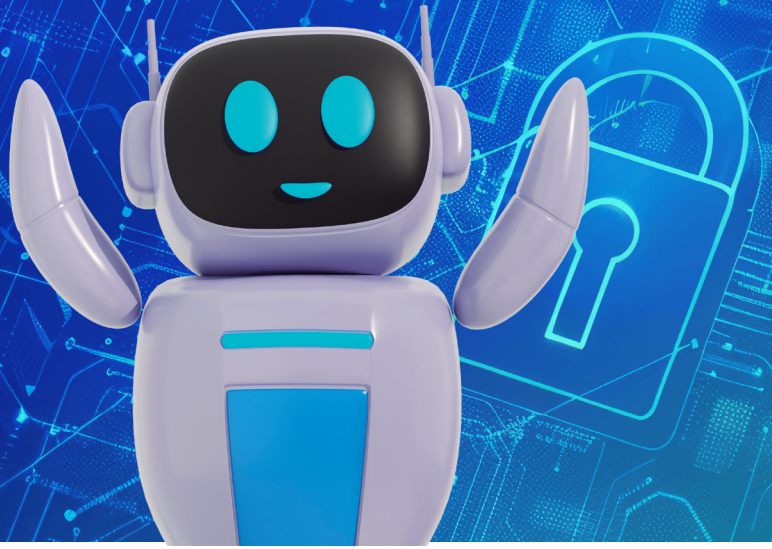
RUTA CIBERSEGURA

NIVEL EN MARCHA



En convenio con:

Global Gateway

UNIÓN EUROPEA

CÁMARA DE COMERCIO DE BARRANQUILLA

Cámara de Comercio de Cali

CAMARA DE COMERCIO DE MEDELLIN PARA ANTIOQUIA

Cámara de Comercio de Bogotá

Equipo de experto/as:

Claudia Yanira Gómez Blanco
Ángela Cristina Villate Moreno
Giovanni Mauricio Malaver Kure

Diseñador: César Ricardo Valencia Jiménez

Equipos técnicos Cámaras de Comercio:

Cámara de Comercio de Barranquilla:

María Elena Bravo Bossio
Jefe Gestión del Conocimiento

María Alejandra Sanabria Muñoz
Estrega de Mercadeo

Cámara de Comercio de Cali:

Jamil Eduardo Mafla
Coordinador Centro de Crecimiento Empresarial

Cristhian Fabián Viafara Arboleda
Gestor Empresarial

Esteban Rodriguez Echeverry
Asesor Empresarial

Cámara de Comercio de Medellín:

Andrés Ricardo Arias Ramírez
Gerente Cluster Negocios Digitales

Luris Arboleda Londoño
Profesional Cluster Negocios Digitales

Gabriel Alberto Cardona Torres
Coordinador de Proyectos

Cámara de Comercio de Bogotá:

Natalia Rojas Mateus
Coordinadora de Seguridad, Transparencia y Cultura de la Legalidad

Heydy Marcela Vela
Profesional junior de Seguridad, Transparencia y Cultura de la Legalidad

Laura Camila Álvarez Martínez
Asesora de Seguridad, Transparencia y Cultura de la Legalidad

ISBN: 978-958-688-560-7

Contenido

No importa el tamaño de tu empresa ni el terreno que enfrentes, conmigo nunca pedaleas solo

¡Hola! Soy Cybersocio,

tu compañero de ruta en este viaje hacia la **ciberseguridad empresarial.**

Imagina que vamos pedaleando juntos por un camino lleno de retos y aprendizajes. Yo estaré contigo en cada parada, mostrándote las señales de alerta, los atajos más seguros y las herramientas que harán tu camino más tranquilo y protegido.

Mi misión es sencilla: acompañar a tu empresa en el recorrido de la Ruta Cibersegura, explicándote de manera clara y práctica cómo proteger tu información, tus clientes y tu negocio.

Así como un ciclista se prepara con casco, luces y un buen mapa, tú también podrás equiparte con las buenas prácticas digitales que te ayudarán a evitar caídas y a pedalear con confianza en el mundo digital.

Soy tu aliado en el camino de la ciberseguridad.

PRESENTACIÓN

Ya no estás en la ciclovía del domingo, con el viento a favor y el jugo de naranja esperando en la esquina. Esa etapa ya pasó. Ahora la ruta se pone un poquito más seria: hay cuestas que exigen cambiar el piñón, bajadas donde no conviene soltar el manubrio y hasta carros que pitan sin compasión.

Tu Mipyme llegó o está en el nivel **En marcha**. Eso significa que ya sabe pedalear, que no se asusta en la primera curva, pero todavía no está lista para coronar el Alto de Letras. Están en esa etapa intermedia: las piernas responden, el aire alcanza, pero cualquier distracción puede costar un raspón o un susto.

Por eso armamos esta cartilla, que funciona como el mapa que marca la ruta y el entrenador que te recuerda que todavía falta aprender a regular el esfuerzo. En esta **Ruta Cibersegura**, y son tres fases que te acompañan en este nuevo tramo:

- **Prevención:** ajustar el casco, revisar frenos y llantas. Esto significa tomar las medidas necesarias en las Mipymes como actualizaciones instaladas o accesos limitados solo a quienes realmente los necesitan. El 80% de los problemas se evita antes de que alguien abra la puerta equivocada.

- **Detección:** sentir que la cadena hace un ruido extraño, que alguien te sigue de cerca o que hay un hueco en la vía. En ciberseguridad es aprender a identificar lo raro: un correo sospechoso, un archivo que no debería estar ahí, un acceso en horas extrañas.

- **Corrección:** porque sí, a veces se pincha o uno se resbala en la curva. En el camino digital esto pasa cuando hay un virus, una cuenta comprometida o un ataque que logra entrar. Lo importante es saber a quién llamar o tener protocolos claros de respuesta.

En esta etapa no se trata de ser el más veloz, sino de ser constante. De aprender a leer el terreno y ganar confianza para que cada kilómetro sea más seguro.

Bienvenido al nivel **En marcha.** Es el tramo donde el pedaleo se hace más firme, la mirada se levanta hacia adelante y, poco a poco, se empieza a disfrutar del camino.

Componente normativo: Ley 1723 del 2009 por medio de la cual se protegen los datos y la información ¿Por qué es importante para mi negocio?

¿Qué es esta ley y para qué sirve?

La Ley 1723 de 2009 protege tu información y tus datos cuando usas internet o cualquier sistema computarizado. Sirve para poner límites, para que nadie use la información de tu negocio —tus correos, tus bases de clientes, tus archivos— como si fueran de libre acceso. En otras palabras, es la policía de tus bits: evita que un desconocido curiosee, copie o destruya lo que a tu negocio le costó años construir.

¿Cómo proteger tu negocio de acciones que pueden causar problemas?

Para evitar incidentes que comprometan la seguridad e información de tu empresa, es fundamental implementar medidas que prevengan conductas indebidas o delic-

tivas en el entorno digital. Aquí te compartimos algunas recomendaciones clave:

- **Control de accesos:** asegúrate de que solo personas autorizadas puedan ingresar a sistemas, redes o computadores. Usa contraseñas seguras y sistemas de autenticación.
- **Monitoreo y mantenimiento:** supervisa el funcionamiento de tus páginas web y redes para detectar y prevenir bloqueos, caídas o alteraciones maliciosas.
- **Gestión de la información:** protege tus datos y los de tus clientes. Evita que se borren, modifiquen o dañen sin autorización mediante respaldos y permisos bien definidos.
- **Prevención de malware** (programas maliciosos que dañan o alteran el funcionamiento de los sistemas sin permiso, como virus, troyanos o spyware): No permitas el uso ni la distribución de este tipo de software. Mantén tus sistemas actualizados y con antivirus confiables.
- **Privacidad de datos personales:** establece políticas claras para el manejo de información sensible. Nunca compartas ni uses datos sin consentimiento.
- **Evita el phishing** (engaños en internet que buscan robar información personal, como contraseñas o datos bancarios, haciéndose pasar por páginas o correos legítimos): Educa a tu equipo sobre cómo identificar páginas falsas o correos engañosos.
- **Seguridad financiera:** Implementa controles para prevenir fraudes o robos de dinero mediante técnicas digitales. Revisa transacciones sospechosas y protege tus activos.

¿Por qué es importante para ti, microempresario?

Porque tienes que cuidar bien los datos de tus clientes y tu negocio. Si alguien en tu empresa hace algo sin permiso o sin seguridad, pueden perder dinero o meterse en problemas legales.

¿Qué hacer?

- Tener buenas claves y sistemas de seguridad.
- No dejar que cualquiera use la información sin permiso.
- Aprender a manejar la información con cuidado.

Historias de ciberseguridad

Un clic que lo cambió todo

Bienestar Laboral del Norte S.A.S. es una empresa reconocida en Norte de Santander por su compromiso con la salud ocupacional y la gestión legal en temas laborales. Cada día, su equipo recibe decenas de correos de juzgados, EPS y ARL, con documentos importantes como resoluciones, fallos y requerimientos. Todo parte de su rutina.

Pero un lunes cualquiera, esa rutina se rompió...

Una asistente administrativa abrió un correo que parecía legítimo. El asunto decía: “Notificación urgente - fallo laboral”, enviado desde una dirección casi idéntica a la de un juzgado. El archivo adjunto prometía ser un documento oficial. Sin sospechar nada, hizo clic.

Nada pasó... al menos en apariencia...

Ese archivo no era lo que parecía. Era un virus (*malware*, es decir, un programa malicioso que daña los sistemas) que se infiltró en la red de la empresa. En menos de una hora:

Varios computadores quedaron bloqueados...

- Los historiales médicos y reportes jurídicos fueron encriptados y secuestrados.
- Un equipo clave se apagó para siempre.

Las consecuencias fueron duras:

Tecnología afectada:

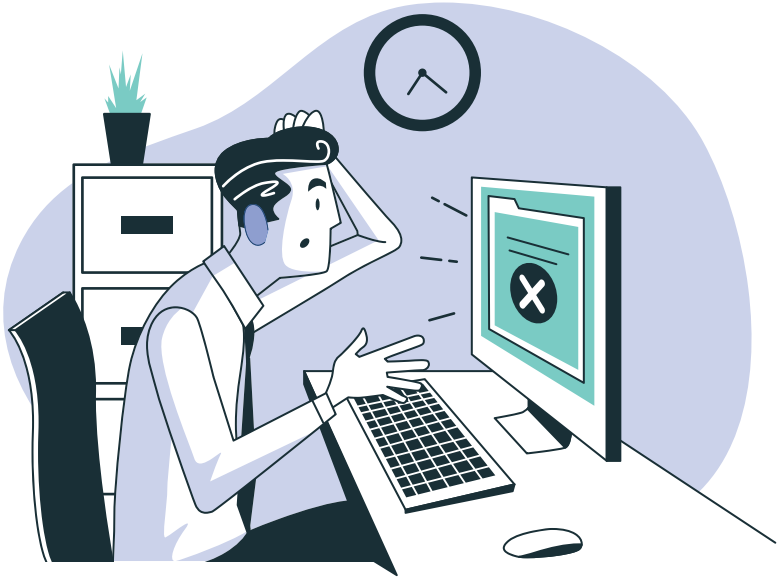
- 6 computadores tuvieron que ser formateados.
- 1 equipo no se pudo recuperar.
- Se perdió información valiosa guardada localmente: historiales, contratos, documentos escaneados.

Operación en jaque:

- Procesos judiciales se retrasaron.
- Exámenes ocupacionales tuvieron que reprogramarse.
- Se invirtieron horas en recuperar y reorganizar todo el caos digital.

Impacto en el bolsillo:

- Compra urgente de nuevos equipos por más de $3 millones.
- Contratación de soporte técnico externo.
- Y lo más delicado: pérdida de confianza con aliados estratégicos



Ruta Cibersegura

Vas a recorrer tres etapas esenciales: **prevención, detección y corrección** de controles en ciberseguridad. Prepárate para asumir un par de retos y, al superarlos, conseguir tu insignia **#PionerosCiberseguros.**

PREVENIR

No eres un principiante en ciberseguridad, ya tienes algunas medidas en marcha. Pero si quieres que esto dure y crezca, no puedes salir a la carretera sin revisar la máquina. La prevención es ese momento justo antes de pedalear, cuando te aseguras de que todo funciona para no terminar en la cuneta.

No hay fórmulas mágicas: no existen cascos que te vuelvan invencible ni candados que espanten a todos los ladrones digitales. Pero sí hay protocolos y rutinas simples que, con constancia, te convierten en un ciclista seguro, en un empresario que avanza con confianza en la ruta digital.

En esta etapa vamos a aprender a:

- **Proteger la información de tus clientes** como quien guarda la bici en un garaje seguro, no en la calle con un candado de juguete.

- **Poner llaves digitales** (contraseñas fuertes, accesos limitados, copias de seguridad) como quien aceita la cadena y revisa los cambios antes de salir.

- **Construir hábitos seguros** en todo el equipo, porque no basta que uses casco si los demás pedalean sin luces en la noche.

La prevención no es un detalle menor, no es solo cruzar la meta primero. La prevención es lo que hace posible que vos, tu Mipyme y tu equipo lleguen hasta ahí.

Bienvenidos a la primera parada de esta ruta: los cuidados básicos e innegociables que te harán avanzar firme, con la certeza de que cada kilómetro es un paso más para ser campeón en la Ruta Cibersegura.

DOBLE AUTENTICACIÓN

¿Cuál es el objetivo de esta etapa?

Queremos que sólo tú, y nadie más, pueda entrar a los sistemas y datos importantes de tu negocio. No queremos que cualquiera con su buena o mala intención se meta a chusmear o hacer desastre en tu negocio ¿verdad?

¿Cómo lo logro?:

Protege tu negocio con doble autenticación (2FA)

Queremos que solo tú, y nadie más, pueda entrar a los sistemas y datos importantes de tu empresa. No queremos que alguien con buenas o malas intenciones se meta a curiosear o hacer desastre, ¿cierto?

La solución: activar la doble autenticación (2FA).

Es como tener dos llaves para abrir la puerta digital de tu negocio. La primera es tu contraseña de siempre. La segunda es un código secreto que solo tú puedes recibir, por ejemplo:

Un mensaje de texto al celular

- Una app de seguridad como Authy o Google Authenticator
- Una llave física que se conecta al computador

Así, aunque alguien adivine tu contraseña, sin la segunda llave no entra.

¿Cómo se activa el 2FA en las apps más usadas?

WhatsApp

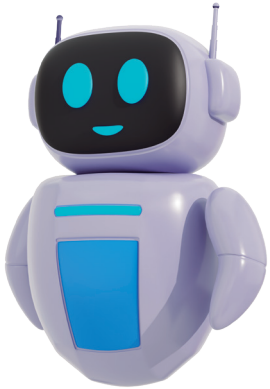
1. Abre WhatsApp.
2. Ve a Configuración > Cuenta > Verificación en dos pasos.
3. Toca Activar.
4. Crea un PIN de 6 dígitos.
5. (Opcional) Agrega tu correo electrónico para recuperar el acceso si olvidas el PIN.

Billeteras digitales (Nequi, Daviplata, etc.)

La mayoría ya tienen protección adicional. Revisa en:

- Configuración de seguridad dentro de la app.
- Activa el PIN de acceso y verifica si ofrecen 2FA por SMS o correo.
- Algunas permiten vincular tu número con una app de autenticación.

Si usas plataformas como redes sociales, bancos o software contable, revisa en sus ajustes de seguridad si ofrecen 2FA. ¡Vale la pena!



Riesgos:

- Que un desconocido se haga pasar por ti y acceda a datos o haga cosas sin permiso.
- Que se pierdan datos valiosos de tu empresa o de tus clientes.
- Que la información escape y te cause problemas grandes, como sanciones o daño a la reputación.

Ventajas de tomar medidas apropiadas:

- Tus cuentas y sistemas quedan bien protegidos, casi como tener dos candados en la puerta.
- Reducción casi garantizada de que entren los malos.
- Cumples con las reglas que piden cuidar bien los datos y la privacidad, sin vueltas.

¿Por qué es importante?

No es cuento: la doble autenticación es la superheroína de la seguridad, y evitaría muchísimos problemas aunque alguien haya conseguido la primera llave.

Errores frecuentes:

- Creer que es demasiado complicado o que no sirve para pymes.
- Quedarse con sólo una llave, sin pedir la segunda.

Ejercicio para superar la etapa:

Primero, aparta un momento para hacer esta tarea que es sencilla, pero cambia mucho las cosas: fíjate si en tus cuentas importantes como el correo electrónico, la cuenta del banco, redes sociales o cualquier sistema que uses para trabajar, ya tienes activada la doble autenticación.

¿Cómo hacer esa revisión?

- Entra a la configuración o seguridad de tu cuenta (por ejemplo, en Gmail está en “Seguridad y acceso”).

- Busca algo que diga “Verificación en dos pasos”, “Autenticación en dos factores” o “Doble autenticación”.

- Si está activada, genial, ¡pasaste el primer filtro de seguridad!

- Si no, ahí es cuando hay que activarla YA.

Y, ¿cómo activarla? Paso a paso para que salga bien a la primera

1. Entra a la configuración de seguridad de la cuenta que vayas a proteger.

2. Busca la opción de “Activar verificación en dos pasos” o similar.

3. Te van a pedir que confirmes tu identidad, que puede ser poniendo tu usuario y contraseña usual.

4. Después, elige cómo recibir el segundo código de seguridad. Hay varias opciones, las más comunes son:

- Un código que te envían por mensaje al celular.
- Un código que genera una app en tu teléfono, como Google Authenticator o Authy, que se renueva cada 30 segundos.

- Una llave física que insertas a la computadora (menos común pero más segura).

5. Una vez elegido, vas a recibir un código para confirmar que funciona. Lo pones y listo, la doble **autenticación queda activada.**

HERRAMIENTAS ANTIPHISHING: QUE NO PESQUEN TUS DATOS

Objetivo de esta etapa:

El objetivo principal es proteger a tu Mipyme del phishing, una técnica de fraude digital en la que un atacante intenta engañarte para que entregues información sensible, como contraseñas, datos financieros o información de tus clientes.

Estos ataques se han vuelto cada vez más comunes y peligrosos, y es clave que tu empresa sepa cómo identificarlos, bloquearlos y responder a ellos. Los mecanismos que usan para engañar suelen ser muy convincentes: correos electrónicos que imitan a entidades oficiales, como bancos o juzgados, con logos y lenguaje profesional; páginas web falsas que se parecen mucho a las reales y que roban tus datos cuando los ingresas; mensajes de texto o WhatsApp con enlaces maliciosos (smishing); llamadas telefónicas que se hacen pasar por funcionarios (vishing); e incluso ataques dirigidos a personal clave como gerentes o contadores (whaling).

¿Cómo lo logro?

Herramientas antiphishing: cómo proteger tu empresa paso a paso.

Para proteger tu negocio del phishing (engaños digitales que buscan robar información), necesitas implementar herramientas que detecten correos, mensajes o sitios falsos antes de que causen daño. Aquí te explicamos cuáles son, cómo funcionan y cómo activarlas.

Filtros de correo electrónico antiphishing

¿Qué son? ... Son sistemas que revisan los correos antes de que lleguen a tu bandeja de entrada. Si detectan algo sospechoso, lo bloquean o lo marcan como peligroso.
¿Cómo activarlos? ... Depende del proveedor de correo que uses:

Por ejemplo, en Gmail empresarial (Google Workspace):

- Ve a admin.google.com
- Ingresa como administrador
- Ve a Apps > Google Workspace > Gmail > Configuración avanzada
- Activa las opciones de protección contra phishing y malware .

Navegadores y extensiones

Usa navegadores como Google Chrome, que ya bloquean sitios peligrosos automáticamente. Refuerza tu seguridad instalando extensiones como Bitdefender TrafficLight o Avast Online Security. Así evitas caer en páginas falsas que roban información.

Reportes y monitoreo

Para cuidar tu negocio, activa las alertas de seguridad en tu correo y revisa los registros de actividad con frecuencia. Herramientas como Microsoft Defender o Google Admin Console te ayudan a detectar accesos sospechosos. Así puedes reaccionar rápido ante cualquier intento de fraude.

Riesgos:

- Si no implementas estas herramientas, tu Mipyme puede estar en riesgo de:
- Robo de datos sensibles (clientes, cuentas bancarias).
- Pérdida económica por transferencias o pagos fraudulentos.
- Daño a la reputación de tu empresa.
- Infección de malware o ransomware tras caer en un enlace malicioso.
- Parálisis temporal del negocio por ataques digitales.

El phishing no solo afecta a grandes empresas; las Mipymes son víctimas frecuentes porque a menudo no están tan protegidas.

Ventajas de tomar medidas apropiadas:

Adoptar herramientas antiphishing en tu Mipyme trae muchos beneficios:

- Mejora la seguridad de la información crítica.
- Protege la confianza de tus clientes y proveedores.
- Reduce pérdidas económicas por fraudes.
- Aumenta la tranquilidad de tu equipo para trabajar sin miedo a engaños.
- Te posiciona como una empresa responsable y comprometida con la ciberseguridad.
- Facilita el cumplimiento de normas y buenas prácticas digitales en Colombia.
- Es una inversión pequeña comparada con el costo que representa un ataque exitoso.

¿Por qué es importante?

El phishing es la puerta de entrada más común para ataques informáticos en Colombia y el mundo. Según fuentes como el Ministerio TIC y expertos en ciberseguridad, más del 90% de los incidentes de seguridad en las pymes empiezan con un email o mensaje fraudulento" (Ministerio de Tecnologías de la Información y las Comunicaciones, citado en CCIT, 2019, p. 7).

Además, estas herramientas no solo protegen datos, sino que también refuerzan la cultura de prevención en tu empresa, haciendo que todo el equipo esté alerta y reduzca el error humano, que es el eslabón más débil en la cadena de seguridad.

Errores frecuentes:

- No capacitar a los empleados en el reconocimiento de phishing.
- Ignorar o no configurar filtros y herramientas básicas en el correo.
- Caer en sitios o enlaces sin verificar su autenticidad.
- No reportar intentos sospechosos a tiempo.
- Pensar que “a mi negocio no le va a pasar”.
- Usar contraseñas débiles o las mismas en varios servicios.
- Evitar estos errores es clave para que las herramientas antiphishing funcionen realmente.

Ejercicio para superar la etapa:

Haz este ejercicio sencillo con tu equipo:

- Simulación de phishing: Envía un correo falso (crear un correo simple tú mismo) con señales claras de ataque (errores ortográficos, links raros).
- Pide a todos tus colaboradores que identifiquen las banderas rojas del mensaje.
- Discute en grupo por qué es importante no clicar en enlaces sospechosos ni compartir información.
- Repasen juntos las herramientas antiphishing que tienen y cómo usarlas.
- Crea un plan de reporte interno para cualquier correo extraño.
- Este pequeño juego ayuda a interiorizar las señales de peligro y mejora la defensa real de tu Mipyme.

CUIDA TUS QR

Objetivo de esta etapa:

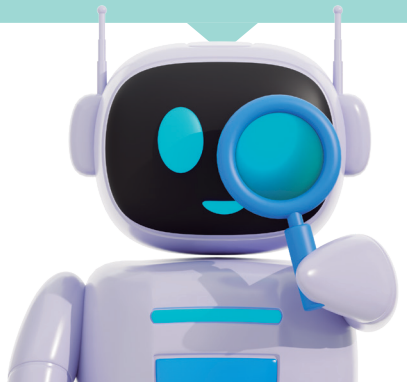
Aprender a cuidar los códigos QR de tu negocio como si fueran las llaves de tu casa: revisarlos, protegerlos y asegurarte de que nadie los cambie por otros truchos que engañen a tus clientes.

¿Cómo lo logro?

Los códigos QR son una herramienta útil, pero también pueden convertirse en una puerta de entrada para fraudes si no se cuidan bien. Por eso, lo primero que debes hacer es un inventario de todos los QR que tienes visibles: en cajas, afiches, etiquetas de productos o en la entrada del local. Luego, revísalos de vez en cuando, como quien se asegura que la cerradura de su negocio no haya sido forzada.

Un truco sencillo para protegerlos es rodearlos con un marco, sello o diseño propio, algo que no sea fácil de copiar. Así, si alguien intenta pegar un QR falso encima, será más evidente. También es clave que tu equipo esté alerta: si ven un código torcido, mal pegado o diferente al habitual, no lo pasen por alto.

Y aquí va una recomendación extra: no dejes los QR expuestos todo el tiempo. Si alguien necesita escanearlo, saca el código en ese momento. Esto reduce el riesgo de que lo manipulen sin que te des cuenta. Además, antes de entregarlo a un cliente, puedes usar una aplicación gratuita que te diga adónde lleva ese código. Así te aseguras de que no haya sido alterado y que la información que se comparte sea segura.



Riesgos:

Un código QR se cambia con la misma facilidad con la que alguien pega un sticker encima de otro. Y si el tuyo lo reemplazan por uno malicioso, tus clientes pueden terminar en páginas falsas que les roben plata o datos personales. Eso no solo significa fraude: también implica que la confianza en tu negocio se va por el inodoro.

Ventajas de tomar medidas apropiadas:

Cuando controlas tus QR, le das tranquilidad a tus clientes de que lo que escanean es seguro. Eso fortalece tu marca, hace que tus promociones funcionen y te permite descubrir intentos de estafa antes de que exploten. En resumen: menos problemas y más confianza.

¿Por qué es importante?

Hoy en día, los QR son la nueva puerta de entrada a tu negocio: un escaneo y ya están adentro. Pero si alguien cambia esa puerta por otra trampa, el visitante termina en un callejón oscuro. Mantener los códigos intactos es, básicamente, cuidar de tu gente y de ti mismo.

Errores frecuentes:

- Dejar los QR desprotegidos, como cartelitos sin candado.
- No revisarlos nunca, confiando en que nadie los toca.
- Usar códigos cualquiera, sin verificar adónde llevan.
- No explicar al equipo por qué esto importa.

Ejercicio para superar la etapa:

1. Haz un listado de todos los códigos QR que tienes en tu negocio.

2. Crea un calendario de revisión semanal para comprobar que estén en condiciones y no hayan sido alterados.

3. Diseña un marco o sello visible para tus QR que sea difícil de copiar o reemplazar.

4. Pide a uno de tus colaboradores que haga una prueba de escaneo con una app confiable para verificar que el código lleve al lugar correcto

5. Reflexiona y anota qué acciones tomarás si detectas un código QR sospechoso o alterado.

APRENDER SOBRE UNA LAS NUEVAS FORMAS DE CIBERDELITOS

Objetivo de esta etapa:

Que todo el equipo conozca las nuevas trampas digitales que acechan a las empresas, para que no se dejen engañar, no cambien contraseñas sin sentido ni abran correos que parecen "normalitos" pero que en realidad son el caballo de Troya que puede dejarte sin los datos de tus clientes ni la tranquilidad que tanto trabajo costó.

¿Cómo lo logro?

Primero, habla sin rodeos con tu equipo. Cuéntales que hoy el ladrón no entra con ganzúas a la ferretería: entra con un click malicioso. Las amenazas digitales evolucionan a diario y ya no se limitan a los clásicos virus o correos sospechosos. Hoy existen nuevas formas de ciberdelitos que afectan especialmente a las MIPYMES: desde los **deepfakes**, que imitan la voz o el rostro de un jefe para dar órdenes falsas; **el phishing**, que se disfraza de correo legítimo para robar claves o dinero; **el ransomware,** que secuestra la información y exige un rescate; hasta los ataques a **dispositivos conectados** (como cámaras o impresoras) o los programas espía que roban datos silenciosamente.

Sin embargo, hay muchos tipos de ciberdelitos, y en esta etapa nos vamos a enfocar en aquellos que usan el engaño y la manipulación —la llamada "ingeniería social"—, porque son los más frecuentes y peligrosos para los pequeños negocios. No requieren grandes conocimientos técnicos del atacante: solo que alguien del equipo caiga en la trampa.

Por eso, conversa con tu equipo sobre estos riesgos. Usa ejemplos reales: el correo que parece de "proveedores" y pide claves, el USB olvidado que trae un virus, o esa app "gratuita" para controlar el stock descargada de un sitio dudoso. Organiza mini charlas periódicas, que no sean monótonas ni llenas de tecnicismos; incluso, pueden tener un toque de humor o ejemplos cotidianos.

Apóyate en videos o relatos reales y crea un manual claro, con ejemplos de qué hacer y qué evitar. Finalmente, asegúrate de que el mensaje quedó claro con pequeñas pruebas o dinámicas prácticas.

Estas charlas deben ser parte de la inducción de nuevos trabajadores. Para facilitarte el proceso, puedes usar recursos como el Cybersecurity Awareness Kit de Proofpoint (2023), que recomienda entrenar al equipo en el uso de autenticación multifactor, mantener el software actualizado y detectar correos falsos mediante simulaciones. Así, la seguridad digital se convierte en una costumbre diaria y no en una tarea más.

Riesgos:

Si tu equipo no está entrenado:

- Pueden caer en correos falsos y dar acceso a hackers.
- Compartir contraseñas o dejarlas fáciles.
- Instalar programas o apps peligrosas sin darse cuenta.
- Perder datos importantes de clientes o proveedores.
- Dañar la reputación del negocio con una fuga de información.

Ventajas de tomar medidas apropiadas:

Al capacitar y sensibilizar a tu equipo:

- Se reduce la posibilidad de ataques informáticos.
- Se protege la información valiosa de tus clientes y proveedores.
- Fomenta un ambiente de confianza y responsabilidad.
- Ayuda a que el negocio pueda seguir funcionando sin interrupciones por problemas digitales.
- Pone el negocio un paso adelante frente a la competencia que no se preocupa por estas cosas.

¿Por qué es importante?

No solo se trata de proteger máquinas o datos, sino de salvar la continuidad del negocio y mantener la confianza, que es el motor para que los clientes sigan eligiendo tu empresa. Como lo señala DocuSign (2025), invertir en seguridad informática no es un lujo reservado para grandes corporaciones o expertos en tecnología, sino una necesidad vital para cualquier pyme que quiera cuidar su historia, su economía y la tranquilidad de todos los que forman parte de ella.

Errores frecuentes:

- Creer que “a nosotros no nos va a pasar”.
- No contestar preguntas o ignorar las charlas de capacitación.
- Usar la misma contraseña en todo (desde la caja hasta el correo).
- Pensar que solo el departamento de informática debe preocuparse.
- No actualizar el software ni cambiar contraseñas periódicamente.

Ejercicio para superar la etapa:

Juego de roles

- Simula situaciones del día a día de tu negocio donde se manejen datos de clientes (pedidos, pagos, datos personales).
- Asigna a algunos participantes el rol de empleados que deben proteger esa información, y a otros, el rol de posibles amenazas internas o externas (ej.: intento de acceso no autorizado).
- Durante el juego, discutan los comportamientos correctos e incorrectos respecto al manejo de la información.
- Concluye con una lista de buenas prácticas para cuidar datos sensibles y minimizar riesgos.

TUS DISPOSITIVOS SON TU FORTALEZA

Objetivo de esta etapa:

Proteger los equipos que usas en tu negocio —computadoras, celulares, tablets— es clave para que se conviertan en una fortaleza y no en una vulnerabilidad. Evitar que haya información personal o de tus clientes guardada sin control ayuda a prevenir problemas si se pierden, son robados o alguien con malas intenciones intenta acceder. Por ejemplo, si eres odontóloga con 15 años de experiencia y llevas registros o citas digitales, asegurar esos datos es cuidar el fruto de todo tu trabajo.

¿Cómo lo logro?

Proteger los equipos que usas en tu negocio —como computadores, celulares o tablets— empieza por aplicar medidas sencillas que hacen una gran diferencia. Una de ellas es no prestar tus dispositivos sin supervisión. Si alguien necesita usarlos, crea una cuenta de usuario con permisos limitados: así podrá trabajar sin acceder a tu información ni modificar configuraciones importantes. En Windows, esto se hace desde el panel de configuración de cuentas, y en celulares puedes activar perfiles restringidos o de invitado.

Otra acción clave es cerrar sesión o bloquear el equipo siempre que no lo estés usando. En los computadores, basta con bloquear la pantalla o configurar el bloqueo automático tras unos minutos de inactividad. En los celulares, activa un método de seguridad —ya sea PIN, huella o reconocimiento facial— y ajusta el tiempo para que el dispositivo se bloquee solo cuando quede sin uso.

Estas prácticas son rápidas, gratuitas y muy efectivas para evitar accesos no autorizados y proteger la información de tu empresa. Porque en seguridad digital, lo simple también salva.

Riesgos:

- Pérdida o robo del equipo con acceso a datos personales o de clientes.
- Instalación de software malicioso (virus, ransomware) que puede secuestrar información o paralizar tu negocio.
- Acceso no autorizado a información confidencial, dañando la confianza y reputación.
- Fallos sin respaldo que pueden causar pérdida irreparable de datos.
- Uso indebido de tus cuentas o herramientas para actividades fraudulentas.

Ventajas de tomar medidas apropiadas:

- Protección real de la información sensible que es la base de tu negocio.
- Evitas dolores de cabeza y costos asociados a recuperaciones o denuncias por filtraciones.
- Generas confianza en tus clientes, quienes saben que sus datos están seguros contigo.
- Mantienes la productividad y continuidad de tus servicios sin interrupciones.
- Creas un hábito que mejora tu cultura digital y la de tu equipo.

¿Por qué es importante?

Cuidado, porque empresas de ciberseguridad locales y regionales, como **Kaspersky**, han destacado que las pymes colombianas enfrentan más de 30 millones de intentos de ataques cibernéticos anuales y enfatizan la necesidad de medidas como copias de seguridad periódicas, capacitación en higiene digital y protección estricta de datos sensibles (Díaz, 2024).

Errores frecuentes:

- Guardar contraseñas y datos personales sin protección o a la vista.
- Ignorar actualizaciones de software y recomendaciones de seguridad.
- Usar el mismo acceso para todos los empleados o colaboradores.
- No hacer copias de seguridad preventivas.
- Compartir equipos sin control o dejarlos desbloqueados en lugares públicos o inseguros.

Ejercicio para superar la etapa:

¿Tus equipos están realmente protegidos? Verifica si los dispositivos que usas en tu negocio están configurados para proteger la información de forma básica pero efectiva.
Instrucciones:

1. Haz una lista rápida de los equipos que usas en tu negocio (computadores, celulares, tablets).

2. Responde estas tres preguntas clave:
   - ¿Tienes activado el bloqueo automático en cada uno de esos dispositivos?
   - ¿Has creado cuentas de usuario con permisos limitados para otras personas que los usan?
   - ¿Cierras sesión o bloqueas la pantalla cada vez que te alejas del equipo?

3. Si respondiste “no” a alguna, el reto de hoy es configurar esa función en al menos un dispositivo. No necesitas ser experto: busca “cómo activar bloqueo automático en tu equipo o “cómo crear cuenta limitada en Windows” y sigue los pasos.

VÍAS DE PAGO SEGURAS

Objetivo de esta etapa:

La idea es sencilla: queremos que tus clientes paguen tranquilos y que tú también lo estés. Porque si al fin y al cabo el dinero no llega ¿para qué tanto esfuerzo?

¿Cómo lo logro?

Primero, usa plataformas de pago reconocidas (bancarias, fintech legales o pasarelas registradas en la Superintendencia). Nada de links raros que te mandó "el primo del primo" que ofrece "transferencias rápidas". Puedes consultar las entidades vigiladas directamente en el portal de la **Superintendencia Financiera de Colombia** (Superintendencia Financiera de Colombia, s. f.).

Segundo, activa la autenticación en dos pasos para tu cuenta y pide siempre comprobante.

Tercero, verifica que el pago no sea solo una captura de pantalla, porque esa es la obra de arte más reproducida en WhatsApp. Mejor, confirma en tu banca en línea o en el panel de la pasarela.

Y cuarto, ten claro que menos es más: un medio de pago seguro, dos o tres máximo, y no veinte que confundan al cliente y abran puertas a errores.

Riesgos:

- Caer en estafas de transferencias falsas o reversadas.
- Que alguien clone tu cuenta de WhatsApp y empiece a pedir anticipos a tu nombre.
- Perder clientes porque no confían en un método de pago que parece salido de una película de bajo presupuesto.
- Multas o sanciones si usas pasarelas no autorizadas.

Ventajas de tomar medidas apropiadas:

- Ganas credibilidad frente a tus clientes: transmitir seguridad es casi tan importante como mostrar una cocina remodelada.
- Tienes trazabilidad: sabes quién te pagó, cuándo y por qué.
- Te cuidas de fraudes y duermes más tranquilo.
- Mejoras tu organización financiera (se acabó eso de andar revisando billetes en la oficina).

¿Por qué es importante?

- La **Superintendencia Financiera de Colombia** insiste en que los comercios solo deben usar medios autorizados.

- **Bancolombia y Davivienda** publican manuales de seguridad digital que recomiendan autenticación en dos pasos y verificación de operaciones.

Errores frecuentes:

- Confiar en capturas de pantalla como prueba de pago.
- Dar los datos de tu cuenta por chat abierto o sin validar al cliente.
- Ofrecer métodos poco claros: “me puede pagar en este Nequi, en esta otra cuenta o si quiere me transfiere a la de mi tía”.
- No capacitar a tus empleados en cómo verificar un pago.
- Dejarse presionar por el cliente al momento de verificar la transacción.

Ejercicio para superar la etapa:

Prueba de estrés con medios de pago digitales.

Un día cualquiera, intenta recibir varios pagos pequeños al mismo tiempo: uno desde banca en línea, otro desde billetera digital y otro con tarjeta. Pídele a dos o tres personas que te ayuden a hacerlos en paralelo.

El reto es ver:

- Si puedes verificar todos rápido sin confundirte.
- Si los comprobantes llegan claros y ordenados.
- Si alguna plataforma se demora más de lo normal.

Al final, apunta qué tan ágil fue el proceso y si tu sistema aguanta la presión. Esto te va a mostrar si, en un día de mucha venta o de cobros simultáneos, estás preparado o te vas a enredar confirmando pagos.

ZONA DE HIDRATACIÓN:

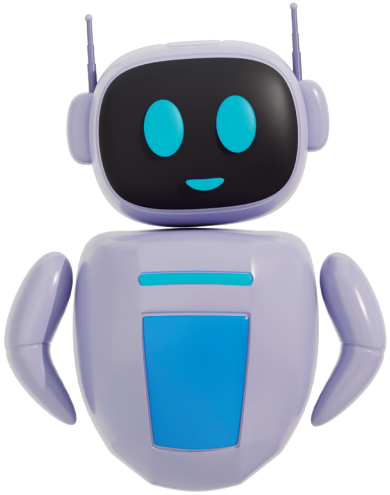
Aprendamos con un caso

Laura era la consultora perfecta: rápida, eficiente, siempre al día. Un martes abre un correo con asunto "Cambios urgentes en contrato XYZ". Estaba justo en ese proyecto, clic inmediato.

Cinco minutos después: servidores bloqueados, accesos caídos, caos total. El adjunto era malware. ¿La raíz del desastre? No mala fe, ni falta de talento: falta de entrenamiento.

Ahora, imaginen otra escena: la empresa le da a cada nuevo consultor 30 minutos de taller anti-phishing, recordatorios semanales y un botón en Outlook para reportar correos raros. La misma Laura duda, reenvía el mensaje, el ataque se frena, y ella pasa de víctima a heroína.

¿Qué podemos aprender? En TI, el problema no siempre es técnico. Lo que salva es una cultura simple y viva de ciberseguridad. Y no lleva una maestría: basta entrenar a tiempo



DETECTAR

Ya ajustaste el casco y saliste a rodar. Pero en la ruta no basta con revisar frenos: lo que salva es notar a tiempo el hueco escondido o el carro que invade tu carril.

En tu Mipyme pasa igual: la prevención no alcanza si no sabes detectar. Un correo raro, un inicio de sesión a medianoche, un archivo que aparece sin explicación, un computador que se pone lento.

La detección es esa intuición que dice: *"mejor reviso antes de que esto se rompa"*.

En esta fase de la Ruta Cibersegura aprenderás:

- Herramientas para vigilar tu negocio digital.
- Señales de alerta que no se pueden ignorar.
- Rutinas simples para mantener la vista en la ruta.

Así como el ciclista que escucha su bicicleta, tu Mipyme puede adelantarse al problema y no al golpe.

PRIORIZA Y MITIGA

Objetivo de esta etapa:

Imagina que tienes una oficina de abogados y que es como una bodega de vino. No cualquier vino: de esos que no se consiguen en el supermercado, sino botellas que un cliente confió porque sabe que las cuidas mejor que nadie. Eso son los datos: testamentos, contratos, litigios, secretos comerciales. El objetivo en esta etapa es simple: decidir cuáles botellas son las más valiosas, cuáles corren más peligro de romperse, y cómo evitar que un descuido las tire al piso.

¿Cómo lo logro?

No se trata de blindar todo con alarmas. El truco está en tres pasos:

1. Haz inventario: documentos, bases de clientes, contraseñas, facturas, diseños, todo.
2. Pregúntate dos cosas:

- ¿Qué pasa si esto se filtra?
- ¿Qué tan fácil es que se pierda o lo roben?

3. Pon prioridades: lo más delicado arriba de la lista, y a cada punto una acción concreta: copias de seguridad, accesos restringidos, contraseñas decentes, cifrado si es necesario.

Riesgos:

- Que alguien mande por error un archivo sensible desde su correo personal.
- Que un celular con fotos de documentos termine perdido en un bus.
- Que la contraseña de la wifi sea “123456” y cualquiera se conecte.
- Que alguien borre un archivo clave pensando que “ya estaba guardado en la nube”.

Ventajas de tomar medidas apropiadas:

- **Tranquilidad:** sabes qué es lo más importante y cómo lo estás cuidando.
- **Confianza:** tus clientes sienten que su información está segura con vos.
- **Ahorro:** prevenir cuesta menos que arreglar un desastre.
- **Orden:** tu equipo sabe qué datos son críticos y cómo manejarlos.

¿Por qué es importante?

La Cámara Colombiana de Informática y Telecomunicaciones (CCIT) insiste en que el primer paso de la ciberseguridad para pymes es identificar riesgos y priorizar. Y organismos como el Centro Cibernético de la Policía Nacional repiten que la fuga de información es uno de los incidentes más comunes en negocios pequeños, precisamente porque no se jerarquizan los datos.

Errores frecuentes:

- Pensar que todo vale lo mismo: un flyer viejo no es igual de delicado que una lista de clientes.
- Decirse: “eso nunca nos va a pasar”. Pasa, y siempre cuando menos lo esperas.
- Confiar en que la nube guarda todo por arte de magia.
- Gastar en herramientas sofisticadas, pero olvidarse de lo básico: cambiar contraseñas, tener un respaldo, capacitar al equipo.

Ejercicio para superar la etapa:

Si mañana alguien de tu equipo pierde un portátil con información de la empresa, ¿qué sería lo más grave que podría pasar? (puedes marcar más de una):

- [ ] Los datos de tus clientes quedan dando vueltas en manos desconocidas.
- [ ] Pierdes información clave para entregar un proyecto a tiempo.

- [ ] Aparece tu competencia con una oferta sospechosamente parecida a la tuya.
- [ ] Tienes que llamar a un cliente a decirle: “disculpa, se me perdió tu información”.
- [ ] Nada grave, porque ya tiene copias de seguridad y accesos restringidos.

Después de marcar, fíjate:

- Si marcaste las primeras cuatro, tu empresa está caminando en la cornisa.
- Si marcaste la última, vas un paso adelante, pero revisa si de verdad es así o es puro optimismo.

ELEGIR EL MEJOR ANTIVIRUS PARA TU MIPYME

Objetivo de esta etapa:

No es que tu empresa sea la NASA ni que manejes planos secretos de la CIA. Pero lo que tienes en tu computador vale más que el auto estacionado en la puerta: facturas, contratos, nóminas, diseños, proveedores, clientes. Elegir un antivirus no es un capricho de paranoico, es ponerle cerradura a la puerta. El objetivo es simple: que tus datos no terminen en manos de alguien que, en el mejor de los casos, te va a pedir plata para devolvértelos.

¿Cómo lo logro?

No basta con googlear “mejor antivirus 2025” y elegir el primero que esté en oferta. Elegir protección digital para tu negocio es como contratar un seguro médico: depende del tamaño de tu empresa, de lo que haces y de cuánto puedes invertir.

Para tomar una buena decisión, empieza por revisar qué dispositivos usas (computadores, celulares, tablets). Pregunta si el antivirus cubre varios equipos o solo uno. Asegúrate de que incluya protección contra ransomware y phishing, que son los ataques más comunes en las pymes. Y aunque las versiones gratuitas pueden servir como punto de partida, no te confíes: es como correr Fórmula 1 con casco de bicicleta.

¿Y si no puedes pagar aún? Hay opciones gratuitas que ofrecen buena protección básica, como Microsoft Defender (ya viene con Windows) o Avast Free Antivirus. No tienen todas las funciones avanzadas, pero ayudan a detectar amenazas comunes mientras evalúas una solución más completa.

Antes de elegir, prueba la interfaz: si tu equipo no entiende cómo usarlo, no servirá. Es como comprar una cafetera italiana sin saber prender la hornalla. Lo importante es que el antivirus se adapte a tu negocio, no al revés.

Riesgos:

- No instalarlo en todos los equipos: el virus entra por la máquina olvidada.
- No actualizarlo: antivirus viejo es igual a puerta cerrada con candado de juguete.

Ventajas de tomar medidas apropiadas:

- Estás tranquilo: lo que más vale de tu empresa está vigilado.
- Te ahorras plata: reparar el desastre de un ataque cuesta diez veces más que pagar la licencia.
- Te ganas la confianza de clientes que saben que sus datos no terminan dando vueltas en foros raros de internet.

¿Por qué es importante?

El microcurso sobre ciberseguridad para mipymes del Banco Interamericano de Desarrollo enseña buenas prácticas para proteger los sistemas empresariales, destacando la importancia de mantener actualizados los antivirus para detectar y prevenir daños cibernéticos (Banco Interamericano de Desarrollo, 2025), puedes consultar a través del siguiente enlace: https://cursos.iadb.org/es/temas/desarrollo-instituciones/microcurso-ciberseguridad-para-mipymes

Errores frecuentes:

- Instalar uno gratis y olvidarse de todo lo demás.
- Poner un buen antivirus pero nunca renovarlo porque “me da pereza meter la tarjeta otra vez”.
- No capacitar al equipo: un clic en un correo trucho tira abajo todo lo que pagaste.

Ejercicio para superar la etapa:

Pregunta:

¿Cuál de estas opciones asegura que tu Mipyme tenga un "equipo completo" en ciberseguridad?

a. Instalar un buen antivirus en un solo computador y confiar en que el resto no será atacado.

b. Descargar versiones gratuitas en algunos equipos y dejar los celulares sin protección.

c. Comprar una licencia empresarial y asegurarte de que todos los computadores y celulares de trabajo estén cubiertos y actualizados.

d. No instalar nada, porque "aquí nunca pasa nada" y lo importante es no gastar.

CONEXIÓN SEGURA PARA TU NEGOCIO Y TUS CLIENTES

Objetivo de esta etapa:

Lo que buscamos acá es simple: saber si tu conexión tiene un huequito escondido. Porque una red con fuga es como una ventana mal cerrada. Lo que buscamos acá es simple: saber si tu conexión tiene alguna fuga escondida.

¿Cómo lo logro?

Observar las luces del router

¿Qué hacer? Mira el router cuando nadie esté usando internet (por ejemplo, fuera del horario laboral).

Si las luces de actividad parpadean constantemente —como un arbolito de Navidad— puede que haya dispositivos conectados sin autorización.

¿Qué significa? Actividad inusual puede indicar que alguien externo está usando tu red sin permiso.

Revisar los registros del router

¿Cómo hacerlo? Abre un navegador web en un computador conectado al WiFi. Escribe la dirección IP del router (generalmente es 192.168.0.1 o 192.168.1.1). Ingresa con el usuario y la contraseña del administrador (puedes consultarlos en el manual del router o en la etiqueta del dispositivo)

¿Qué verás?

Una lista con los nombres, direcciones IP y horarios de conexión de todos los dispositivos conectados. Si ves algo desconocido (como un celular que no reconoces), puede ser una señal de intrusión.

Riesgos:

Si no vigilas la conexión, te expones a cosas feas:

- Un vecino o desconocido usando tu internet gratis para cosas que después te comprometen a ti.
- Un ataque directo: alguien entra a tu red y desde ahí a tus archivos, como quien se mete a tu oficina por la ventana de atrás.
- Tus operaciones de pago, correos y datos de clientes pueden quedar al desnudo.

Ventajas de tomar medidas apropiadas:

- **Más confianza para los clientes:** cuando un proveedor o cliente se conecta a tu red y nota que todo está ordenado y seguro, transmite profesionalismo (nadie confía en un negocio con candados flojos).
- **Ahorro escondido:** cada intruso fuera significa menos consumo de internet, menos caídas y menos horas de técnico corriendo detrás de un “no sé qué pasó”.
- **Tranquilidad para crecer:** si mañana sumas más equipos o empleados, lo haces sobre una base firme, no sobre arena movediza.

¿Por qué es importante?

Como señala Interempresas (2023), “el router es tu primera línea de defensa… pero si lo dejas con la configuración default, es solo una puerta abierta. No es magia: es tu fortaleza” (https://www.interempresas.net/TIC/Articulos/467608-El-router-primera-linea-de-defensa-o-una-puerta-de-entrada-ante-un-ciberataque.html).

Ejercicio para superar la etapa:

Practica esto

Entra al panel de tu router (la dirección suele estar en una etiqueta pegada atrás).

1. **Busca la sección de “usuarios conectados”** y sácale un pantallazo.
2. **Haz tres columnas en una hoja:**

- En la primera pon los nombres que reconoces.
- En la segunda los que dudas.
- En la tercera los que no tienes idea quiénes son.

La tarea de la semana: limpiar la tercera columna. Y si en la segunda no puedes confirmar quién es, también afuera.

Errores frecuentes:

- Confiar ciegamente en el proveedor de internet: creer que porque te instalaron el router ya viene “a prueba de balas”. Spoiler: no.
- Dejar la red abierta fuera del horario laboral: tu WiFi trabajando toda la noche mientras duermes. A veces el único que descansa es el dueño.
- Nunca mirar los logs del router: esos registros parecen jeroglíficos, pero te dicen quién se conectó. Ignorarlos es como no leer el extracto bancario.
- Pensar que “seguridad” es solo antivirus: cuando la puerta está abierta, da igual que tengas cámaras.

DETECTA LAS SUPLANTACIONES CON IA

Objetivo de esta etapa:

Que no te vean la cara con una voz robótica que suena igualita a tu proveedor o con un correo que parece escrito por tu mejor cliente. La meta es simple: que cuando alguien te hable “raro”, se te prenda el bombillo de la desconfianza antes de abrir la billetera de la empresa.

Las suplantaciones digitales están evolucionando a pasos agigantados, y hoy no basta con desconfiar de un correo mal escrito. Ahora, los delincuentes usan inteligencia artificial para crear voces clonadas, correos falsificados y hasta videos manipulados que parecen completamente reales.

Suplantación por voz robótica

Gracias a herramientas de clonación de voz, los ciberdelincuentes pueden generar audios que imitan con precisión la voz de una persona real. Basta con tener unos segundos de grabación para que la IA aprenda el tono, ritmo y acento. Luego, esa voz puede usarse para hacer llamadas falsas que suenan igual que tu proveedor, tu jefe o un cliente importante. En Colombia, esta técnica ya se considera agravante legal bajo la nueva Ley 2502 de 2025, que castiga la suplantación con IA.

Correos que parecen legítimos

También están enviando correos que copian el estilo, firma y lenguaje de personas conocidas. Usan logos, direcciones similares y hasta frases que parecen sacadas de conversaciones reales. El objetivo es que confíes y hagas clic en enlaces maliciosos o transfieras dinero creyendo que es una solicitud legítima.

¿Cómo lo logro?

Usando algo que no tiene ninguna inteligencia artificial: la costumbre humana. Si tu proveedor nunca te manda audios de WhatsApp a las 8 de la mañana, ¿por qué justo hoy sí? Si tu proveedor escribe con faltas de ortografía hasta en las facturas, ¿cómo ahora manda un correo perfecto digno de la RAE? Esos detalles son los que te salvan.

La clave está en desconfiar de lo que suena "demasiado real" o "demasiado perfecto

Riesgos:

El riesgo más grande es caer por inocente: transferir plata a una cuenta equivocada porque creíste en una voz clonada, entregar datos de clientes porque confiaste en un correo pulidito, o perder la reputación cuando cuentas que te robaron con un "video deepfake" (video deepfake es un video falso que imita situaciones reales, como un simulacro) que parecía de ciencia ficción.

Ventajas de tomar medidas apropiadas:

Cuando aprendes a detectar la suplantación, ganas un superpoder: dormir tranquilo. Porque no es que la IA deje de intentar estafarte, sino que ya sabes mirar dos veces. Además, puedes educar a tu equipo: desde la secretaria hasta el mensajero terminan siendo radares de fraudes disfrazados.

¿Por qué es importante?

La Superintendencia Financiera de Colombia (2025) ha alertado sobre comunicaciones fraudulentas falsamente firmadas por ellos, incluyendo supuestas "cobranzas" o "impuestos" para liberar créditos, algo que la entidad aclara que nunca solicita.

Ejercicio para superar la etapa:

Imagina esta situación: recibes una videollamada de tu jefe pidiéndote transferir dinero urgente. Se ve igual, se escucha igual. Solo que te pide enviarlo a una cuenta que no conoces.

¿Qué haces?

1. Transferís enseguida, porque tu jefe es tu jefe.

2. Cortas la llamada y verificas por otro canal (llamada directa, mensaje, reunión).

3. Le pides que te cante la canción de cumpleaños al revés para comprobar que es él.

Errores frecuentes:

- **El complejo de invisibilidad:** "¿Quién me va a clonar a mí si apenas vendo empanadas por WhatsApp?". Justo por eso: porque pasas desapercibido para la prensa pero no para el estafador que busca un blanco fácil.

- **No todo lo digital es real:** tu proveedor escribe correos como cavernícola ("grasia por su atencion señora"), y de repente te manda un mail con comas perfectas y tildes en su lugar. En vez de alegrarte, eso debería sonar como alarma de incendio.

- **El chiste mal contado:** algunos se ríen del asunto, como si la suplantación fuera un capítulo de una serie de televisión que no les toca. Hasta que un día están contando la anécdota en el asado: "me robaron con un audio mío que nunca grabé". Y ahí la carcajada es de los otros.

EL CIBERACOSO A LA VUELTA DE LA CIENCIA

Objetivo de esta etapa:

Entender que el ciberacoso no solo les pasa a los adolescentes que pelean por “likes”. También puede llegar a tu negocio: un cliente molesto que arma campaña en redes, un ex empleado despechado que suelta rumores, o un competidor con tiempo libre y mala leche. El objetivo es que sepas identificar cuándo algo es broma de mal gusto y cuándo puede empezar a dañar tu reputación y tus ventas.

¿Cómo lo logro?

Primero, reconociendo que no tienes que aguantar en silencio. El ciberacoso no distingue género, pero sí puede afectar de forma distinta; por ejemplo, muchas mujeres emprendedoras reciben comentarios sexistas, burlas sobre su liderazgo o insinuaciones personales disfrazadas de “críticas”. Si un mensaje se repite, si alguien insiste en ofender, acosar o ridiculizar tu empresa —o tu rol como mujer al frente— hay que actuar.

No se trata de bloquear sin pensar, pero sí de poner límites claros y proteger tu espacio digital. Aquí algunos pasos clave:

- Guardar evidencia: toma capturas de pantalla, guarda mensajes y registra fechas. Esto te da respaldo si decides denunciar.
- Reportar en la plataforma: redes como Instagram, Facebook o WhatsApp tienen opciones para denunciar acoso o suplantación.
- Definir un protocolo interno: establece con tu equipo quién responde, quién no, y cuándo es momento de acudir a asesoría legal o a las autoridades. Si eres mujer emprendedora, considera incluir una red de apoyo o asesoría especializada en violencia digital.

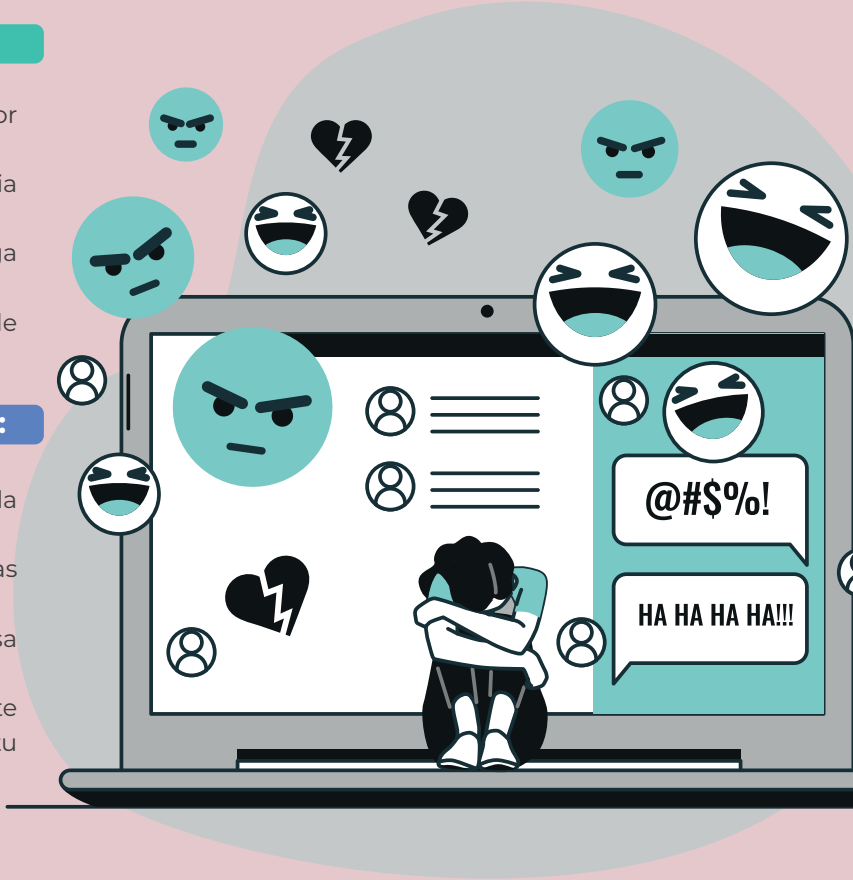
Recuerda: cuidar tu reputación también es cuidar tu bienestar. Y en tu negocio, tu voz merece respeto, sin importar quién esté del otro lado de la pantalla.

Riesgos:

- Que un rumor crezca más rápido que tu mejor campaña de marketing.
- Que empleados empiecen a dudar de su propia seguridad digital.
- Que el miedo o el desgaste emocional te distraiga del negocio.
- Que un ataque sostenido termine en pérdida de clientes o contratos.

Ventajas de tomar medidas apropiadas:

- Al detectar a tiempo el ciberacoso, evitas que la bola de nieve se convierta en avalancha.
- Aprendes a blindar tu reputación: demuestras que eres firme y transparente
- Le das confianza a tu equipo: saben que, si pasa algo, no están solos.
- Conviertes un ataque en oportunidad: un cliente que ve cómo reaccionaste puede valorar más tu profesionalismo que el de la competencia.



¿Por qué es importante?

Según Pymas, citando datos de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), se registraron 28.827 incidentes informáticos en Colombia en 2019, y las pymes fueron las más afectadas. Esto evidencia que los riesgos digitales —como el ciberacoso— tienen implicaciones reales en la estabilidad y confianza empresarial (Pymas, 2020).

Errores frecuentes:

- Pensar que el acoso “se resuelve ignorando”. Ignorar sirve un rato, pero si hay un patrón, hay que actuar.
- Contestar con la misma furia (El acosador se alimenta de tu enojo).
- No guardar pruebas. Después, cuando quieres denunciar, no queda rastro.
- Minimizar lo que pasa porque “no es físico”. El daño emocional y reputacional sí se siente en la caja registradora.

Ejercicio para superar la etapa:

Selecciona la respuesta adecuada

Un desconocido empieza a dejar comentarios ofensivos en tu página de Facebook. Al principio parecen bromas pesadas, pero luego empiezan a repetirse, a etiquetar a clientes y hasta a inventar datos falsos sobre tu negocio. ¿Qué haces primero?

A. Le contesto en público con la misma intensidad, para que la gente vea que no me dejo.

B. Lo dejo pasar porque “al fin y al cabo, el que me conoce sabe que no es verdad”.

C. Reviso si hay un patrón, hago captura de pantalla de todo, guardo la evidencia y lo reporto en la plataforma.

D. Le pido a un amigo o empleado que le responda con humor, a ver si así se calma.

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Marcela es auxiliar de enfermería en una empresa de exámenes ocupacionales. Todos la quieren: siempre sonríe, siempre paciente.

Un día, un compañero administrativo — con el que apenas había cruzado dos palabras— empezó a mandarle caritas por WhatsApp. Después vinieron las preguntas personales. Luego, comentarios sobre su ropa. Cuando ella no respondió, llegaron las burlas en redes.

Marcela pensaba: “Seguro exagero, no quiero problemas”. Hasta que un día él compartió una foto editada de ella en el grupo del trabajo. Ahí se rompió todo.

Habló con la psicóloga, se activó el protocolo, el comité de convivencia intervino. Hubo sanciones y acompañamiento. Lo más importante: el equipo entendió que el ciberacoso no es broma.

Ahora bien, imaginemos otra empresa. Una que ya dio talleres de respeto digital, que tiene un canal anónimo para denunciar y que deja claro que acosar en línea también es delito. En ese escenario, Marcela habría hablado antes. Y tal vez él lo habría pensado dos veces.

El acoso digital no se ignora ni se minimiza. Una empresa segura no solo protege los datos de sus pacientes: protege la dignidad de su gente.

CORREGIR

Si llegaste a este punto es porque ya superaste lo básico: aprendiste a detectar riesgos y tomaste medidas de prevención. Eso significa que no solo pedaleas, sino que lo haces con confianza y experiencia acumulada.

Ahora toca la corrección: el momento en que algo falla y tu madurez se nota en la reacción. No se trata de evitar caídas, sino de levantarte rápido, ajustar lo necesario y volver a rodar sin perder el rumbo. Esa es la diferencia entre la improvisación y la preparación.

Estás cerca del nivel senior, donde la verdadera fortaleza es tener planes listos, contactos de soporte y la certeza de que ningún tropiezo frena el recorrido. Corregir es demostrar que tu negocio sabe reaccionar y que siempre puede seguir avanzando.

CÓMO DENUNCIAR DELITOS DIGITALES: DE LA EVIDENCIA AL RADICADO OFICIAL

Objetivo de esta etapa:

No se trata de ser Sherlock Holmes ni de jugar a CSI, ni de quejarse en un grupo de WhatsApp. El objetivo es aprender a recopilar pruebas digitales válidas y poner la denuncia oficial de manera que tenga valor legal, aumentando las probabilidades de que la investigación avance de verdad. Esto aplica si te roban dinero, alguien suplanta tu empresa en redes o recibes correos fraudulentos.

¿Cómo lo logro?

1. Guardar la evidencia correctamente

- No alteres los archivos: si el ataque llegó por correo, no lo copies en Word ni imprimas capturas de pantalla. Usa la opción “ver original” o “.eml/.msg” para conservar todo: texto, cabeceras, hora y ruta de envío.
- Respeta los metadatos: no renombres ni abras archivos sospechosos. Son el “ADN” de la prueba.
- Duplica sin modificar: copia a un USB, disco duro o nube sin cambiar nada. Así tienes un respaldo idéntico al original.

2. Denuncia virtual oficial

- Entra a la plataforma oficial: adenunciar.policia.gov.co.
- Regístrate o inicia sesión con tu cédula y un correo activo.
- Selecciona el tipo de hecho: ciberacoso, fraude electrónico, suplantación de identidad, etc.

- Completa el formulario indicando qué pasó, cuándo, dónde y adjunta las pruebas digitales.

- Al finalizar, obtendrás un número de radicado, que te permite hacer seguimiento y sirve como respaldo legal.

Riesgos:

- Presentar pantallazos incompletos que la Fiscalía no puede validar.
- Creer que denunciar por la plataforma ya resuelve todo; la investigación puede tardar.
- No guardar pruebas ni número de radicado.
- Usar computadores públicos y dejar tus credenciales expuestas.

Ventajas de tomar medidas apropiadas:

- Aumentas las oportunidades de que la denuncia avance de verdad.
- Ganas respaldo legal: un número de radicado oficial tiene la misma validez que una denuncia presencial (Policía Nacional de Colombia, s. f.).
- Ahorras tiempo y reduces errores al entregar pruebas completas y originales.
- Contribuyes a estadísticas oficiales, ayudando a que se asignen más recursos para combatir ciberdelitos.

Ejercicio para superar la etapa:

Imagina que recibes un correo sospechoso de tu “banco” pidiéndote actualizar tus datos, o que te roban dinero mediante un correo fraudulento. Tienes varias opciones:

A. Sacar una foto con el celular y borrar el correo.
B. Hacer un pantallazo en JPG y adjuntarlo a la denuncia.
C. Descargar el correo en formato .eml o .msg, conservar metadatos, duplicar a un USB y radicar la denuncia completa en adenunciar.policia.gov.co con número de radicado seguro.
D. Mandar solo un correo informal al banco sin usar la plataforma oficial.

Pregunta única: Si tu objetivo es que la denuncia avance y quede con respaldo legal, ¿cuál opción elegirías?

¿CÓMO RECUPERAR MI CUENTA WHASTAPP?

Objetivo de esta etapa:

Recuperar el control de la cuenta de WhatsApp de tu empresa después de un ataque o suplantación, sin perder la calma, los contactos ni la dignidad. Porque sí, el hacker puede quitarte el número, pero no tus buenos modales ni tus ganas de vender.

¿Cómo lo logro?

Primero, respira.y sigue el siguiente protocolo:

1. **Bloquea la SIM de inmediato.** Llama a tu operador (Claro, Tigo, Movistar, WOM) y pide que bloqueen la línea. Diles que te robaron el WhatsApp; ellos ya tienen un guion preparado.

2. **Pide un duplicado del número.** Cuando tengas la nueva SIM, reinstala WhatsApp y solicita el código de verificación.

3. **Ingresa el código que llega por SMS o llamada.** Eso desconectará automáticamente al intruso.

4. **Activa la verificación en dos pasos.** Esta vez, no la saltees. Elige un PIN y agrega un correo de recuperación.

5. **Aprovecha y cierra todas las sesiones activas.** En "Dispositivos vinculados" vas a ver si alguien anda curioseando tu WhatsApp Web desde otro país.

6. **Avisa a tus contactos.** Manda un mensaje breve: "Recuperamos el control. Si te pidieron plata, no era yo".

Si todo sale bien, en unos minutos vuelves a ser el dueño de tus stickers y tus clientes.

Riesgos:

- Que el atacante bloquee tu cuenta antes que tú.
- Que uses un correo inseguro o repetido para la verificación.
- Que tu operador tarde días en entregarte la nueva SIM (sucede más de lo que quisiéramos).
- Que te olvides del PIN y tengas que esperar una semana para recuperarlo.

Ventajas de tomar medidas apropiadas:

- Recuperas tu reputación digital y tus chats de negocio.
- Evitas que los delincuentes sigan suplantando tu empresa.
- Ganas confianza en tu equipo: todos aprenden del susto ajeno.
- Duermes mejor, sabiendo que el próximo ataque no te agarra desprevenido.

¿Por qué es importante?

Porque en muchas Mipymes, WhatsApp es la oficina, el mostrador y el servicio al cliente al mismo tiempo. Si alguien te roba la cuenta, no sólo te roba un número: se lleva tus cotizaciones, tus conversaciones y la confianza que tanto te costó construir. Y recuperar eso cuesta más que una SIM nueva.

Errores frecuentes:

- Reutilizar contraseñas o PINs como “123456”.
- Confiar en mensajes o llamadas que dicen ser del “soporte de WhatsApp”.
- No tener activada la verificación en dos pasos.
- Pensar que a uno “no le va a pasar”.
- Ignorar los avisos de inicio de sesión en otros dispositivos.

Ejercicio para superar la etapa:

- Entra ahora a WhatsApp → Ajustes → Privacidad → Verificación en dos pasos.
- Actívala y escribí el PIN en un gestor seguro o anótala en papel (sí, papel, ese invento del siglo XV).
- Verifica tus “Dispositivos vinculados” y cerrá los que no reconozcas.
- Crea un plan interno: ¿quién actúa si se pierde el acceso? ¿Quién avisa a los clientes?
- Finalmente, compartí con tu equipo esta frase para pegar junto al router:
  “En internet, el olvido no existe. Así que mejor prevenir que restaurar.”

CÓMO LEVANTARSE DESPUÉS DE UNA CAÍDA: CONTINUIDAD Y RECUPERACIÓN PARA MIPYMES

Objetivo de esta etapa:

Aprender que un incidente digital, técnico o natural no tiene por qué significar el fin de tu negocio. Tener un plan de continuidad y recuperación permite mantener operaciones críticas, reducir pérdidas y recuperar la confianza de clientes y aliados rápidamente. Según IDC, "solo el 30% de las MiPYMES cuenta con un plan de continuidad. De ellas, el 80% sobrevivió a eventos críticos."

¿Cómo lo logro?

1. **Entender la continuidad del negocio (BCP)**

- Capacidad de mantener o reanudar operaciones críticas tras un ciberataque, falla técnica, desastre natural o error humano.
- Elementos del plan:
  - Identificación de procesos críticos (facturación, atención al cliente, inventario).
  - Evaluación de riesgos (amenazas que podrían detener la operación).
  - Plan de acción (cómo responder y quiénes son responsables).
  - Comunicación de crisis (informar sin generar pánico).
  - Recuperación (procedimientos para volver a la normalidad).

2. **Plan de Recuperación ante Desastres (DRP)**

- Documento técnico para restaurar sistemas informáticos y datos tras un evento grave.
- Incluye respaldos, infraestructura alterna, procedimientos técnicos y tiempos de recuperación (RTO y RPO).

- Diferencia con BCP:
    - BCP: abarca toda la empresa para que el negocio no se detenga.
    - DRP: se centra en los sistemas tecnológicos que soportan las operaciones.

3. **Gestión de crisis**

- Requiere liderazgo, comunicación clara y decisiones rápidas.
- Mantiene la reputación, la confianza del cliente y la coordinación del equipo.

4. **Buenas prácticas internacionales**

- Requiere liderazgo, comunicación clara y decisiones rápidas.
- Mantiene la reputación, la confianza del cliente y la coordinación del equipo.

5. **Tips para MiPYMES**

- Identifica procesos vitales (facturación, atención al cliente, inventario).
- Mantén copias de seguridad fuera de línea o en la nube.
- Define roles de emergencia (quién comunica, quién ejecuta, quién documenta).
- Realiza simulacros de crisis al menos una vez al año.
- Documenta lecciones aprendidas tras cada incidente.

Riesgos:

- Pérdida total de información y continuidad del negocio.
- Impacto financiero y legal.
- Deterioro de la confianza de clientes y aliados.
- Dependencia de soluciones improvisadas.

Ventajas de tomar medidas apropiadas:

- Mantener operaciones críticas funcionando pese a incidentes.
- Recuperar la confianza de clientes y aliados.
- Reducir pérdidas económicas y legales.
- Demostrar profesionalismo y resiliencia ante cualquier eventualidad.

¿Por qué es importante?

Un plan de continuidad no es un lujo, es una inversión estratégica. Permite responder sin pánico, recuperar operaciones rápidamente y demostrar resiliencia ante clientes y aliados. Las MiPYMES que planifican su “Plan B” hoy serán las que sigan operando mañana.

Errores frecuentes:

- No identificar procesos críticos ni roles de emergencia.
- Confiar únicamente en copias de seguridad locales sin respaldo en nube.
- No realizar simulacros ni documentar lecciones aprendidas.
- Confundir BCP con DRP y no cubrir todos los aspectos de la empresa.
- Dejar la gestión de crisis solo en manos de un individuo sin coordinación.

Ejercicio para superar la etapa:

Escenario práctico: Tu empresa enfrenta un ataque de ransomware, caída del sistema contable o robo de equipos/datos de clientes. Responde:

1. ¿Qué áreas se verían más afectadas?
2. ¿Qué acciones inmediatas tomarías?
3. ¿Cómo continuarías operando las funciones críticas?
4. ¿Qué deberías comunicar y a quién?

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Camilo trabaja en una Mipyme digital y siempre va contra el reloj. Un correo falso le roba diez millones de pesos de la cuenta de la empresa. El susto es grande y, apurado, hace la denuncia virtual sin adjuntar pruebas ni guardar el número de radicado. Resultado: la denuncia no sirve para nada.

La empresa no lo regaña. En lugar de eso, organiza un taller exprés sobre cómo usar la plataforma **A Denunciar**, qué pruebas subir y por qué es crucial guardar el radicado oficial. Todo explicado de forma simple, para que nadie pierda tiempo ni datos valiosos.

Camilo aprende rápido y ahora lidera al equipo que acompaña a empleados y clientes en incidentes digitales. Su error se convierte en ejemplo: la capacitación evita que otros tropiecen con lo mismo.

Denunciar sin pruebas ni radicado es como gritar en el vacío. Usar la plataforma oficial, respaldar la información y seguir un procedimiento claro es lo que realmente protege a tu empresa.

Herramientas de ciberseguridad :

La ciberseguridad ya no es solo cosa de grandes empresas. Hoy, cualquier Mipyme —desde una panadería hasta una firma contable— puede ser blanco de ataques digitales. Por eso, es clave contar con herramientas que te ayuden a proteger tu información, tus equipos y tus transacciones.

A continuación, te presentamos una serie de herramientas prácticas, muchas de ellas gratuitas o de bajo costo, organizadas por etapas clave de protección. Desde cómo crear contraseñas seguras hasta cómo mantener tus equipos en buen estado, estas soluciones están pensadas para que puedas aplicarlas sin ser experto en tecnología.

Lo importante no es saberlo todo, sino dar el primer paso. Porque cuidar tu negocio también significa cuidar lo digital

#Etapa	Herramientas	¿Para qué sirve?
1. Contraseñas	HaveIBeenPwned, Bitwarden, Authy	Para crear, guardar y proteger claves seguras.
2. Copia de seguridad	Duplicati, Cobian Backup, Google Takeout	Para recuperar tu información si se borra o se daña.
3. Control de Accesos	OpenLDAP, FreeIPA, IAM de Google	Para decidir quién entra y qué puede hacer en el sistema.
4. Capacitación en Seguridad de la Información	CyberEdu, Gophish, Infosec IQ (free limitada)	Para que el equipo aprenda a evitar riesgos digitales.
5. Protección de datos	RedGDPR, LDPDTool	Para cumplir con normas y cuidar la información sensible.
6. Mantenimiento de equipos	HWMonitor, CCleaner (uso responsable), LibreHardwareMonitor	Para mantener computadores rápidos y seguros.
7. Billeteras digitales	Nequi, Daviplata, Tpaga, MercadoPago	Para recibir y hacer pagos seguros en línea.
8. Antivirus	Windows Defender, Avast Free, Bitdefender Free	Para detectar y bloquear virus y programas peligrosos.

#Etapa	Herramientas	¿Para qué sirve?
9. Software de MiPYMES	LibreOffice, Zoho Invoice, Bitrix24	Para trabajar de forma organizada y productiva.
10 . Red WiFi	Fing, WiFi Analyzer, RouterCheck	Para revisar y proteger la conexión a internet
11. Seguridad de la web	Mozilla Observatory, Sucuri Scanner, SSL Labs	Para comprobar si tu página web es segura.
12. IA	Poe, Notion AI, Microsoft Copilot (en pruebas), Canva AI	Para apoyar tareas con inteligencia artificial.
13. Ciberacoso a mujeres	Línea 155, PantallasAmigas, Recursos ONU Mujeres	Para denunciar y recibir apoyo en casos de acoso digital.
14. Denuncias	ColCERT, Centro Cibernético Policial, SIC	Para reportar fraudes, suplantación o mal uso de datos.
15. Plan de Continuidad de negocio	Open-AudIT, LibrePlan	Para que tu empresa siga funcionando después de un ataque.

REFERENCIAS

Banco Interamericano de Desarrollo. (2025). Microcurso sobre ciberseguridad para MIPYMES [Curso en línea]. Banco Interamericano de Desarrollo. https://cursos.iadb.org/es/temas/desarrollo-instituciones/microcurso-ciberseguridad-para-mipymes

Cámara Colombiana de Informática y Telecomunicaciones (CCIT). (2019). Identificación de riesgos y priorización en ciberseguridad empresarial.

Certify Web Content. (2023). A screenshot has no legal value, you have to certify the content. https://www.certifywebcontent.com/es/a-screenshot-has-no-legal-value-you-have-to-certify-the-content/
Defelipe Díaz. (2024). Ciberseguridad para pymes en Colombia. Impacto TIC. https://impactotic.co/ciber-seguridad/ciberseguridad-para-pymes-de-colombia/

DocuSign. (2025). Importancia de la seguridad informática para pymes. https://www.docusign.com
Interempresas. (2023, mayo 15). El router: primera línea de defensa o una puerta de entrada ante un ciberataque. https://www.interempresas.net/TIC/Articulos/467608-El-router-primera-linea-de-defensa-o-una-puerta-de-entrada-ante-un-ciberataque.html

Kaspersky. (2024). Estadísticas sobre ataques cibernéticos en Colombia.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos. Diario Oficial No. 47.223, enero 5 de 2009.

REFERENCIAS

Ley 2502 de 2025. Por medio de la cual se tipifica la suplantación de identidad mediante el uso de inteligencia artificial.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2019). Política de seguridad digital en Colombia [Citado en CCIT, p. 7].

Proofpoint. (2023). Cybersecurity Awareness Kit [Recurso educativo]. Proofpoint.

Pymas. (2019). Datos sobre incidentes informáticos en Colombia.

Bancolombia & Davivienda. (s.f.). Manuales de seguridad digital [Recursos institucionales].

Entidades y recursos

Centro Cibernético de la Policía Nacional. (s.f.). Reportes sobre incidentes de fuga de información.

Centro Cibernético Policial (CCP) – DIJIN. (s.f.). Centro Cibernético Policial. https://caivirtual.policia.gov.co

ColCERT. (s.f.). Grupo de Respuesta a Emergencias Cibernéticas del Estado Colombiano. https://colcert.gov.co

Policía Nacional de Colombia. (s.f.). Plataforma A Denunciar. https://adenunciar.policia.gov.co

REFERENCIAS

Superintendencia Financiera de Colombia. (s.f.). Entidades e industrias supervisadas. https://www.superfinanciera.gov/publicaciones/61694/industrias-supervisadas https://www.superfinanciera.gov.co/publicaciones/10106240

Superintendencia de Industria y Comercio (SIC). (s.f.). Habeas Data: Protección de datos personales en Colombia. https://www.sic.gov.co/habeasdata

ONU Mujeres, PantallasAmigas & Línea 155. (s.f.). Recursos y líneas de apoyo para casos de ciberacoso.