alude a la protección frente a daños corporales y situaciones de violencia o accidente en espacios como el hogar, la calle o el trabajo. La seguridad emocional se relaciona con la capacidad de manejar el miedo, la ansiedad y la incertidumbre de manera realista, sin caer ni en la negación del riesgo ni en la paranoia. Finalmente, la seguridad digital se refiere al conjunto de hábitos y decisiones que protegen la información personal, financiera y profesional en un entorno marcado por la hiperconectividad, donde el uso intensivo de internet y redes sociales puede aportar recursos, pero también aumentar la exposición a fraudes, acoso o sobrecarga mental (Mousoulidou et al., 2024).

#### ***4.1.2 Seguridad consciente: pasar del piloto automático a la atención plena***

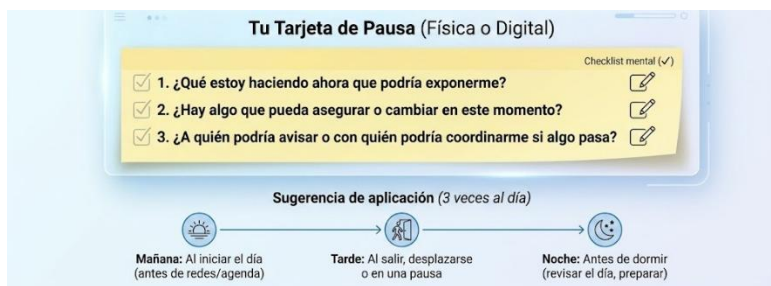
Vivimos muchos de nuestros días en lo que podría llamarse “modo automático”: rutinas de trabajo, trayectos habituales, revisar el celular, contestar correos, desplazamientos, tareas domésticas. En ese contexto, es fácil que nuestra alerta básica ante riesgos físicos, emocionales o digitales se adormezca: dejamos de observar lo que hacemos, cómo lo hacemos y qué efectos puede tener. La

“seguridad consciente” propone una pausa radical: dejar por un momento el piloto automático, y asumir una actitud de atención plena ante nuestras acciones cotidianas.

La atención plena o Mindfulness ha sido ampliamente estudiada por su capacidad para mejorar la regulación emocional, disminuir el estrés percibido y aumentar el bienestar subjetivo (Hepburn et al., 2021). En un estudio con estudiantes universitarios, quienes reportaron niveles altos de “mindful attention awareness” (conciencia plena atenta) mostraron estrés percibido significativamente menor y bienestar subjetivo más alto: una correlación inversa entre atención plena y estrés y una correlación directa entre atención plena y bienestar.

La Figura 34 presenta el mini-tip “Pausa de seguridad en 30 segundos”, una herramienta rápida para evaluar riesgos cotidianos mediante tres preguntas clave sobre exposición, acciones de prevención y coordinación.

**Figura 34**  
*Pausa de seguridad en 30 segundos*



#### **4.1.3 De la preocupación a la acción: redefinir qué significa “vivir sin miedo”**



El miedo o la preocupación ante lo incierto suele percibirse como un enemigo a eliminar. Pero en un mundo pospandemia, con múltiples vulnerabilidades (físicas, emocionales, digitales), vivir

siempre “sin miedo” es tanto irreal como contraproducente. Más útil resulta concebir la seguridad como un proceso activo, continuo, donde el miedo funciona como una señal de alerta, no como una prisión. Cambiar la mentalidad de “preocupación paralizante” a “acción consciente” implica reconocer que, aunque no podemos controlar todo, sí podemos mejorar nuestros hábitos y con ello aumentar nuestra resiliencia, sentido de control y tranquilidad interior.

Este enfoque de micro-acciones diarias (pequeños cambios conscientes, consistentes y sostenibles) ha demostrado ser una estrategia eficaz para reducir el estrés, mejorar la salud mental y fortalecer la resiliencia frente a eventos adversos. Un estudio reciente sugiere que incluso acciones breves de bajo esfuerzo; por ejemplo, actividades diarias simples— pueden producir mejoras concretas en el bienestar, la salud emocional y la percepción del control (Hepburn et al., 2021). En ese sentido, estas micro-acciones no requieren un cambio radical ni una gran inversión de tiempo: con constancia, pueden producir transformaciones significativas en el largo plazo.

Por tanto, “vivir sin miedo” no implica desatención o negación de riesgos, sino cultivar un estado de alerta equilibrada, conciencia activa y responsabilidad personal.

## Ejercicio 7

 <b>Reenfocando el miedo</b> 	
<p><b>1. “No puedo controlar todo, pero sí puedo mejorar mis hábitos.”</b></p> <p> Copia la frase aquí para interiorizarla: .....</p>	<p>Mi nota personal / Acción concreta:</p> <input type="text"/> <input type="text"/>
<p><b>2. “Prepararme me da calma, no paranoia.”</b></p> <p> Copia la frase aquí para interiorizarla: .....</p>	<p>Mi nota personal / Acción concreta:</p> <input type="text"/> <input type="text"/>
<p><b>3. “Poco a poco es mejor que no hacer nada.”</b></p> <p> Copia la frase aquí para interiorizarla: .....</p>	<p>Mi nota personal / Acción concreta:</p> <input type="text"/> <input type="text"/>

Este recurso ayuda a reconfigurar mentalidades desde un enfoque reactivo o evitativo, hacia uno proactivo, consciente y empoderado, y a transformar la preocupación en acción concreta.

## **4.2. Autoprotección cotidiana sin complicaciones**

En la vida diaria, la autoprotección no debería sentirse como una carga ni como un conjunto de reglas difíciles de cumplir, sino como un hábito sencillo integrado en la rutina. La evidencia científica muestra que las personas que adoptan pequeñas conductas preventivas reducen significativamente su exposición a riesgos físicos y sociales (López & Garrido, 2022). Del mismo modo, estudios recientes destacan que la autoprotección efectiva no depende de medidas sofisticadas, sino de la capacidad de anticipar escenarios cotidianos y actuar de manera consciente dentro de ellos (Rosenbaum et al., 2021). Este enfoque práctico permite al lector comprender que la seguridad personal no se construye desde el miedo, sino desde la claridad: observar el entorno, identificar señales tempranas, comunicar sus desplazamientos cuando es pertinente y evitar rutinas demasiado predecibles.

### ***4.2.1 Hogar y entorno cercano: tu primer espacio seguro***

El hogar sigue siendo nuestro refugio principal: es el espacio donde descansamos, nos recuperamos y proyectamos estabilidad. Pero esa seguridad no está garantizada por defecto: se construye o se refuerza con decisiones conscientes, buenas prácticas y mantenimiento constante. Después de la pandemia, muchas personas redescubrieron el valor del hogar: lo convirtieron en oficina, aula, punto de encuentro social. Esa multiplicidad de funciones incrementa los riesgos: de seguridad, de accidentes domésticos, de vulnerabilidad ante intrusos. Por tanto, garantizar que nuestro hogar sea un “espacio seguro” es un pilar fundamental del bienestar integral.

Diversos estudios muestran que aplicar medidas de seguridad estructurales (buenas cerraduras, accesos controlados, monitoreo, iluminación) reduce significativamente la vulnerabilidad al delito y al robo. Un reciente análisis sobre “factors influencing burglary and home security measures” concluye que hogares que adoptan medidas de protección activas disminuyen la percepción de inseguridad, y los riesgos de victimización bajan cuando existe conciencia preventiva (Bankiewicz & Papadouka, 2024).

Por otro lado, la seguridad del hogar no se limita al riesgo de robo; incluye también la prevención de accidentes (caídas, incendios, fugas, descuidos domésticos) especialmente si conviven niños, adultos mayores o mascotas. Instituciones dedicadas a la seguridad familiar enfatizan la importancia de detectar y mitigar riesgos domésticos: asegurar muebles, proteger ventanas, revisar conexiones eléctricas, evitar materiales inflamables, entre otros.

#### ***4.2.2 Calle, transporte y espacios públicos: moverse con atención, no con pánico***

Moverse en la calle, tomar transporte o transitar por espacios públicos forma parte de la vida diaria, pero después de la pandemia estos entornos adquirieron nuevas capas de complejidad: más movilidad urbana, más distracciones digitales y, en muchos casos, un incremento de la percepción de inseguridad. La clave no es vivir con miedo, sino con atención estratégica: pequeños hábitos que reducen riesgos sin afectar la autonomía ni la tranquilidad (ver Figura 35).

La evidencia reciente muestra que la percepción de inseguridad en espacios públicos está fuertemente influida por la atención, la planificación del trayecto y el uso prudente del teléfono móvil. Además, el uso del celular en movilidad se ha convertido en un factor de riesgo relevante. Estudios han demostrado que la distracción digital aumenta la vulnerabilidad no solo ante delitos

oportunistas, sino también frente a accidentes en cruce de calles, transporte y espacios concurridos. Chen y Pai (2018) encontraron que las personas que caminan mirando el teléfono presentan menor percepción del entorno, tiempos de reacción reducidos y mayor exposición a amenazas externas.

Asimismo, la planificación de trayectos aporta seguridad emocional y física. Un estudio de McIlroy (2023) sobre movilidad segura encontró que las personas que planifican rutas alternativas identifican zonas críticas y establecen un contacto de referencia experimentan menos ansiedad y muestran mayor resiliencia ante situaciones imprevistas. Estos micro-hábitos crean una estructura interna de confianza que permite moverse sin caer en la paranoia, pero tampoco en la ingenuidad.

**Figura 35**  
*Mapa personal de rutas seguras*



### 4.2.3 Trabajo y estudio: seguridad en entornos compartidos

Los espacios de trabajo y estudio son escenarios donde convergen múltiples personas, rutinas diversas y niveles distintos de responsabilidad. Esta mezcla puede generar puntos de vulnerabilidad que muchas veces pasan desapercibidos: pertenencias sin supervisión, dispositivos desbloqueados,

información sensible expuesta, rutas de evacuación desconocidas o protocolos que se asumen, pero no se practican. La seguridad en estos entornos no depende únicamente de las instituciones; también requiere hábitos personales consistentes y cooperación entre quienes comparten el espacio.

La evidencia científica destaca que los entornos laborales y educativos bien organizados reducen riesgos físicos y psicológicos, mejoran la percepción de seguridad y fortalecen la confianza institucional. Por ejemplo, un estudio reciente encontró que la claridad en los protocolos, la identificación de riesgos y la capacitación básica aumentan la sensación de control y reducen incidentes relacionados con fallas humanas y descuidos (López & Quinde, 2024).

En el contexto actual, la gestión segura de dispositivos digitales es esencial. Con el trabajo híbrido y el uso frecuente de plataformas en la nube, muchas personas manejan archivos sensibles, credenciales y datos personales desde laptops o teléfonos que quedan expuestos en espacios compartidos. Por otro lado, la seguridad emocional es un componente relevante en entornos compartidos. Saber a quién acudir si ocurre una situación de riesgo, incomodidad o acoso, así como conocer los canales institucionales de reporte, contribuye a un ambiente más saludable.

La Figura 36 presenta una mini-guía con tres hábitos de seguridad esenciales en el trabajo o aula, enfocada en el bloqueo de dispositivos, el conocimiento del entorno y la preparación de una red de apoyo rápido.

## Figura 36

### 3 hábitos clave en el trabajo/aula



## 4.3 Seguridad digital accesible para todos

En un mundo hiperconectado, la seguridad digital dejó de ser un tema exclusivo para expertos en informática. Hoy, cualquier persona maneja información crítica desde su celular o computadora: datos bancarios, correos laborales, fotografías personales, conversaciones privadas, documentos de salud o trámites oficiales. Por ello, la protección digital básica se ha convertido en una forma cotidiana de autocuidado. Los ciberataques actuales no buscan únicamente infiltrarse en grandes empresas; una parte importante de ellos está dirigida a individuos comunes mediante contraseñas débiles, descuidos con los dispositivos o enlaces fraudulentos.

### 4.3.1 Lo mínimo indispensable: claves, 2FA y dispositivos

La literatura científica confirma que las contraseñas inseguras siguen siendo una de las principales puertas de entrada para ataques digitales, especialmente para robo de identidad, accesos no autorizados y fraudes financieros. Según un estudio reciente, más del 60 % de las brechas de seguridad examinadas tuvieron como causa inicial una contraseña vulnerable o reutilizada (Ezugwu et al., 2023). Por esta razón, los expertos recomiendan

crear claves largas, únicas, difíciles de adivinar y basadas en “frases de paso”, ya que aumentan la fuerza criptográfica sin sacrificar la memorización.

El segundo pilar indispensable es la autenticación en dos pasos (2FA). Este mecanismo añade una barrera adicional (generalmente un código o confirmación desde un dispositivo confiable) lo que reduce drásticamente la posibilidad de acceso no autorizado incluso si un atacante logra obtener la contraseña. Estudios recientes demuestran que las cuentas con 2FA activado reducen su probabilidad de ser comprometidas en más de un 90 % (Naik et al., 2024). La evidencia también señala que la mayoría de usuarios que activan 2FA perciben mayor tranquilidad, aun cuando no comprendan todos los aspectos técnicos del mecanismo.

#### ***4.3.2 Higiene digital mensual: limpiar, actualizar, respaldar***

En un entorno digital donde usamos múltiples dispositivos (celular, laptop, Tablet) para trabajar, estudiar, socializar o hacer trámites, la seguridad no se garantiza solamente con buenas contraseñas y autenticación, sino también con el mantenimiento regular del sistema digital. Esto es lo que llamamos “higiene digital”: un conjunto de prácticas periódicas orientadas a mantener la salud, integridad y privacidad de nuestros datos, sistemas y vida en línea.

La higiene digital incluye acciones como actualizar sistemas y aplicaciones, revisar permisos de apps, eliminar contenido innecesario y respaldar (backup) la información importante (Armoogum et al., 2025). En su famosa analogía, mantener una buena higiene digital es tan importante como lavarse las manos en la vida real para prevenir enfermedades.

**Figura 37**

*Rutina digital de 30 minutos al mes*

Paso	Acción Clave	✓
1.	<b>Actualizar todo:</b> S.O. y apps en PC, móvil y tablet.	<input type="checkbox"/>
2.	<b>Permisos de apps:</b> Revocar accesos innecesarios (cámara, micro, ubicación).	<input type="checkbox"/>
3.	<b>Backup:</b> Respalda archivos importantes en nube/disco y verifica.	<input type="checkbox"/>
4.	<b>Limpieza digital:</b> Borra apps, cuentas y archivos que no uses.	<input type="checkbox"/>
5.	<b>Seguridad Wi-Fi:</b> Usa WPA2/3 y evita redes públicas.	<input type="checkbox"/>
6.	<b>Contraseñas:</b> Cambia las débiles por frases robustas o usa gestor.	<input type="checkbox"/>
7.	<b>Privacidad RRSS:</b> Revisa qué compartes y cierra sesiones antiguas.	<input type="checkbox"/>

Por esta razón, se propone institucionalizar una rutina mensual de higiene digital. Al dedicar 20–30 minutos una vez al mes para realizar una revisión básica y ajustes necesarios, el usuario puede mantener su ecosistema digital bajo control y con menor vulnerabilidad, sin necesidad de ser un experto técnico (ver Figura 37).

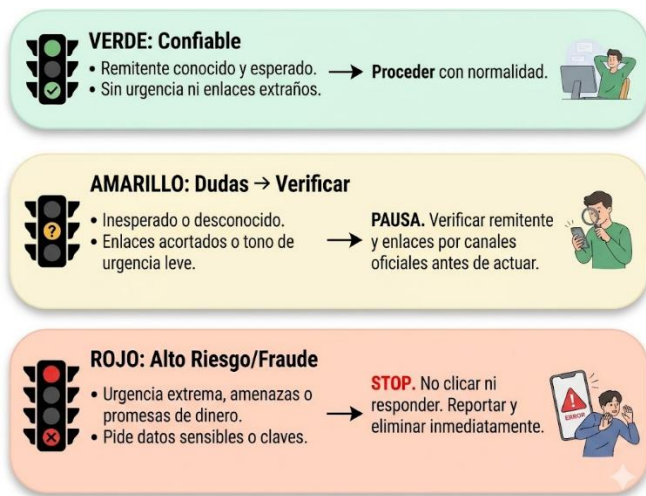
Empíricamente, revisiones recientes muestran que las organizaciones que adoptan rutinas de higiene digital (y fomentan cultura de seguridad) logran reducir sustancialmente incidentes de ciberataques derivados de descuidos, versiones obsoletas, o malas prácticas de los usuarios (Armoogum et al., 2025).

#### **4.3.3 Reconocer fraudes y engaños en línea**

En la actualidad, la circulación masiva de información convirtió al engaño digital (fraudes, estafas, phishing, smishing, etc.) en uno de los riesgos más frecuentes para personas de todo tipo de perfiles. Que alguien caiga en una estafa no siempre depende de su nivel técnico: muchas veces basta un momento de distracción, una urgencia aparente o una emoción. Comprender cómo funcionan estos engaños, y aprender a reconocer sus señales de alerta, es una forma esencial de autoprotección en la era digital.

El fraude más común se conoce como phishing, tácticas mediante las cuales un estafador suplanta a una entidad confiable (banco, empresa, institución, conocido) para engañar al usuario y obtener datos personales, contraseñas, credenciales, o inducirlo a realizar una acción que expone sus cuentas (Campos et al., 2025). Un estudio reciente sobre phishing en redes sociales señala que muchos usuarios desconocen las nuevas variantes del engaño (como enlaces falsos, suplantación de perfil, solicitudes urgentes), lo que incrementa su vulnerabilidad (Mouncey & Ciobotaru, 2025). Otra investigación especializada advierte que con el uso creciente de códigos QR, surge una nueva modalidad llamada qrishing. La Figura 38 presenta una versión sintetizada del “semáforo de mensajes sospechosos”, que clasifica las comunicaciones en verdes, amarillas y rojas según su nivel de confianza o riesgo.

**Figura 38**  
*Semáforo de alerta*



Entre las señales más frecuentes de fraude digital destacan: comunicaciones inesperadas de remitentes desconocidos,

solicitudes urgentes, ofertas demasiado buenas para ser reales, invitaciones a hacer clic en enlaces o abrir archivos adjuntos, etc.

## **4.4 Manejo del miedo y resiliencia emocional**

El miedo, frecuentemente asociado con peligro, ansiedad y evasión, cumple también una función fundamental de alarma adaptativa: nos alerta de riesgos reales, activa mecanismos de protección, y nos invita a responder con prudencia. En ese sentido, el miedo no debe ser percibido únicamente como un enemigo a eliminar, sino como un aliado informativo cuando sabemos escucharlo y comprender sus señales con conciencia.

### **4.4.1 Entender el miedo como aliado, no solo como amenaza**

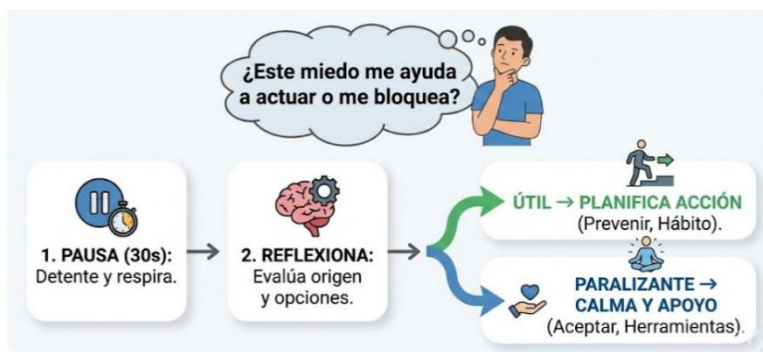
En la época postpandemia, la exposición constante a noticias negativas, incertidumbre social, riesgos de salud, vulnerabilidades digitales, frenéticos cambios sociales y tecnológicos aumentó la sensibilidad al miedo colectivo y personal. En ese contexto, muchas personas tienden a ver el miedo como una amenaza perenne, lo que puede derivar en ansiedad crónica, hipervigilancia, estrés e incluso decisiones impulsadas por pánico. Sin embargo, tratar de eliminar totalmente esa emoción es tanto utópico como contraproducente. Como señalan varios estudios recientes, lo más saludable es aprender a reconocer cuándo el miedo está señalando un riesgo real, interpretarlo con criterio, y transformar esa alerta en acciones concretas y equilibradas (Cabanach et al., 2018).

Para muchas personas, este reencuadre del miedo requiere un cambio de mentalidad profundo. Implica pasar de concebir seguridad como “ausencia de miedo” a concebirla como “capacidad de actuar con conciencia, pese al miedo”. Este paradigma transforma la seguridad integral en una práctica diaria de autocuidado, presencia consciente y responsabilidad: una vida con miedo informado, no con miedo inútil. La Figura 39 muestra un

esquema para diferenciar entre miedo útil y miedo paralizante, comenzando por una pausa y reflexión para decidir entre planificar una acción o buscar calma y apoyo.

### Figura 39

*Pregunta clave cuando sientes miedo*



#### 4.4.2 Técnicas breves para bajar la ansiedad en el día a día

La ansiedad es una respuesta natural del organismo frente a situaciones de incertidumbre, estrés o amenaza percibida. Sin embargo, en la vida cotidiana muchas personas experimentan picos de ansiedad en momentos inesperados: al leer noticias negativas, al recibir un mensaje urgente, al caminar en espacios públicos, o incluso sin un detonante claro.

La evidencia científica respalda la efectividad de los ejercicios cortos de respiración, atención plena y reconexión corporal para reducir ansiedad, tensión muscular y reactividad emocional. Por ejemplo, estudios experimentales muestran que la respiración diafragmática lenta (4-4-6 o 4-4-4) reduce la activación del sistema simpático, disminuye el estrés percibido y promueve sensación de calma en menos de 5 minutos (Ma et al., 2017). Asimismo, otras investigaciones señalan que técnicas de grounding como el método 3-3-3 ayudan a interrumpir pensamientos

catastróficos, restablecer control atencional y disminuir ansiedad aguda (Crane, 2024)

Estas técnicas no están diseñadas para eliminar la ansiedad por completo, sino para regularla, devolver al cuerpo una sensación de estabilidad y permitir a la persona actuar con claridad. Su simplicidad las convierte en aliadas para estudiantes, trabajadores, cuidadores, y cualquier persona que necesite un recurso rápido para recuperar equilibrio emocional durante el día.




Además, su frecuencia de uso influye directamente en los beneficios: la práctica repetida fortalece la capacidad del cerebro para gestionar emociones intensas, modula la respuesta fisiológica y favorece el bienestar mental general. En este sentido, integrar estas técnicas en rutinas breves, como pausas de trabajo, desplazamientos o momentos de espera, contribuye a una vida más consciente, estable y saludable.

La Figura 40 presenta la mini-guía del ejercicio 3-3-3, una técnica breve para reducir ansiedad centrada en observar, escuchar y mover tres elementos del entorno o del cuerpo.

### Figura 40

#### *Ejercicio 3-3-3 en un minuto*

Técnica rápida para reducir la ansiedad y volver al presente.

- **1. Mira 3 cosas que ves**  
Detente y observa tres objetos cerca de ti (ej. mesa, ventana, cuaderno).  
**Objetivo:** Activar la corteza visual y traer la atención al presente.
- **2. Escucha 3 sonidos**  
Identifica tres sonidos, no importa si son lejanos o suaves (ej. ventilador, autos, voces).  
**Objetivo:** Interrumpir pensamientos ansiosos y abrir foco sensorial.
- **3. Mueve 3 partes del cuerpo**  
Mueve suavemente tres partes del cuerpo (ej. cuello, manos, piernas).  
**Objetivo:** Descargar tensión, reconectar con el cuerpo, disminuir activación fisiológica.

#### **4.4.3 Construir resiliencia: recuperar el equilibrio después de un susto**

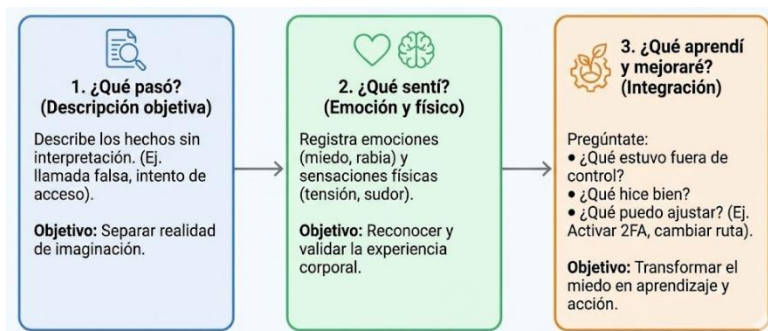
Tras un evento que genera miedo como un intento de estafa, un robo, una noticia impactante, un mensaje sospechoso o una situación amenazante en la calle, es común que la persona experimente desequilibrio emocional, hipervigilancia, pensamientos intrusivos o una sensación de pérdida de control. Estas reacciones no son signo de debilidad: representan una respuesta normal del sistema nervioso ante un estímulo potencialmente peligroso. Sin embargo, si no se gestionan adecuadamente, pueden prolongarse y afectar la vida cotidiana. Por ello, construir resiliencia emocional es clave para recuperarse de manera saludable.

La resiliencia no significa “no sentir miedo” o “hacerse el fuerte”, sino procesar la experiencia, integrar lo ocurrido y reconstruir una sensación de seguridad interna. La literatura reciente destaca que, después de un evento de impacto emocional, prácticas como hablar con alguien de confianza, escribir lo ocurrido, reorganizar la narrativa interna del suceso y planificar acciones preventivas ayudan a disminuir síntomas de estrés y favorecer la adaptación positiva (Schoutrop et al., 2002). Estas estrategias permiten que el cerebro contextualice lo sucedido, evitando que la memoria emocional quede fijada como una amenaza constante.

Asimismo, estudios contemporáneos indican que la resiliencia se fortalece cuando la persona identifica qué estuvo bajo su control, qué no, qué aprendió y qué ajustes puede hacer para sentirse mejor preparada ante situaciones futuras. Esta reflexión reduce la culpa, reemplaza la sensación de impotencia por agencia personal, y mejora la autopercepción de competencia emocional (Hamza et al., 2024)

Además, la resiliencia implica reconocer la necesidad de apoyo externo. La evidencia señala que compartir la experiencia con alguien empático disminuye la activación fisiológica y favorece el procesamiento emocional. El acompañamiento social se asocia con menor estrés post-evento y mayor recuperación psicológica (Wang et al., 2021)

## Ejercicio 8



## 4.5. Comunidad y cooperación

### 4.5.1 Redes de apoyo cercanas: familia, vecinos, amistades

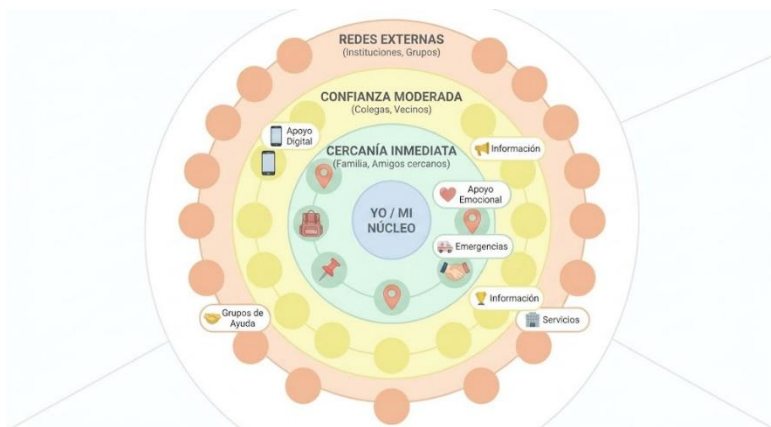
La seguridad personal y colectiva no recae únicamente en decisiones individuales. Una parte fundamental del bienestar y de la protección en la vida contemporánea radica en la calidad de nuestras redes de apoyo: familia, amigos, vecinos, colegas, comunidad. Después de la pandemia, muchas personas se dieron cuenta de que la vida no puede sostenerse en aislamiento absoluto: la colaboración, la solidaridad y el apoyo mutuo son pilares esenciales para construir entornos más seguros, confiables y preparados.

Las investigaciones en psicología social y comunitaria muestran que contar con redes de apoyo reduce los efectos negativos del estrés, disminuye la vulnerabilidad emocional frente a eventos traumáticos, y fortalece la resiliencia individual y

colectiva (Medina et al., 2019). Cuando una persona sabe que puede acudir a alguien en caso de necesidad su sensación de seguridad real y subjetiva aumenta. En contextos urbanos o de alta rotación, las redes sociales informales funcionan como mecanismos de prevención, vigilancia colectiva y cuidado mutuo: alertas ante riesgos, acompañamiento en trayectos, apoyo en emergencias, distribución de responsabilidades, entre otros.

Por otro lado, establecer conexiones de confianza no solo sirve para reaccionar ante emergencias, sino también como forma de prevención y bienestar continuo. Compartir información sobre riesgos, estrategias de protección, coordinar salidas o rutas, mantenerse mutuamente al tanto de situaciones inusuales, intercambiar consejos de autoprotección todo esto incrementa el capital social del grupo y reduce el miedo individual. En una era de múltiples amenazas (físicas, emocionales, digitales), las redes de apoyo son una de las defensas más sólidas, accesibles y humanizadoras.

**Figura 41**  
*Mi red de apoyo*



#### **4.5.2 Seguridad en entornos laborales y educativos**

Los entornos laborales y educativos reúnen a personas con distintos niveles de responsabilidad, hábitos, niveles de conciencia sobre la seguridad y acceso a información sensible. Por ello, la seguridad en estos espacios no depende únicamente de medidas institucionales; también requiere la participación de quienes los habitan. La combinación de protocolos claros, conductas preventivas individuales y acuerdos colectivos de cuidado es fundamental para reducir riesgos y fortalecer un clima organizacional sano.

La literatura reciente señala que los ambientes donde existen normas explícitas de seguridad, señalización adecuada y cultura de comunicación transparente presentan índices significativamente más bajos de accidentes, incidentes críticos y conflictos interpersonales (Martínez et al., 2023). Por otra parte, estudios en psicología organizacional muestran que los espacios donde se fomenta la cultura de “cuidado mutuo” desde acciones tan simples como avisar cuando alguien observa algo inusual, acompañarse al transporte o verificar accesos presentan una mayor percepción de seguridad, cohesión social y confianza entre miembros del grupo (Martinelli, 2023). Esto demuestra que la seguridad no es únicamente una estructura técnica, sino un valor compartido que se construye mediante relaciones humanas sostenidas.

La Figura 42 presenta los cinco puntos esenciales para un lugar de trabajo o aula segura, abarcando planes de emergencia, protección de dispositivos, gestión de datos, alerta colaborativa y compromiso activo.

## Figura 42

### Puntos esenciales de seguridad de dispositivos

- 1. Plan de Emergencia**  
Conozco las rutas de evacuación, puntos de encuentro, protocolos de emergencia, y sé a quién contactar en caso de incidente.
- 2. Protección de Dispositivos**  
Mis dispositivos están siempre bloqueados y nunca desatendidos en áreas compartidas.
- 3. Gestión de Datos Segura**  
Protejo la información sensible (cifrado/seguridad) y evito compartir datos personales/laborales innecesariamente.
- 4. Alerta y Colaboración**  
Mantengo comunicación activa y reporto inmediatamente cualquier anomalía, riesgo o comportamiento inusual.
- 5. Compromiso Activo**  
Participo en todos los simulacros y capacitaciones obligatorias de seguridad física y digital.

### 4.5.3 Proyectos colaborativos de seguridad y bienestar

La seguridad y el bienestar no dependen únicamente de medidas individuales o institucionales: ambos se fortalecen de manera significativa cuando existen iniciativas colaborativas, es decir, esfuerzos organizados por grupos de personas (vecinos, estudiantes, trabajadores, docentes, familias) que deciden coordinarse para crear espacios más seguros, informados y cohesionados.

Los proyectos colaborativos pueden tomar múltiples formas: charlas sobre seguridad digital, grupos vecinales de vigilancia, círculos de apoyo emocional, talleres de prevención de fraudes, simulacros de emergencia, campañas de comunicación, acompañamiento en rutas, reuniones informativas o espacios de escucha. Lo importante no es la magnitud del proyecto, sino que

exista voluntad de participar, construcción de confianza y un objetivo común. Incluso acciones muy pequeñas pueden generar efectos positivos en la percepción de seguridad y bienestar general.

Además, los proyectos colaborativos fomentan una cultura preventiva: no se espera a que ocurra una crisis para actuar; al contrario, se generan prácticas sostenidas que reducen vulnerabilidades y promueven hábitos seguros (Kern et al., 2017).

La Figura 43 presenta una mini-guía para organizar una reunión de seguridad en cinco pasos, desde definir el objetivo hasta establecer un seguimiento claro y medible.

**Figura 43**  
*Cómo organizar una reunión de seguridad en 5 pasos*



## Referencias Bibliográficas

- Alderete, M. (2019). Broadband adoption in Latin American countries: does geographic proximity matter? *Problemas Del Desarrollo*, 50(198), 31–56. <https://doi.org/10.22201/IIEC.20078951E.2019.198.67411>
- American Psychological Association. (2023). *Stress in America 2023: A nation recovering from collective trauma*. [https://www.apa.org/news/press/releases/stress/2023/collective-trauma-recovery?utm\\_source=](https://www.apa.org/news/press/releases/stress/2023/collective-trauma-recovery?utm_source=)
- Armoogum, S., Armoogum, V., Chandra, A., Dewi, D. A., Kurniawan, T. B., Bappoo, S., Salikon, M. Z. M., & Alanda, A. (2025). A Comprehensive Review of Cyber Hygiene Practices in the Workplace for Enhanced Digital Security. *International Journal on Informatics Visualization*, 9(1), 137–145. <https://doi.org/10.62527/JOIV.9.1.3787>
- Augustín, M., Baculáková, K., & Baleha, A. (2022). International Relations 2022: Current issues of world economy and politics. *Ekonom*.
- Bankiewicz, U., & Papadouka, M. (2024). Factors influencing burglary and home security measures in England and Wales. *European Journal of Criminology*, 21(2), 274–300. <https://doi.org/10.1177/14773708231182777>;ISSUE:ISSUE:DOI
- Bartolomé, M. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. *RESI: Revista de Estudios En Seguridad Internacional*, ISSN-e 2444-6157, Vol. 7, No. 2, 2021, Págs. 167-185, 7(2), 167–185. <https://doi.org/10.18847/1.14.9>
- BID. (2020). *BID | Banco Interamericano de Desarrollo*. <https://www.iadb.org/es>
- Bisca, P., Chau, V., Espinoza, R., Fournier, J.-M., Guérin, P., & Salas, J. (2024). Violent Crime and Insecurity in Latin America and the Caribbean. *Departmental Papers*, 2024(009), 1. <https://doi.org/10.5089/9798400288470.087>
- Bourgault, S., Peterman, A., & O'Donnell, M. (2021). Violence against Jordanian Women during COVID-19 Outbreak. *International Journal of Clinical Practice*, 75(3). <https://doi.org/10.1111/IJCP.13824>

- Cabanach, R. G., Souto-Gestal, A., Doniz, L. G., & Vázquez, T. C. (2018). Afrontamiento y regulación emocional en estudiantes de fisioterapia. *Universitas Psychologica*, 17(2). <https://doi.org/10.11144/javeriana.upsy17-2.aree>
- Campos, M., Moreno, R., & Jiménez, B. (2025). Detección de fraudes y estafas basadas en ingeniería social en Ecuador. *Revista InveCom*, 5(3). <https://doi.org/10.5281/ZENODO.14263156>
- Castillo, J., Espinoza, V., & Barozet, E. (2022). *Cohesión social en Chile en tiempos de cambio: indicadores, perfiles y factores asociados*. CEPAL. <https://hdl.handle.net/11362/47735>
- Caycho-Rodríguez, T., Tomás, J. M., Vilca, L. W., Carbajal-León, C., Cervigni, M., Gallegos, M., Martino, P., Barés, I., Calandra, M., Anacona, C. A. R., López-Calle, C., Moreta-Herrera, R., Chacón-Andrade, E. R., Lobos-Rivera, M. E., del Carpio, P., Quintero, Y., Robles, E., Lombardo, M. P., Recalde, O. G., ... Videla, C. B. (2021). Socio-Demographic Variables, Fear of COVID-19, Anxiety, and Depression: Prevalence, Relationships and Explanatory Model in the General Population of Seven Latin American Countries. *Frontiers in Psychology*, 12, 695989. <https://doi.org/10.3389/FPSYG.2021.695989/FULL>
- CEPAL. (2020). *Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19 | CEPAL*. <https://www.cepal.org/es/publicaciones/45938-universalizar-acceso-tecnologias-digitales-enfrentar-efectos-covid-19>
- Chen, P. L., & Pai, C. W. (2018). Pedestrian smartphone overuse and inattentive blindness: an observational study in Taipei, Taiwan. *BMC Public Health*, 18(1), 1342. <https://doi.org/10.1186/S12889-018-6163-5>
- Clemente-Suárez, V. J., Navarro-Jiménez, E., Jimenez, M., Hormeño-Holgado, A., Martínez-González, M. B., Benítez-Agudelo, J. C., Pérez-Palencia, N., Laborde-Cárdenas, C. C., & Tornero-Aguilera, J. F. (2021). Impact of COVID-19 Pandemic in Public Mental Health: An Extensive Narrative Review. *Sustainability* 2021, Vol. 13, Page 3221, 13(6), 3221. <https://doi.org/10.3390/SU13063221>
- Crane, K. (2024). *3-3-3 Rule for Anxiety: Grounding Technique for Panic & Stress* .

- <https://www.southdenvertherapy.com/blog/3-3-3-rule-for-anxiety>
- Curry, D. (2025). *Zoom Revenue and Usage Statistic*. [https://www.businessofapps.com/data/zoom-statistics/?utm\\_source=](https://www.businessofapps.com/data/zoom-statistics/?utm_source=)
- Europol. (2020). *COVID-19 sparks upward trend in cybercrime - Europol's 2020 cybercrime report updates on the latest trends and the current impact of cybercrime within the EU and beyond*. | Europol. [https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime?utm\\_source=](https://www.europol.europa.eu/media-press/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime?utm_source=)
- Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, 21, e01743. <https://doi.org/10.1016/J.SCIAF.2023.E01743>
- Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics*, 10(3), 71. <https://doi.org/10.3390/INFORMATICS10030071>
- Gallegos, M., Consoli, A. J., Franco Ferrari, I., Cervigni, M., de Castro Pecanha, V., Martino, P., Caycho-Rodríguez, T., & Razumovskiy, A. (2021). *COVID-19: psychosocial impact and mental health in Latin America*. <https://doi.org/10.22409/1984-0292/v33i3/51234>
- Ginés, A. (2021). *Sesgo de omisión y la fuerza de la normalidad: en busca del fin del error moral*.
- González, M., & Quevedo, A. (2025). Tendencias actuales en ataques de Ingeniería social. Revisión de literatura. *MQRInvestigar*, 9(1), e203. <https://doi.org/10.56048/MQR20225.9.1.2025.e203>
- González, R. (2024). Seguridad ciudadana como metaderecho humano y rendición de cuentas como garantía: algunas notas conceptuales. *Estado & Comunes*, 1(18), 181-199. [https://doi.org/10.37228/estado\\_comunes.v1.n18.2024.320](https://doi.org/10.37228/estado_comunes.v1.n18.2024.320)
- Guo, C., Wong, K. F., Xu, Y., Hung, K. K. C., & Ho, H. C. (2024). Personal Wellbeing Amid Pandemic Response: Impacts of

- Neighborhood Built Environment, Risk Communication and Health. *Applied Research in Quality of Life* 2024, 1-27. <https://doi.org/10.1007/S11482-024-10395-W>
- Hale, T., Angrist, N., Goldszmidt, R., Kira, B., Petherick, A., Phillips, T., Webster, S., Cameron-Blake, E., Hallas, L., Majumdar, S., & Tatlow, H. (2021). A global panel database of pandemic policies (Oxford COVID-19 Government Response Tracker). *Nature Human Behaviour* 2021 5:4, 5(4), 529-538. <https://doi.org/10.1038/s41562-021-01079-8>
- Hamza, J., Vytkačová, S., Janšáková, K., & Rajčáni, J. (2024). Cognitive reappraisal and acceptance following acute stress. *Stress and Health: Journal of the International Society for the Investigation of Stress*, 40(5). <https://doi.org/10.1002/SMI.3469>
- Hepburn, S. J., Carroll, A., & McCuaig, L. (2021). The relationship between mindful attention awareness, perceived stress and subjective wellbeing. *International Journal of Environmental Research and Public Health*, 18(23). <https://doi.org/10.3390/IJERPH182312290>
- Hernández, J., & Zurita, F. (2022). Inseguridad objetiva, miedo al delito y preocupación por la inseguridad en América Latina. *Contextos: Estudios de Humanidades y Ciencias Sociales*, 50, 25-46. <https://dialnet.unirioja.es/servlet/articulo?codigo=8531955&info=resumen&idioma=ENG>
- IBM. (2020). *¿Qué es la Ingeniería Social?* . <https://www.ibm.com/es-es/think/topics/social-engineering>
- INEC. (2019). *Tecnologías de la Información y Comunicación-TIC 2019* |. <https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic-2019/>
- International Labour Organization. (2020). *Teleworking during the COVID-19 pandemic and beyond A Practical Guide*. [www.ilo.org/publns](http://www.ilo.org/publns).
- Interpol. (2022). *INTERPOL Working Group highlights cyber threats across the Americas*. [https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-Working-Group-highlights-cyber-threats-across-the-Americas?utm\\_source=](https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-Working-Group-highlights-cyber-threats-across-the-Americas?utm_source=)

- ITU. (2019). *Measuring digital development: Facts & figures 2019 - ITU*. [https://www.itu.int/hub/2020/05/measuring-digital-development-facts-figures-2019/?utm\\_source=](https://www.itu.int/hub/2020/05/measuring-digital-development-facts-figures-2019/?utm_source=)
- ITU. (2020). *Measuring digital development*.
- Kemp, S. (2021). *Digital 2021: Global Overview Report*. [https://datareportal.com/reports/digital-2021-global-overview-report?utm\\_source=](https://datareportal.com/reports/digital-2021-global-overview-report?utm_source=)
- Kern, L., Mathur, S. R., Albrecht, S. F., Poland, S., Rozalski, M., & Skiba, R. J. (2017). The Need for School-Based Mental Health Services and Recommendations for Implementation. *School Mental Health*, 9(3), 205–217. <https://doi.org/10.1007/S12310-017-9216-5>
- Kupcova, I., Danisovic, L., Klein, M., & Harsanyi, S. (2023a). Effects of the COVID-19 pandemic on mental health, anxiety, and depression. *BMC Psychology*, 11(1), 108. <https://doi.org/10.1186/S40359-023-01130-5>
- Kupcova, I., Danisovic, L., Klein, M., & Harsanyi, S. (2023b). Effects of the COVID-19 pandemic on mental health, anxiety, and depression. *BMC Psychology*, 11(1), 108. <https://doi.org/10.1186/S40359-023-01130-5>
- Lallie, H., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/J.COSE.2021.102248>
- Lederer, E. (2020). *UN reports sharp increase in cybercrime during pandemic | AP News*. <https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cbd99115bca>
- Leiss, W., Beck, U., Ritter, M., Lash, S., & Wynne, B. (1994). Risk Society, Towards a New Modernity. *Canadian Journal of Sociology*, 19(4), 544. <https://doi.org/10.2307/3341155>
- López, C., & Quinde, Á. (2024). Factores de riesgo que afectan en la accidentabilidad de los trabajadores en la industria de la construcción caso de estudio: Constructora PLADECO S.A. *MQRInvestigar*, 8(4), 227–246. <https://doi.org/10.56048/MQR20225.8.4.2024.227-246>
- Ma, X., Yue, Z. Q., Gong, Z. Q., Zhang, H., Duan, N. Y., Shi, Y. T., Wei, G. X., & Li, Y. F. (2017). The effect of diaphragmatic

- breathing on attention, negative affect and stress in healthy adults. *Frontiers in Psychology*, 8(JUN), 234806. <https://doi.org/10.3389/FPSYG.2017.00874/BIBTEX>
- Martinelli, V. (2023). Student Emotional Well-being, School Climate and Classroom Anxiety. *SCIREA Journal of Sociology*. <https://doi.org/10.54647/SOCIOLOGY840992>
- Martínez, T., Zura, M., & Lomas, C. (2023). Desafíos en la seguridad urbana de Ecuador: un análisis centrado en la ciudad de Quito. *Dilemas Contemporáneos: Educación, Política y Valores*. <https://doi.org/10.46377/DILEMAS.V11IESPECIAL.3967>
- Mcclain, C., Vogels, E., Perrin, A., Sechopoulos, S., & Raine, L. (2021). *The Internet and the Pandemic*. [https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/?utm\\_source=](https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/?utm_source=)
- McIlroy, R. (2023). "This is where public transport falls down": Place based perspectives of multimodal travel. *Transportation Research Part F: Traffic Psychology and Behaviour*, 98, 29–46. <https://doi.org/10.1016/J.TRF.2023.08.006>
- Medina, C. P., Zambrano, C. M. N., & Andrade, M. F. B. (2019). Conciencia Emocional y Regulación Emocional. *Visionario Digital*, 3(3), 75–83. <https://doi.org/10.33262/visionariodigital.v3i3.645>
- Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. *Journal of Economic Criminology*, 7, 100125. <https://doi.org/10.1016/J.JECONC.2025.100125>
- Mousoulidou, M., Christodoulou, A., Averkiou, E., & Pavlou, I. (2024). Internet and Social Media Addictions in the Post-Pandemic Era: Consequences for Mental Well-Being and Self-Esteem. *Social Sciences*, 13(12). <https://doi.org/10.3390/SOCSCI13120699>
- Murphy, C., Lim, W. W., Mills, C., Wong, J. Y., Chen, D., Xie, Y., Li, M., Gould, S., Xin, H., Cheung, J. K., Bhatt, S., Cowling, B. J., & Donnelly, C. A. (2023). Effectiveness of social distancing measures and lockdowns for reducing transmission of COVID-19 in non-healthcare, community-based settings. *Philosophical Transactions. Series A*,

- Mathematical, Physical, and Engineering Sciences*, 381(2257). <https://doi.org/10.1098/RSTA.2023.0132>
- Nagata, J. M., Al-Shoaibi, A. A. A., Leong, A. W., Zamora, G., Testa, A., Ganson, K. T., & Baker, F. C. (2024). Screen time and mental health: a prospective analysis of the Adolescent Brain Cognitive Development (ABCD) Study. *BMC Public Health*, 24(1), 2686-. <https://doi.org/10.1186/S12889-024-20102-X>
- Naik, A. C., Vanteru, M. K., Sanjeev, B., Sravan Kumar, V., & Vaigandla, K. K. (2024). A Comprehensive Survey on Applications, Security Concerns, Attack Mitigation and Secure Routing in IoT. *International Research Journal of Multidisciplinary Scope*, 5(3), 894–906. <https://doi.org/10.47857/IRJMS.2024.V05I03.0885>
- OECD. (2020). *Focus on Latin America from the 2018 Risks that Matter Survey*. [https://www.oecd.org/en/publications/focus-on-latin-american-from-the-2018-risks-that-matter-survey\\_of81365d-en.html](https://www.oecd.org/en/publications/focus-on-latin-american-from-the-2018-risks-that-matter-survey_of81365d-en.html)
- OECD. (2021). *Measuring the economic value of data*. [https://www.oecd.org/en/publications/measuring-the-economic-value-of-data\\_f46b3691-en.html](https://www.oecd.org/en/publications/measuring-the-economic-value-of-data_f46b3691-en.html)
- OECD. (2022). *Going Digital to Advance Data Governance for Growth and Well-being*. <https://doi.org/10.1787/e3d783bo-en>
- OECD. (2025). *Data-Driven Innovation: Big Data for Growth and Well-Being*. *Data-Driven Innovation*. <https://doi.org/10.1787/9789264229358-EN>
- OMS. (2020). *WHO reports fivefold increase in cyber attacks, urges vigilance*. [https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance?utm\\_source=](https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance?utm_source=)
- OMS. (2022a). *COVID-19: Depression, anxiety soared 25 per cent in a year*. <https://news.un.org/en/story/2022/03/1113162>
- OMS. (2022b). *La pandemia de COVID-19 aumenta en un 25% la prevalencia de la ansiedad y la depresión en todo el mundo*. [https://www.who.int/es/news/item/02-03-2022-covid-19-pandemic-triggers-25-increase-in-prevalence-of-anxiety-and-depression-worldwide?utm\\_source=](https://www.who.int/es/news/item/02-03-2022-covid-19-pandemic-triggers-25-increase-in-prevalence-of-anxiety-and-depression-worldwide?utm_source=)

- ONU. (2020). *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean*. <https://doi.org/10.18235/0002513>
- ONU. (2021). *La planificación urbana juega un papel importante en la prevención del crimen*. <https://onu-habitat.org/index.php/reduccion-del-crimen-a-traves-de-la-planificacion-y-gestion-urbana>
- ONU Mujeres. (2020). *COVID-19 and violence against women and girls: Addressing the shadow pandemic | Digital library: Publications | UN Women – Headquarters*. [https://www.unwomen.org/en/digital-library/publications/2020/06/policy-brief-covid-19-and-violence-against-women-and-girls-addressing-the-shadow-pandemic?utm\\_source=](https://www.unwomen.org/en/digital-library/publications/2020/06/policy-brief-covid-19-and-violence-against-women-and-girls-addressing-the-shadow-pandemic?utm_source=)
- Owl labs. (2025). *Statistics On Remote Workers That Will Surprise You (2025 )*. [https://www.apollotechnical.com/statistics-on-remote-workers/?utm\\_source=](https://www.apollotechnical.com/statistics-on-remote-workers/?utm_source=)
- PASPUEL, J. E., CRIOLLO, A. C., MERA, S., & SEGURA, W. M. (2024). Organized Crime And Cybercrime In Ecuador, A New Reality Of Complex Criminality. *Migration Letters*, 21(S10), 734-747. <https://doi.org/10.59670/ml.v21iS11.10561>
- Perez-Vincent, S. M., & Carreras, E. (2021). *Reporte de la violencia doméstica durante la pandemia de COVID-19: evidencia de América Latina*. <https://doi.org/10.18235/0003744>
- PNUD. (2022). *Informe Anual 2022*. <https://annualreport.undp.org/2022/es/>
- Prado, J. (2021). Ingeniería social, un ejemplo práctico. *Revista Odigos*, 2(3), 47-76. <https://dialnet.unirioja.es/servlet/articulo?codigo=8453142&info=resumen&idioma=ENG>
- Primicias. (2021). *Grupos delictivos roban datos bancarios a través de engaños por Internet*. [https://www.primicias.ec/noticias/sociedad/grupos-delictivos-datos-bancarios-internet/?utm\\_source=](https://www.primicias.ec/noticias/sociedad/grupos-delictivos-datos-bancarios-internet/?utm_source=)
- Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World From Edge to Core*.
- Resende, M., Da Fonseca, M., De Freitas, J., Gesteira, E., & Rossato, L. (2023). Impacts caused by the use of screens during the COVID-19 pandemic in children and adolescents: an

- integrative review. *Revista Paulista de Pediatria*, 42, e2022181. <https://doi.org/10.1590/1984-0462/2024/42/2022181>
- Reyes, J. (2021). Victimización y miedo al crimen en Latinoamérica: ¿cómo se relacionan con el bienestar subjetivo? *Intervención: Revista Del Departamento de Trabajo Social de La Universidad Alberto Hurtado*, 11(1), 51-76. <https://dialnet.unirioja.es/servlet/articulo?codigo=10311901&info=resumen&idioma=SPA>
- Riedl, R. (2021). On the stress potential of videoconferencing: definition and root causes of Zoom fatigue. *Electronic Markets*, 32(1), 153. <https://doi.org/10.1007/S12525-021-00501-3>
- Rodríguez, É., Rollón, M., Aguilar, A., Del Campo, E., Güemes, C., Miled, S., Andrea, H., Sofia, M.-M., Gil, P., Tickner, A. B., Ramos, M., Érika, R., Pinzón, R., Sampó, C., Welp, Y., & Zelicovich, J. (2024). *América Latina en un mundo perplejo: Inseguridad, turbulencias económicas y democracias asediadas*.
- Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabae, S., Choo, K. K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, 9(1), 211. <https://doi.org/10.1016/J.DCAN.2022.06.005>
- Schoutrop, M. J. A., Lange, A., Hanewald, G., Davidovich, U., & Salomon, H. (2002). Structured writing and processing major stressful events: a controlled trial. *Psychotherapy and Psychosomatics*, 71(3), 151-157. <https://doi.org/10.1159/000056282>
- Sharot, T. (2011). Why do we overestimate the probability of success? *Current Biology*, 21(23). <https://doi.org/10.1016/J.CUB.2011.10.030>
- Stanford Report. (2021). *Four causes for 'Zoom fatigue' and their solutions* | *Stanford Report*. [https://news.stanford.edu/stories/2021/02/four-causes-zoom-fatigue-solutions?utm\\_source=](https://news.stanford.edu/stories/2021/02/four-causes-zoom-fatigue-solutions?utm_source=)
- The Guardian. (2025). *The Guardian Foundation call on the government to embed news and media literacy into the curriculum*. <https://www.theguardian.com/guardian->

- foundation/2024/dec/02/the-guardian-foundation-call-on-the-government-to-embed-news-and-media-literacy-into-the-curriculum?utm\_source=
- UNESCO. (2021). *One year into COVID-19 education disruption: Where do we stand?* <https://www.unesco.org/en/articles/one-year-covid-19-education-disruption-where-do-we-stand>
- UNESCO. (2025). *Media and Information Literacy* . [https://www.unesco.org/en/media-information-literacy?utm\\_source=](https://www.unesco.org/en/media-information-literacy?utm_source=)
- UNICEF. (2020). *Prevenir y responder a la violencia contra las niñas y los niños en las Américas | UNICEF.* <https://www.unicef.org/lac/informes/prevenir-y-responder-la-violencia-contra-las-ninas-y-los-ninos-en-las-americas>
- UNICEF. (2021). *At least 1 in 7 children and young people has lived under stay-at-home policies for most of the last year, putting mental health and well-being at risk.* [https://www.unicef.org/press-releases/least-1-7-children-and-young-people-has-lived-under-stay-home-policies-most-last?utm\\_source=](https://www.unicef.org/press-releases/least-1-7-children-and-young-people-has-lived-under-stay-home-policies-most-last?utm_source=)
- UNODC. (2022). *UNODC opens new office in Ecuador amidst increasing instability and insecurity.* <https://www.unodc.org/unodc/en/frontpage/2024/May/unodc-opens-new-office-in-ecuador-amidst-increasing-instability-and-insecurity.html>
- UNODC. (2023). *An Epidemic on the Move: The Shifting Landscape of Citizen Security in Latin America and the Caribbean* . <https://www.undp.org/latin-america/blog/epidemic-move-shifting-landscape-citizen-security-latin-america-and-caribbean>
- Vargas, O., Hurley, J., Peruffo, E., Rodríguez s, R., Adascalitei, D., Botey, L., & Staffa, E. (2022). *The rise in telework: Impact on working conditions and regulations.* <https://doi.org/10.2806/956428>
- Vaziri, A. (2025). *COVID mental recovery can take 9 months, study finds.* [https://www.sfchronicle.com/health/article/mental-health-recovery-covid-nine-months-ucla-stud-20365578.php?utm\\_source=](https://www.sfchronicle.com/health/article/mental-health-recovery-covid-nine-months-ucla-stud-20365578.php?utm_source=)

- Vilalta, C., Castillo, J., & Torres, J. (2016a). *Delitos violentos en ciudades de América Latina*. <https://doi.org/10.18235/0007973>
- Vilalta, C., Castillo, J., & Torres, J. (2016b). Violent Crime in Latin American Cities. *IDB*. <https://doi.org/10.18235/0007973>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/SCIENCE.AAP9559>
- Wang, Y., Chung, M. C., Wang, N., Yu, X., & Kenardy, J. (2021). Social support and posttraumatic stress disorder: A meta-analysis of longitudinal studies. *Clinical Psychology Review*, 85, 101998. <https://doi.org/10.1016/J.CPR.2021.101998>
- Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820. <https://doi.org/10.1037/0022-3514.39.5.806>
- Wepy, C. (2021). International Migration from the Latin American-Caribbean Region: Taking Environmental Indicators into Consideration. *City University of New York* . <https://academicworks.cuny.edu>
- World Bank. (2018). *El Telégrafo - El cibercrimen cuesta \$ 600 mil millones al año*. <https://www.eltelegrafo.com.ec/noticias/tecnologia/213/el-cibercrimen-cuesta-usd-600-mil-millones-al-ano>





Red de Investigación  
Científica y Desarrollo  
Tecnológico **Del Pacífico**

  
EDITORIAL  
**SAGA**

ISBN: 978-9907-803-32-7



9 789907 803327