RUTA CIBERSEGURA

NIVEL JUNIOR

En convenio con:

Global Gateway

UNIÓN EUROPEA

Cámara de Comercio de Barranquilla

Cámara de Comercio de Cali

Cámara de Comercio de Medellín 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: 978-958-688-559-1

La ciberseguridad también es un asunto tuyo

Tu negocio —sea una tienda, peluquería, verdulería o ferretería— es mucho más que un lugar de trabajo: es el esfuerzo de tu familia, tu fuente de ingresos y parte del motor que hace crecer a tu comunidad y al país.

Sabemos que cada día te levantas para darle un impulso más a ese proyecto que construiste con dedicación. Y también sabemos que los tiempos cambiaron: antes bastaba con cerrar la puerta y activar la alarma; ahora hay que cuidar también lo que pasa en tu celular, en tus cuentas bancarias y en los correos electrónicos que recibes.

Los riesgos digitales llegaron para quedarse: mensajes sospechosos, estafas en línea, aplicaciones inseguras, contraseñas que se filtran y delincuentes que ya no usan ganzúas, sino pantallas.

Por eso creamos esta ruta de la ciberseguridad: para acompañarte en el camino de proteger tu negocio en el mundo digital. Aquí encontrarás consejos sencillos, ejemplos prácticos y pasos claros para que la ciberseguridad no sea un dolor de cabeza, sino una herramienta que te ayude a seguir creciendo con confianza.

¿Qué encontrarás en esta caja de herramientas?... Primero que todo, historias. Pero no de gente lejana, no. Historias de personas como tú, insistentes, que tienen su negocio en el barrio, en el centro, en la esquina de siempre. Gente que también ha pasado sustos con correos raros, con mensajes que parecían de un banco, pero no eran, con llamadas sospechosas. Y que, gracias a una buena decisión a tiempo, lograron proteger su empresa.

También vas a encontrar definiciones sencillas. Nada de palabras enredadas ni tecnicismos de ingeniero. Acá todo está explicado de forma simple, para que lo entiendas sin necesidad de hacer un curso en Harvard.

Y lo más importante: vas a tener una ruta. Una guía paso a paso con actividades prácticas, amigables, sin complicaciones, que te van a dar herramientas y tips para blindar tu negocio. Porque sí, tu empresa también puede ser cibersegura, sin importar si vendes tintos, repuestos o cortas el pelo.

Adelante, comienza tu ruta cibersegura.

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.

¿Cuándo recoges datos de tus clientes, de qué eres responsable?: Ley 1581 de 2012 de protección de datos personales

Sabemos que tienes varias tareas pendientes, así que lo que no te vamos a quitar mucho tiempo.

Te vamos a contar en un dos por tres, cómo debes proteger los datos de tus clientes según la Ley 1581 de 2012 y lo más importante: **cómo hacerlo en la práctica.** Los datos son el corazón de tu negocio: nombres, correos, teléfonos, historiales de compra. Si caen en manos equivocadas, no solo se pierde dinero, también la confianza de tus clientes. **Por eso, la ciberseguridad no es solo un tema técnico, es una forma de cuidar la reputación de tu empresa y de cumplir con la Ley 1581 de 2012, que protege la información personal en Colombia.**

Garantizar la seguridad de la información

- **Qué hacer:** si tienes una base de datos en Excel, no la guardes en una memoria USB sin clave que anda rodando en el cajón con clips y galletas.
- **Cómo hacerlo:** ponle contraseña al archivo, activa el cifrado y guarda siempre copias seguras. Usa la nube solo si tiene medidas de seguridad.

Conservar prueba del consentimiento

- **Qué hacer:** si alguien aceptó recibir tus correos, guarda ese formulario físico o digital.
- **Cómo hacerlo:** diseña un formulario de prueba con estos mínimos: nombre completo, número de identificación, correo o celular, fecha y casilla de aceptación ("Acepto que mis datos sean usados para..."). Guarda siempre copia digital o física firmada.

Informar sobre el uso de los datos

- **Qué hacer:** si recoges teléfonos para confirmar pedidos, dilo claro desde el inicio.
- **Cómo hacerlo:** incluye una breve nota en el formulario o en el contrato: "Estos datos se usarán únicamente para confirmar pedidos y enviar información sobre promociones de la tienda".

Responder reclamos y garantizar derechos

- **Qué hacer:** si un cliente llama y dice "quiero ver qué datos míos tiene", debes mostrarlos.
- **Cómo hacerlo:** ten un registro organizado (Excel, cuaderno o software) donde quede fácil buscar los datos. Define quién en tu negocio atenderá estas solicitudes y en cuánto tiempo.

Piensa que los datos son como la bicicleta que el vecino te deja en la casa porque se va de viaje:

- No es tuya.
- Tienes que cuidarla.
- Y si el vecino vuelve y dice "dámela ya", se la devuelves sin chistar.

Historias de ciberseguridad

La contabilidad de Don Álvaro

Don Álvaro tiene una pequeña papelería en un barrio de Medellín. Atiende solo con su esposa y usa un computador viejo para llevar las facturas, enviar correos a clientes y descargar formatos para colegios. Como el negocio creció un poco, decidió abrir una cuenta de correo electrónico para recibir pedidos y adjuntos.

Una tarde, recibió un correo con el asunto: “Cotización urgente – colegios 2025”. Sin sospechar nada, hizo clic en el archivo adjunto, pensando que era una oportunidad de ventas. El archivo venía con un **virus tipo ransomware** (software malicioso que secuestra la información y pide rescate por ella) que bloqueó todos sus archivos. Al día siguiente, no pudo abrir Excel, Word ni las facturas. Todo estaba encriptado y un mensaje le pedía pagar en bitcoins para recuperar la información.

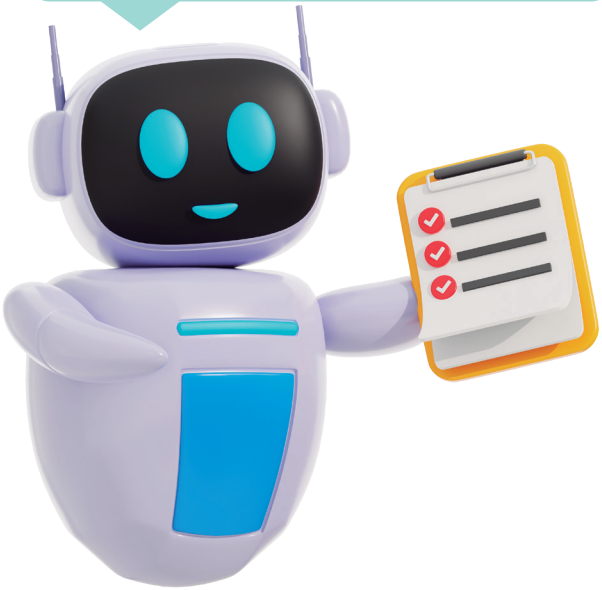
Don Álvaro no tenía copias de seguridad, ni antivirus actualizado. Tampoco sabía a quién acudir. Perdió el historial de pedidos, las facturas del año y varios documentos importantes. Durante una semana no pudo operar, tuvo que rehacer cuentas manualmente y perdió credibilidad con algunos clientes.

Afectaciones:

- **Tecnológicas:** pérdida total de archivos del equipo principal.
- **Operativas:** interrupción del servicio por 7 días y aumento en errores manuales.
- **Financieras:** pérdida de clientes y tiempo dedicado a reconstruir datos.
- **Emocionales:** frustración, angustia y desconfianza para volver a usar el computador.

LECCION APRENDIDA

Con solo haber tenido un antivirus actualizado, copias de seguridad funcionales en una USB, y algo de capacitación básica, este incidente se pudo evitar. La ciberseguridad también es para los negocios más pequeños.



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.**

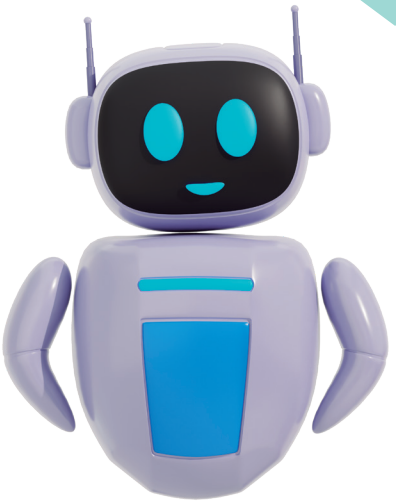
PREVENIR

Imagínate que estás por salir a dar una vuelta en bici. Pero, antes de pedalear, ¿qué haces? Te fijas si la cadena está bien, si las ruedas tienen aire, si el freno no te va a dejar en la bajada. Nadie en su sano juicio se tira a la calle sin revisar eso, ¿no?

Con la ciberseguridad pasa lo mismo. Antes de avanzar en esta ruta, hay que prevenir: ajustar el casco, revisar las llantas y asegurarse de que no se nos va a desarmar la bici en plena pedaleada. Y ojo, que no importa si tu empresa es una tienda de barrio o una Mipyme que ya tiene dos sucursales y un logo muy posicionado: lo que importa es que tu negocio es prioritario para ti. Así que hay que cuidarlo.

Acá vas a aprender lo básico para arrancar con buena velocidad: cómo armar contraseñas que no se rompan al primer tropiezo, cómo guardar una copia de tus cosas importantes por si alguien husmea donde no debe, y cómo limitar el acceso para que tu información no sea un parque de diversiones al que cualquiera entra sin pagar entrada.

La prevención es el primer pedaleo en esta ruta cibersegura. Y como toda buena salida en bici, no importa lo rápido que vayas: lo importante es que empieces con los frenos ajustados y las ruedas infladas. Después, el viaje se disfruta mucho más.



DISEÑA UNA CONTRASEÑA SEGURA

¿Cuál es el objetivo de esta etapa?

Que tu clave no sea tan débil como un candado de bicicleta en el centro de Bogotá. Vamos a aprender a inventar contraseñas que no se adivinan ni con bola de cristal.

¿Cómo lo logro?:

Usa iniciales de la estrofa de una canción

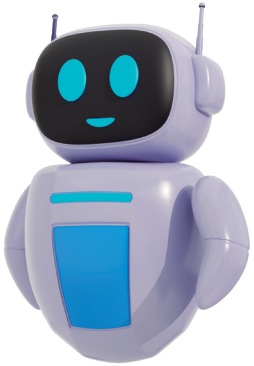
- En “Sol solecito caliéntame un poquito”, usas sscup por ejemplo.
- Usa sílabas combinadas de 3 clases de frutas, objetos, colores.
- En “piña limón lulo”, usas pililu, por ejemplo: Combina esto con números y signos Sscup234* o p1l1l9$, por ejemplo

Bonus track: Use herramientas que sí saben guardar secretos

Porque no basta con tener una buena contraseña. Hay que guardarla como si fuera la fórmula de la Coca-Cola. Para eso existen herramientas que son como cajas fuertes digitales:

Herramienta	¿Qué hace?
Bitwarden	Guarda tus contraseñas encriptadas y sincronizadas entre dispositivos.
KeePass	Funciona sin conexión, ideal si no confías ni en el WiFi del café.
1Password	Tiene interfaz amigable y hasta te avisa si tu clave fue filtrada.

Estas herramientas no solo almacenan contraseñas, también pueden generar unas que ni tú mismo podrías inventar. Pero tranquilo, ellas se encargan de recordarlas por ti.



Riesgos:

- Tus cuentas bancarias respiran tranquilas.
- Tu información personal deja de ser un chisme público.
- Nadie la adivina: ni el hacker, ni el cuñado, ni tú cuando estás medio dormido.

Ventajas de tomar medidas apropiadas:

- Tus cuentas bancarias respiran tranquilas.
- Tu información personal deja de ser un chisme público.
- Nadie la adivina: ni el hacker, ni el cuñado, ni tú cuando estás medio dormido.

¿Por qué es importante?

ERC Colombia. (2025). Las pymes en Colombia son las más expuestas a ciberataques debido a la falta de infraestructura, talento y formación especializada, con vulnerabilidades asociadas al factor humano y configuraciones inseguras. Reportes recientes indican que aproximadamente 7 de cada 10 pymes en Colombia han sido víctimas de ataques cibernéticos, atribuido a la falta de cultura de seguridad y la creencia errónea sobre costos de inversión en seguridad.

Errores frecuentes:

- Creer que “admin–admin” es gracioso.
- Pensar que “123456” es ingenioso.
- Apuntar la clave en un papelito y pegarla en la pantalla.
- Darla por teléfono porque “el banco” la pidió. No, señor. El banco nunca llama a pedir claves.

Ejercicio para superar la etapa:

Haz de cuenta que tu negocio es una casa con varias puertas: la del correo, la de la banca en línea, la de las redes sociales. Ahora imagina que todas esas puertas las cerraste con el mismo candado barato que se abre con un clip. ¿Te sientes seguro? Claro que no.

Entonces, manos a la obra:

1. Toma lápiz y papel (o el celular, si es más moderno) y haz una lista de todas las llaves que tiene tu empresa: correo, banco, redes.

2. Bota la basura las llaves viejas que son pura chatarra (123456, el nombre de su perro, la fecha de cumpleaños).

3. Fabrica llaves nuevas con el truco del sancocho: iniciales de una canción, sílabas mezcladas de frutas, un par de números, un símbolo raro. Ejemplo: QuBoCeMa!27 (Quiero–Borrador–Celular–Manzana + un signo y dos números).

4. Como nadie se aprende de memoria veinte llaves distintas (ni Einstein), instal a un gestor de contraseñas gratuito, tipo Keepass, aplicación que hace un inventario de todas tus claves para organizarlas mejor. Piensa en él como una caja fuerte digital donde guardas todas esas llaves nuevas.

La meta es simple: cuando un ladrón digital intente abrir tus puertas, se estrella contra un muro. Y tú, en cambio, puedes entrar con un solo clic, sin sudar ni inventar cuentos.

HAZ COPIA DE SEGURIDAD DE TU INFORMACIÓN

Objetivo de esta etapa

Un día, la computadora de Don Ramiro —dueño de una papelería de barrio— amaneció con la pantalla azul y un pitido que sonaba como alarma de incendio. Ahí estaban: las facturas, los pedidos, los correos de clientes... todo muerto. Su hijo le dijo:

—¿Y la copia de seguridad, papá?

Y Ramiro, con esa cara que uno pone cuando se da cuenta de que nunca guardó nada, se quedó en silencio.

Evitar que su negocio quede como Ramiro: con la caja vacía y la memoria del computador más limpia que el alma de un santo.

¿Cómo lo logro?:

1. **Automatiza las copias de seguridad**
   - **Descarga una aplicación gratuita** como **Cobian Backup** o activa la opción de copia automática en tu sistema (Windows o Mac).
   - **Programa la frecuencia: lo ideal es diaria** si manejas pedidos, facturas o inventarios todos los días.
   - **Elige qué carpetas quieres respaldar:** por ejemplo, “Facturas”, “Clientes”, “Proveedores”.
2. **Guarda la copia en distintos sitios**
   - **USB o disco externo:** conecta el dispositivo y deja que el programa guarde ahí la copia.

- **La nube:** usa servicios como Google Drive, OneDrive o Dropbox. Esto te protege en caso de que el computador se dañe o te roben el equipo.

- **Consejo:** nunca guardes la única copia en el mismo computador donde está la información original.

3. Verifica que las copias realmente funcionen

- Una vez al mes, toma un archivo de la copia y **haz la restauración de prueba.**

- Abre el archivo recuperado y revisa que esté completo (por ejemplo, que un Excel no esté vacío o dañado).

- Así evitarás descubrir en medio de un problema que tu copia estaba incompleta o corrupta.

4. Crea un hábito sencillo

- Define un día fijo **para revisar tus copias** (ejemplo: el primer lunes de cada mes).

- Si delegas esta tarea a alguien de tu equipo, asegúrate de que **sepa cómo verificar la restauración.**

Riesgos:

- Perder en un segundo todo lo que levantaste en años, como si alguien entrara a tu negocio, barriera con la escoba el mostrador, y se llevara hasta la campanita de la puerta.

- Quedarte en blanco: sin facturas, sin inventario, sin clientes. Como abrir la persiana a la mañana y descubrir que el local ahora vende aire. Y después, lo peor: pagar una fortuna en “recuperación de datos”, más de lo que te costaría empezar otra empresa desde cero, con logo nuevo y todo.

Ventajas de tomar medidas apropiadas:

- El negocio sigue andando aunque se muera un computador.
- Duermes tranquilo, sin pesadillas de pantallas azules.
- Cumples con normas que, créelo o no, también exigen estas precauciones.

¿Por qué es importante?

Seis de cada diez empresas que pierden sus datos no alcanzan a soplar la velita del medio año: cierran antes. **Lo dice Boston Computing Network (s. f., https://www.bostoncomputing.net)**, pero uno no necesita un estudio para entenderlo. Un negocio sin memoria es como un carnicero sin cuchillos: no dura ni seis meses abierto.

Errores frecuentes:

- Confiar en “yo hago la copia manual cada tanto” (y ese tanto nunca llega).

- No probar si las copias realmente funcionan.

- Guardar solo una versión y en el mismo sitio: si se quema la oficina, adiós copias también.

Ejercicio para superar la etapa:

Piensa en la carpeta más valiosa de tu negocio: facturas, contratos, inventarios, todo lo que si se pierde te deja mudo frente a un cliente. Esa carpeta será la elegida.

1. **Elige la carpeta vital.** No vale “luego miro cuál”. Decide hoy mismo.

2. **Programa una copia automática semanal.** Puede ser en una memoria USB, en un disco externo o en la nube (Google Drive, OneDrive, el que prefiera).

3. **Haz la prueba.** Abre la copia y revisa que los archivos de verdad estén ahí, no solo la carpetica con nombre elegante pero vacía como nevera de estudiante.

Así, cuando tu computador decida morirse de repente, podrás seguir trabajando como si nada hubiera pasado.

CADA QUIEN CON LO SUYO

Objetivo de esta etapa:

En la ferretería de Don Jorge todos tenían llave de la caja registradora: el sobrino, el vecino que ayudaba a barrer, incluso un cliente que pasaba tanto tiempo ahí que ya parecía socio. Un día, el cajón apareció vacío y nadie sabía quién había metido la mano. Don Jorge juraba que era un fantasma, pero la verdad era más simple, cuando todo el mundo tiene acceso a todo, es imposible saber quién hizo qué.

Evitar que tu negocio sea como la ferretería de Don Jorge, un lugar donde cualquiera entra a cualquier parte. La regla es simple, cada quien con lo suyo.

¿Cómo lo logro?

- Define perfiles de usuario: el que factura no tiene por qué ver las nóminas, y el de nómina no necesita entrar a las bases de clientes.
- Usa autenticación fuerte (contraseñas seguras, doble factor)
- Revisa de vez en cuando quién tiene acceso a qué, porque lo que sobra de permisos, también sobra de riesgos

Bonus Track

Con **JumpCloud**, puedes crear perfiles específicos para cada rol:

- Accede al portal de administración de JumpCloud.
- Crea grupos de usuarios: “Ventas”, “Contabilidad”, “Logística”.
- Asigna permisos por grupo: por ejemplo, el grupo “Ventas” solo puede acceder a la carpeta de clientes y facturación.
- Si usas sistemas como Google Workspace o Microsoft 365, JumpCloud se integra y sincroniza los accesos automáticamente

Riesgos:

- Robo interno (que a veces duele más que el externo).
- Filtraciones de información confidencial.
- Accesos indebidos que dejan al negocio en calzoncillos frente a un competidor.

Ventajas de tomar medidas apropiadas:

- Los datos sensibles quedan bajo llave.
- Puedes rastrear quién hizo qué y cuándo.
- Cumples con normas que, aunque aburridas, te protegen.

¿Por qué es importante?

Solo el 27% de las Mipymes revisa quién entra y sale de sus sistemas, lo que significa que en siete de cada diez negocios digitales **cualquier persona podría estar accediendo sin control,** desde un mensajero o un exempleado hasta un desconocido que aparenta ser un invitado. Esta falta de supervisión en el acceso a los sistemas puede derivar en pérdidas graves que solo se descubren cuando “la caja aparece vacía” (Sophos, s. f.).y la creencia errónea sobre costos de inversión en seguridad.

Errores frecuentes:

- Dar acceso ilimitado “para no complicarse”, como si todos los empleados necesitaran la llave maestra de la bóveda.
- Olvidar quitar accesos a ex empleados: lo mismo que dejarle la llave de la casa al ex... y confiar en que nunca se le ocurra pasar por ahí.

Ejercicio para superar la etapa:

En la panadería de Doña Gloria todos tenían la llave del cuarto de la harina. Un día faltó harina. Misterio. Desde entonces, Doña Gloria hizo algo sencillo: cada quien con su llave y solo de su puerta. Hagamos lo mismo con tu negocio

Lo que vas a hacer (15–20 min)

1. Lista rápida de puertas. Escribe los sistemas y carpetas críticas: *Facturación, Clientes/CRM, Inventario, Nómina, Bancos, Drive/OneDrive "Administración"*.

2. Quién entra hoy. Al lado de cada puerta, anota nombres o cargos que hoy tienen acceso.

3. Necesidad real. Revisa uno por uno y pregúntate: *¿este rol necesita ver/editar esto para trabajar?*

4. Quitar sobrantes. Si la respuesta es no, revoca o reduce el permiso (de "editar" a "solo lectura", o "sin acceso").

5. Refuerzo. Activa doble factor a quienes se quedan con acceso y guarda un registro de cambios.

1. Mínimo privilegio

- **Cómo se hace:** en la mayoría de herramientas (la nube, el correo empresarial, un software de inventario) puedes elegir si un usuario tiene solo lectura, edición o administrador.

- **Ejemplo práctico:** en Google Drive o OneDrive, al compartir un archivo, selecciona “lector” si solo necesita consultar, “editor” si debe modificar, y deja el rol de administrador solo a 1 o 2 personas de máxima confianza.

2. Doble factor activado (2FA)

- **Cómo se hace:** activa la verificación en dos pasos en todos los servicios críticos (correo, bancos, nube).

- **Ejemplo práctico:** imagina que tu contraseña es la llave de la puerta de tu oficina. La verificación en dos pasos es como tener además un candado que solo se abre con un código que llega a tu celular. Así, aunque alguien copie tu llave, no podrá entrar sin ese segundo seguro.

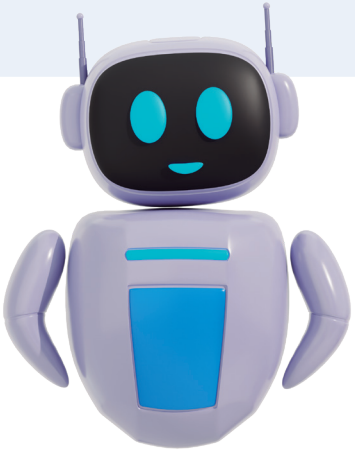
3. Salida limpia

- **Cómo se hace:** cada vez que alguien sale de la empresa (empleado, practicante, proveedor), ese mismo día se debe desactivar su usuario en las plataformas.

- **Ejemplo práctico:** si usaba la cuenta de la nube, elimínala o quítale el acceso. Si compartía contraseñas (Wi-Fi, correo, software de facturación), cámbialas de inmediato.

Checklist de cierre (√ marca)

- ☐ Tengo la lista de puertas críticas.
- ☐ Cada puerta tiene dueños claros.
- ☐ Quité accesos sobrantes y documenté cambios.
- ☐ Activé 2FA en cuentas críticas.
- ☐ Agendé revisión mensual de accesos (pon una alerta en el calendario).

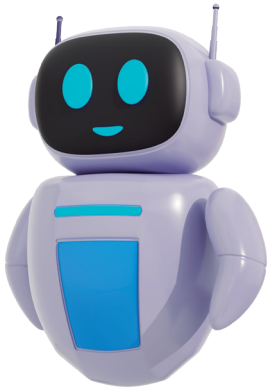


CAPACITAR Y SENSIBILIZAR

Objetivo de esta etapa:

En la empresa de Doña Marta todos creían que la ciberseguridad era “cosa de ingenieros”. Hasta que un empleado abrió un correo que decía: “Ganaste un viaje a Cancún, haz clic aquí”. Tres segundos después, la pantalla quedó negra y el sistema pidió rescate en bitcoins. Ahí entendieron que no basta con tener antivirus: el verdadero cortafuegos está entre la silla y el teclado, o sea, la gente.

El objetivo de esta etapa es que cada empleado entienda que no es un espectador, sino parte del equipo de seguridad.



¿Cómo lo logro?

- Haz capacitaciones cada seis meses (no cada seis años). Usa medios divertidos, didácticos y con alta recordación, como juegos, videos, concursos, que tengan de ser posible, una medición de aprendizaje (ej: kahoot).
- Usa ejemplos prácticos y cercanos: correos falsos, llamadas sospechosas, claves fáciles.
- Mide si la gente aprendió o solo aplaudió al final.

Riesgos:

- Errores humanos que abren la puerta al atacante.
- Suplantación de identidad dentro y fuera del negocio.
- Malware instalado porque alguien “no sabía qué era un adjunto raro”.

Ventajas de tomar medidas apropiadas:

- Menos incidentes y menos sustos.
- Una cultura de seguridad que se respira en la oficina.
- Empleados que se vuelven vigías: detectan lo raro y lo avisan.

¿Por qué es importante?

El 88 % de las brechas de seguridad actuales se deben a errores humanos, según el informe The Psychology of Human Error elaborado por Tessian en colaboración con Jeff Hancock de la Universidad de Stanford (Tessian, 2022). En otras palabras: casi nueve de cada diez incidentes no nacen en un sofisticado ataque externo, sino en algo tan cotidiano como un clic apresurado, una contraseña compartida o un archivo abierto sin pensar. **La lección es clara: la seguridad empieza en los hábitos diarios de la oficina, más que en la nube o en el hacker del otro lado del mundo.**

Errores frecuentes:

- Hacer una capacitación al año y creer que con eso es suficiente.
- Hablar en idioma marciano: phishing, malware, ransomware sin traducir a la vida real.
- No medir impacto: dar la charla y nunca comprobar si alguien aprendió algo.

Ejercicio para superar la etapa:

Arma una trivia relámpago de 5 preguntas en Google Forms sobre buenas prácticas digitales.

Pregunta cosas sencillas, del día a día, como:

- ¿Qué harías si recibes un correo con un enlace sospechoso?
- ¿Compartirías tu contraseña si te la pide un compañero por chat?

Envía el link a los empleados y deja que jueguen con él. Después, reúne al equipo cinco minutos y revela las respuestas correctas como si fueran trucos de magia: sin regaños, sin jerga técnica, rápido y divertido.

La idea es que la seguridad deje de sonar a sermón y se convierta en parte de la rutina. Porque cuando todos saben desconfiar de un “viaje gratis a Cancún”, el negocio respira tranquilo.

LA JOYA DE LA CORONA: INFORMACIÓN DE CLIENTES, EMPLEADOS Y ALIADOS

Objetivo de esta etapa:

Si tienes una Mipyme en Colombia, sabes que hay algo más valioso que las máquinas, la bodega o hasta el local donde trabajas: la información. Sí, esa lista de clientes que te compran cada mes, los datos de tus empleados y los contactos de tus aliados. Esa es la verdadera joya de la corona. Y como toda joya, si la dejas tirada en cualquier cajón, tarde o temprano alguien se la roba.

La misión es simple: proteger la información personal de clientes, empleados y aliados. Piensa que esos datos no son tuyos, son prestados. Y como buen anfitrión, hay que cuidarlos.

¿Cómo lo logro?

No hace falta un ejército de ingenieros. Empieza por lo básico:

- Clasifica los datos. ¿Cuál es sensible? (ej. orientación sexual, datos de historia clínica) ¿Cuál es público? (ej. número de cédula, nombre).
- Permite el uso de las cuentas solo por quien es el dueño,

Tipo de dato	Descripción	Ejemplos	Protección especial
Datos personales públicos	Son los que la ley o la Constitución determinan como públicos, o que no son de carácter privado o semiprivado.	Nombre, número de cédula, estado civil, profesión u oficio, información contenida en registros públicos.	No requieren autorización para su tratamiento, pero sí deben usarse conforme a la ley.
Datos personales privados	Son aquellos que solo interesan al titular y cuyo uso está restringido	Dirección de residencia, número de teléfono personal, información financiera básica.	Requieren autorización del titular para su tratamiento.
Datos personales sensibles	Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación.	Orientación sexual, datos de historia clínica, ideología política, huella dactilar, origen étnico.	La ley prohíbe su tratamiento salvo en casos excepcionales (consentimiento explícito, fines médicos, interés público).
Datos semiprivados	No son íntimos, pero tampoco son públicos; su conocimiento puede interesar a ciertos sectores o grupos.	Información financiera, datos de crédito, comportamiento comercial.	Su tratamiento requiere autorización y tiene restricciones específicas.

Riesgos:

Si no cuidas esta joya, prepárate para el desfile de desgracias: sanciones legales, pérdida de confianza y ataques de ransomware que te pueden dejar en ceros. Y créeme, en este negocio de la confianza, una sola filtración hace más daño que mil chismes.

Ventajas de tomar medidas apropiadas:

La otra cara es más alegre:

- Cumples con la ley.
- Ganas ventaja competitiva (porque un cliente prefiere a quien lo cuida).
- Y duermes más tranquilo reduciendo riesgos.

¿Por qué es importante?

Según el Consumer Privacy Survey de Cisco (s. f.), el 67 % de los consumidores dejaría de tratar con una empresa que no protege sus datos.

Errores frecuentes:

- Los tropiezos son casi de cajón: no saber qué datos se manejan y no informar al titular. Es como pedirle a alguien las llaves de su casa y no contarle para qué.

Ejercicio para superar la etapa:

Hoy no hay excusas: haz este pequeño ejercicio en su empresa. No necesitas ingenieros, solo quince minutos y algo de sentido común.

1. **Toma un cuaderno o abre un excel.** Escribe los datos personales que tu empresa suele pedir o guardar. Ejemplo: cédula, EPS, teléfono, dirección, correo electrónico. Nada de adornos, solo la lista cruda.

2. **Guarda esa lista bajo llave.** Si lo hiciste en Excel, ponle contraseña al archivo. Ojo: no uses “1234” ni “contraseña”. Piensa una clave que solo tú recordarás (como el apodo que le tenía su abuela o el nombre de su primer perro, con números y símbolos mezclados).

3. **Elige a quién le das copia de la llave.** Pregúntate: ¿quién necesita de verdad ver esa lista para hacer su trabajo? Si la respuesta es “nadie más que yo”, entonces nadie más la abre.

4. **Haz la prueba.** Intenta abrir el archivo desde el computador de un empleado al que no le diste la clave. Si no puedes, ¡felicitaciones! Ya protegiste tu primera joya de la corona.

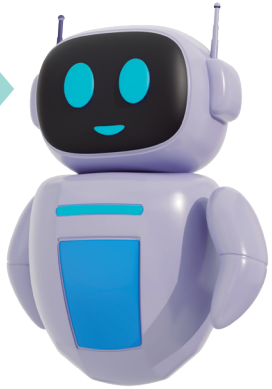
La idea no es que te conviertas en un hacker bueno de la noche a la mañana. La idea es que entiendas que proteger datos es como cuidar la receta de la abuela: no está enmarcada en la sala, sino guardada en un cajón que solo abre quien entra a la cocina.

YO CUIDO LO MÍO: PROLONGAR LA SEGURIDAD DE DISPOSITIVOS DE TRABAJO

Objetivo de esta etapa:

Prolongar la vida útil y la seguridad de los dispositivos de trabajo (computadores, celulares y tablets), porque nada peor que perder medio día esperando que el computador arranque o, peor, que un virus lo convierta en ladrillo.

¿Cómo lo logro?
No necesitas un doctorado en sistemas ni contratar al primo ingeniero. Basta con aplicar estas tres vitaminas mensuales que mantienen tus computadores sanos, rápidos y confiables:



Actualiza el software como quien se pone la vacuna a tiempo

Cada vez que el sistema te diga “hay una actualización disponible”, no lo ignores. Es como cuando el médico te dice “ya toca el refuerzo”.

¿Cómo hacerlo?

- En Windows: ve a Configuración → Actualización y seguridad → Buscar actualizaciones.
- En Mac: abre Preferencias del sistema → Actualización de software.
- Haz clic en “Actualizar” y deja que el sistema haga su trabajo.

Estas actualizaciones corrigen errores, cierran puertas a virus y hacen que todo funcione mejor.

Limpia el hardware como quien le pasa el trapo al mostrador

El polvo es enemigo silencioso. Se mete en los ventiladores, calienta el equipo y lo vuelve lento.

¿Cómo hacerlo?

- Usa aire comprimido (lo venden en tiendas de tecnología).
- Limpia pantallas con paños de microfibra y líquidos especiales.
- Si no te sientes seguro, contrata mantenimiento técnico cada 6 meses.

Un computador limpio dura más y falla menos. Es como tener el motor del carro sin mugre.

Revisa que todo funcione, como quien hace inventario cada tanto

No esperes a que el equipo se bloquee en plena factura. Haz chequeos preventivos.

¿Cuándo hacerlo?

- Haz un chequeo cada 6 meses o al menos una vez al año.
- Revisa que los programas abran bien, que el disco no esté lleno, que no haya errores raros.

Y para hacerlo fácil, usa herramientas que hacen el trabajo por ti:

Herramientas que ayudan sin complicarte la vida

Glary Utilities
Ideal para limpiar el sistema, borrar archivos innecesarios y acelerar el equipo.

¿Cómo instalarlo?

1. Ve al sitio oficial de Glary Utilities.
2. Haz clic en “Download Now”.
3. Abre el archivo descargado y sigue los pasos (clic en “Sí” cuando te lo pida).
4. Instala y abre el programa desde el escritorio.

¿Cómo usarlo?

- Haz clic en “Mantenimiento en 1 clic”.

- Marca las opciones que quieras (limpiar registro, eliminar archivos basura, etc.).

- Presiona “Buscar problemas” y luego “Reparar”.

Es como tener un técnico digital que hace limpieza profunda sin que tú muevas un dedo.

CCleaner
Otra opción confiable para limpiar el sistema y mejorar el rendimiento.

¿Cómo instalarlo?

- Descárgalo desde su sitio oficial.

- Instálalo como cualquier programa (siguiente, siguiente, instalar).

- Ábrelo y selecciona “Limpieza personalizada”.

¿Cómo usarlo?

- Marca lo que quieres borrar (archivos temporales, historial, etc.).

- Haz clic en “Analizar” y luego en “Ejecutar limpieza”.

Ambas herramientas son fáciles de usar y tienen versiones gratuitas que funcionan perfecto para Mipymes.

Riesgos:

Si los descuidas, prepara el bolsillo: fallas operativas, vulnerabilidades de seguridad y costos elevados por arreglos de última hora que pueden doblar el valor de tus equipos

Ventajas de tomar medidas apropiadas:

Un equipo que se cuida funciona como un carro bien aceitado: arranca rápido, no lo deja botado en la carretera y consume menos gasolina. Si actualizas y limpias tus dispositivos, ganas tres cosas al mismo tiempo:

- **Equipos funcionales.** No tienes que esperar cinco minutos mirando la pantalla negra del computador para que “coja”. Entra, trabaja y rinde.

-

- **Menos interrupciones.** Un antivirus actualizado evita que se meta un bicho que te saque de la reunión justo cuando ibas a cerrar un negocio.

- **Menos gastos.** Mantener un equipo cuesta centavos; arreglarlo después de un ataque o comprar uno nuevo cuesta millones.

¿Por qué es importante?

No es exageración: según el Verizon Data Breach Investigations Report (DBIR, s. f.), el 70 % de las fallas de seguridad en PYMEs está relacionado con software obsoleto. O sea, no es culpa de los hackers rusos ni de los extraterrestres: es simplemente que alguien apretó "recordar más tarde" en una actualización demasiadas veces.

Errores frecuentes:

- Ignorar alertas de actualización ("Lo hago mañana").
- Postergar mantenimientos hasta que el equipo colapse.
- Solo actuar después de la tragedia.

Ejercicio para superar la etapa:

Hoy la tarea es sencilla, casi como la lista del mercado, pero para tus equipos:

1. **Abre un Excel y crea un checklist** Pon cuatro filas con estos ítems:

    - Limpiar archivos temporales: en Windows, abre el menú inicio y escribe "Liberador de espacio en disco". Selecciona la unidad (generalmente C:), marca la casilla "Archivos temporales" y haz clic en Aceptar.
    - Revisar antivirus.
    - Actualizar sistema operativo.
    - Limpiar físicamente el equipo (teclado, pantalla, ventilador).

2. **Ponle fecha fija.** Una vez al mes, como quien paga los servicios o cambia el agua del florero
3. **Haz la ronda** Dedica media hora a repasar la lista en cada dispositivo de la empresa.
4. **Marca con √ o hecho.** Es casi terapéutico ver cómo la hoja se llena de chulos.

Así, sin darte cuenta tus equipos empiezan a durar más y a fallar menos. Y lo mejor: dejas de sentir que el computador es un adolescente caprichoso que se bloquea cuando quiere. En realidad, es un adulto agradecido... siempre y cuando lo bañes, lo alimentes y lo dejes dormir tranquilo.

BILLETERAS DIGITALES SEGURAS

Objetivo de esta etapa:

Hoy los ladrones ya no esperan en la esquina con una navaja. Esperan en su celular, disfrazados de app bonita o de mensajito sospechoso. Y si tú manejas plata en Nequi, Daviplata o cualquier billetera digital, la billetera ya no está en el bolsillo: está en la nube. Protegerla es, entonces, como andar con la mano siempre sobre el bolsillo, pero versión digital.

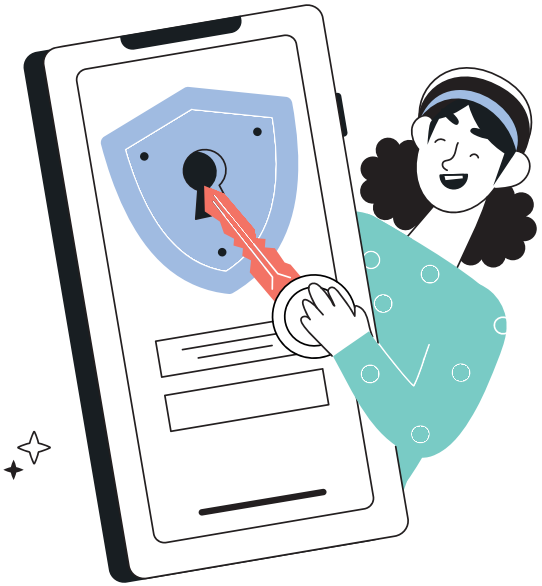
La meta es clara: proteger el uso de aplicaciones y plataformas para pagos digitales. Porque si se cuida la caja registradora física, ¿por qué no haría lo mismo con la virtual?

¿Cómo lo logro?

- **Activa la autenticación en dos pasos:** Sí, ese trámite molesto que siempre pensamos “mañana lo hago”. Ese segundo código, la huella, el token que vibra o la cara frente a la cámara parecen exageraciones, pero son como la **doble vuelta de llave** cuando uno vive en barrio bravo: lo que realmente salva la casa digital. La contraseña sola ya no alcanza; hoy cualquiera la adivina, o peor, la compra barata en internet. Por eso, activa ese segundo seguro en tus servicios críticos. **Cómo se hace en Nequi:** Abre la app de Nequi en tu celular. Ve a **Ajustes > Seguridad**. Selecciona **Autenticación en dos pasos.** Activa la opción y confirma con tu **PIN Nequi**. Cada vez que intentes entrar desde un dispositivo nuevo, además de la clave, te pedirá un código de verificación.

- **Usa solo aplicaciones oficiales:** nada de esas versiones “lite” que un primo manda por WhatsApp, con un icono medio chueco y promesa de gastar menos datos. Esas apps son como comprar whisky en la licorería de la esquina sabiendo que la tapa está floja: barato, sí, pero al otro día uno termina en el hospital. Descarga siempre desde Google Play o Apple Store.

- **Monitorea tus movimientos.** mira el extracto de la cuenta como quien revisa que la caja no tenga un billete falso. Esos dos minutos al día, chequeando que no haya compras en Uzbekistán o recargas de celular que tú no hiciste, valen oro. Detectar raro a tiempo es la diferencia entre un susto controlado y un agujero en la caja.



Riesgos:

Si te descuidas, los resultados son rápidos y preocupantes: fraudes, robo de dinero y, peor aún, la pérdida de confianza de los clientes. Porque si la gente sospecha que contigo se pierde plata, ahí sí no te salva ni el mejor producto.

Ventajas de tomar medidas apropiadas:

- **Seguridad en las transacciones.** Duermes tranquilo sabiendo que cada pago pasa por su control
- **Trazabilidad.** Puedes seguir el destino de cada peso
- **Ahorro de tiempo.** No tienes que gastar horas resolviendo fraudes o peleando con el banco.

En pocas palabras: cuando proteges tus pagos digitales, ganas paz mental y ahorras disgustos.

¿Por qué es importante?

Según Statista (2025), **el 62% de usuarios de billeteras digitales ha sufrido intentos de fraude.** O sea, más de la mitad ya se tropezó con el ladrón digital en la esquina.

Errores frecuentes:

- Descargar apps falsas (que parecen originales pero son trampas).
- No revisar las transacciones con regularidad o confiarse de QR que pueden ser falsos.
- Compartir claves “solo por esta vez” (ese favorcito que siempre termina caro).

Ejercicio para superar la etapa:

Hoy el reto es práctico y muy fácil:

1. Entra a la app donde manejas tu billetera digital (Nequi, Daviplata o la que uses).
2. Busca en configuración y activa las alertas de movimiento: cada vez que salga o entre un peso, tu celular debe avisarte.
3. Activa también la opción de bloquear compras o pagos sin PIN o clave.

4. Haz una prueba: transfiere un monto pequeño (por ejemplo, $1.000 a usted mismo o a un colega).
5. Verifica que la notificación llegó y que el bloqueo funciona.

Si lo hiciste bien, acabas de blindar tu billetera digital contra el 90% de los intentos de fraude cotidiano. Es como ponerle candado a la alcancía del marranito: sigues metiendo monedas, pero ningún vivo se las lleva sin que te enteres.

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Mariana tiene una pequeña panadería en el barrio. Hace pandebonos gloriosos, de esos que te hacen olvidar la dieta. Como se animó a vender por redes y a recibir pedidos en línea, abrió una cuenta bancaria digital para manejar los pagos. El problema es que, en su apuro, puso de contraseña el clásico 123456. Fácil de recordar, claro. Tanto, que también fue fácil de adivinar.

Una mañana, en vez de revisar los pedidos, Mariana se encontró con que su cuenta estaba vacía. Un ciberdelincuente le había robado la plata con la misma rapidez con la que un cliente se lleva tres almojábanas recién salidas del horno. Resultado: angustia, días sin poder operar y la sensación amarga de que, por no tomar las medidas adecuadas, perdió tiempo, producto y dinero.

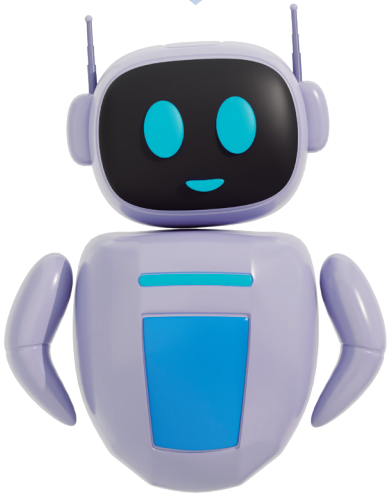
Ahora imaginemos otro escenario: Mariana decide tomarse en serio el tema de la contraseña. En vez de 123456, crea una con este truco: toma las iniciales de su canción favorita, mezcla sílabas de frutas (ki-pla-ma de kiwi, plátano y mango), le agrega un color abreviado (az) y un número con un símbolo: Ymlcyslrpdv25*. Difícil de pronunciar, pero casi imposible de descifrar.

Con esa pequeña acción, Mariana blinda su negocio:

- Nadie puede suplantar su identidad.
- Sus cuentas bancarias están seguras.
- Puede enfocarse en lo que realmente importa: amasar pan y atender a sus clientes.

Y todo por dedicarle cinco minutos a inventar una clave ingeniosa.

Moraleja:
La contraseña es como la cerradura de tu casa. Si usas admin-admin, es como dejar la puerta abierta y un cartel que diga “pase quien quiera”. Pero si juegas un rato con letras, frutas, colores, números y símbolos, tienes un candado de esos imposibles de forzar. Y dormir tranquilo nunca fue tan fácil.



DETECTAR

En la bici hay un momento clave: cuando empiezas a escuchar un ruidito raro en la cadena o sientes que el pedal no responde igual. No es que la bici se rompa de golpe, siempre avisa. El tema es si uno sabe escucharlo o sigue pedaleando como si nada.

En ciberseguridad pasa exactamente lo mismo. La detección es ese oído atento, esa intuición que te avisa que algo no anda bien: un correo que parece demasiado bueno para ser cierto, una conexión inalámbrica que aparece como por arte de magia, una “oferta” en línea que suena sospechosa. Incluso en el trato diario, es notar cuando alguien insiste demasiado en pedirte información que no debería.

En esta etapa vamos a ejercitar ese sexto sentido digital. Vamos a aprender a reconocer las señales, a distinguir lo normal de lo sospechoso y a no dejarnos engañar por la primera sonrisa de internet. Porque el empresario que detecta a tiempo, evita el golpe.

Y lo mejor: no hace falta ser un experto en tecnología. Basta con abrir los ojos, agudizar el oído y confiar en que cada síntoma extraño —como el chirrido en la bici— tiene algo para decirnos.

CERO VIRUS
CERO AMENAZAS

Objetivo de esta etapa:

Que tus computadores no agarren resfriados digitales. La idea es vacunar a tiempo contra malware y virus, y cortarles el camino antes de que contagien a toda la oficina.

¿Cómo lo logro?

Piensa en el antivirus como ese amigo exagerado que no deja entrar a nadie a la fiesta sin revisar la mochila. Para que funcione, hay que mantenerlo actualizado, programar análisis automáticos y, sobre todo, no invitar a dos amigos celosos al mismo tiempo (usar dos antivirus juntos es como poner dos porteros en la misma puerta: se pelean entre sí y al final dejan pasar al colado).

Los hay gratuitos como **Microsoft Defender, Malwarebytes o Bitdefender**; deben estar activos de manera que tengan sus antenitas sintonizadas listas para identificar la presencia de un enemigo.

Y sí, **existen antivirus gratuitos y buenos:** cumplen lo básico y en muchos casos alcanzan para una Mipyme que empieza. ¿Cómo saber si realmente están funcionando? Fácil: el icono en la esquina de la pantalla debe estar en verde o mostrar “protegido”, nunca en rojo ni con signos de alerta. Además, todos tienen un registro de actividades donde aparece qué revisaron y qué bloquearon.

En cuanto a las **funciones básicas que todo empresario debe conocer,** son tres:

- Que el antivirus se actualice solo.
- Que ejecute análisis automáticos.
- Y que pueda poner en cuarentena cualquier archivo raro sin que tengas que decidir en ese momento.

Así de simple: un antivirus bien configurado es como un portero atento; no hace falta que sepas artes marciales, solo confirmar que el guardia sigue despierto.

Riesgos:

Si no se toma en serio, la empresa se expone a infecciones que son como gripes mal curadas: empiezan con un estornudo (una máquina lenta) y terminan en hospital (robo de datos, bloqueo de sistemas, pérdida de confianza de los clientes).

Ventajas de tomar medidas apropiadas:

La protección activa es como dormir con la puerta de la casa cerrada y el perro vigilando: uno descansa tranquilo. Con un antivirus bien configurado hay confianza en los dispositivos y los riesgos se reducen de manera notable.

¿Por qué es importante?

El 43 % de los ataques en PYMEs entran por malware que nadie vio venir, como el vecino simpático que pasa sin saludar al portero (Malwarebytes, 2024). Por eso el antivirus no es lujo, es ese amigo exagerado que revisa mochilas en la fiesta. La regla es simple: mantenerlo despierto, actualizado y con el ojo puesto en cada archivo sospechoso.

Errores frecuentes:

- **Usar antivirus pirata** es como comprar un casco de bicicleta en una esquina: bonito, barato, pero el primer golpe lo rompe.
- **No actualizarlo:** un antivirus desactualizado es como un diccionario viejo, busca “Instagram” y no lo encuentra.
- **Ignorar alertas:** eso es como el pitido del humo en la cocina y pensar “seguro es la pila que está fallando”.

Ejercicio para superar la etapa:

1. Abre tu antivirus. Si ya tienes uno instalado, búscalo en la barra de inicio o en el escritorio.

2. Si no tienes, instala uno gratuito y confiable. Por ejemplo, Avast, que funciona bien para Mipymes y no exige ser experto en tecnología.

3. Ejecuta un análisis completo. No el rápido, porque ese solo revisa la “superficie”. El completo es como una limpieza a fondo: revisa cada rincón del equipo.

4. Sigue las recomendaciones del programa. Si el antivirus te dice “eliminar”, hazlo. Si le sugiere “reparar” o “poner en cuarentena”, también acepta. La idea es no ignorar las alertas.

5. Programa análisis automáticos. Así no dependerá de la memoria de nadie y cada semana el sistema revisará solo.

Cuando termines, podrás decir con tranquilidad: ***“esta oficina tiene cero virus, cero amenazas”.***

SOFTWARE 1A: HERRAMIENTAS SEGURAS

Objetivo de esta etapa:

Tener software legal y actualizado es clave para evitar problemas como quedarse sin acceso a facturas o interrumpir el negocio. Usar programas pirata puede detener la operación, generando pérdidas y frustración. Asegúrate de tener licencias y actualizaciones para prevenir estos contratiempos.

En esta prueba aprenderás que tener programas legales y seguros es justamente eso: evitar que tu negocio se detenga por un descuido digital. Como Don Pedro, nadie quiere ver su operación paralizada por algo que se puede prevenir con una licencia y un par de actualizaciones.

¿Cómo lo logro?

Usa software legal (y gratuito si quieres)

No todo lo legal cuesta. Hay versiones gratuitas que funcionan perfecto para Mipymes y no vienen con virus escondidos ni pantallas de casino.

LibreOffice (alternativa gratuita a Microsoft Office)

¿Para qué sirve?
Para crear facturas, hojas de cálculo, presentaciones y documentos sin pagar licencias.

¿Cómo instalarlo?
Ve al sitio oficial de LibreOffice.
Descarga la versión para tu sistema operativo (Windows, Mac o Linux).
Abre el archivo descargado y sigue los pasos de instalación.
¡Listo! Ya puedes empezar a trabajar legal y tranquilo.

Microsoft Defender (antivirus gratuito para Windows)

¿Para qué sirve?
Protege tu equipo contra virus, malware y amenazas sin necesidad de instalar otro antivirus.

¿Cómo instalarlo?
En Windows 10/11, ya viene instalado.
Ve a Configuración → Actualización y seguridad → Seguridad de Windows.
Asegúrate de que esté activado y actualizado.

Google Workspace básico (correo, documentos y almacenamiento en la nube)

¿Para qué sirve?
Para tener correo profesional, compartir archivos, trabajar en equipo y guardar todo en la nube.

¿Cómo instalarlo?
Ve a Google Workspace y elige el plan básico.
Regístrate con tu dominio o crea uno nuevo.
Configura usuarios y empieza a usar Gmail, Drive, Docs, Sheets, etc.

Riesgos:

- **Brechas de seguridad:** un virus entra por el huequito que dejó ese Office pirata.
- **Problemas legales:** si la DIAN te revisa, no basta con decir "es que me lo descargué de Taringa".
- **Baja productividad:** programas que se cuelgan más que videollamada con mala señal.

Ventajas de tomar medidas apropiadas:

- Mejor rendimiento: la computadora vuela y no tarda media hora en abrir Excel.
- Cumplimiento normativo: puedes dormir tranquilo, no te caerá una multa de sorpresa.
- Menos riesgos: tu información no se va de paseo a manos de un hacker ruso con demasiado tiempo libre.

¿Por qué es importante?

El 34 % de las Mipymes usan software pirata (BSA, 2018, https://www.bsa.org). En otras palabras: un tercio de los negocios trabaja con programas descargados de páginas inseguras. Y claro, después aparecen los virus, se pierde la información y nadie entiende qué pasó. Usar software pirata es como dejarle copia de la llave de tu negocio a un desconocido: tarde o temprano, vuelve y entra..

Errores frecuentes:

- Usar software sin licencia, porque “total, funciona igualito”.
- No actualizar, porque “qué pereza reiniciar el PC”..
- Compartir licencias como si fueran Netflix.

Ejercicio para superar la etapa:

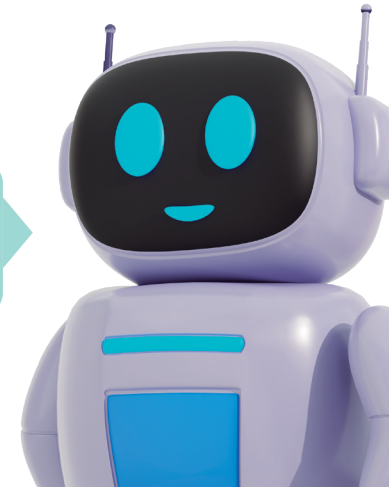
- Revisa cada computador de la empresa. Sí, toca hacerlo uno por uno; nadie dijo que era divertido, pero vale la pena.
- Abre el “Panel de control” o “Configuración” y revisa la lista de programas instalados. Fíjate bien: algunos llevan años sin tocarse, otros podrían ser peligrosos.
- Crea un registro en Excel con tres columnas:
  - Nombre del software: tal cual aparece en la lista.
  - Para qué sirve: una breve descripción.
  - ¿Se usa aún?: marca sí o no. Esto te ayuda a decidir qué mantener.
- Desinstala lo innecesario, pero con cuidado.
- Si no estás seguro de para qué sirve un programa, búscalo en Google antes de borrarlo.
- Evita eliminar cosas críticas, como impresoras virtuales o software de contabilidad, para no bloquear operaciones importantes.

CONEXIÓN INALÁMBRICA FULL

Objetivo de esta etapa:

Nadie que no sea de la empresa debe tener acceso libre al WiFi. Un WiFi abierto facilita la entrada de malware que puede robar información confidencial y causar grandes problemas. Por eso, es fundamental proteger el acceso inalámbrico para evitar estos riesgos y mantener segura la información de la empresa.

¿Cómo lo logro?



- **Cambiar la contraseña de fábrica:** esa clave larga que viene pegada al módem suele ser la misma para miles de equipos. Lo mejor es entrar al panel del router (normalmente escribiendo algo como 192.168.1.1 en el navegador) y cambiarla por una propia. Si se te complica, llama al proveedor de Internet: ellos lo hacen contigo en minutos.

- **Usar protocolos seguros (WPA2 o WPA3):** no es un programa extra, es la "cerradura" que usa tu red WiFi. En el mismo panel del router puedes ver qué protocolo tienes activo. Si aparece algo viejo como WEP, hay que cambiarlo por WPA2 o WPA3. Otra vez: si no sabes cómo, el proveedor te lo configura en una llamada.

- **Separar la red de invitados:** la mayoría de los routers modernos traen la opción "Red de invitados". Sirve para que clientes, amigos o el muchacho del domicilio se conecten a internet, pero sin tocar tus archivos ni tus dispositivos internos. Basta con activarla en la configuración del router y darle otra contraseña. Si tu equipo no lo tiene, tu operador puede habilitarlo o sugerirte un módem más actualizado.

Riesgos:

Si no lo haces, cualquiera podría entrar a tu red, husmear en tus datos y hasta lanzar ataques desde adentro. Es como dejar la puerta de tu oficina abierta con un letrero que dice "Tomen lo que quieran".

Ventajas de tomar medidas apropiadas:

- Mayor seguridad.
- Control sobre quién entra y quién no.
- Evitas sorpresas desagradables tipo virus, robo de información

¿Por qué es importante?

El 24 % de las brechas en PYMEs nacen en un WiFi mal cuidado, como esa puerta que queda entreabierta toda la noche *(Cisco, 2019, https://www.cisco.com)*. Tres teclas mal puestas en el router y cualquiera entra a la cocina digital. A veces, el ladrón ni fuerza la cerradura: la encuentra abierta.

Ejercicio para superar la etapa:

- **Abre la configuración del router**
- La dirección suele ser 192.168.1.1.
- Es como abrir la puerta del cuarto de máquinas de tu oficina: no te asustes, solo necesitas entrar.

- **Cambia la contraseña por una segura**
- Que puedas recordarla, pero que nadie pueda adivinarla (olvídate de “12345678” o “contraseña”).
- Una buena idea: combina letras, números y símbolos. Si quieres, inventa una frase que solo tenga sentido para vos.

- **Activa el cifrado WPA2 o superior**
- Es como ponerle llave a la puerta: hace que lo que viaja por tu WiFi viaje protegido.

- **Reconecta todos los dispositivos**
- Computadoras, impresoras, teléfonos. Todos deben entrar con la nueva clave.
- Aprovecha para revisar si hay dispositivos desconocidos: si algo no te suena, desconéctalo e investígalo.

- **Respira tranquilo**
- Felicitaciones: tu WiFi ya no es un club abierto de hackers. Ahora puedes trabajar sin miedo a que alguien entre a husmear tus archivos o robar información.

LA WEB PODEROSA: PROTEGER LOS SITIOS Y PLATAFORMAS

Objetivo de esta etapa:

Proteger los sitios y plataformas web de tu empresa, para que no sean puertas abiertas a ladrones digitales ni a visitas indeseadas. Queremos que tu página inspire confianza, funcione bien y no te traiga dolores de cabeza.

¿Cómo lo logro?

Usa HTTPS: el candadito no es decoración, es blindaje

Ese candado que aparece en la barra del navegador significa que la conexión está cifrada. Sin él, los datos de tus clientes viajan como cartas abiertas por la calle.

¿Cómo activarlo?:

- Instala un certificado SSL. La mayoría de los proveedores de hosting (como Hostinger, GoDaddy, DonWeb) ofrecen certificados gratuitos con un clic.

- Si usas WordPress, puedes instalar el plugin Really Simple SSL:
  - Ve al panel de WordPress → Plugins → Añadir nuevo.
  - Busca “Really Simple SSL” y haz clic en “Instalar”.
  - Actívalo y sigue las instrucciones para forzar el uso de HTTPS.

  - Para verificar que todo esté bien configurado, usa Qualys SSL Labs. Solo ingresas tu dominio y te da un informe de seguridad con recomendaciones.

Mantén todo actualizado: los parches son como vacunas digitales

Cada vez que tu sistema te diga “hay una actualización disponible”, no lo ignores. Es como cerrar una ventana que los atacantes ya conocen.

¿Cómo hacerlo?:

En WordPress:

- Ve al panel → Escritorio → Actualizaciones.
- Actualiza el núcleo, los plugins y los temas.
- Activa las actualizaciones automáticas si no quieres estar pendiente cada semana.

En Joomla:

- Ve al panel → Componentes → Actualizaciones de Joomla.
- Haz clic en “Instalar la actualización”.

En tu computador:

- Windows: Configuración → Actualización y seguridad → Buscar actualizaciones.

En tu MAC:

- Preferencias del sistema → Actualización de software.
- Actualiza todo al menos una vez al mes. Y si ves un mensaje de “reiniciar para completar”, hazlo. No es capricho, es protección.

Riesgos:

Si no haces nada, puedes encontrarte con:

- **Suplantación de identidad:** Alguien finge ser tu empresa y engaña a tus clientes.
- **Pérdida de reputación:** Que tu página sea insegura hace que la gente pierda confianza.
- **Robo de datos:** Información de clientes, pagos, correos... todo puede irse por el desagüe digital.

Ventajas de tomar medidas apropiadas:

- **Sitios confiables:** Tu cliente entra, compra o consulta y se va tranquilo.
- **Mejor experiencia de usuario:** Sin errores, sin advertencias de seguridad, sin complementos de software errados.

¿Por qué es importante?

Resulta que el 43% de los ataques apunta a sitios web de pequeñas empresas. Sí, esos sitios que uno cree que nadie mira... hasta que alguien los mira. (CNBC).

Errores frecuentes:

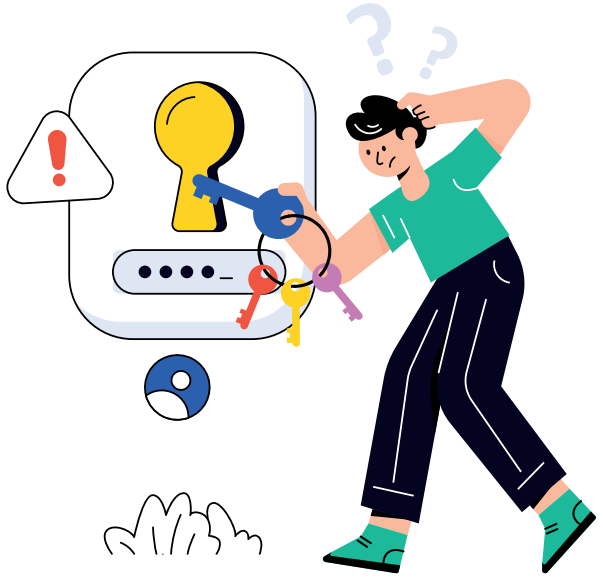
- Usar plantillas bajadas de cualquier rincón de Internet, como ponerle calzado viejo a un maratón: puede funcionar, pero no querrás ver las consecuencias.
- No actualizar plugins, dejando puertas abiertas como cuando uno olvida cerrar la llave del gas.
- Contraseñas débiles tipo “12345” o “admin”. Si tu contraseña es tu nombre, cámbiala antes de que alguien más lo haga por ti.

Ejercicio para superar la etapa:

- Abre tu navegador y entra a tu página web. Mira si hay un candadito Si no lo hay, es como salir a la calle sin llaves.

- Pregunta a quien maneja la web si el **certificado SSL (es un archivo digital que se aloja en el servidor de un sitio web y sirve para autenticar su identidad y establecer una conexión cifrada entre el navegador del usuario y el servidor web)** sigue vigente. Revisen la fecha de vencimiento; si caduca pronto, renuévalo antes de que alguien haga fiesta con tus datos.

- **Bonus:** invita a un amigo a hacer de hacker por cinco minutos. No hay mejor manera de descubrir lo que tú no ves... y sí, reirá mientras tú sudas un poquito.



USO RESPONSABLE DE LA IA

Objetivo de esta etapa:

La inteligencia artificial (IA) puede ser una gran ayuda para tareas como redactar o generar ideas, pero no se debe usar sin supervisión. Si se confía ciegamente en ella, puede dar información incorrecta que afecte negativamente el negocio. Es importante usar la IA de forma responsable, entendiendo sus limitaciones y adaptando sus respuestas a la realidad propia de cada empresa.

Por eso, esta etapa busca sensibilizar sobre el uso responsable de las herramientas de inteligencia artificial y los riesgos que trae si uno las usa sin pensar. No se trata de desconfiar del todo, sino de recordar que el robot es brillante, sí, pero todavía no conoce a tus clientes, ni sabe que en tu barrio el fiado funciona mejor que cualquier algoritmo.

¿Cómo lo logro?:

- **Nada de secretos en el confesionario digital.** Así como no le cuentas a tu vecino cuánto vendiste este mes o dónde guardas las llaves de la caja fuerte, tampoco le cuentes a ChatGPT, Bard o cualquier otra IA tus datos sensibles.

- **Siempre pasa la tarea por tus ojos.** La IA puede ser brillante para redactar un informe o para ordenar una idea, pero a veces se inventa cosas como si fuera el primo que opina de todo sin saber nada. Antes de mandar algo al cliente, revisa, corrige, y ponle tu toque humano.

Riesgos:

- **Se te escapan secretos de empresa** y terminan rodando por internet.

- **Tomas decisiones erróneas** porque confiaste en lo que te dijo un algoritmo que ni siquiera vive en Colombia.

- **Caes en trampas digitales:** plagios, fraudes, y hasta videos falsos que parecen reales.

Ventajas de tomar medidas apropiadas:

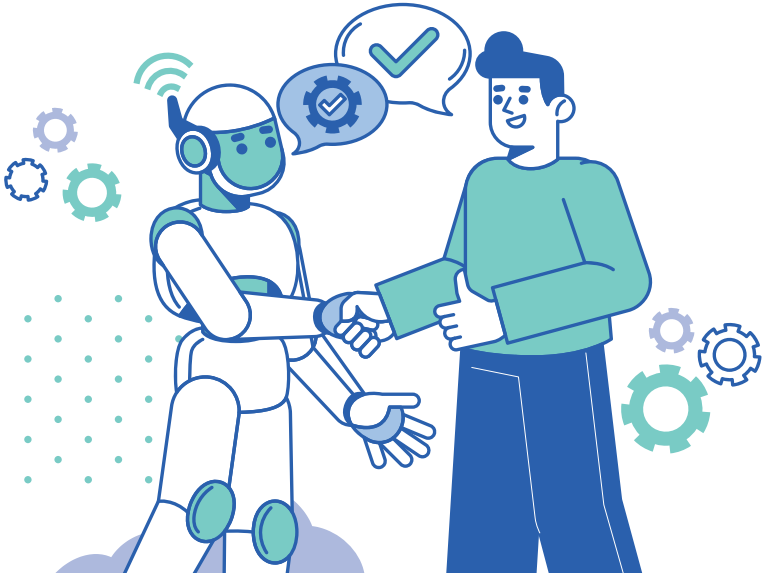
- Decisiones más inteligentes (pero ahora sí con fundamento).
- Tiempo libre porque la IA hace lo repetitivo, y tú te concentras en lo que importa.
- Una puerta de entrada tranquila al mundo tecnológico que, sí o sí, se viene.

¿Por qué es importante?

En las charlas de café de oficina uno escucha de todo: que la IA va a reemplazar trabajos, que ya escribe mejor que el jefe, que sirve para espiar o hasta para enamorar. Pero lo que casi nadie admite es que, cuando uno mira las cifras en frío, el panorama es más humilde: según el Global AI Adoption Index 2023 de IBM, apenas un 35% de las pequeñas empresas tiene reglas claras sobre cómo usar esta tecnología. El resto anda como ciclista sin casco en bajada: pedaleando fuerte, pero a la buena de Dios, sin manual, sin mapa, confiando en que la curva no sea tan cerrada.

Errores frecuentes:

- Usar la IA como si fuera el jefe y no el asistente.
- Creer en todo lo que sale en un video o documento generado por IA (spoiler: muchos son falsos).
- Subir información sensible a plataformas públicas “porque seguro nadie lo ve” (hasta que alguien lo ve).



Ejercicio para superar la etapa:

- No lo olvides, la regla de oro es clara: la IA sí te ayuda, pero siempre eres el filtro. Realiza la siguiente actividad.

Paso 1. Haz tu lista de tareas repetitivas:

- Responder correos de clientes con preguntas básicas.
- Cotizar productos que cambian solo en precio y cantidad.
- Redactar informes simples, como reportes de ventas semanales.

Paso 2. Pregúntate:

- ¿Cuál de estas tareas me roba tiempo valioso?
- ¿Cuál puede hacer la IA en un borrador que yo luego reviso?

Paso 3. El truco (el más importante):
Siempre revisa lo que la IA escriba antes de mandarlo. Es como revisar un cartel antes de colgarlo en la vitrina: si quedó con una letra torcida, el cliente lo nota.

EL CIBERACOSO: LUGARES SEGUROS PARA HACER NEGOCIOS

Objetivo de esta etapa:

Que tu empresa sea un espacio donde todos puedan trabajar sin miedo a comentarios ofensivos, mensajes intimidantes o conductas inapropiadas en línea. Que nadie tenga que mirar dos veces su pantalla antes de responder un correo, porque aquí, el respeto no es opcional: es la norma.

¿Por qué hablar de esto en una cartilla de ciberseguridad?

Porque la seguridad digital no es solo poner contraseñas fuertes o activar el doble factor. También es garantizar que las personas que usan la tecnología en tu negocio lo hagan en un ambiente sano y libre de violencia. El ciberacoso es un delito que no distingue horarios ni cargos: puede darse en un chat interno, en un correo corporativo o en redes sociales.

Y algo clave: el impacto no es igual para todos. La evidencia muestra que este tipo de violencia es interseccional y afecta en mayor proporción a las mujeres y a las diversidades de género. Por eso, integrarlo aquí no es un “extra”: es parte del compromiso real de que tu empresa sea un lugar seguro, justo y respetuoso para trabajar y hacer negocios.

¿Cómo lo logro?

Crea un protocolo de denuncia que no dependa del "habla con tu amiga"

Cuando alguien recibe un mensaje intimidante, ofensivo o incómodo, debe saber exactamente qué hacer. Nada de improvisar

¿Qué debe tener el protocolo?

- **Un canal claro de denuncia** Puede ser un correo exclusivo (ej. denuncias@tuempresa.com), un número de WhatsApp o una línea fija. Lo importante es que esté visible y sea fácil de usar.

- **Una persona responsable** Nombra a alguien de confianza, con formación básica en manejo de conflictos. No tiene que ser psicólogo, pero sí alguien que escuche, actúe y no minimice.

- **Un paso a paso sencillo**

1. Recibir la queja.
2. Revisar lo ocurrido (sin juicios ni chismes).
3. Dar respuesta clara.
4. Proponer solución (puede ser advertencia, mediación, capacitación, etc.).

Puedes armar una infografía o cartel digital con este protocolo y compartirlo en el grupo interno.

Capacita en respeto digital: el chat no es para pelear con stickers.

Haz una charla breve (puede ser virtual) donde expliques:

- Qué es el respeto digital.
- Qué tipo de mensajes, emojis o actitudes son ofensivas.
- Qué hacer si alguien se siente incómodo.
- Que todos tienen derecho a trabajar sin miedo ni burlas.

Usa ejemplos reales (sin nombres) para que el equipo entienda que esto no es exageración, es prevención.

Instala filtros de contenido: como guardianes que cuidan el castillo.

Si usas plataformas como Microsoft Teams, Google Workspace o Slack, puedes activar filtros que bloquean palabras ofensivas o alertan sobre lenguaje inapropiado.

- En **Google Workspace**, puedes configurar reglas en Gmail para detectar palabras clave y reenviar a revisión.

- En **Microsoft Teams,** puedes usar políticas de comunicación para limitar lenguaje ofensivo.

- En **Slack**, hay apps como Sift Ninja que detectan lenguaje tóxico y lo reportan automáticamente.

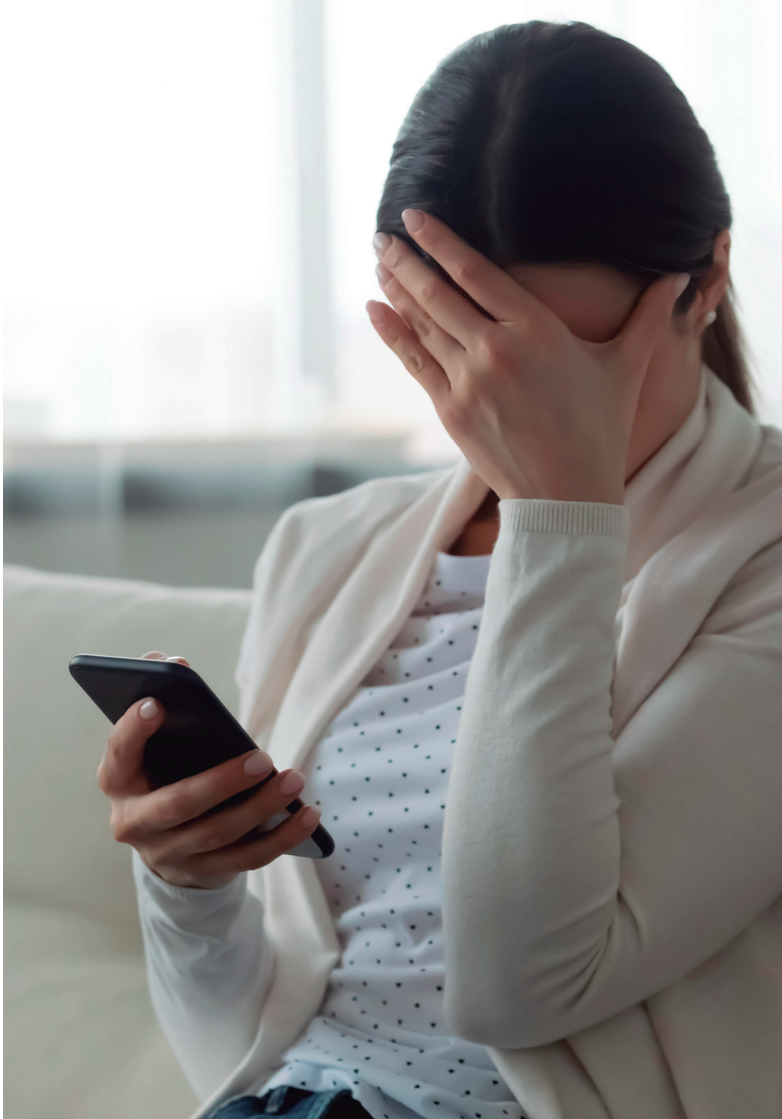
No se trata de censurar, sino de prevenir que el ambiente se vuelva hostil.

Revisa periódicamente correos y chats internos (sin espiar).

No es para leer conversaciones privadas, sino para detectar patrones:

- ¿Hay alguien que siempre responde con sarcasmo o agresividad?
- ¿Se están usando canales para enviar memes ofensivos o burlas?
- ¿Hay colaboradores que evitan participar por miedo?

Puedes hacer encuestas anónimas cada trimestre para medir el clima digital.



Ciberacoso a mujeres: no lo ignores, actúa

Si alguna colaboradora sufre hostigamiento digital, no basta con decir “eso pasa en todas partes”. Hay que intervenir.

La Fundación Karisma tiene un manual práctico sobre cómo actuar ante el ciberacoso. Léelo, compártelo, y úsalo como base para tu protocolo. Esta organización colombiana trabaja por los derechos digitales y tiene recursos accesibles para empresas pequeñas.

Riesgos:

Si ignoras esto, las consecuencias son como dejar una llave en la puerta del cuarto de máquinas:

- Afectaciones psicológicas en quien recibe el acoso.
- Talento valioso que decide irse a otra empresa.
- Posibles problemas legales que nadie quiere en el escritorio

Ventajas de tomar medidas apropiadas:

- Ambiente seguro e inclusivo.
- Cumplimiento legal sin dramas.
- Empleados más tranquilos, felices y productivos.

¿Por qué es importante?

Una de cada tres mujeres en el mundo ha sufrido acoso en línea, lo que evidencia la dimensión global del problema de la violencia de género en entornos digitales. Según **ONU Mujeres** (Abuso digital, trolling, stalking y otras formas de violencia asistida por tecnología contra mujeres, s. f., https://www.unwomen.org/es), este tipo de acoso incluye hostigamiento, insultos, amenazas y la difusión no consentida de imágenes íntimas, entre otras conductas que vulneran la integridad, afectan la salud mental y reducen la participación de las mujeres en espacios sociales, culturales y laborales. Además, muchos de estos episodios no se denuncian, lo que implica que las cifras podrían estar subestimadas.

Errores frecuentes:

- Minimizar los casos: “Bah, solo fue un comentario”.
- No actuar ni dar seguimiento: es como tapar un agujero con cinta adhesiva.
- Dejar que la víctima cargue sola con el problema: nadie debe enfrentarlo sin apoyo.

Ejercicio para superar la etapa:

Toma una hoja o abre un documento en tu computadora. No hace falta nada sofisticado: con papel y lápiz alcanza.

Ahora, escribe un protocolo sencillo para manejar el acoso digital, que cualquiera pueda entender:

- A quién avisar: el contacto dentro de la empresa que sabe cómo actuar sin dar vueltas.
- Cómo guardar evidencia: capturas de pantalla, mensajes, correos... todo lo que pruebe lo que pasó.
- Qué hacer con los mensajes ofensivos: bloquear, reportar y documentar. Nada de ignorar ni responder con un emoji de fuego.

ZONA DE HIDRATACIÓN:

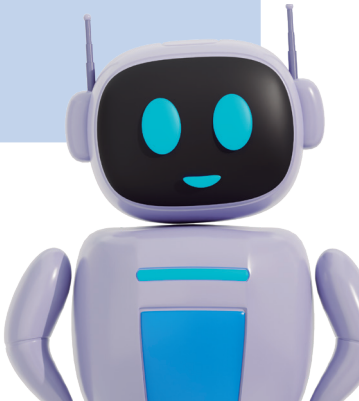
Aprendamos con un caso

En Yumbo, Doña Patricia tiene un café internet. Atiende con delantal y le pone tinto cargado a los estudiantes que van a imprimir el trabajo a última hora. Todo funciona bien... hasta que empieza a pasar algo raro: el internet se cae, las páginas cargan lentamente; un estudiante le reclama a Doña Patricia porque en su correo aparece un inicio de sesión desde Bucaramanga... ¡y él nunca salió del Valle!

Patricia piensa que es "la mala señal de siempre", porque en Colombia es frecuente que falle el internet. Sin embargo, en esta ocasión, el problema no era el proveedor, sino que la red de su negocio seguía con la clave que venía pegada debajo del módem: admin1234. Medio edificio estaba colgado de su WiFi. Y no para ver novelitas, justamente: alguien usaba la red para colarse en las cuentas de los clientes.

Ahí es donde entra la detección. Patricia podría haber notado los síntomas: la lentitud extraña, los accesos raros. Con cambiar la clave por una más compleja, activar la seguridad WPA2 y separar la red del negocio de la de los clientes, evitaba que cualquiera se metiera como Pedro por su casa.

Moraleja:
La diferencia es simple: con la clave de fábrica, Patricia manejaba el café internet como quien deja la caja registradora en la vereda, abierta, con un cartel que dice "sírvase usted mismo". Con un poco de atención y detección, en cambio, logra que su negocio siga andando sin que le roben ni el internet ni la confianza de los clientes.



CORREGIR

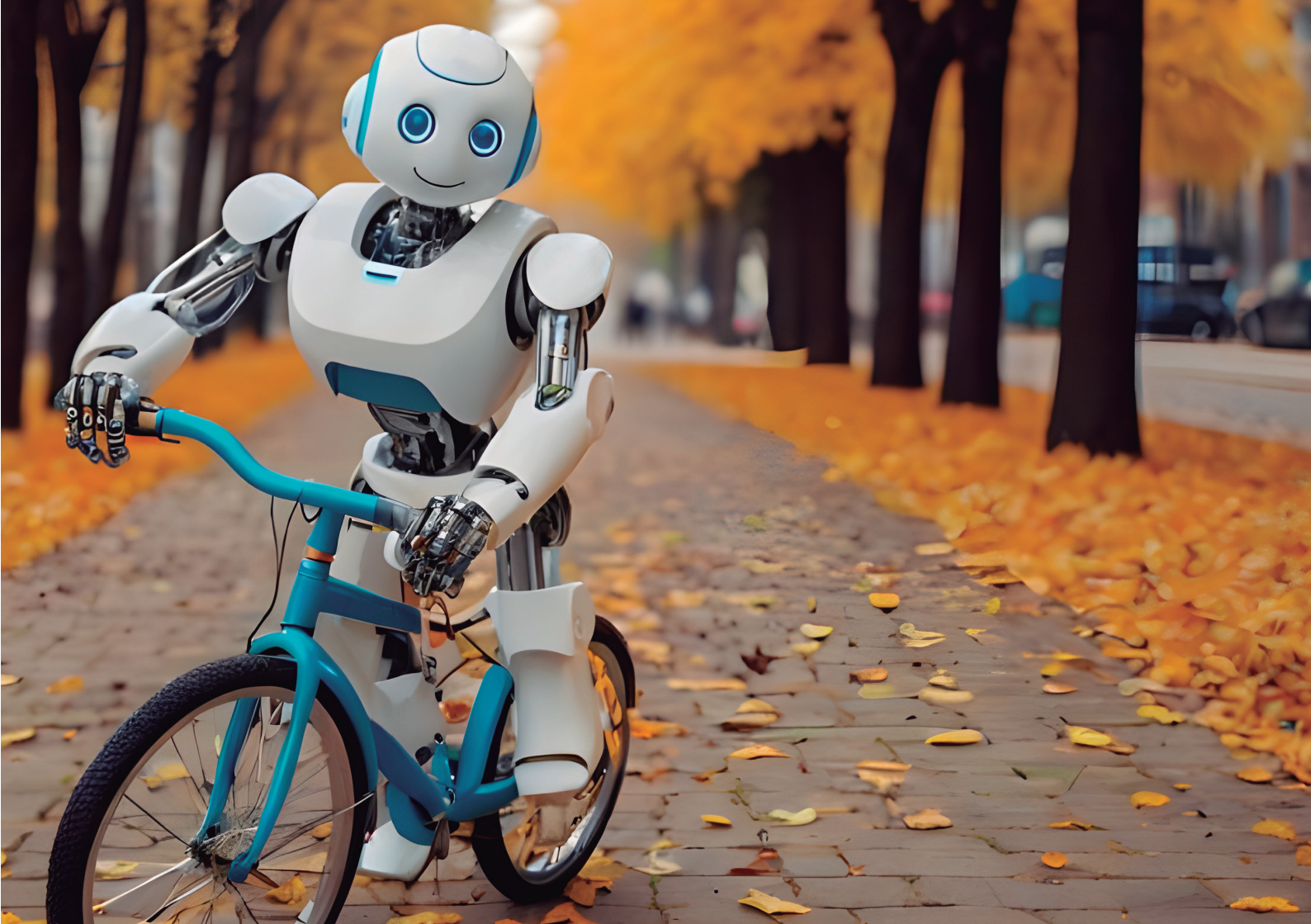
Mira, si llegaste hasta acá es porque no te caíste de la bici en la primera curva. Eso ya habla bien de ti. Superaste la etapa de detección (que fue como aprender a mirar para atrás antes de doblar) y superaste la prevención (ese momento en que te pusiste el casco aunque te despeine). Y ahora, te toca la parte más difícil y necesaria: la corrección.

La ruta no siempre es bajada ni viento a favor. A veces la cadena se sale, el freno no responde, o el pedal chirría justo cuando ibas embalado. Y no pasa nada: es parte del viaje. En este tramo de la ruta cibersegura, no se trata de evitar caídas (ya aprendiste a detectarlas) ni de pedalear con casco puesto (ya entendiste la prevención). Ahora toca lo más simple y lo más sabio: saber qué hacer cuando algo falla.

Porque corregir no es rendirse. Es parar al costado del camino, sacudir el polvo y ajustar lo que se aflojó. Es tener a mano la bomba para inflar la rueda pinchada o el número del que sabe arreglarla.

En esta etapa vas a conocer los canales, las rutas de ayuda, las manos que te dan soporte para volver a subirte a la bici. La corrección es eso: la certeza de que ningún error, ningún ataque ni ningún tropiezo significa el final del recorrido.

La buena noticia es que no estás solo. En esta etapa te vamos a mostrar los caminos y atajos, los canales y las autoridades que te van a dar una mano cuando la rueda se pinche. Porque ningún empresario se detiene a la primera. Y tú tampoco.



DÓNDE DENUNCIAR

Objetivo de esta etapa:

La empresa es como una salida en bicicleta: todos pedaleamos juntos, y cuando alguno siente que la cadena salta o el freno no responde, lo primero es avisar rápido, sin miedo ni vergüenza, porque callarse solo hace que todo el grupo termine en el piso; en sistemas, correos o archivos pasa igual: denunciar algo raro no es un drama, es un gesto simple que protege al negocio y le da ventaja a las autoridades para atrapar a los delincuentes digitales, como levantar la mano en plena ruta para que nadie se estrelle detrás de ti.

¿Cómo lo logro?

Dentro de la empresa:

- **Correo corporativo específico** (ejemplo: seguridad@miempresa.com) para que cualquier persona reporte rápido.
- **WhatsApp o Telegram empresarial** usado solo para alertas de seguridad.
- **Formularios internos rápidos,** donde solo se pida: nombre, fecha, descripción del incidente y acción tomada.

Fuera de la empresa:

- **Plataforma ADenunciar:** allí se registra oficialmente el ciberdelito en minutos.
- **Línea gratuita 018000-910112** de la Policía Nacional para orientación.

La combinación es clave: primero el aviso interno para reaccionar rápido, y luego la denuncia oficial para proteger a la empresa y ayudar a que las autoridades persigan a los ciberdelincuentes.

1. **Usa el canal oficial en Colombia:**

- Desde 2016 existe la plataforma ADenunciar.
- Entra a la web, selecciona “Denuncia virtual”, luego “Delitos Cibernéticos” y sigue el formulario guiado.
- Si no sabes exactamente qué delito sufriste, el sistema te hace preguntas sencillas para orientarte.
- También puedes llamar a la línea gratuita **018000-910112** de la Policía Nacional.

2. **Usa el canal oficial en Colombia:**

- Ten a la mano fechas, horas, pantallazos o correos sospechosos.
- Describe con claridad lo que pasó, aunque no uses lenguaje técnico (la plataforma te va guiando).
- Si tienes testigos o información de quién pudo estar detrás, inclúyela.

3. **Cultura sin culpa:**

- Reportar no es acusar ni buscar culpables en la empresa.
- Al denunciar, proteges tu negocio, tus clientes y a otros empresarios que podrían ser la próxima víctima.

Riesgos:

- Ataques que pasan desapercibidos y afectan datos críticos de la empresa.
- Propagación de malware que puede bloquear sistemas completos o filtrar información confidencial.
- Daños mayores por demora en la respuesta: pérdida de clientes, multas, reputación dañada.

Ventajas de tomar medidas apropiadas:

- **Detección temprana de amenazas**, evitando crisis mayores.
- **Protección de activos críticos**, como bases de datos de clientes, contratos y finanzas.
- **Confianza y eficiencia del equipo**, porque todos saben cómo actuar y no se quedan con dudas.
- **Cumplimiento normativo**, evitando sanciones legales por no gestionar incidentes.

¿Por qué es importante?

Según el *ENISA Threat Landscape Report (2023)*, "el 47 % de incidentes de seguridad no se reportan por miedo o desconocimiento."

Errores frecuentes:

- No denunciar incidentes por miedo a represalias o a "hacer quedar mal" al equipo.
- Ignorar señales de ataque que parecen menores.
- No tener claro **a quién avisar** y cómo registrar la información.

Ejercicio para superar la etapa:

Imaginemos que un correo raro llega a tu bandeja, con un archivo adjunto que huele a problemas o un link que promete "ganar dinero fácil en 3 pasos".

¿Qué hacer?:
Reportarlo como si fueras un detective digital, siguiendo un formato simple:

Nombre: quién está reportando.

Fecha y hora: exacto, para no confundir la línea del tiempo del misterio.

Asunto o descripción del mensaje/archivo: detalles claros, nada de "algo raro llegó".

Acción tomada: por ejemplo, "no abrí el archivo y lo envié a seguridad@miempresa.com".

Revisión en equipo:
¿Detectamos correctamente el riesgo?
¿Se siguió el protocolo paso a paso, sin inventar atajos peligrosos?

RESTABLECIMIENTO PASO A PASO DE CUENTA DE INSTAGRAM

Objetivo de esta etapa:

Que no te quedes mirando tu pantalla como quien llega a la casa y encuentra la cerradura cambiada. La idea es que, si un día amaneces con tu cuenta de Instagram hackeada, sepas el camino para tocar la puerta correcta, probar que eres tú y puedas recuperar las llaves digitales sin desesperar en el intento.

¿Cómo lo logro?

Imagina que tu Instagram es como el candado de la bicicleta con el que viajas todos los días a la tienda o la oficina. Si un ladrón te lo rompe, no basta con gritar: hay que ir al taller, demostrar que la bici es tuya y que no la sacaste prestada de la acera.

El taller, en este caso, está en https://www.facebook.com/help/instagram/368191326593075. Ahí empieza el trámite:

1. Haces clic en “Si crees que han hackeado tu cuenta de Instagram”.
2. Entras a “visita esta página”.
3. Seleccionas “Hackearon mi cuenta” y das en siguiente.
4. Pones el correo o número que estaba asociado. Si no, el username.
5. Pasas la prueba del CAPTCHA para demostrar que eres humano

6. Eliges cómo te van a reconocer:
   - Si tu correo sigue siendo el mismo, lo seleccionas.
   - Si el atacante lo cambió, vas por **“Usar otro método”**.
   - Y si sueles subir selfies, puedes optar por el **video-selfie:** la app te pide mover la cabeza como cuando el médico dice “seguí mi dedo con la mirada”.
7. Registras un correo nuevo, limpio, sin ataduras. Ahí llegará el código de validación.
8. Ingresas el código que te mandan.
9. Si hiciste el videoselfie, esperas a que lo revisen.
10. Si todo sale bien, llega a tu correo el mensaje con el link mágico: el de cambiar la contraseña y recuperar tu Instagram.

Riesgos:

- Que uses el mismo correo de siempre y también lo tengan comprometido.
- Que te desesperes y hagas clic en enlaces falsos (phishing) que prometen ayudarte más rápido.
- Que no completes bien el videoselfie y tengas que repetirlo desde cero.

Ventajas de tomar medidas apropiadas:

- Recuperas tu vitrina digital: clientes, seguidores y comunidad.
- Evitas que usen tu cuenta para estafar a otros en tu nombre.
- Aprendes el procedimiento real y no dependes de “el primo que sabe de tecnología”.

¿Por qué es importante?

Instagram mismo —que es como el dueño de la casa— tiene su propio manual de emergencias. Es un sitio escondido en la página de ayuda de Facebook, donde detallan el protocolo oficial cuando alguien te roba la cuenta.

Ese enlace funciona como la comisaría del barrio digital: ingresas y cuentas lo que sucedió y ellos te dicen exactamente qué papeles mostrar y qué puerta tocar. Y ojo, no es cualquier blog ni un tutorial de YouTube con música electrónica de fondo; es la voz oficial de la plataforma.

Ahí, paso a paso, te explican cómo recuperar el acceso, cómo mandar el videoselfie si hace falta y, sobre todo, cómo cerrar la puerta después para que el ladrón no vuelva a entrar. Guárdalo como quien anota en un papelito el número del cerrajero de confianza: nunca se necesita... hasta que se necesita: https://www.facebook.com/help/instagram/368191326593075

Errores frecuentes:

- Pensar que con cambiar la contraseña ya basta (si no activas la autenticación en dos pasos, te la pueden volver a quitar).
- Usar un correo viejo o compartido para la recuperación.
- Olvidar que Instagram nunca envía mensajes por WhatsApp ofreciéndote ayuda para recuperar tu cuenta.

Ejercicio para superar la etapa:

Haz un simulacro: entra al enlace oficial, navega las opciones como si fueras a recuperar tu cuenta y guarda los pasos en un papel o documento. Luego, activa de inmediato la **autenticación en dos pasos** en tu Instagram empresarial. Es como ponerle no solo candado, sino también cadena y alarma a tu bicicleta: menos glamuroso que la foto de tu producto, pero mucho más útil cuando alguien intente robártela.

EL PLAN B QUE NOS SALVA

Objetivo de esta etapa:

Preparar a la empresa para seguir operando ante cualquier crisis, desde un fallo de sistemas hasta un corte de internet que dure horas. La idea es que el negocio no se detenga, los clientes sigan atendidos y los ingresos protegidos, incluso cuando la tecnología decida tomarse vacaciones.

¿Cómo lo logro?

Identificar procesos críticos:

- Determinar qué operaciones son imprescindibles para la continuidad del negocio: ventas, pagos, atención al cliente, producción, logística.
- Asignar **responsables claros** para cada proceso; que no quede nadie preguntando "¿y ahora qué hago?".

Tener copias de seguridad funcionales y actualizadas:

- No basta con tener backups; hay que probarlos periódicamente y asegurarse de que se restauren correctamente.
- Considerar **copias locales y en la nube**, para no depender de un solo punto de falla.

Simular escenarios críticos:

- Hacer ejercicios de prueba donde un sistema falla, internet se cae o un proveedor no entrega.
- Revisar cómo responde cada responsable y ajustar el plan según lo aprendido.

Riesgos:

- La empresa se detiene y no puede atender clientes.
- Se pierden ingresos.
- La reputación se daña y los clientes se van a la competencia.

Ventajas de tomar medidas apropiadas:

- El negocio sigue funcionando aunque algo falle.
- Cumples con normas y contratos.
- Los clientes confían en que siempre recibirán un buen servicio.
- El equipo sabe cómo actuar y no entra en pánico.

¿Por qué es importante?

De acuerdo con la Agencia Federal para el Manejo de Emergencias (FEMA), alrededor del 60 % de las pequeñas y medianas empresas (PYMES) que no cuentan con un plan de continuidad operativa no logran reabrir después de una crisis o desastre. Esta cifra pone de relieve la importancia de la planificación anticipada frente a emergencias naturales, tecnológicas o cibernéticas, ya que la falta de estrategias de recuperación puede tener consecuencias irreversibles para los negocios. Disponer de un plan de continuidad no solo permite mantener las operaciones críticas durante un evento adverso, sino también proteger los activos, los datos y la confianza de los clientes, garantizando la resiliencia organizacional ante imprevistos (FEMA, s. f., https://www.fema.gov).

Errores frecuentes:

- Tener un plan que nunca se prueba ni se actualiza.
- No enseñar al equipo cómo usar el plan.
- Ignorar procesos secundarios que pueden parar todo si fallan.

Ejercicio para superar la etapa:

Paso 1: Identificar lo crítico

- Haz una lista de lo que realmente no puede parar en tu negocio:
- Ventas: recibir pedidos y cobrar.
- Pagos: pagar proveedores y empleados.
- Atención al cliente: responder dudas, reclamos o consultas.
- Producción: fabricar o preparar productos.
- Entrega de pedidos: enviar a clientes lo que compraron.

Si, por ejemplo, eres dueño de una cafetería, los procesos críticos serían: recibir pedidos, preparar café y entregar a los clientes. Si se cae el sistema de caja, nadie toma pedidos y se forma fila larga.

Paso 2: Asignar responsables claros

- Para cada proceso crítico, decide **quién se encarga si algo falla.**
- Es importante que todos sepan a quién acudir y qué hacer, sin dudas ni confusión.

Paso 3: Pensar en los posibles fallos y plan de respaldo

- Pregúntate: "¿Qué pasa si esto falla mañana?"
- Escribe un plan simple y práctico para cada situación:
- Si no hay internet, registrar pedidos en papel o en Excel temporalmente.
- Si no funciona el sistema de pagos, usar **efectivo, transferencia.**

Paso 4: Hacer un simulacro práctico

- Simula que ocurre un problema real, siguiendo tu plan de respaldo.
- Observa **qué funcionó y qué no.**
- Ajusta el plan según lo aprendido para que la próxima vez sea más rápido y eficiente.

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

En una ferretería de Ibagué llamada “El Tornillo Pintor”, todo marchaba bien hasta que una de las cajeras recibe un archivo extraño por correo: “Lista de proveedores actualizada”. Lo abre sin pensarlo y al rato el antivirus empieza a lanzar alertas.

Ella se asusta, cierra todo y no dice nada. Piensa: “Seguro fui yo, mejor no cuento, lo más posible es que me culpen”. Pasan dos días. El sistema de inventario empieza a fallar, se caen las facturas y los clientes se quejan porque no les aparece la compra registrada.

Ahí recién se enteran todos de que algo raro pasó. Pero ya era tarde: el malware se había metido hasta en la caja registradora. Lo curioso es que Doña Mariela, la dueña, sí había dicho varias veces que si algo extraño sucedía había que avisar de inmediato. Tenía incluso un WhatsApp exclusivo para incidentes. Pero claro, la cajera nunca se animó a usarlo porque pensó que iban a decirle “fue culpa suya”.

La conclusión es sencilla: no se trata de culpas, sino de rapidez. Reportar a tiempo puede ser la diferencia entre una alerta pequeña y un caos que paraliza la empresa. La corrección no es esconder la caída, es levantar la mano y avisar: “me tropecé, necesito ayuda”. ¿Y qué pasa si igual la cosa se complica?

Bueno, ahí entra el famoso Plan B. Porque si se cuenta con un respaldo es posible reconstruir las ventas.

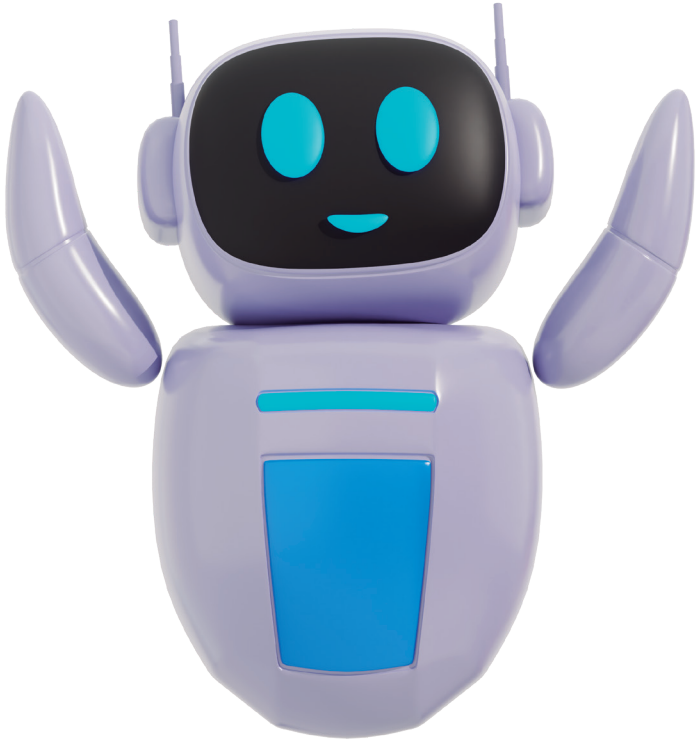
El mensaje de la ruta es claro: denunciar sin miedo y tener un plan alternativo es como llevar un kit de herramientas en la bici. No evita que se pinche la llanta, pero sí asegura que puedes seguir pedaleando.

Herramientas de ciberseguridad para el Nivel INICIO.

Tener una Mipyme en Colombia es como abrir la persiana metálica de tu negocio cada mañana: todos esperan que funcione, pero nunca sabes si al bajar la cortina en la noche alguien intentó forzarla. En lo digital pasa lo mismo: entre ventas, proveedores y clientes, la seguridad parece un detalle... hasta que un correo raro, una clave robada o un virus te frenan el trabajo. Y ahí descubres que no, que esto no solo le pasa a los bancos o a las multinacionales.

Por eso armamos esta cartilla: un kit de supervivencia digital hecho a la medida de negocios pequeños y medianos. Nada de manuales eternos ni tecnicismos. Aquí hay **herramientas concretas,** muchas gratuitas y fáciles de usar, que pueden ser la diferencia entre seguir operando o perder semanas de esfuerzo.

Lo organizamos en tres pasos simples: **prevenir** (ponerle seguro a tu negocio digital), **detectar** (darse cuenta a tiempo de que algo anda mal) y **corregir** (cómo reaccionar cuando ya hay un problema). Cada etapa trae nombres, links y ejemplos diseñados para que cualquier pyme, sin importar su tamaño o sector, pueda aplicarlos desde mañana mismo.



PREVENIR

1. **Contraseñas:** Olvídate del cuaderno en el cajón o del Excel llamado “claves”. Usa un guardián digital: **Bitwarden, KeePass o 1Password.** Es como tener un portero que nunca se cansa de cuidar tus llaves.

2. **Copias de seguridad:** Si mañana tu computador se prende en blanco, ¿qué pierdes? Fotos, facturas, contratos. Para que eso no duela, instala **Cobian Backup, Google Drive o Duplicati.** Copias automáticas que se guardan como quien esconde un tesoro.

3. **Control de accesos:** No todos necesitan entrar a todo. Con **JumpCloud o Apache Directory Studio** decides quién abre la bodega y quién solo pasa por recepción, pero en versión digital.

4. **Capacitación en seguridad:** La mejor alarma es la cabeza de tu equipo. Haz juegos con **Kahoot**, usa cursos básicos de **Google Actívate,** o descarga las plantillas de **INCIBE.** Lo importante: que tu gente sepa qué hacer y qué no tocar.

5. **Protección de datos:** No es solo un lujo de multinacionales. **La SIC Colombia** tiene guías gratuitas y claras sobre cómo tratar la información de clientes. Léelas, te ahorran multas y dolores de cabeza.

6. **Mantenimiento de equipos:** Computadores lentos, empresas lentas. Usa **Glary Utilities o CCleaner** para barrer la basura digital y que todo fluya.

7. **Billeteras digitales:** Si recibes o pagas con apps como **Ualá, Nequi o Daviplata**, activa la autenticación. Es como ponerle doble cerradura a la caja registradora.

DETECTAR

8. **Antivirus:** un clásico que todavía sirve: Windows Defender, Avast o Kaspersky. Mejor tenerlos que cruzar los dedos.

9. **Software para Mipyme:** herramientas como FacturaTech, Alegra o ContaPyme ayudan a llevar las cuentas claras. Y cuando las cuentas están claras, cualquier cosa rara canta sola.

10. **Red WiFi:** Tu WiFi no es café Internet. Con Fing o NetSpot ves quién está conectado. Así pillas al vecino que se cuelga sin permiso.

11. **Seguridad web.** Tu página también necesita un chaleco. Qualys SSL Labs revisa si tu candadito (HTTPS) está en orden y Wordfence protege tu WordPress de intrusos.

12. **Inteligencia Artificial.** No es magia, pero ayuda: ChatGPT, Canva con IA, Google Gemini o Grammarly. Son asistentes gratuitos (o casi) que detectan errores y pulen lo que produces.

13. **Ciberacoso a mujeres:** si alguna colaboradora sufre hostigamiento digital, la Fundación Karisma tiene un manual práctico: web.karisma.org.co. Léelo, compártelo. Es parte de cuidar tu equipo.

CORREGIR

14. **Denuncias.** Si ya pasó el desastre, no te quedes callado:

- **Centro Cibernético Policial (DIJIN**) → caivirtual.policia.gov.co | centro.cibernetico@policia.gov.co
- **Superintendencia de Industria y Comercio (SIC)** (si se roban o usan mal tus datos) → sic.gov.co/habeasdata.
- **ColCERT** (Grupo de Respuesta Cibernética del Estado) → colcert.gov.co | contacto@colcert.gov.co

15. **Plan de Continuidad.** Piensa qué harías si se cae todo: ¿cómo atiendes clientes?, ¿cómo facturas? Usa la plantilla gratuita de Ready.gov para tener tu propio “plan B” en papel

PREVENIR

#Etapa	Herramientas
1. Contraseñas	Bitwarden, Keepass, 1Password
2. Copia de seguridad	Cobian Backup, Google Drive, Duplicati
3. Control de Accesos	JumpCloud, Apache Directory Studio Kahoot para dinámicas
4. Capacitación en Seguridad de la Información	Cursos básicos de Google Actívate Plantillas de INCIBE para sensibilización
5. Protección de datos	Guías de protección de datos en la SIC Colombia - https://www.sic.gov.co
6. Mantenimiento de equipos	Glary Utilities, CCleaner
7. Billeteras digitales	Ualá, Nequi, Daviplata (con autenticación activa)

DETECTAR

#Etapa	Herramientas
8. Antivirus	Windows Defender, Avast Free, Kaspersky Security Cloud
9. Software de MiPYMES	FacturaTech, Alegra, ContaPyme
10. Red WiFi	Fing, NetSpot
11. Seguridad de la web	Qualys SSL Labs, Wordfence
12. IA	ChatGPT (modo gratuito), Canva con IA, Google Gemini, Grammarly
13. Ciberacoso a mujeres	Manual de Ciberacoso - Fundación Karisma - https://web.karisma.org.co

CORREGIR

#Etapa	Herramientas
14. Denuncias	ColCERT – Grupo de Respuesta a Emergencias Cibernéticas del Estado Colombiano Enlace: https://colcert.gov.co Correo: contacto@colcert.gov.co Centro Cibernético Policial (CCP) – Policía Nacional (DIJIN) https://caivirtual.policia.gov.co También puedes reportar a: centro.cibernetico@policia.gov.co Superintendencia de Industria y Comercio (SIC) Si el incidente implica tratamiento indebido de datos personales. Denuncia aquí: https://www.sic.gov.co/habeasdata”

#Etapa	Herramientas
15. Plan de Continuidad de negocio	Plantilla de BCP en Ready.gov

REFERENCIAS

Boston Computing Network. (s. f.). [Estadística sobre el cierre de empresas por pérdida de datos]. Recuperado de https://www.bostoncomputing.net

BSA. (2018). [Estadística sobre el uso de software pirata en MiPYMES]. Recuperado de https://www.bsa.org

Cisco. (s. f.). Consumer Privacy Survey. Recuperado de https://www.cisco.com

Cisco. (2019). [Estadística sobre brechas de seguridad en PYMEs relacionadas con WiFi]. Recuperado de https://www.cisco.com

CNBC. (s. f.). [Estadística sobre ataques dirigidos a sitios web de pequeñas empresas].

ENISA. (2023). Threat Landscape Report 2023.

ERC Colombia. (2025). Las pymes en Colombia son las más expuestas a ciberataques debido a la falta de infraestructura, talento y formación especializada.

Federal Emergency Management Agency (FEMA). (s. f.). Stay in business after a disaster: Planning ahead. Recuperado de https://www.fema.govIBM. (2023). Global AI Adoption Index 2023.

Malwarebytes. (2024). [Estadística sobre ataques de malware en PYMEs].

REFERENCIAS

ONU Mujeres. (s. f.). Abuso digital, trolling, stalking y otras formas de violencia asistida por tecnología contra mujeres. ONU Mujeres. Recuperado el 13 de octubre de 2025, de https://www.unwomen.org/es

Sophos. (s. f.). [Estadística sobre la revisión de accesos en Mipymes]. Recuperado de https://www.sophos.com

Statista. (2025). [Estadística sobre intentos de fraude en billeteras digitales]. Recuperado de https://www.statista.com

Tessian. (2022). The Psychology of Human Error. [Informe].

Verizon. (Data Breach Investigations Report (DBIR). Recuperado de https://www.verizon.com/business/resources/reports/dbir/

Entidades y recursos

Centro Cibernético Policial (CCP) – Policía Nacional (DIJIN). (s. f.). [Portal de denuncia y contacto]. https://caivirtual.policia.gov.co.

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

Fundación Karisma. (s. f.). Manual de Ciberacoso. Recuperado de https://web.karisma.org.co

REFERENCIAS

Superintendencia de Industria y Comercio (SIC). (s. f.). Guías de protección de datos en la SIC Colombia. Recuperado de https://www.sic.gov.co

Colombia. (2012). Ley 1581 de 2012 de protección de datos personales