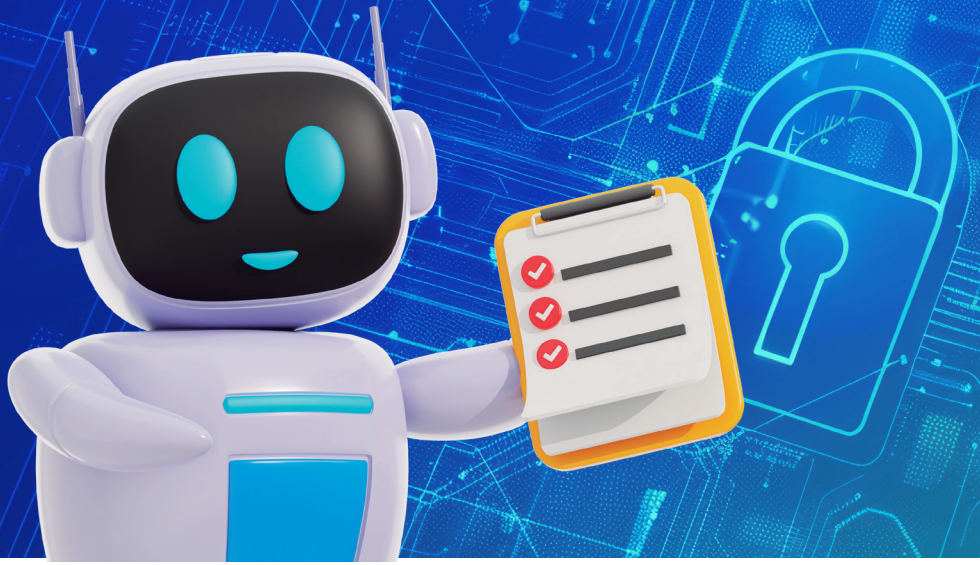
RUTA CIBERSEGURA

NIVEL SENIOR



En convenio con:

Global Gateway

UNIÓN EUROPEA

CÁMARA DE COMERCIO DE BARRANQUILLA

Cámara de Comercio de Cali

CAMARA DE COMERCIO DE MEDELLIN PARA ANTIOQUIA

Cámara de Comercio de Bogotá

Equipo de experto/as:

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

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: 978-958-688-561-4

Contenido

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

¡Hola! Soy Cybersocio,

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

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

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

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

Soy tu aliado en el camino de la ciberseguridad.

PRESENTACIÓN

Tercera etapa: Ya casi eres campeón de la ciberseguridad

Qué bien lo que has hecho. Si estás acá es porque tu nivel de riesgo es muy bajo e hiciste la tarea. Hiciste respaldos de información, pusiste contraseñas decentes (dejaste de usar "123456", ¡por fortuna!), hablaste con tu equipo sobre no abrir correos electrónicos sospechosos, instalaste antivirus sin pagar con el alma, en fin: hiciste lo que muchos no hacen.

Estás en la tercera etapa de esta travesía cibersegura y, créeme, eso no es poca cosa. Estás ahí, muy cerca de la cima como ciclista veterano que se sabe cerca de la meta, con las piernas temblando, pero con el corazón contento. ¿Y ahora qué? Bueno, ahora viene la parte final, la de los detalles. En esta fase vas a aprender algunos conceptos nuevos. Nada de ponerse el sombrero de hacker ni de hablar en binario, tranqui.

Son herramientas útiles, medio desconocidas quizás, pero fundamentales si quieres que tu empresa no solo sobreviva, sino que crezca sin tropezar con cada virus que anda suelto por ahí.

Además, muchas de estas recomendaciones no son para salir del paso, sino para sostener el negocio en el tiempo. Sí, leíste bien: sostener, como quien pone buenas columnas en una casa que quiere que dure.

Y si lo haces bien (y lo vas a hacer bien, porque ya vienes impulsado), vas a ganar una insignia poderosa que dice: "Mi empresa es #MipymeCibersegura". Una insignia que habla de lo buen empresaria o empresario que eres.

Así que, felicitaciones por llegar hasta acá. No muchos lo hacen.

Quedan solo un par de retos y pasos más.
Y cuando los des, vas a mirar para atrás y vas a decir:
"Mira todo lo que pedaleé. Y valió la pena."

Componente normativo: los CONPES en los que se aborda la ciberseguridad 3701 – 3854 y 3995

Este asunto de la ciberseguridad no es un tema de moda ni un invento de Silicon Valley para vender antivirus más caros. Es, más bien, como la alarma del barrio: si suena en una casa, los vecinos inevitablemente se asoman a la ventana, porque lo que le pase a uno puede terminar tocando la puerta de todos.

En Colombia, esta preocupación colectiva comenzó a tomar forma oficial en 2011. Ese año, el gobierno sacó el CONPES 3701, un plan para ponerle orden a la defensa digital. En palabras simples: el país se dio cuenta de que los ataques informáticos crecían como maleza y había que sacar tijeras. Por eso se fortalecieron instituciones como el COLCERT, el Centro Cibernético de la Policía Nacional y el Comando Conjunto Cibernético.

Cinco años después, en 2016, llegó el CONPES 3854. Este documento puso el acento en fortalecer capacidades institucionales: identificar riesgos, gestionarlos, tratarlos y, sobre todo, mitigarlos. Colombia empezó a pensar no solo en reaccionar, sino en anticiparse.

El tercer hito vino en 2020. Cuando se lanzó el CONPES 3995, se planteó un desafío distinto, construir confianza digital. Se trataba de que la gente confíe en los entornos digitales para propiciar el desarrollo. Que empresarios, ciudadanos y hasta escépticos se animen a usar la tecnología sin sentir que, al dar clic, están abriendo la puerta a un ladrón invisible.

Así, poco a poco, Colombia ha tejido una normativa que busca equilibrar dos mundos: la innovación y la seguridad.

Historias de ciberseguridad

A continuación, vas a encontrar un par de historias reales que dejaron a más de un empresario con dolor de cabeza (y de bolsillo). Son casos famosos en los que la ciberseguridad se vino abajo como un castillo de naipes. Estas historias nos ayudan a responder preguntas incómodas, pero necesarias: ¿cuánto le cuesta a una empresa no tener políticas claras de recolección y protección de la información?

Historia uno: **¿sabes cuánto le cuesta a una empresa no contar con políticas claras en protección de la información?**

A finales de noviembre de 2022, el grupo SANITAS vivió un capítulo que parecía sacado de una película de hackers: un ataque tipo *ransomware*. ¿Qué significa? Que alguien entra por la ventana digital de tu empresa, se sienta en la sala de servidores, cierra con llave todos tus archivos y después te dice: “si quieres recuperarlos, paga el rescate”.

El ataque paralizó casi un 90% de la operación en salud, usuarios intentando agendar citas y la plataforma caída,

pacientes esperando resultados de exámenes que nunca cargaban, médicos sin acceso a historias clínicas. Lo digital dejó de funcionar y todo el mundo corrió a las sedes físicas, generando filas, enojo y hasta problemas de orden público.

SANITAS no cedió al chantaje, y los delincuentes hicieron lo que suelen hacer filtraron información. Entre los datos expuestos estaban registros contables, operacionales, e incluso información de proveedores como Cruz Verde y Farmasanitas. Y, por si fuera poco, amenazaron con publicar más material sensible del grupo internacional Keralty, dueño de SANITAS.

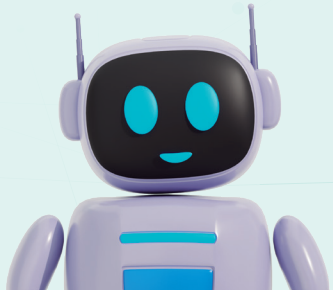
Las cifras asustan:

- 5,5 millones de pacientes quedaron sin atención normal durante semanas.
- Se encriptaron 3 terabytes de información, que incluían carpetas con estados financieros, balances, presupuestos y datos personales.
- El golpe reputacional fue tan fuerte que no se mide solo en dólares, sino en confianza perdida.

¿Se pudo haber evitado? Tal vez. Con medidas que suenan técnicas, pero son tan necesarias como ponerle cerrojo a la puerta de la casa:

- Políticas estrictas de contraseñas y autenticación multifactor (MFA).
- Segmentación de la red y control de accesos.
- Actualizaciones y parches al día (sí, esos que uno suele postergar).
- Copias de seguridad desconectadas de la red.
- Sistemas de monitoreo avanzado para detectar intrusos a tiempo.
- Y algo clave: capacitación constante del personal, porque el error humano sigue siendo la puerta favorita de los atacantes.

En lo económico, se habla de un pago cercano a 1,5 millones de dólares para recuperar parte de la información. Pero el costo más alto fue otro: la confianza rota de millones de usuarios y el esfuerzo titánico (y carísimo) de volver a levantar toda la infraestructura tecnológica.



Historia dos: **¿sabes cómo clasificar la información para sobrevivir a un ciberataque?**

Cuando una empresa sufre un ciberataque, lo primero que se rompe no siempre es el servidor ni la base de datos: se rompe la calma. Y en ese caos, la única pregunta que realmente importa es: ¿cómo restablecemos el servicio lo más rápido posible sin perder la información?

La respuesta parece obvia, pero no lo es: depende de cómo hayas clasificado tu información. Piensa en tu empresa como una biblioteca. Si los libros están tirados en el suelo, mezclados entre novelas, manuales y enciclopedias, cuando alguien apague la luz (léase: un hacker), encontrar el tomo que necesita será un infierno. En cambio, si cada cosa está ordenada, sabrá dónde encender la linterna primero.

Clasificar bien los datos no es un capricho técnico, es lo que permite que un negocio vuelva a ponerse de pie después de un golpe. Y no solo se trata de guardar copias, sino de hacerlo con lógica, sabiendo qué es crítico, qué es sensible y qué puede esperar.

Categoria	Descripción	Ejemplos	Tiempos
Mision critica	Sin estos datos o sistemas, el negocio se detiene	ERP, core bancario, portal de venta en línea, base de datos clientes	< 1 hora
Alta prioridad	Impacto significativo, pero operaciones pueden continuar parcialmente.	Correo corporativo, aplicaciones de gestión interna, intranet	4 - 8 horas
Media prioridad	Impacto moderado, afecta eficiencia pero no paraliza operaciones.	Repositorio documental, sistemas de reportes, backups secundarios.	24 horas
Baja prioridad	No críticos para operaciones inmediatas, restauración puede esperar.	Históricos, archivos de referencia, material de marketing.	72 horas ó más

Te compartimos las mejores prácticas para lograr esa “alta disponibilidad” que tanto mencionan los expertos:

- **Inventario actualizado:** conoce qué sistemas y datos tienes, y qué depende de qué.
- **Copias de respaldo diversificadas:** unas locales, otras en la nube, y otras offline, lejos del alcance del atacante.
- **Pruebas periódicas:** no basta con tener backups o copias de seguridad, hay que usarlos en simulacros cada 6 o 12 meses para asegurarse de que sirven.
- **Plan de continuidad documentado:** porque el día del desastre, nadie tiene tiempo de improvisar.

¿El costo de no hacerlo? El mismo de siempre, pero multiplicado:

- Riesgo reputacional (porque clientes y socios pierden la confianza).
- Pérdidas económicas por cada minuto de operaciones caídas.
- Y la sensación amarga de saber que la recuperación pudo ser más rápida... si se hubiera tenido un mapa claro de la información.

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.**

PREVENCIÓN

Un empresario sin prevención es como ese ciclista que sale a la carretera sin revisar los frenos ni inflar las llantas: pedalea tranquilo... hasta que en la bajada descubre que el manubrio tiembla y la bici no frena. Ya es tarde. En la ciberseguridad pasa lo mismo: si no ajustas todo antes de salir, después el golpe duele más.

Por eso la fase de prevención es el inicio de tu pedaleada digital. Es donde calibras la bici, revisas que la cadena no esté floja, ajustas el casco y te aseguras de tener agua en la caramañola. No es el tramo más emocionante del recorrido, pero sí el que define si llegas a la meta o te quedas a medio camino.

En esta parte de la ruta vas a aprender a:

- Hacer **copias de seguridad** que son como llevar una rueda de repuesto: no la usas todos los días, pero el día que te pinches, te salva el viaje.

- Detectar las **suplantaciones en WhatsApp**, que son como los falsos ciclistas que se te ponen al lado para confundirte y meterte en un atajo peligroso.

- **Cuidar los accesos remotos,** como si fueran las curvas cerradas en bajada, si no estás atento, cualquiera se te mete en el carril.

- Y varias medidas más que son como revisar las luces y los reflectores, parecen un detalle, pero son lo que evita que te choquen en la oscuridad.

Así que ponte el casco, hidrátate, ajusta bien el sillín y arranca a pedalear: comienza tu **RutaCibersegura Senior** en la fase de Prevención. Pedalea fuerte, porque las siguientes etapas —Detección y Corrección— se parecen a esas subidas empinadas donde necesitas todo el aire y toda la preparación que acumulaste acá.

COPIAS DE SEGURIDAD DE LA INFORMACIÓN

¿Cuál es el objetivo de esta etapa?

Asegurar que, si la información se pierde o queda inaccesible, pueda recuperarse rápido para que el negocio siga operando sin pausas y sin dar señales de crisis, evitando así daños a la reputación y la confianza de clientes y socios.

¿Cómo lo logro?:

Realizando pruebas de integridad de datos

- Verificar la existencia del respaldo
- Confirmar que el archivo o conjunto de archivos de la copia se generó en la fecha y hora programada.

Revisar registros y reportes de la copia

- Consultar el log del software de backup para confirmar que no hubo errores o interrupciones durante el proceso.

Un log es el cuaderno de bitácora del programa: anota todo lo que hizo y si algo falló. Revisarlo en el software de backup es leer ese registro para confirmar que la copia se hizo completa, sin errores ni cortes.

Comprobar el tamaño y consistencia de los archivos

- Revisar que los respaldos tengan el tamaño esperado y no estén corruptos o incompletos.

Si el archivo original pesaba 2 GB y el respaldo pesa 300 KB, algo no cuadra. Es como pedir una pizza familiar y que te traigan una empanada. Hay que revisar que el tamaño sea el esperado y que no esté corrupto. Porque un archivo corrupto no es un archivo con mala conducta, es uno que no se puede abrir.

Validar la legibilidad del medio de almacenamiento

- Asegurarse de que el medio (disco, cinta, nube, etc.) se pueda montar o acceder sin fallos.

Prueba de restauración parcial

- Restaurar un archivo o conjunto de archivos de prueba y abrirlos para confirmar que se pueden usar correctamente.

Prueba de restauración completa (periódica)

- Restaurar todo el sistema o base de datos en un entorno de prueba y validar que funciona igual al original.

No basta con tener la copia. Hay que restaurarla. Abrirla. Ver si se puede usar. Como cuando uno prueba el paraguas antes de salir con amenaza de lluvia. Restaura un archivo chiquito cada tanto. Y de vez en cuando, haz la prueba grande: restaura todo en un ambiente de prueba. Si no arranca, mejor enterarse hoy que el día del desastre.

Comparación con el origen

- Revisar que los datos restaurados coincidan con los datos originales (fechas, versiones, estructura).

Validación de integridad lógica

- Abrir archivos de base de datos, documentos o aplicaciones restauradas para confirmar que funcionan de manera correcta.

Revisión de retención y ciclos

- Confirmar que los respaldos antiguos todavía pueden restaurarse y que cumplen con la política de retención establecida.

Documentación del resultado

- Registrar los pasos, observaciones y cualquier error encontrado para auditoría y mejora del proceso

Haciendo pruebas de restauración de las copias de seguridad.

- Seleccionar periódicamente copias para hacer pruebas de restauración.
- Restaurar en un ambiente de prueba, no en producción.
- Validar que los datos restaurados estén completos y utilizables.
- Medir tiempos de restauración y compararlos con el RTO (Recovery Time Objective por sus siglas en inglés) definido. El RTO es el tiempo máximo tolerable que puede pasar desde que ocurre una falla o desastre hasta que el sistema, servicio o información vuelve a estar operativo.
- Documentar los resultados de cada prueba.

Evitar tenerlas en un mismo sitio, diversificar su ubicación sin sacrificar seguridad

- Disco duro externo (HDD/SSD portátil) – Ideal para una copia rápida y desconectarla después.

- NAS (Network Attached Storage) – Almacenamiento en red dentro de la empresa o el hogar.
- Servidor local dedicado – Un equipo exclusivo para centralizar copias de seguridad.
- Servicios en la nube – Ej.: Google Drive, OneDrive, Dropbox, AWS S3, Azure Backup.
- Servicios de respaldo en la nube especializados – Ej.: Backblaze, Carbonite, Acronis.
- Medios ópticos – Blu-Ray/DVD, aunque cada vez menos usados.
- Ubicación externa (off-site) – Una copia guardada físicamente en otro lugar (otra oficina, caja fuerte, etc.).

La regla de oro:

- 3 copias de tus datos.
- En 2 tipos de medios distintos.
- Y al menos 1 fuera del sitio principal.

Como tener tres llaves de tu casa: una en el llavero, otra en el cajón, y otra en casa de tu mamá.

Riesgos:

En una Mipyme, perder datos no es solo un problema técnico, es como que se te borre de golpe la memoria de todo lo que hiciste. Si esos datos incluyen información sensible de clientes, el lío se multiplica y pueden llegar cartas de abogados y reclamos que no esperabas. Y mientras todo eso pasa, la empresa empieza a perder dinero, porque cada hora sin operar o cada cliente que se va es plata que no vuelve.

Ventajas de tomar medidas apropiadas:

Cuando todo se cae —el sistema, la red, el servidor, la esperanza— lo único que salva el día es tener una copia de seguridad que funcione. No es magia, es prevención. ¿Qué significa esto para tu Mipyme?

Que puedes seguir vendiendo, atendiendo clientes y pagando sueldos aunque te hackeen, se te queme el disco o alguien borre sin querer la base de datos. Porque si tienes respaldo, tienes futuro.

¿Por qué es importante?

Según un informe de **Computing,** basado en datos de **Veeam,** el 58 % de las copias de seguridad fracasa, lo que deja a muchas empresas sin una protección efectiva frente a la pérdida de datos (Computing, 2024). Además, una encuesta de **Arcserve** muestra que el 32 % de las organizaciones ni siquiera prueba sus sistemas de respaldo de forma regular (Arcserve, 2023).

Errores frecuentes:

- Se debe tener una adecuada clasificación de la información para saber cuál es crítica para la continuidad del negocio.
- Según la criticidad se escogen los Sistemas de respaldo (nubes, NAS)

Una NAS es como un "disco duro inteligente" conectado a la red de tu empresa. Permite que varios usuarios accedan a la información y que las copias se hagan de forma automática y segura.

Ejercicio para superar la etapa:

Ejercicio práctico – Checklist sobre Copias de Seguridad de la Información.

Instrucciones para el participante:
Marca las opciones que consideres correctas en cada ítem. Algunas preguntas pueden tener más de una respuesta válida.

¿Dónde es más seguro almacenar las copias de seguridad?

- [ ] En el mismo servidor de producción
- [ ] En un disco externo conectado permanentemente.
- [ ] En un sitio físico diferente al de producción.
- [ ] En la nube con cifrado y controles de acceso.

Respuesta sugerida: *Nunca en el mismo servidor. Lo ideal es copias externas y separadas físicamente (off-site o cloud con seguridad).*

SUPLANTACIONES POR WHATSAPP

Objetivo de esta etapa:

Prevenir y responder ante intentos de suplantación de identidad en WhatsApp, porque no hay nada más incómodo que descubrir que alguien está escribiéndole a tus clientes, proveedores o incluso a tu mamá haciéndose pasar por ti. La idea es minimizar riesgos para las personas y las empresas, antes de que un delincuente digital convierta un chat inocente en una estafa.

¿Cómo lo logro?

Formas comunes de suplantación

- Mensajes de un “número nuevo” que finge ser un familiar o amigo (“perdí mi celular, escríbeme acá”).
- WhatsApp Business falso que se hace pasar por una empresa (bancos, tiendas, aerolíneas).
- Enlaces maliciosos que imitan páginas de pago o verificación.
- Solicitud de códigos de verificación (ejemplo: te dicen que les llegó por error un SMS y te piden reenviarlo).

Cómo evitar la suplantación

- No compartas tu código de verificación de 6 dígitos jamás.
- Activa la verificación en dos pasos en WhatsApp (un PIN adicional de 6 dígitos).
- Verificación en dos pasos: esto es como tener una segunda llave que solo tú conoces. Si alguien quiere instalar tu WhatsApp en otro celular, va a necesitar ese PIN. Y si no lo tiene, se queda mirando la puerta cerrada.

¿Cómo se activa?

- Abre WhatsApp.
- Toca los tres puntitos arriba a la derecha → Configuración.

- Entra en la Cuenta → Verificación en dos pasos.
- Activa y pon un PIN de 6 dígitos.
- Agrega tu correo electrónico por si se te olvida el PIN.

Consejos para no caer en trampas

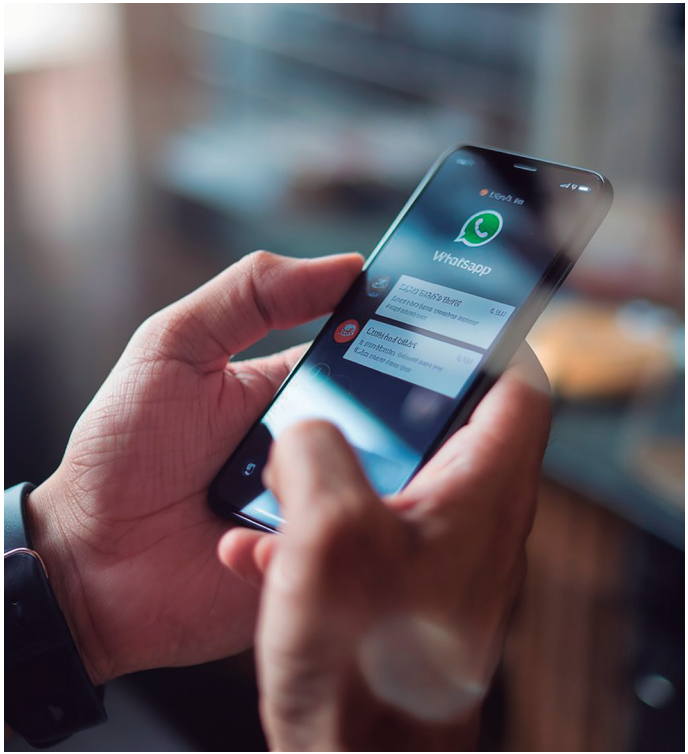
- Si te llega un mensaje urgente pidiendo plata o datos, no respondas sin llamar primero.
- Revisa la foto y el historial de chat. Si no coincide con lo que recuerdas, algo está mal.
- Bloquea y reporta números sospechosos directamente en WhatsApp.
- Mantén la app actualizada. Las nuevas versiones traen mejores candados.

Riesgos:

El más inmediato, el robo de información sensible. No hacer nada es como dejar la puerta abierta y confiar en que nadie va a entrar. Pero alguien siempre entra.

¿Qué puede pasar si no proteges tu negocio? Te pueden robar los datos de tus clientes, las contraseñas, los correos, los números de cuenta. Y no, no es exageración.

¿Y después qué? Pues lo que sucede es que pierdes la confianza de tus clientes y hasta te puedes meter en líos legales.



Ventajas de tomar medidas apropiadas:

- Disminución drástica de intentos exitosos de fraude.
- Mayor confianza interna y externa.
- Detección oportuna y rápida respuesta ante incidentes.

¿Por qué es importante?

- Según Kaspersky (2024): 1 de cada 8 usuarios en Latinoamérica reportó intentos de fraude por WhatsApp.
- En Colombia, según la Policía Nacional, en el 2024 se recibieron más de 13.000 denuncias por suplantación digital, siendo WhatsApp el canal más reportado.

Errores frecuentes:

- Confiar solo por ver el nombre y foto de perfil.
- No activar la verificación en dos pasos.
- Compartir información corporativa por chats personales sin cifrado adicional.[1]
- No tener protocolo interno para validar solicitudes financieras.
- Ignorar señales de suplantación como cambios súbitos de número o escritura diferente.

[1] El cifrado adicional se refiere a implementar medidas que nos brinda la misma plataforma para evitar un fraude, por ejemplo, la autenticación de dos pasos, en la configuración de la cuenta activar “Mostrar notificaciones de Seguridad” y así sabes si se intenta reinstalar WhatsApp en otro dispositivo.

Ejercicio para superar la etapa:

Objetivo: Reconocer señales de suplantación y aplicar buenas prácticas de respuesta.

Escenario
Recibes un mensaje en WhatsApp de un número desconocido que dice:
“Hola, cambié de número, guárdalo. Te escribo porque necesito que me ayudes con una transferencia urgente, después te devuelvo el dinero. Soy tu jefe.”
√ *Lista de Chequeo (con opciones múltiples)*

¿Qué es lo primero que debes identificar en el mensaje?

- [ ] El número es desconocido.
- [ ] El tono de urgencia en la solicitud.
- [ ] El intento de generar confianza diciendo que es alguien cercano.
- [ ] Nada extraño, parece legítimo.

√ Respuesta sugerida: Todas excepto la última.

Acción inmediata más adecuada:

- [ ] Realizar la transferencia para evitar problemas con el jefe.
- [ ] Responder preguntando más detalles personales para confirmar identidad.
- [ ] Verificar por otro canal (llamada al número habitual del jefe).
- [ ] Ignorar y bloquear el número.

√ Respuesta sugerida: Verificar por otro canal y, en caso de confirmarse fraude, bloquear el número.

CLASIFICACIÓN DE LA INFORMACIÓN PARA RESPALDO

Objetivo de esta etapa:

Identificar, organizar y proteger la información según su nivel de importancia, sensibilidad y valor, de manera que la más crítica esté respaldada con prioridad y de forma segura, optimizando las capacidades de almacenamiento de nuestros dispositivos.

¿Cómo lo logro?

Con una adecuada clasificación para respaldo y recuperación dado el caso de un ciberataque. Una manera indicada sería la siguiente.

Crítica / Misión Vital

- Sistemas esenciales para la operación diaria (bases de datos financieras, nómina, clientes, ERP o Enterprise Resource Planning (en español se traduce como Sistema de Planificación de Recursos Empresariales).
- Respaldos en tiempo real o con mínima latencia.
- Deben estar replicados en sitios alternos (on-premise y nube).

Confidencial / Sensible

- Información estratégica (planes de negocio, contratos, propiedad intelectual).
- Respaldos diarios, con cifrado fuerte.
- Restauración prioritaria tras recuperar lo crítico.

Operacional

- Documentos de proyectos, reportes, archivos compartidos de áreas.
- Respaldos semanales, con controles de acceso.
- Restauración programada según el área afectada.

Histórica / Archivada

- Información legal y de cumplimiento que debe conservarse por años.
- Respaldos en almacenamiento de bajo costo (ej. cintas, nube tipo Glacier).
- Restauración lenta pero aceptable, no prioritaria.

Riesgos:

- Respaldo incompleto o con datos irrelevantes.
- Pérdida de información crítica.
- Costos excesivos por almacenar basura digital.
- Exposición de datos sensibles por mala segregación. Incumplimiento de normativas (Habeas Data, ISO 27001, GDPR o Reglamento General de Protección de Datos).

¿En qué consiste la ISO 27001? Es el escudo digital que toda empresa necesita: protege tus datos como si fueran joyas.

Se basa en un sistema de gestión que detecta riesgos, los mide y los neutraliza antes de que hagan daño. No es solo papel: exige acción, mejora continua y que todos en la organización se pongan las pilas.

El GDPR es la norma europea que manda en protección de datos: si manejas información personal, tienes que jugar limpio y seguro. Exige ciberseguridad seria: cifrado, control de accesos, y reacción rápida ante brechas. Nada de dejar puertas abiertas. Transparencia total: el usuario manda sobre sus datos, y tú como empresa, a cumplir o pagar multas que duelen.

Ventajas de tomar medidas apropiadas:

- Recuperación rápida ante incidentes.
- Optimización de almacenamiento.
- Cumplimiento legal y normativo.
- Mejor control de acceso a la información.
- Reducción del tiempo de búsqueda.

¿Por qué es importante?

Según el 2025 State of SaaS Backup and Recovery Report (HYCU, 2025), los niveles de cobertura de estrategias de respaldo entre plataformas SaaS varían significativamente: el 70 % de las organizaciones dispone de una estrategia de respaldo para Microsoft 365, el 66 % cuenta con algún plan en Google Workspace y solo el 53 % tiene una estrategia dedicada en Salesforce. Esto evidencia que hasta el 47 % de las empresas no tienen clasificados o respaldados datos críticos en Salesforce y una proporción similar en otras plataformas.

Errores frecuentes:

- Respaldar absolutamente todo sin distinción.
- No etiquetar la información antes de copiarla.
- Mantener versiones antiguas innecesarias.
- Guardar copias en el mismo lugar que el original.
- No proteger respaldos con cifrado.
- Falta de pruebas de restauración.

Ejercicio para superar la etapa:

Identificación de información sensible

Pregunta: ¿Cuál de las siguientes categorías de información debe clasificarse como “Crítica” y por tanto tener prioridad alta en respaldos?

- ☐ Datos financieros de la organización (balances, cuentas bancarias).
- ☐ Videos de entretenimiento descargados por empleados.
- ☐ Base de datos de clientes con información personal (PII).
- ☐ Manuales internos de uso general (no confidenciales).

Respuesta sugerida:

√ Datos financieros de la organización

√ Base de datos de clientes con información personal

PROTOCOLOS DE RECUPERACIÓN DE INFORMACIÓN

Objetivo de esta etapa:

Volver a poner en marcha el corazón digital de la empresa cuando algo sale mal. Se trata de restablecer el acceso, la integridad y la disponibilidad de la información después de una pérdida, corrupción o ataque, minimizando al máximo el impacto operativo, legal y económico. En otras palabras: que la empresa no se quede varada en medio de la carretera digital, sino que pueda arrancar de nuevo con la menor demora y el menor daño posible.

¿Cómo lo logro?

1. Manos a la obra: inventario de activos críticos
Antes de hablar de antivirus, firewalls y otras palabras que pueden parecer extrañas, hay que saber qué de todo esto, es lo que realmente importa en tu negocio.

- ¿Tienes una base de datos con los correos de tus clientes?
- ¿Un sistema de facturación?
- ¿Un archivo con las recetas secretas de tus empanadas?

Todo eso es un “activo crítico”. Es decir, si desaparece o se borra, estás en problemas. Entonces, lo primero es hacer una lista de lo que no puedes perder ni por error ni por ataque.

2. RTO y RPO (tranqui, no es una banda de rock)
Estos dos conceptos suenan a tecnicismo, pero son muy sencillas, ya verás:

RTO y RPO

Concepto	Sigla	¿Qué significa?	Ejemplo práctico
Tiempo máximo de inactividad aceptable	RTO (Recovery Time Objective)	Es el tiempo que tu negocio puede estar “caído” sin que se vuelva un desastre	Si tu sistema de ventas se cae, ¿puedes aguantar 1 hora sin vender? ¿O 1 día? Ese es tu RTO
Antigüedad máxima aceptable de los datos recuperados	RPO (Recovery Point Objective)	Es cuánta información estás dispuesto a perder si hay un problema	Si haces respaldo cada noche y te hackean a las 5 p.m., pierdes todo lo que hiciste ese día. ¿Está bien eso? Ese es tu RPO

3. Respaldos regulares y verificados

Hacer copias de seguridad es como tener un paraguas: no lo usas todos los días, pero cuando llueve, lo bendices

- Realiza copias diarias, semanales o mensuales, según lo importante que sea la información.
- Pero no alcanza con hacerlas: hay que probar que se pueden restaurar. Porque si el archivo está corrupto, es como tener un paraguas con agujeros.

4. Almacenamiento seguro y diversificado

Guarda tus respaldos en distintos lugares: en tu compu, en la nube, en un disco externo. Y si la información es sensible (como datos de tarjetas), usa cifrado. Es como guardar la información en una caja fuerte con clave.

5. Procedimientos de restauración claros
Cuando hay un incendio, no te pones a leer el manual. Lo mismo pasa con los ciberataques.

Ten un documento que diga paso a paso qué hacer si se pierde la información. ¿Quién llama al técnico? ¿Quién avisa a los clientes? ¿Dónde está el respaldo?.

Todo eso tiene que estar escrito y accesible.

6. Pruebas periódicas del protocolo
Haz simulacros.

- Prueba que el plan funcione.
- Mide si cumples con los tiempos del RTO y RPO.
- Si algo falla, ajusta el protocolo. No esperes a que el desastre sea real.

7. Registro y auditoría
Cada vez que algo se rompe o se recupera, documéntalo.

¿Qué pasó? ¿Cómo se solucionó? ¿Qué se podría haber hecho mejor? Esto no es para castigar a nadie, sino para aprender y mejorar.

8. Capacitación del personal
No sirve de nada tener el mejor protocolo si nadie sabe usarlo.

Enseña a tu equipo qué hacer. Asigna roles: el que llama al proveedor, el que comunica a los clientes, el que restaura el sistema.

Todos deben saber qué hacer sin entrar en pánico.

9. Revisión y actualización continua
Tu negocio cambia. La tecnología cambia. Los riesgos cambian.

Revisa el protocolo cada vez que cambies de sistema, contrates gente nueva o te enteres de una nueva amenaza.

La ciberseguridad no es una receta fija, es una dieta que se ajusta con el tiempo.

Riesgos:

- Pérdida irreversible de datos no respaldados: lo que no se guardó, se fue para siempre.
- Parálisis operativa prolongada: la empresa queda en pausa, sin poder producir ni vender.
- Sanciones legales por incumplir normas de protección de datos: además del golpe tecnológico, llega la factura jurídica.
- Pérdida de clientes por la interrupción prolongada: cuando el servicio no responde, la confianza se rompe y muchos no vuelven.

Ventajas de tomar medidas apropiadas:

- Reducción del tiempo de inactividad.
- Cumplimiento normativo.
- Preservación de la confianza del cliente.
- Disminución de pérdidas económicas.
- Robo de datos durante la recuperación si no hay medidas de seguridad.

¿Por qué es importante?

Según estimaciones ampliamente citadas en el sector, el 58 % de las empresas que no cuentan con un plan de recuperación documentado cierran en menos de un año tras sufrir un incidente grave, como un ciberataque o desastre natural. Esta cifra, atribuida originalmente a la Agencia Federal para el Manejo de Emergencias de EE. UU. (FEMA), sigue siendo un llamado de atención para las mipymes que aún no han formalizado sus protocolos de continuidad (IT Masters Mag Network, 2025).

Errores frecuentes:

- Dar por hecho que el backup “se hizo” sin comprobarlo: confiar en la máquina como si fuera infalible.
- No priorizar la información crítica: tratar igual un catálogo viejo que la base de datos de clientes.
- Guardar las copias en el mismo lugar que los datos originales: como tener el duplicado de la llave en la misma bolsa que la original.
- No entrenar al personal en el protocolo: porque el mejor plan en papel se cae si la gente no sabe aplicarlo.
- Usar medios obsoletos o defectuosos: confiar el futuro de la empresa a un disco duro que ya suena como licuadora vieja.

Ejercicio para superar la etapa:

Identificación del incidente. Pregunta: *Ante un ataque de ransomware que cifra archivos críticos, ¿qué acción inicial debería realizar el equipo?*

- ☐ · Apagar inmediatamente todos los servidores.
- ☐ · Aislar los equipos afectados de la red.
- ☐ · Restaurar desde la copia más reciente sin verificar origen del ataque..
- ☐ · Esperar confirmación de la alta dirección para actuar.

√ Respuesta sugerida:
Aislar los equipos afectados de la red

SEGMENTACIÓN DE REDES

Objetivo de esta etapa:

Imagina que tu empresa es un barrio. Si todas las casas estuvieran conectadas con las puertas abiertas, bastaría con que un ladrón entre en una sala para terminar en las cocinas, dormitorios y cajas fuertes. Eso pasa cuando la red está “plana”: un intruso se cuela por un hueco y, de repente, tiene acceso a todo.

La segmentación de redes es como poner rejas, muros y portones en ese barrio digital. Se trata de dividir la infraestructura en subredes o segmentos lógicos-físicos, de modo que un problema quede contenido en una zona y no contagie al resto.

Con esto se logran dos cosas claves:

- **Reducir la superficie de ataque:** al delincuente se le hace más difícil moverse de un lado a otro.
- **Optimizar el rendimiento y el control:** cada zona tiene su propio semáforo, y el tráfico fluye según su nivel de riesgo y necesidad operativa.

En otras palabras: no dejes que el que entra a la recepción pueda, sin querer, terminar en la caja fuerte.

¿Cómo lo logro?

Primero, comprende que no se trata de llenar la red de muros por capricho, sino de poner puertas donde realmente importa.

- Clasifica los activos como quien separa vajilla fina de los platos de plástico: servidores, estaciones, impresoras... cada uno con su etiqueta de criticidad y exposición.
- Crea zonas de seguridad (DMZ, interna, invitados, OT/SCADA, administración). Acá las VLANs y el subnetting son como pasillos: uno lleva a la cocina, otro al depósito, otro al living.

Accede al panel de configuración de tu switch o router (ej. TP-Link, Cisco, MikroTik).

- Crea VLANs (Virtual LANs) para cada zona:
- VLAN 10: Administración
- VLAN 20: Usuarios
- VLAN 30: Invitados
- VLAN 40: Servidores
- VLAN 50: OT/SCADA (si aplica)
- Asigna puertos físicos del switch a cada VLAN.

Pon firewalls internos o ACLs que funcionen como porteros entre segmentos. No todo tráfico es “amigo”.

Configura ACLs (Access Control Lists) en el router o firewall:

- Permitir solo que la VLAN de administración acceda a los servidores.
- Bloquear acceso de la VLAN de invitados a cualquier otra VLAN.
- Usa firewalls como pfSense, OPNsense o Fortinet para definir reglas:

Aisla lo crítico (bases de datos, Backups) como si fueran las reliquias de la abuela: en un cuarto cerrado con llave

Ubica servidores críticos en VLAN exclusiva (ej. VLAN 40).

- Configura acceso solo desde VLAN de administración.
- Activa cifrado en disco (BitLocker, VeraCrypt) y en tránsito (TLS/SSL).
- Desactiva servicios innecesarios (ej. compartir archivos, impresoras).

Monitorea interconexiones con IDS/IPS o SIEM. Es la alarma de movimiento, la que avisa cuando algo se mueve donde no debería.

- Instala un IDS/IPS en un servidor dedicado.
- Configura alertas por correo o dashboard.
- Usa un SIEM como Wazuh, Graylog o Splunk Free para centralizar logs y correlaciones.

Aplica el principio de mínimo privilegio: que cada red tenga acceso solo a lo que necesita. Como darle al vecino la llave del buzón, pero no de tu dormitorio.

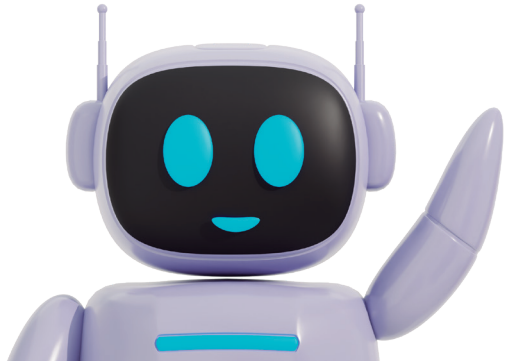
Documenta el mapa de segmentación. Porque en unos meses, cuando alguien pregunte “¿y este cable a dónde va?”, más vale tener el plano a mano y no andar adivinando.

(El siguiente cuadro es un resumen de lo que se debe tener en cuenta en la segmentación de redes, son las restricciones que debe tener una segmentación adecuada)

Objetivo	Acción Concreta	Beneficio Principal
Separar dominios de seguridad	Dividir usuarios, servidores, aplicaciones críticas, IoT/OT en segmentos distintos	Limita el movimiento lateral de atacantes
Aplicar mínimo acceso	Permitir solo comunicaciones estrictamente necesarias entre segmentos	Reduce superficie de ataque
Aislar funciones	Crear VLANs/subredes dedicadas para Finanzas, RH, Producción, Invitados, etc.	Mejora control y visibilidad
Control entre segmentos	Implementar firewalls internos o microfirewalls con reglas L3/L4/L7	Contiene amenazas dentro de cada segmento
Proteger la administración	Separar tráfico de gestión en VLAN exclusiva sin acceso directo de usuarios.	Asegura la infraestructura de red
Aislar sistemas críticos	Separar ICS/SCADA, bases de datos y servidores de identidad	Protege activos de misión crítica
Control granular	Definir ACLs con “deny all by default” y permitir solo flujos autorizados	Refuerza el modelo Zero Trust
Detección temprana	Monitorear y registrar tráfico intersegmentos (NetFlow/sFlow, logs)	Posibilita anomalías y accesos indebidos
Microsegmentación avanzada	Usar SDN o soluciones Zero Trust para políticas dinámicas por identidad y contexto	Aumenta seguridad y flexibilidad; garantiza que el diseño cumpla los objetivos
Validar eficacia	Realizar pruebas de penetración y auditorías periódicas de la segmentación	Garantiza que el diseño cumpla los objetivos

Riesgos:

- **Movimiento lateral sin restricciones:** Un atacante que compromete un equipo puede desplazarse libremente por toda la red.
- **Ampliación del impacto de un ciberataque:** Un ransomware o gusano puede propagarse rápidamente a toda la organización.
- **Fuga de información sensible:** Datos confidenciales pueden extraerse sin barreras de control ni detección.
- **Interrupción total de la operación:** Un ataque afecta simultáneamente áreas administrativas, productivas y de servicios esenciales.



Ventajas de tomar medidas apropiadas:

- Contención de incidentes en un solo segmento afectado.
- Mayor visibilidad y control del tráfico.
- Reducción del impacto de ciberataques.
- Cumplimiento de normativas principalmente la ISO 27001
- Optimización del rendimiento y reducción de colisiones-broadcast innecesarios.

¿Por qué es importante?

- Verizon DBIR (2024) cuenta que el 45% de las brechas en empresas no vinieron por la puerta de adelante, sino porque el atacante se paseó de cuarto en cuarto (movimiento lateral) como si nada. Una segmentación decente los hubiera dejado encerrados en el baño.

- IBM Security (2023) dice que, cuando segmentas bien, ahorras en promedio USD $1.5 millones por incidente. Es decir, con lo que se evita perder en una sola fuga, puedes pagar toda la infraestructura nueva... y todavía te sobra para el café de la oficina.

Errores frecuentes:

- Crear VLANs pero no configurar reglas de control entre ellas (segmentación “falsa”).
- No aislar servidores de administración o backups.
- Falta de monitoreo en los puntos de interconexión.
- No actualizar la segmentación cuando cambia la infraestructura.

Ejercicio para superar la etapa:

Contexto:
Una empresa financiera detecta intentos de intrusión en su red corporativa. El CISO pide implementar segmentación de red para minimizar el impacto de un posible ataque.

1. Objetivo principal de segmentar una red

- ☐ · Mejorar la estética del cableado.
- ☐ · Limitar el movimiento lateral de un atacante dentro de la red.
- ☐ · Aumentar el ancho de banda de Internet.
- ☐ · Cumplir con normativas de seguridad y privacidad.

Respuesta sugerida:
√ Limitar el movimiento lateral de un atacante dentro de la red.
√ Cumplir con normativas de seguridad y privacidad.

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Imagina que sales a rodar con tu bici por la ruta. El sol está perfecto todo parece ir sobre ruedas. Pero a los 20 km, ¡pum! te pinchas. Miras la llanta y te das cuenta de que no trajiste, ni kit de parches, ni inflador. Tienes dos opciones: empujar la bici hasta la ciudad más cercana (perdiendo la carrera, el día y probablemente la paciencia) o esperar a que alguien se apiade de ti.

Eso mismo le pasó a una Mipyme de confecciones en Medellín: tenían toda su base de clientes y proveedores guardada en un único servidor, sin pruebas de respaldo. Una mañana, un ataque de ransomware encriptó todo. Como nunca habían probado sus copias de seguridad, descubrieron tarde que estaban corruptas. Perdieron contratos, clientes y hasta recibieron demandas por incumplimiento. Fue el equivalente empresarial a quedarse tirado en la ruta, sin repuestos y con la carrera perdida.

¿Qué te recomendamos? llevar el kit en la maleta.

La solución es simple pero vital, siempre cuenta con tu rueda de repuesto y pruébala antes de salir. En términos digitales, eso significa:

- Hacer pruebas de integridad de los datos (asegúrate que el archivo no esté dañado).
- Hacer pruebas de restauración periódicas en un servidor de prueba (como inflar la cámara de repuesto antes de guardarla).
- Guardar los *backups* en diferentes lugares (local y nube), no todos en la misma “alforja”.

De esa forma, si te pinchas en medio de la ruta (pérdida de datos, ataque o corrupción del sistema), simplemente sacas el repuesto, lo montas y sigues pedaleando. Eso garantiza la continuidad del negocio y evita la vergüenza de quedarte “tirado” frente a tus clientes.

DETECCIÓN

Ya inflaste las llantas, revisaste los frenos y cargaste la caramañola. O sea, ya previniste todo lo prevenible. Pero los que pedaleamos sabemos una verdad incómoda: aunque revises la bici mil veces, siempre hay cosas que se te escapan. Un perro que se cruza, un hueco que no viste, un carro que abre la puerta justo cuando pasas. La ruta siempre tiene imprevistos.

En la ciberseguridad pasa lo mismo. Puedes tener los mejores backups, protocolos y accesos blindados, pero el peligro aparece igual. Y no siempre avisa. Por eso esta segunda fase de la RutaCibersegura es la etapa de Detección. Acá aprendes a tener el ojo entrenado, a escuchar cuando la cadena empieza a sonar raro, a ver la sombra de un auto que se te viene encima, a detectar la amenaza antes de que te haga caer.

En este tramo de la ruta vas a aprender a:

- **Detectar riesgos** con la inteligencia artificial, esa que puede disfrazar un *phishing* de correo real o inventar un video tuyo diciendo lo que nunca dijiste.

- **Tener seguridad en las videollamadas y herramientas colaborativas**.

La detección es eso: entrenar el ojo y el oído para reaccionar a tiempo. Es ver la grieta en el asfalto antes de que te quiebre la rueda, o escuchar un silbido raro y saber que la llanta está por pinchar. Si aprendes a detectar, no evitas todos los problemas, pero sí reducís el golpe y ganas tiempo para maniobrar.

Así que ajusta la visera del casco, ponte atento y no te confíes: esta parte de la **RutaCibersegura** es de reflejos rápidos.

RIESGOS CON LA INTELIGENCIA ARTIFICIAL (IA)

Objetivo de esta etapa:

La idea es simple, no esperar el golpe, sino cubrirse antes. Hoy los ataques no vienen con pasamontañas, vienen con inteligencia artificial. Correos que parecen escritos por tu mamá, audios que suenan igualito a tu jefe, trampas digitales que se activan mientras duermes.

Por eso, el objetivo es claro: anticiparse. Que la defensa no sea un chaleco agujereado después del balazo, sino un muro que detecta al impostor, al video falso y a los ataques automáticos que aprovechan fallas invisibles en tus sistemas antes de que entren.

¿Cómo lo logro?

Entrenando a la tropa

- El primer escudo es la gente. Capacita a tu equipo para que sepa reconocer un correo auténtico de uno escrito con inteligencia artificial.
- Verifica siempre el remitente: que sea alguien conocido y con dirección confiable.
- Desconfía de archivos comprimidos o adjuntos sospechosos.
- Revisa la redacción: los errores ortográficos o frases forzadas son señales de alerta.
- Nunca hagas clic en enlaces desconocidos; pueden llevarte a páginas falsas que roban contraseñas.
- Hoy los ataques no llegan con pasamontañas, sino con IA generando phishing avanzado (engaños digitales muy realistas) y deepfakes (videos o audios falsos que imitan voces y rostros). No se trata de paranoia, sino de entrenamiento: que nadie caiga en la trampa del “jefe” pidiendo dinero por WhatsApp o del correo que parece urgente pero huele raro.

Vigilando la IA propia y la ajena:

- La IA es útil, pero también puede volverse un caballo de Troya si no se controla.
- Aquí entra el concepto de **Shadow AI**: cuando los empleados usan herramientas de inteligencia artificial sin informar al área de tecnología.
- Parece inofensivo (“solo le pedí a ChatGPT que me ayudara con un correo”), pero puede implicar fuga de datos sensibles o exposición de información interna
- Por eso, establece una **política clara de uso de IA**, donde se definan qué herramientas están aprobadas, cómo se usan y qué tipo de datos nunca deben compartirse.

Eliminando las herramientas truchas:

- No todo lo que brilla es IA confiable. Existen aplicaciones que prometen productividad, pero en realidad instalan **malware** (software malicioso) o abren brechas de seguridad.
- Antes de instalar cualquier herramienta, verifica su **origen, reputación y permisos solicitados.**
- Si pide acceso a todo (archivos, micrófono, cámara, ubicación), desconfía. Mejor pocas herramientas seguras que muchas peligrosas.

Poniendo reglas firmes de acceso y control

- Así como nadie entra a la caja fuerte sin autorización, las plataformas de IA y los sistemas de la empresa deben tener **controles de acceso estrictos.** Define quién puede entrar, con qué permisos y en qué momentos.
- Usa **autenticación multifactor** (por ejemplo, contraseña más código por celular) y gestión de identidades para evitar accesos indebidos.
- También vigila las **APIs**, que son como puentes que conectan diferentes sistemas. Una **API (Application Programming Interface)** es un conjunto de reglas que permite que dos programas se comuniquen entre sí.
- Si ese puente no está protegido, un atacante podría usarlo como entrada. Supervísalas como un banco: con registros (logs), alertas y revisiones periódicas que aseguren que nadie se cuela por ahí.

Riesgos:

- Automatización masiva de ataques
- Incremento del robo de credenciales
- Campañas hiperrealistas con alta tasa de efectividad.
- El 20 % de brechas se deben a uso no autorizado de IA, y solo el 3 % de empresas tiene controles adecuados (IBM Cost of a Data Breach Report, 2025).

Ventajas de tomar medidas apropiadas:

- Respuesta más rápida y precisa a amenazas emergentes.
- El informe IBM Cost of a Data Breach Report 2024 establece que el costo promedio global de una brecha de datos fue de USD 4.88 millones
- Secureframe: Es una plataforma SaaS (software como servicio) que ayuda a las empresas a automatizar y simplificar el cumplimiento de normas de seguridad y privacidad) es una Ventaja competitiva, mayor seguridad y cumplimiento regulatorio.

¿Por qué es importante?

- El 87 % de las organizaciones ha enfrentado ataques impulsados por inteligencia artificial en el último año, según las investigaciones presentadas en Cybercrime Trends 2025 de SoSafe (SoSafe, 2025).

- El periódico Axios reporta (2025), basándose en una investigación de Deep Instinct, que el 45 % del sector financiero ha sido objetivo de ataques IA (phishing, deepfake, malware)

Errores frecuentes:

- Pensar que un antivirus del 2010 te va a salvar de un phishing hecho por IA en 2025.
- Hacerte el de la vista gorda con las herramientas de IA que los equipos usan sin permiso, el famoso “Shadow AI”, como si no fueran un problema.
- Creer que los deepfakes son solo chistes de TikTok y no una amenaza seria para tu empresa.
- No entrenar a la gente en estas trampas modernas, como si aprendieran por osmosis.

Ejercicio para superar la etapa:

Instrucciones:
Lea cada afirmación y seleccione las opciones que considere representan un riesgo real del uso de la IA en ciberseguridad.

1. Generación de phishing y smishing con IA

- ☐ La IA puede generar correos o mensajes fraudulentos con errores ortográficos y fácilmente detectables.
- ☐ La IA puede crear mensajes muy realistas, personalizados y difíciles de distinguir de comunicaciones legítimas.
- ☐ La IA no tiene impacto en la efectividad del phishing.

Respuesta sugerida:
√ La segunda opción.

SEGURIDAD EN VIDEOCONFERENCIAS Y HERRAMIENTAS COLABORATIVAS

Objetivo de esta etapa:

Blindar las videoconferencias y los espacios colaborativos como si fueran una sala cerrada con llave. Se trata de cuidar la confidencialidad, la integridad y la disponibilidad de la información, evitando que un curioso no invitado se cuele, que los datos se filtren como agua por las rendijas o que la privacidad se rompa por descuido.

¿Cómo lo logro?

Algunas recomendaciones para evitar un Ciberataque en el uso de estas tecnologías son las siguientes:

Usar enlaces seguros con contraseñas o autenticación para entrar a las reuniones.

- Habilitar la sala de espera para aprobar manualmente a los participantes.
- Desactivar grabaciones automáticas si no son necesarias.
- Restringir el uso de pantalla compartida solo al anfitrión o a personas autorizadas.
- Actualizar regularmente el software para cerrar vulnerabilidades.
- Evitar usar redes Wi-Fi públicas o no seguras para reuniones.
- Usar nombres reales y perfiles corporativos para identificar participantes.
- Desactivar micrófonos y cámaras de manera predeterminada para invitados.

Según TechJury (2024), Zoom lidera el mercado global de videoconferencias con un 43 % de participación y más de 300 millones de reuniones diarias. En Colombia, aunque no hay cifras precisas, se mantiene como una de las más usadas, junto a Microsoft Teams y Google Meet. Otras como Webex, GoToMeeting y Jitsi Meet destacan en sectores que valoran seguridad o software abierto.

Riesgos:

- Intrusión no autorizada (“Zoombombing”)
- Filtración de información confidencial por grabaciones o capturas no autorizadas.
- Suplantación de identidad de participantes.
- Robo de credenciales mediante enlaces falsos.
- Malware distribuido por archivos compartidos.

Ventajas de tomar medidas apropiadas:

- Protección de información crítica.
- Cumplimiento de normativas como Ley de Habeas Data.
- Mayor confianza de clientes y empleados.
- Reducción de ataques de ingeniería social.
- Flujo de trabajo más ordenado y seguro.
- Menor riesgo de sanciones legales.

¿Por qué es importante?

- En 2020, cuando gran parte del mundo adoptó las videollamadas como medio principal de comunicación, Zoom reportó un aumento del 500 % en los intentos de ingreso no autorizado a reuniones, lo que reflejó la magnitud de los riesgos de seguridad asociados al uso masivo de plataformas digitales (Zoom, 2020).
- Asimismo, Fortinet (2020) advirtió que uno de cada tres ataques durante el teletrabajo no provenía de grupos de ciberdelincuentes altamente sofisticados, sino del uso inadecuado de las propias herramientas colaborativas que permitían mantener la conexión entre los equipos.

Errores frecuentes:

- Compartir el enlace de la reunión por redes sociales o chats no seguros.
- Usar la misma ID de reunión para todas las sesiones.
- No configurar permisos antes de iniciar la videollamada.
- Olvidar cerrar la sesión o expulsar a usuarios al final.
- No capacitar al personal en el uso seguro de la herramienta.
- Descargar archivos sin verificar su procedencia. Usar contraseñas débiles o repetidas.

Ejercicio para superar la etapa:

1. Configuración de reuniones virtuales

Al crear una videollamada, ¿qué medidas fortalecen la seguridad?

- ☐ Compartir el enlace en redes sociales para que todos puedan acceder.
- ☐ Usar contraseñas de reunión y salas de espera.
- ☐ Limitar el acceso solo a usuarios autenticados.
- ☐ Permitir que cualquier participante pueda iniciar la reunión antes del anfitrión.

Respuesta sugerida:

√ La segunda y tercera opción.

GESTIÓN DE VULNERABILIDADES Y PARCHES

Objetivo de esta etapa:

La gestión de vulnerabilidades y parches consiste en mirar a los sistemas con lupa, encontrar dónde están las grietas, medir qué tan peligrosas son, ponerlas en orden de urgencia y cerrarlas a tiempo. Todo esto para evitar que alguien las aproveche, reducir el riesgo de incidentes y cumplir con lo que exigen las normativas.

¿Cómo lo logro?

- Inventario actualizado de hardware, software y servicios.
- Aplicar parches críticos primero, especialmente en sistemas expuestos a internet. Recordemos que los parches son una actualización puntual liberada por el fabricante para corregir errores, cerrar vulnerabilidades de seguridad o mejorar la funcionalidad de un programa sin necesidad de reinstalarlo por completo.
- Mantener entornos de pruebas para validar los parches antes de producción.
- Automatizar actualizaciones cuando sea posible.

Riesgos:

- Explotación de vulnerabilidades conocidas (ataques automatizados en minutos)
- Pérdida de información confidencial. Interrupciones del negocio por Ransomware o sabotaje.
- Sanciones legales por incumplir regulaciones (ej. GDPR, Ley 1581 en Colombia). Daño reputacional irreversible.

Ventajas de tomar medidas apropiadas:

- Reducción significativa del riesgo de ciberataques.
- Mayor estabilidad y rendimiento de sistemas.
- Cumplimiento de normativas y auditorías.
- Menor costo de recuperación ante incidentes.
  Confianza de clientes y socios comerciales.

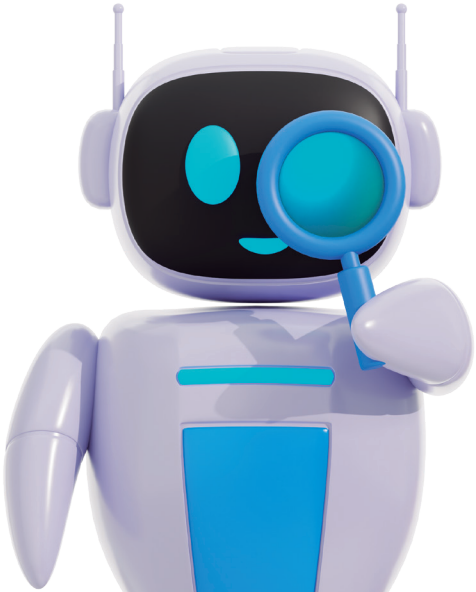
¿Por qué es importante?

Porque la mayoría de los ataques no nacen de vulnerabilidades nuevas, sino de viejas grietas que nadie tapó. En 2024, el 80% de las vulnerabilidades explotadas tenían más de un año de antigüedad (Verizon DBIR). Más de la mitad de las organizaciones un 57% sufrieron incidentes simplemente por no aplicar parches a tiempo (Ponemon Institute, 2024). Y en nuestra región, la realidad es más cruda, el 65% de los ataques de ransomware en América Latina en 2023 se debieron a fallas de parcheo (Fortinet LATAM Threat Report, 2023).

En otras palabras, no parchar es como dejar la puerta abierta y esperar que nadie entre.

Errores frecuentes:

- No incluir sistemas antiguos o “legado” en el plan.
- No probar parches antes de aplicarlos.
- Falta de priorización (actualizar cosas irrelevantes antes que lo crítico).
- No documentar los cambios.
- Depender solo de actualizaciones automáticas sin monitoreo.



Ejercicio para superar la etapa:

Buenas prácticas de parcheo

¿Cuáles son prácticas recomendadas en un programa de gestión de parches?

- ☐ Probar los parches en un ambiente controlado antes de aplicarlos en producción.
- ☐ Documentar los cambios realizados en cada actualización.
- ☐ Aplicar los parches solo cuando ocurra un incidente.
- ☐ Definir ventanas de mantenimiento regulares.

Respuesta sugerida (instructor):

√ Probar en ambiente controlado.

√ Documentar cambios.

√ Definir ventanas regulares.

ACCESO REMOTOS Y TELETRABAJO

Objetivo de esta etapa:

Garantizar que los usuarios puedan conectarse de forma segura a los recursos de la Empresa desde ubicaciones externas, protegiendo la confidencialidad, integridad y disponibilidad de la información y de los sistemas de información.

¿Cómo lo logro?

- Usar siempre una VPN corporativa segura para conectarse.
- Habilitar la autenticación multifactor (MFA) en los accesos.
- Mantener el equipo actualizado con parches y antivirus al día.
- Contar solo con los permisos mínimos necesarios para las funciones.
- Separar el acceso remoto de los sistemas críticos mediante segmentación.
- Monitorear y registrar las conexiones remotas en la organización.
- Estar capacitado en ciberseguridad y detección de amenazas.

Riesgos:

- Aumento exponencial de phishing y Ransomware.
- Pérdida de visibilidad y control para investigaciones ante incidentes
- Credenciales robadas y dispositivos inseguros.

Ventajas de tomar medidas apropiadas:

- Garantizar la continuidad operativa
- Proteger datos sensibles
- Reducir riesgos de ciberataques en entornos remotos

¿Por qué es importante?

Un estudio de Help Net Security (2025) reportó que, según una encuesta a profesionales de riesgo en empresas del Reino Unido:

- El 64 % de las empresas dijeron haber sufrido un ciberataque o brecha en los últimos 18 meses.
- Y de esas empresas, el 82 % afirmó que la brecha fue causada por problemas tecnológicos o de comportamiento relacionados con el trabajo desde casa.

Errores frecuentes:

- Uso de dispositivos personales sin protección ni administración centralizada
- Falta de formación en seguridad
- Políticas débiles o inexistentes de protección de datos y respuesta ante incidentes.

Ejercicio para superar la etapa:

Dispositivos en Teletrabajo

Pregunta: ¿Qué prácticas son correctas respecto al uso de dispositivos en teletrabajo?

- [ ] Permitir el uso de equipos personales sin control de seguridad.
- [ ] Mantener software y parches actualizados
- [ ] Instalar y mantener activo un EDR/antivirus corporativo
- [ ] Deshabilitar cifrado de disco para mejorar el rendimiento

Respuesta sugerida: √ Actualizaciones +√ EDR/antivirus corporativo. √ No equipos personales sin control ni deshabilitar cifrado.

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Imagina que vas pedaleando tranquilo por la ciclovía de tu barrio. Tienes casco, chaleco reflectivo y hasta la botellita de agua bien fría: todo lo que aprendiste en la fase de prevención. Pero de repente, se te cruza un auto que no debería estar en la ciclovía.

Ese auto es un correo electrónico que parece legítimo, con logo de la DIAN, con tu nombre completo, tono formal y hasta una firma digital que parece real. Lo abres (porque confías) y ahí está: un enlace que dice “revise su estado tributario urgente”.

Lo que no sabías es que el correo fue escrito por una IA. Una de esas que no se equivoca con las tildes, que sabe tu cargo en LinkedIn, que usa el tono exacto con el que hablaría tu contador.

El clic equivocado en ese enlace equivale a frenar de golpe con la bicicleta en una alcantarilla sin tapa: caes de frente y te cuesta caro.

¿Cómo actuar frente a este tipo de situaciones?

- Por suerte, en la empresa ya habían hecho simulacros de phishing con IA. Uno de los empleados, antes de cliquear, notó que la URL no era “.gov.co” sino “.g0v.co” (con un cero). Esa mínima sospecha disparó la alerta:
- El correo fue reportado al área de Tecnología.
- El enlace se bloqueó en los filtros.
- Se envió un aviso interno explicando por qué era un intento de suplantación.

El incidente quedó en un susto y no en una catástrofe. Fue como esquivar el auto en la ciclovía gracias al timbre de tu bici y a estar bien atento.

¿Qué medidas deben tomar las empresas?

- Capacitación previa: el equipo sabía cómo lucen los deepfakes de correos.
- Políticas claras: solo se responden comunicaciones tributarias desde la plataforma oficial de la DIAN, nunca desde correos.
- Monitoreo IA: se revisan patrones de correos entrantes para detectar automatización sospechosa.

CORRECCIÓN

Imagina lo siguiente: vienes pedaleando tranquilo en tu ruta cibersegura, con casco, luces, chaleco reflectivo, hasta con timbre de bicicleta nuevo. Hiciste todo lo que había que hacer en prevención. También aprendiste a detectar riesgos, viste venir al perro que se te quería cruzar, esquivaste el hueco a tiempo, te diste cuenta de que la moto venía sin luces. Pero, de golpe, se te pincha la llanta. No importa cuánta prevención ni detección hayas hecho, ahora lo único que queda es bajarte, arremangarte y arreglar la pinchadura.

Eso es la fase de corrección. Es el momento en el que dejamos de especular con "qué pasaría si" y pasamos al "ya pasó, y ahora qué". Acá no sirve llorar sobre la leche derramada ni buscar culpables; lo que importa es cómo corregimos rápido, con método y sin perder el rumbo.
En esta etapa vas a aprender a:

- **Activar protocolos de denuncia:** ¿A quién aviso si me hackearon la cuenta corporativa? ¿Cómo documento el incidente? ¿Qué autoridad me puede respaldar en Colombia?

- **Contactar a las autoridades:** existe un camino formal para no pelear esta batalla solo.
- **Ejecutar planes de contingencia:** ese famoso "plan B" que uno siempre promete tener, pero que en ciberseguridad es vital. Desde restaurar respaldos hasta redirigir operaciones a canales seguros.
- **Aplicar herramientas de corrección:** desde parches de emergencia hasta bloqueos inmediatos de accesos, cambios de contraseñas, auditorías exprés.

La corrección es un poco como tener un kit de reparación en la bici: palancas, parches, pegamento. Nadie quiere usarlo, pero cuando lo necesitas, te alegras de haberlo cargado durante toda la ruta.

Lo bueno es que, si llegaste hasta acá, ya tienes experiencia: entendiste que la seguridad digital no es un seguro de vida que se paga una vez y listo, sino una ruta con curvas, subidas y bajadas. Y ahora estás en la parte final del recorrido.

Así que, ánimo. La fase de corrección no es un fracaso, es la confirmación de que tu negocio está listo para levantarse de un golpe y seguir pedaleando. Porque lo verdaderamente inseguro no es que te pase algo; lo inseguro es no tener idea de qué hacer cuando te pasa.

PROTOCOLOS DE DENUNCIA ANTE CIBERDELITO CONSUMADO

Objetivo de esta etapa:

Proporcionar una guía clara y estandarizada para que, una vez detectado y confirmado un ciberdelito, la víctima (particular o empresa) pueda documentar, preservar evidencia y denunciar formalmente, maximizando las posibilidades de recuperación de activos y judicialización del responsable.

¿Cómo lo logro?

- Preservar evidencia digital inmediatamente: no apagar equipos, no borrar mensajes, no formatear dispositivos.
- Documentar cronológicamente el incidente (fechas, horas, acciones, capturas de pantalla, correos).
- Notificar al área de Tecnología o ciberseguridad interna antes de informar externamente, para contener el incidente.
- Informar a proveedores/servicios afectados (banco, redes sociales, proveedor de hosting) para *bloquear* accesos.
- Mantener la cadena de custodia de la evidencia (bitácoras, logs, dispositivos, mensajes originales). Para este fin debemos tener en cuenta:
  - Recolectar la evidencia de forma controlada (logs, discos, mensajes originales).
  - Registrar quién la obtiene, fecha, hora, método y lugar (bitácora o formulario de cadena de custodia).
  - Proteger contra alteraciones (hashes, copias forenses, almacenamiento seguro).
  - Transferir solo a personal autorizado, documentando cada entrega.
  - Almacenar en entornos seguros hasta su análisis o uso legal.
- No negociar con atacantes en casos de ransomware o extorsión, salvo instrucción de autoridades.
- Denunciar ante autoridades competentes:
- CAI Virtual de la Policía Nacional y Centro Cibernético Policial (CCP).
- Fiscalías con unidades de delitos informáticos.

Riesgos:

- Pérdida irreversible de evidencia que impida investigación.
- Imposibilidad de rastrear al autor por falta de datos técnicos.
- Sanciones legales si el incidente involucró datos personales y no se notificó (Ley de Habeas Data en Colombia).
- Reputación dañada por filtraciones no controladas.
- Aumento de ataques por aparecer como objetivo “vulnerable” ante redes criminales.

Ventajas de tomar medidas apropiadas:

- Mayor probabilidad de identificación y judicialización del atacante.
- Posibilidad de recuperación de activos o reversión de operaciones fraudulentas.
- Cumplimiento normativo y reducción de sanciones.
- Mejora de la postura de seguridad y credibilidad de la organización.

¿Por qué es importante?

- Interpol (2024): solo el 27% de las víctimas de cibercrimen en Latinoamérica denuncian formalmente.
- Centro Cibernético Policial – Colombia (2023): más de 58.000 denuncias por ciberdelitos, con un subregistro estimado del 60%.
- IBM Security: las empresas que notifican incidentes en menos de 72 horas reducen el impacto económico en un 40% en promedio.

Errores frecuentes:

- Borrar chats, correos o registros “para limpiar” antes de denunciar.
- No capturar metadatos junto con la evidencia (IP, hora, URL completa). Recordemos que los metadatos se capturan principalmente desde logs, registros de red, sistemas y archivos, y deben almacenarse de forma íntegra para que nos sirvan como constancia verificable de lo ocurrido.
- Pensar que si la pérdida es pequeña “no vale la pena” denunciar.
- Denunciar solo verbalmente, sin entregar evidencia documental.
- No seguir los canales oficiales y usar redes sociales para pedir ayuda (lo que puede alertar al atacante).

Ejercicio para superar la etapa:

Ejercicio práctico – Protocolo de Denuncia de Ciberdelito Consumado

Caso base:

Un empleado de la empresa detecta que le vaciaron la cuenta bancaria tras haber recibido un correo fraudulento con un enlace de phishing. El área de TI confirma que hubo exfiltración de credenciales corporativas.

Confirmación inicial del incidente:

- [ ] ¿Se ha verificado que efectivamente se trata de un ciber-delito consumado?
- [ ] Sí, con evidencia técnica (logs, capturas, hash de archivos maliciosos).
- [ ] Sí, con reporte del afectado y validación mínima.
- [ ] No, aún es sospecha sin validar.

Respuesta sugerida: Lo ideal es tener validación técnica preliminar (logs, evidencias) antes de pasar a la denuncia formal.

CIBERACOSO Y CANALES DE DENUNCIA

Objetivo de esta etapa:

Prevenir, detectar y responder de manera efectiva al ciberacoso en entornos digitales, fomentando un uso seguro y respetuoso de la tecnología y protegiendo la integridad psicológica y reputacional de las personas. A continuación, citamos una clasificación por género en cuanto a ciberacoso:

Afecta más a las mujeres

- Misoginia, acoso sexual, amenazas de violación.
- Cyberstalking y envío de imágenes explícitas no solicitadas
- Revenge porn exposición no consentida de fotos íntimas
- Ciberhostigamiento indirecto: humillaciones, difamaciones, exclusión social

Afecta más a los hombres

- **Insultos ofensivos en línea**
- **Amenazas físicas**

Entidades a las que se puede acudir para denuncia o atención del ciberacoso:

Centro Cibernético Policial – Policía Nacional: recibe denuncias de delitos informáticos, incluyendo ciberacoso. Puedes reportar casos directamente en su sitio oficial.

Fiscalía General de la Nación: permite presentar denuncias penales cuando el ciberacoso afecta la honra, salud mental o seguridad de la víctima.

Plataforma Te Protejo: canal virtual para denunciar contenidos ilegales y situaciones de ciberacoso, especialmente en menores. Disponible en www.teprotejo.org y como app móvil.

¿Cómo lo logro?

Educar al personal: capacita a todo el equipo para reconocer qué es el ciberacoso y cómo se manifiesta. Explica

las distintas formas de violencia digital y cómo pueden afectar de manera diferenciada a hombres y mujeres. Ejemplos: publicación de fotos sin consentimiento, insultos por orientación sexual, burlas por apariencia, etc.

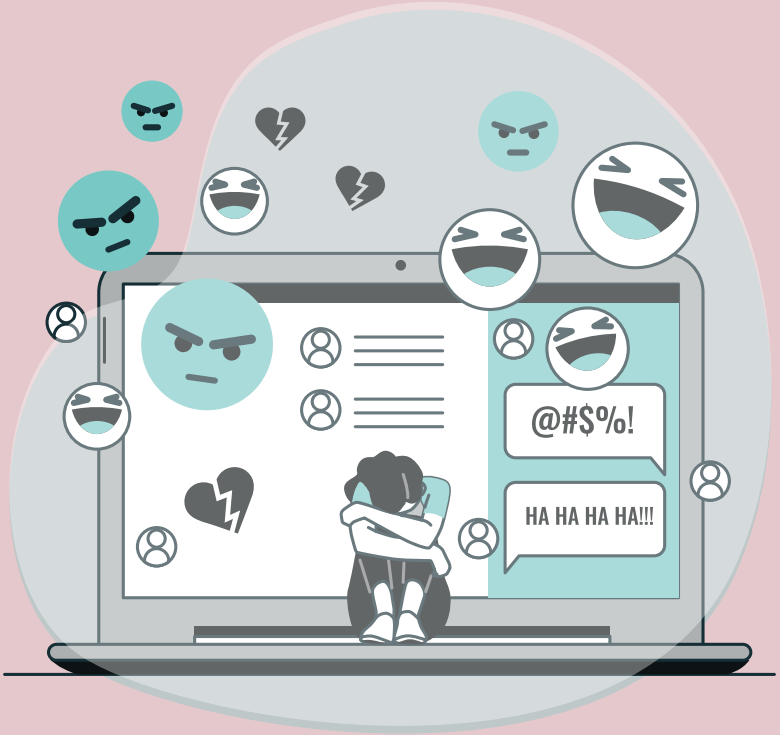
Implementar políticas claras de comportamiento digital: incluye cláusulas sobre respeto en redes corporativas, videollamadas, mensajería interna y correos electrónicos. Define qué conductas constituyen acoso y cuáles serán las sanciones.

Crear canales confidenciales de denuncia: un correo institucional exclusivo o buzón digital seguro. Posibilidad de denuncia anónima si la persona teme represalias. Designar responsables capacitados en enfoque de género y atención psicosocial.

Documentar las evidencias: conservar capturas de pantalla, mensajes, correos, URLs y cualquier rastro digital del hecho. Estos materiales son fundamentales para la investigación.

Actuar rápido y en coordinación: cuanto más se demore la respuesta, mayor será el daño. Involucra Recursos Humanos, el área legal y el área de seguridad informática en los primeros pasos de atención.

Promover la empatía digital: fomenta una cultura donde se entienda que la violencia digital también es violencia real, que deja huellas psicológicas, sociales y laborales.



Riesgos:

- Daño a la salud mental (ansiedad, depresión, estrés laboral).
- Pérdida de talento (renuncias por ambiente hostil).
- Riesgo reputacional de la empresa.
- Posibles demandas legales y sanciones por inacción.
- Disminución de productividad por clima laboral deteriorado.
- Conflictos internos prolongados.
- Filtración de datos personales como forma de hostigamiento.

Ventajas de tomar medidas apropiadas:

- Entorno laboral o académico más sano y colaborativo.
- Mayor confianza de empleados o estudiantes en la institución.
- Reducción del riesgo legal y reputacional.
- Mejora en la retención de personal.
- Incremento en productividad y compromiso.
- Refuerzo de la cultura organizacional positiva.

¿Por qué es importante?

- El 73% de las empresas no tienen protocolos claros para actuar frente al ciberacoso (Estudio Kaspersky, 2023).
- En entornos educativos, la UNESCO reporta que 1 de cada 3 jóvenes ha sufrido acoso en línea.
- En Latinoamérica, la OEA ha identificado un crecimiento del 40% en casos reportados de ciberacoso laboral desde 2020.

Errores frecuentes:

- No tomar en serio las primeras denuncias.
- Creer que “solo es una broma” o que “en línea no es tan grave”.
- Falta de protocolos claros de acción.
- No guardar evidencias.
- Responder de forma impulsiva al agresor.
- No involucrar al área legal o de seguridad.

Ejercicio para superar la etapa:

Medidas inmediatas de protección
Frente a una situación de ciberacoso,
¿qué medidas inmediatas son recomendadas?

- ☐ Guardar capturas de pantalla como evidencia.
- ☐ Bloquear al acosador.
- ☐ Responder con insultos para defenderse.
- ☐ Configurar mayor privacidad en redes sociales.

Respuesta sugerida: √ Guardar evidencia, √ Bloquear, √ Aumentar privacidad. X Responder con insultos.

PLANES DE CONTINGENCIA Y CONTINUIDAD

Objetivo de esta etapa:

Garantizar que la organización pueda responder, recuperarse y continuar operando después de un ciberataque o incidente de seguridad, minimizando el impacto en operaciones, finanzas y reputación.

¿Cómo lo logro?

- Identificar activos críticos (servidores, bases de datos, aplicaciones, redes).
- Realizar un Análisis de Impacto al Negocio (BIA) para priorizar procesos. Recomendamos:
  - Identificar procesos críticos: listar las actividades esenciales del negocio.
  - Definir dependencias: recursos, sistemas, personal y proveedores necesarios para cada proceso.
  - Evaluar impacto: medir consecuencias de la interrupción (financieras, legales, reputacionales).
  - Determinar RTO y RPO: tiempo máximo de inactividad y tolerancia de pérdida de datos.
  - Priorizar procesos: ordenar de mayor a menor criticidad según el impacto.
  - Documentar y aprobar: generar informe y validarlo con la dirección.
- Definir tiempos de recuperación (RTO) y puntos de recuperación (RPO) claros.
- Crear procedimientos escritos y actualizados para cada escenario posible.
  - Identificar escenarios críticos
    Ej. Ransomware, caída de red, fuga de datos, indisponibilidad de nube.
  - Definir responsables y roles
    Establecer quién actúa, cómo y en qué orden durante cada incidente.

- Redactar procedimientos claros y accionables
  Incluir pasos concretos, contactos, accesos alternos y criterios de escalamiento.

- Validar y aprobar los documentos
  Revisar con equipos técnicos, legales y de negocio antes de oficializarlos.

- Actualizar periódicamente
  Ajustar tras auditorías, incidentes reales o cambios en infraestructura.

- Capacitar al personal
  Entrenar a los equipos con simulacros y ejercicios de mesa (tabletop exercises).

- Almacenar y distribuir copias seguras
  Asegurar disponibilidad física y digital de los procedimientos (en sitio y fuera de sitio).

- Asignar roles y responsabilidades en un equipo de respuesta a incidentes.

- Incluir planes alternos de comunicación (por ejemplo, correo fuera de la red corporativa).
- Realizar simulacros periódicos para probar la efectividad del plan.
- Mantener copias de seguridad fuera de línea o en la nube segura.
- Documentar proveedores críticos y contactos de emergencia.
- Actualizar el plan después de cada incidente o simulacro.

Riesgos:

- Paralización total del negocio durante horas o días.
- Pérdida permanente de datos críticos.
- Sanciones legales y regulatorias (por incumplimiento de normativas como GDPR o Habeas Data).
- Pérdida de clientes y reputación.
- Costos de recuperación hasta 10 veces mayores que si existiera un plan.
- Mayor vulnerabilidad a ataques repetidos.

Ventajas de tomar medidas apropiadas:

- Recuperación más rápida y organizada.
- Menor pérdida de ingresos y productividad.
- Protección de la imagen y confianza del cliente.
- Cumplimiento con regulaciones y auditorías.
- Capacidad de mantener operaciones críticas en medio de un ataque.

¿Por qué es importante?

- Según IBM Cost of a Data Breach 2024, las empresas que tienen un plan probado de continuidad reducen el costo de un incidente en un 43%.
- Gartner (2024) indica que el 93% de las empresas que sufren una pérdida grave de datos y no tienen plan de continuidad cierran en menos de 1 año.
- El Ponemon Institute (2025) reporta que las organizaciones que realizan pruebas de su plan recuperan operaciones 2.5 veces más rápido.

Errores frecuentes:

- No actualizar el plan después de cambios en infraestructura.
- No probar el plan con simulacros reales.
- Depender solo de respaldos sin procedimientos claros.
- No considerar la comunicación interna y externa durante el incidente.
- Asumir que la nube es “automáticamente segura” y no requiere respaldo.
- No incluir la cadena de suministro y terceros críticos.

Ejercicio para superar la etapa:

Contexto del ejercicio
Tu empresa ha detectado un ataque de Ransomware que encriptó el 70% de sus servidores críticos. Debes evaluar si los planes de contingencia y continuidad definidos son adecuados para garantizar la operación.

Evaluación del Plan de Contingencia y Continuidad
1. Identificación de Procesos Críticos

¿Cuál es el primer paso ante un incidente grave como un ransomware?

- ☐ Reiniciar los servidores afectados inmediatamente
- ☐ Identificar procesos y sistemas críticos afectados.
- ☐ Pagar el rescate al ciberdelincuente.

Respuesta sugerida: B – se deben priorizar los procesos críticos antes de actuar)

SEGURIDAD EN DISPOSITIVOS MÓVILES

Objetivo de esta etapa:

Proteger los dispositivos móviles y la información personal/empresarial que contienen, evitando que apps maliciosas o configuraciones inseguras sean una puerta de entrada para ciberataques, robo de datos o fraude.

¿Cómo lo logro?

- Usar contraseñas y biometría: Bloquea el dispositivo con PIN, huella o reconocimiento facial.
- Mantener el sistema actualizado: Instala parches y actualizaciones de seguridad en cuanto estén disponibles.
- Instalar solo apps confiables: Usa tiendas oficiales (Google Play, App Store) y revisa permisos antes de instalar.
- Activar cifrado: Protege la información en caso de pérdida o robo.
- Habilitar borrado remoto: Permite eliminar datos si el dispositivo es robado.
- Desactivar Wi-Fi y Bluetooth cuando no se usen: Reduce riesgos de ataques por redes inseguras.
- Usar antivirus y soluciones MDM: Detecta malware y permite control centralizado en entornos corporativos.
- Respaldar datos periódicamente: Asegura la recuperación en caso de incidente.
- Educar al usuario: Evita clics en enlaces sospechosos y descargas inseguras.

Riesgos:

- Robo de información personal, financiera o corporativa.
- Instalación de malware, ransomware o spyware.
- Uso no autorizado de cuentas (redes sociales, correo, banca).
- Suplantación de identidad.
- Pérdida de control del dispositivo.
- Filtración de datos confidenciales (por permisos excesivos o mal uso de apps).

Ventajas de tomar medidas apropiadas:

- Reducción de riesgos de ciberataques móviles.
- Protección de datos sensibles.
- Mayor confianza en el uso de apps y servicios móviles.
- Cumplimiento de normativas de protección de datos (ej. GDPR, Ley 1581 en Colombia).
- Menor probabilidad de costos por incidentes de seguridad.

¿Por qué es importante?

- Check Point Research (2024): 1 de cada 10 dispositivos Android tiene al menos una app maliciosa instalada.
- Symantec/Norton (2024): El 70% de las brechas de datos móviles provienen de apps no seguras.
- Kaspersky Lab (2023): El 25% de los ataques de phishing se originan en dispositivos móviles.

Errores frecuentes:

- Descargar apps piratas o desde sitios web no oficiales.
- Ignorar actualizaciones de seguridad.
- Conceder todos los permisos sin revisarlos.
- No usar bloqueo de pantalla.
- No respaldar la información del dispositivo.
- Guardar contraseñas en texto plano o en apps no seguras.

Ejercicio para superar la etapa:

Ejercicio práctico: Seguridad en Dispositivos Móviles
1. Autenticación y acceso

¿Qué mecanismos de autenticación son más seguros para un dispositivo móvil de uso corporativo?

- ☐ Solo PIN de 4 dígitos
- ☐ Contraseña larga + bloqueo biométrico (huella, FaceID)
- Patrón de desbloqueo
- ☐ Ningún bloqueo (acceso directo).

Respuesta sugerida: √ Contraseña larga + bloqueo biométrico (huella, FaceID)

RECUPERAR LA INFORMACIÓN EN LA NUBE

Objetivo de esta etapa:

Que el empresario pueda recuperar archivos almacenados en servicios en la nube (Google Drive, OneDrive, Dropbox u otros) de forma rápida, segura y ordenada, minimizando la pérdida de información y el impacto en la operación. También busca que aprenda a determinar la causa del problema (borrado accidental, sincronización fallida, ransomware, acceso no autorizado) y tomar medidas correctivas para que no vuelva a pasar.

¿Cómo lo logro?

Voy a ponértelo como una receta: pasos numerados, una pizca de sentido común y varios trucos que te pueden servir para ti y tu empresa:

Paso 0 — Respira

Antes de hacer clic frenético en cualquier lado: respira. Las decisiones apresuradas empeoran la recuperación.

Paso 1 — Identifica el servicio y la cuenta afectada

- ¿Dónde estaban los archivos? (Google Drive, OneDrive, Dropbox, Box, iCloud, servidor S3 o un servicio contratado localmente).
- ¿Qué usuario o carpeta está afectada? ¿Es una cuenta personal o la cuenta corporativa/administrativa?

Paso 2 — Revisa lo obvio (5 minutos)

- Carpeta Papelera / Trash / Bin: muchas veces el archivo está allí y se restaura con un clic.
- Carpeta “Archivos sin conexión” o la copia local sincronizada en el equipo.
- Revisa la carpeta “Compartidos conmigo” o los accesos recibidos.

Paso 3 — Revisa el historial / versiones

- Muchos servicios conservan versiones antiguas (versioning). Puedes restaurar la versión anterior en vez de buscar un archivo borrado.
- En Google Drive: clic derecho → Gestionar versiones (o Version history en Docs/Sheets).

- En OneDrive/SharePoint: historial de versiones desde la interfaz web.
- (Google Play, App Store) y revisa permisos antes de instalar.
    - En Dropbox: Version history / Deleted files.(Si la interfaz te intimida, abre la ayuda rápida del servicio; en general te permiten restaurar versiones por días/ semanas.)

Paso 4 — Consolida evidencia (si es posible)

- Anota fechas y horas en que ocurrió la pérdida.
- Captura pantallas del estado actual (logs de errores, mensajes). Esto ayuda si necesitas soporte técnico o un informe interno.

Paso 5 — Usa la consola de administrador (si es cuenta corporativa)

- En cuentas empresariales (Google Workspace, Microsoft 365, Dropbox Business) un administrador puede:
    - Ver actividad de usuarios (quién borró qué y cuándo).
    - o Restaurar carpetas o usuarios completos según políticas de retención.
- Si no eres el administrador, contacta rápido con el administrador de TI de la empresa.

Paso 6 — Restauración desde copias de seguridad

- Si la empresa tiene backup (sistema de backup, snapshots en la nube, o copia local): restaura desde allí.
- Para servicios como Google Workspace / Microsoft 365, muchas empresas contratan soluciones de backup (independientes) —si existe, el proceso de recuperación suele ser por el panel del backup.

Paso 7 — Si creemos que hubo ataque (ransomware o acceso no autorizado)

- Aislar: desconectar equipos que muestran comportamientos extraños de la red (sin apagar discos).
- No pagar inmediatamente: primero consultar con especialista forense/contador/abogado.
- Cambiar contraseñas y forzar MFA en cuentas administrativas.
- Contactar al proveedor de servicio en la nube: suelen tener protocolos para incidentes y retención de datos.
- Documentar todo para posibles reclamaciones o investigaciones.

Paso 8 — Contactar soporte del proveedor

- Abre ticket con soporte (adjunta evidencias: pantallazos, IDs de archivo, fechas).
- En cuentas empresariales, soporte suele tener herramientas para restaurar datos que ya no están en la papelera del usuario.
- Pregunta por retención legal o retención forense si hay sospecha de delito.

Paso 9 — Validar la recuperación y comunicar

- Confirma que los archivos recuperados abren bien y son íntegros.
- Informa a las personas afectadas y deja registro interno del incidente y la recuperación.

Paso 10 — Corregir y aprender (acciones post-mortem)

- Revisa y ajusta políticas de backup y retención.
- Configura versionado automático y retención más amplia si el negocio lo requiere.
- Habilita autenticación multifactor (MFA) obligatoria para administradores y usuarios críticos.
- Plan de respuesta y roles: dejar claro quién hace qué ante pérdida de datos.

Riesgos:

- Borrado permanente por políticas de retención cortas o falta de backups.
- Sobrescritura de archivos (si se restauran versiones incorrectas).
- Pérdida de integridad: archivos recuperados corruptos o incompletos (ej.: por ransomware que cifra versiones antiguas).
- Exposición de datos durante la recuperación, si se usa una red insegura.
- Errores humanos: restaurar la versión equivocada, eliminar en masa sin revisar.
- Dependencia de un solo proveedor: si el proveedor falla o quiebra y no hay backup externo, la recuperación puede ser imposible.

Ventajas de tomar medidas apropiadas:

- Velocidad: la nube facilita restauraciones rápidas (muchas veces con un par de clics).
- Versionado automático: muchos servicios guardan historial y evitan pérdidas por ediciones accidentales.
- Acceso remoto: se puede recuperar sin estar físicamente en la oficina.

Ventajas de tomar medidas apropiadas:

- Menos inversión en hardware: la responsabilidad del almacenamiento físico la lleva el proveedor.
- Escalabilidad: las políticas de retención y backup pueden ajustarse al crecimiento de la empresa.

¿Por qué es importante?

Porque la información es activo: si pierdes contratos, contabilidad o correos clave puedes perder clientes, empleados o la tranquilidad. Para una Mipyme en Colombia, la recuperación rápida evita horas-hombre perdidas y sanciones (si la información afecta obligaciones legales o tributarias). Además, una buena práctica de recuperación reduce el riesgo reputacional: pierdes menos tiempo explicando por qué no tienes backups.

Errores frecuentes:

- Confiar solo en la papelera del servicio (no substituir backups regulares).
- No tener un administrador o responsable claro para la nube.
- No verificar las copias restauradas (se da por hecho que “ya está” y luego falta información).
- No auditar actividad: no saber quién hizo qué ni cuándo.
- No utilizar MFA y contraseñas débiles — puerta abierta para atacantes.
- No hacer pruebas: muchas empresas creen que la copia de seguridad funciona hasta que la necesitan y descubren que no.

Ejercicio para superar la etapa:

Un ejercicio práctico —rápido, sin dramas— para que tu equipo no llegue al incendio sin saber apagar fuego.
Simulación: "Recuperar el contrato borrado" (duración: 30–60 minutos)

1. Objetivo: Recuperar un archivo llamado Contrato_Cliente_X.pdf borrado por error por un usuario interno.

2. Participantes: 1 dueño/gerente, 1 administrador de la cuenta en la nube (si no hay, que lo haga quien más entienda la plataforma), 1 colaborador.

3. Escenario preparado:
- El organizador borra el archivo en su cuenta (o indica que "fue borrado hace 2 días").

4. Pasos del ejercicio:
- Paso A: Todos intentan encontrar el archivo en "Papelera" (5 min).
- Paso B: Si no está, el administrador revisa historial/versiones (10 min).
- Paso C: Si no aparece, se simula restauración desde backup (el organizador entrega una copia de seguridad ficticia o desde un *snapshot* previo).
- Paso D: Verificar integridad (abrir el PDF, confirmar que es el correcto).
- Paso E: Documentar tiempo total y pasos realizados (10 min).
- Paso F: Reunión corta (15 min) — detectar 3 mejoras para el plan de recuperación (ej.: activar *versioning*, aumentar retención, capacitar a personal).

Checklist rápido para el día a día

- [ ] Papelera revisada.
- [ ] Historial/versiones revisadas.
- [ ] Admin notificado si es cuenta corporativa.
- [ ] Backup disponible (local o servicio tercero).
- [ ] MFA activo para cuentas críticas.
- [ ] Registro del incidente (fechas, usuarios, acciones).

RECUPERAR TU CUENTA DE FACEBOOK SI TE HAN HACKEADO

Objetivo de esta etapa:

Que el empresario o encargado de redes sociales pueda recuperar el acceso a su cuenta de Facebook (personal o empresarial) en caso de hackeo, suplantación o pérdida de control, y reforzar la seguridad para evitar que vuelva a ocurrir.

¿Cómo lo logro?

Piensa en esto como un plan de emergencia digital: pasos cortos, cabeza fría y acción ordenada.

Paso 0 — Respira: antes de escribirle al hacker o hacer clic en correos sospechosos: detente. La calma evita errores como entregar más información o bloquearte definitivamente.

Paso 1 — Verifica si realmente fue hackeo, las siguientes pistas te pueden ayudar:

- Tu foto de perfil o nombre han cambiado.
- Aparecen publicaciones o mensajes que no escribiste.
- No puedes iniciar sesión, o tu autenticación en dos pasos no funciona.
- Recibes correos de Facebook notificando cambios que tú no hiciste (contraseña, correo, número de teléfono).
- En la sección “Dónde has iniciado sesión” (Configuración > Seguridad e inicio de sesión) aparece un dispositivo o ubicación que no reconoces.

Si alguno de estos casos aplica, pasa al siguiente paso.

Paso 2 — Usa el enlace oficial de recuperación

Ve a www.facebook.com/hacked.
Desde allí, Facebook te guiará en cuatro posibles escenarios:

1. Alguien accedió a tu cuenta.
2. Has olvidado tu contraseña.
3. Hay una cuenta que se hace pasar por ti.
4. Tienes otro problema relacionado con seguridad.

Recomendación: usa el mismo equipo o celular donde ya hayas iniciado sesión antes; Facebook reconocerá el dispositivo y facilitará la verificación.

Paso 3 — Revisa tu correo electrónico asociado

Si alguien cambió tu correo en la cuenta:

- Facebook envía un mensaje al correo anterior con un enlace para revertir el cambio.
- Haz clic en ese enlace lo antes posible para recuperar el acceso.

ATENCIÓN: No uses enlaces de correos dudosos. Verifica que el remitente sea una dirección oficial de Facebook (por ejemplo, @facebookmail.com).

Paso 4 — Cierra sesiones desconocidas

Una vez recuperes el acceso:

1. Entra a Configuración → Seguridad e inicio de sesión → Dónde has iniciado sesión.
2. Revisa la lista y selecciona “Cerrar sesión” en dispositivos o ubicaciones que no reconozcas.

Paso 5 — Restablece contraseñas y seguridad

- Cambia tu contraseña por una larga y única.
- Activa la autenticación en dos pasos (MFA) con aplicación de autenticación (Google Authenticator o similar).
- Revisa las direcciones de correo y números asociados a tu cuenta.
- Si administras una Página empresarial, cambia también los roles de administrador y verifica que no haya usuarios desconocidos

Paso 6 — Informa a tu comunidad

Si la cuenta publicó contenido extraño, haz una publicación informando que fue hackeada y que ya tomaste medidas.

Esto protege la reputación de la empresa y evita que tus clientes caigan en fraudes.

Paso 7 — Refuerza la protección

- No uses la misma contraseña en otras redes.
- Revisa tus correos de recuperación.
- Mantén actualizado tu dispositivo y navegador.
- Si administras varias páginas, usa Facebook Business Manager con acceso de administradores limitados.

Riesgos:

- Pérdida de acceso total si el atacante cambia correos y números sin recuperación.
- Daños reputacionales: publicaciones falsas o mensajes ofensivos desde la cuenta.
- Robo de información privada (chats, contactos, datos de clientes).
- Phishing: correos falsos que imitan a Facebook.
- Reutilizar contraseñas comprometidas en otras plataformas.

Ventajas de tomar medidas apropiadas:

- **Recuperación rápida** mediante herramientas oficiales.
- **Restauración de credibilidad** ante clientes y comunidad.
- **Mayor seguridad futura** al activar MFA y revisar accesos.
- **Prevención de fraudes** que puedan afectar la marca.

¿Por qué es importante?

Porque para una Mipyme colombiana, la **cuenta de Facebook suele ser el canal principal de comunicación y ventas.**

Perder el control puede significar **pérdida de clientes, fraudes, publicidad malintencionada o daño de imagen.**

Además, muchas Pymes gestionan sus campañas y catálogos directamente en Meta Business Suite, por lo que recuperar el acceso **es crítico para mantener la operación comercial.**

Errores frecuentes:

- Buscar ayuda en páginas falsas de “soporte” que roban más datos.
- Hacer clic en enlaces de correos no verificados.
- No activar la autenticación en dos pasos.
- Usar la misma contraseña en todas las plataformas.
- No revisar los roles de administrador en páginas empresariales.
- Esperar demasiado para reportar el hackeo (el atacante cambia todo).

Ejercicio para superar la etapa:

Simulación: “Cuenta de Facebook comprometida” (duración: 30–45 minutos)

Objetivo: practicar los pasos de recuperación ante un supuesto hackeo.

Participantes:

- 1 encargado de redes sociales.
- 1 gerente o dueño.
- 1 persona que actúe como “soporte técnico”.

Escenario:

El administrador de la página recibe un correo que indica “Tu cuenta se ha bloqueado temporalmente por seguridad”.

Pasos del ejercicio:

1. Verificar si el correo es legítimo (dominio, ortografía, enlace).
2. Intentar iniciar sesión en un dispositivo anterior.
3. Visitar www.facebook.com/hacked.
4. Simular cambio de contraseña y cierre de sesiones desconocidas.
5. Revisar roles en la página y eliminar usuarios extraños.
6. Registrar las acciones tomadas y el tiempo total del proceso.
7. Reflexionar: ¿qué mejorarías? (por ejemplo, activar MFA, tener lista de contactos de recuperación, documentar cuentas).

ZONA DE HIDRATACIÓN:

Aprendamos con un caso

Seguricam Ltda. es una Mipyme que instala y mantiene sistemas de videovigilancia en locales comerciales. Tienen veinte clientes activos, un pequeño servidor donde guardan grabaciones de respaldo y un equipo de soporte de tres personas.

El pasado lunes, al revisar los equipos de un cliente, descubrieron que varias cámaras dejaron de transmitir. Al conectarse al servidor, aparece el aviso clásico: **los archivos han sido cifrados y piden un rescate en bitcoins.**

¿Qué ha sucedido?

Es como ir pedaleando en bajada, confiado, y que de repente la llanta delantera reviente. La bici simplemente se va al piso. En este caso, el negocio se frena porque:

- No pueden acceder a grabaciones de clientes.
- El sistema de monitoreo en vivo está comprometido.
- Los clientes llaman, preocupados, porque la información que confiaron a la Mipyme parece perdida.

¿Cómo actuar en estas situaciones?

- **Aislar el sistema:** desconectan el servidor de la red y detienen todo acceso remoto.
- **Evidencia digital:** capturan pantallas del mensaje, copian registros de conexión (logs) y guardan todo en un disco externo.
- **Comunicación inmediata:** informan a los clientes lo que pasó, con transparencia y sin adornos. (La confianza se sostiene más cuando se habla claro).
- **Denuncia formal:** reportan el incidente al **CAI Virtual de la Policía Nacional (caivirtual.policia.gov.co).**
- **Presentan denuncia en la Fiscalía General de la Nación,** en la unidad de delitos informáticos.

- Notifican al **CSIRT Colombia** (equipo nacional de respuesta a incidentes), que da lineamientos técnicos.

¿Hay algo más que hacer?

Contingencia: restauran desde copias de seguridad guardadas en un servidor externo (no conectado a internet). Recuperan el 80% de la información.

Plan de mejora: revisan accesos de usuarios, cambian contraseñas, instalan un firewall adicional y definen protocolos de recuperación en menos de 24 horas.

La etapa de corrección es ese momento en que no alcanza con casco ni luces: te caíste, punto. Lo que hace la diferencia es si sabes cómo levantarte.

Si llevabas parches y herramientas (copias de seguridad y protocolos), vuelves a rodar.

Herramientas de ciberseguridad que debe usar un senior

Hoy en día, tu negocio, ya sea una panadería, una consultora o un emporio de software, vive en la red. Y si algo vive en la red, tiene que estar protegido. Muchos dueños de empresas ven la ciberseguridad como un costo gigante, una pared de oro que solo las grandes corporaciones pueden permitirse. Y eso, déjenme decirles, es una idea vieja y peligrosa.

A continuación, te presentamos una hoja de ruta con herramientas concretas y, lo mejor de todo, ¡gratuitas o de código abierto! Es como si el universo de la tecnología les dijera: “No hay excusas”.

Herramientas para la prevención

Piensen en su empresa como un hogar.

Antes de que alguien entre, pones una puerta segura y un cerrojo. Para tu negocio, eso significa **pfSense o OPNsense** para blindar la red y **ClamAV** para mantener a raya a los virus. Y, por favor, dejen de usar la misma contraseña para todo. Usen un gestor como **KeePassXC** o **Bitwarden.** Es como tener una llave maestra para cada cerradura, y cada llave es diferente. ¿Necesitas que tus empleados se conecten desde casa? **OpenVPN o WireGuard** son el puente seguro que necesitas.

Herramientas para la detección

Si alguien intenta colarse, tienes que saberlo. Imagina un sistema de cámaras y sensores. **Wazuh** te dice si algo raro pasa en tus equipos y **Snort o Suricata** son los guardias que te alertan de cualquier movimiento sospechoso en la red. Con estas herramientas, dejas de ser un objetivo a ciegas para convertirte en un negocio con ojos bien abiertos.

Herramientas para la corrección:

Un incidente no es el fin del mundo, es una oportunidad para aprender. Tienes que poder reaccionar. **Duplicati y BorgBackup** son tus paracaídas: te permiten hacer copias de seguridad para que, si todo se va al diablo, puedas recuperar tu información. Y si el problema es más serio, hay herramientas como **Autopsy y Volatility** para analizar qué pasó y cómo arreglarlo. Para los que quieren un

control total, **TheHive + Cortex** te permiten orquestar la respuesta, como si tuvieras un centro de comando para cada incidente.

HERRAMIENTAS DE CIBERSEGURIDAD GRATUITAS POR ETAPA		
Etapa	**Herramienta (Free/Open/Source)**	**Uso práctico**
Prevención	pfSense / OPNsense	Firewalls de código abierto para segmentar la red y bloquear accesos no autorizados.
	ClamAV	Antimalware gratuito, útil para servidores Linux y correo electrónico.
	KeePassXC / Bitwarden (self-hosted)	Gestores de contraseñas para reducir riesgos de credenciales débiles o repetidas
	OpenVPN / WireGuard	VPNs gratuitas para cifrar el tráfico y proteger accesos remotos.
	Lynis	Auditoría de seguridad para sistemas Linux, verifica configuraciones débiles.
Detección	Wazuh (SIEM gratuito)	Correlación de logs, detección de intrusiones y anomalías en endpoints y red
	Snort / Suricata	IDS/IPS para detectar intentos de intrusión y tráfico sospechoso en red.
	OSSEC	Monitoreo de integridad de archivos y actividad sospechosa en servidores
	Wireshark / tcpdump	Analizar paquetes de red en tiempo real para detectar malware o filtraciones.

HERRAMIENTAS DE CIBERSEGURIDAD GRATUITAS POR ETAPA		
Etapa	**Herramienta (Free/Open/Source)**	**Uso práctico**
Corrección	Duplicati / BorgBackup / Restic	Copias de seguridad cifradas y recuperación de datos tras un ataque.
	Autopsy	Herramienta forense gratuita para analizar discos comprometidos.
	Volatility	Análisis de memoria RAM para incidentes de malware avanzado
	TheHive + Cortex	SOAR open source para gestionar incidentes, bloquear IPs y coordinar respuesta.
	Clonezilla / Rescuezilla	Restauración de sistemas completos desde imágenes de disco..

REFERENCIAS

Arcserve. (2023). Data protection and backup practices report 2023. Arcserve. https://www.arcserve.com
Axios. (2025). AI-driven attacks in the financial sector. Axios. https://www.axios.com

Centro Cibernético Policial - Colombia. (2023). Informe anual de cibercrimen en Colombia 2023. Policía Nacional de Colombia. https://caivirtual.policia.gov.co

Check Point Research. (2024). Mobile security report 2024. Check Point Software Technologies. https://research.checkpoint.com

Computing. (2024). Veeam data protection trends report 2024. Computing. https://www.computing.co.uk

Federal Emergency Management Agency (FEMA). (2025). Business continuity and disaster recovery statistics. U.S. Department of Homeland Security. https://www.fema.gov

Fortinet. (2020). Telework security report 2020. Fortinet. https://www.fortinet.com

Fortinet. (2023). LATAM threat landscape report 2023. Fortinet.

Gartner. (2024). Data loss and business continuity report 2024. Gartner Inc. https://www.gartner.com

Help Net Security. (2025). Cybersecurity trends and remote work threats report 2025. Help Net Security. https://www.helpnetsecurity.com

REFERENCIAS

IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/security/data-breach
IBM. (2025). Cost of a data breach report 2025. IBM Security.

IBM Security. (2023). Incident response and segmentation effectiveness study. IBM Security.

Interpol. (2024). Global crime trend report 2024. Interpol. https://www.interpol.int

Kaspersky. (2023). Informe sobre ciberacoso empresarial 2023. Kaspersky Lab. https://www.kaspersky.com

Kaspersky. (2024). Threat landscape report 2024: América Latina. Kaspersky Lab.

Kaspersky Lab. (2024). Mobile phishing report 2024. Kaspersky Lab.

Network Media. (2025). Business continuity and resilience benchmark report 2025. Network Media.

Organización de los Estados Americanos (OEA). (2023). Informe regional sobre ciberacoso laboral en América Latina. OEA.

Policía Nacional de Colombia. (2024). Estadísticas de denuncias por suplantación digital 2024. Policía Nacional de Colombia.

Ponemon Institute. (2024). Cost and impact of unpatched vulnerabilities 2024. Ponemon Institute.

REFERENCIAS

SoSafe. (2025). Cybercrime trends 2025: AI-driven threats. SoSafe. https://www.sosafe.de

Symantec/Norton. (2024). Mobile threat landscape report 2024. NortonLifeLock.

TechJury. (2024). Video conferencing market share 2024. TechJury.

UNESCO. (2023). Informe mundial sobre violencia y acoso en línea en jóvenes 2023. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Verizon. (2024). Data breach investigations report 2024 (DBIR). Verizon Communications. https://www.verizon.com/business/resources/reports/dbir

Veeam. (2024). Data protection trends report 2024. Veeam Software.

Keepit / Enterprise Strategy Group. (2025). 2025 state of SaaS backup and recovery report: SaaS backup strategies for Microsoft 365, Google Workspace, and Salesforce. Keepit.

Zoom Video Communications. (2020). Zoom transparency report: Security and privacy in virtual meetings. Zoom Communications Inc.

RECURSOS

CONPES 3701. (2011). Política de Seguridad Digital y Defensa Cibernética de Colombia. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co

CONPES 3854. (2016). Fortalecimiento de las capacidades institucionales en seguridad digital. Departamento Nacional de Planeación.

CONPES 3995. (2020). Política Nacional de Confianza y Seguridad Digital. Departamento Nacional de Planeación.
GDPR. (2016). Reglamento General de Protección de Datos (Reglamento UE 2016/679). Parlamento Europeo y del Consejo de la Unión Europea.

ISO. (2013). ISO/IEC 27001:2013 — Information security management systems — Requirements. International Organization for Standardization.

Ley 1581 de 2012. (2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República de Colombia. Diario Oficial No. 48.587.