Introducción y riesgos

Módulo 1: Introducción y riesgos

Unidad 1: Conceptos esenciales

- Seguridad de la información vs. ciberseguridad
- Propiedades “confidencialidad-integridad-disponibilidad” (CIA) y no repudio
- Activos y superficies de ataque
- Amenazas, vulnerabilidades y riesgo

Unidad 2: Riesgos típicos y pymes

- *Phishing* y BEC
- *Ransomware* y extorsión
- Malconfiguraciones y *Shadow IT*
- Terceros y cadena de suministro

Unidad 1: Conceptos esenciales

Las pequeñas y medianas empresas (pymes) se enfrentan cada vez más a **riesgos de seguridad digital**. En 2024, Argentina registró 438 incidentes de ciberseguridad según el CERT.ar, un aumento del 15 % respecto al año anterior. Además, la primera mitad de 2025 registró 1600 millones de intentos de ciberataques, con la industria y la salud en la mira, impulsados por atacantes que utilizan IA para escanear redes y automatizar la explotación de vulnerabilidades. Las amenazas incluyen el robo de información, el acceso indebido a sistemas y el aumento de ataques de *phishing*. A menudo, las pymes cuentan con menos recursos técnicos y humanos dedicados a la seguridad, lo que las hace más vulnerables.

En este módulo introductorio, exploraremos los conceptos básicos de seguridad de la información y ciberseguridad, las principales propiedades que buscamos proteger, y los riesgos típicos que afectan a las pymes. El enfoque será **práctico**, con ejemplos de casos reales por unidad y

recomendaciones para mitigar amenazas en entornos de pequeñas empresas.

Unidad 1: Conceptos esenciales

En esta unidad, definiremos conceptos fundamentales para sentar las bases de la seguridad informática y organizacional. Veremos la diferencia entre seguridad de la información, seguridad informática y ciberseguridad, las propiedades clave que se deben proteger (confidencialidad, integridad, disponibilidad, etc.), lo que entendemos por activos y superficie de ataque, y, además, definiremos amenazas, vulnerabilidades y riesgo. Estos pilares conceptuales nos permitirán comprender mejor los riesgos específicos que se tratarán en la unidad 2.

Seguridad de la información vs. seguridad informática, vs. ciberseguridad

Es común usar **“seguridad de la información”, “seguridad informática”** y **“ciberseguridad”** como sinónimos, pero no son exactamente lo mismo.

La **seguridad de la información** es un concepto amplio. Es el conjunto de medidas preventivas y reactivas, incluyendo políticas, procedimientos y controles, que permiten proteger la información en **todas sus formas** y medios, tanto digitales como físicos, ya sean de una empresa, de una institución o de un particular. En este sentido, la información puede ser almacenada, procesada o transmitida de diferentes maneras: en formato electrónico, de forma verbal o a través de mensajes escritos o impresos. Así, la seguridad de la información consiste en proteger tanto un archivador de documentos importantes como la base de datos de su organización; consiste en proteger tanto datos impresos, documentos, conversaciones, etc., como los sistemas informáticos. Si pensamos en términos más concretos, la seguridad de la información protege tantos archivos físicos en una caja fuerte como el acceso a ciertos documentos digitales confidenciales.

La **seguridad informática** es la disciplina que se encarga de proteger la disponibilidad, la integridad y la privacidad de la información almacenada, procesada y transmitida en sistemas informáticos. La seguridad informática:

- está orientada a la seguridad interna y perimetral (tanto de empresas y organizaciones como del ámbito hogareño);
- está orientada a las amenazas en general (por ejemplo, el mal uso de los sistemas sin malas intenciones); y

- tiene un enfoque principalmente defensivo. Es decir, la función de la seguridad informática consiste en la gestión de riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos, y con los sistemas y procesos empleados en la realización de dichas actividades.

La **ciberseguridad** es la práctica de defender, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos llevados a cabo por cibercriminales, cuyos objetivos son principalmente el ciberdelito, por ejemplo, obtener ganancias de la información adquirida.

Es decir, al igual que la seguridad informática, su objetivo es proteger la información digital en los sistemas interconectados, pero, a diferencia de la seguridad informática, la ciberseguridad:

- está orientada a la seguridad sobre Internet (seguridad en los medios abiertos fuera del control de las organizaciones);
- está orientada a las amenazas y los ataques de los ciberdelincuentes (siempre con malas intenciones, es decir, ataques cuyo objetivo es el ciberdelito);
- tiene un enfoque principalmente ofensivo, por ejemplo, uno de sus métodos es el *hacking* ético (*ethical hacking*).

En la siguiente tabla, se resaltan las diferencias y similitudes de los tres conceptos.

Tabla 1: Diferencias y similitudes de seguridad de la información, seguridad informática y ciberseguridad

Seguridad de la información	Seguridad informática	Ciberseguridad
Tiene un alcance más amplio.	Es una subdisciplina de la seguridad de la información.	Es una subdisciplina de la seguridad de la información, aunque extendió explícitamente la seguridad de la información al ciberespacio no gobernado (Internet) y a usuarios finales de la tecnología en general.
Protege la información en	Protege la información en	Protege la información en

cualquiera de sus formas.	formato digital (datos).	formato digital (datos).
Está orientada principalmente a organizaciones y medios empresariales de cualquier tamaño (aunque aplicable también a ámbitos hogareños y a las personas).	Está orientada a organizaciones y medios empresariales de cualquier tamaño, y al ámbito hogareño (aplicable también a las personas).	Está orientada al ciberespacio y a las personas.
Abarca medidas técnicas y no técnicas (o administrativas).	Abarca medidas técnicas principalmente.	Abarca aspectos técnicos.
Incluye medidas defensivas de todo tipo (físicas, administrativas y técnicas).	Incluye principalmente medidas defensivas sobre	Incluye principalmente medidas ofensivas sobre sistemas

	sistemas informáticos.	informáticos y las personas.

Fuente: elaboración propia.

Los tres conceptos se complementan: una estrategia robusta de protección empresarial debe abordar elementos de seguridad de la información (como políticas organizativas, control de acceso físico, copias en papel, etc.), debe implementar medidas de seguridad informática (como protección de redes, cifrado de datos electrónicos, monitoreo de sistemas) y de ciberseguridad, como pruebas de *hacking* ético, para mantener la superficie de ataque controlada. En una pyme, esto significa que no solo debemos pensar en antivirus o contraseñas (ciberseguridad), sino también en quién maneja la información, cómo se almacenan documentos sensibles, qué hábitos tienen los empleados, etc.

Propiedades de confidencialidad, integridad, disponibilidad (CIA)

Al proteger la información, existen **tres propiedades fundamentales** que siempre buscamos garantizar: **confidencialidad, integridad y disponibilidad**, a menudo llamadas en conjunto la **tríada CIA**. A estas a veces se les suman otros atributos importantes, como la **autenticidad** y el **no repudio**. Veamos en qué consiste cada concepto:

Confidencialidad: propiedad de la información que asegura que la información **solo sea accesible por personas autorizadas**. Significa prevenir divulgaciones no autorizadas. Por ejemplo, la confidencialidad de la base de datos de clientes implica que nadie fuera del personal autorizado pueda ver esos datos. Se logra mediante controles de acceso, cifrado, políticas de "necesidad de saber", etc. En resumen, protege los datos contra la lectura o visualización indebida.

Integridad: propiedad de la información que asegura mantener la **exactitud y completitud** de la información, protegiéndola de modificaciones no autorizadas o accidentales. Implica que los datos no sean alterados ni manipulados indebidamente, y que cualquier cambio legítimo sea detectado y registrado. Por ejemplo, la integridad de un registro contable garantiza que no pueda ser editado sin autorización y que, si se modifica, quede evidencia de ello. Controles como firmas digitales, sumas de verificación (*hash*), controles de versiones y permisos de escritura ayudan a preservar la integridad.

Disponibilidad: propiedad de la información que asegura que la información y los sistemas estén **accesibles y funcionando** cuando se necesitan. Un dato o servicio es valioso solo si se puede usar en tiempo y forma. Por ejemplo, la disponibilidad del servidor web de una tienda en línea significa que esté en funcionamiento para

atender a los clientes en todo momento. Para garantizar disponibilidad, se implementan medidas como redundancia (servidores de respaldo), respaldos periódicos (*backups*) y planes de contingencia para recuperarse ante fallos o ataques (por ejemplo, ante un *ransomware* o ataque de denegación de servicio). La disponibilidad se ve amenazada por caídas del sistema, desastres naturales, sabotajes o *malware* que "**secuestra**" los datos e impide el acceso.

En esta representación de la tríada de seguridad de la información **CIA,** se sitúa a la **información** en el centro. Este diagrama ilustra que la información debe estar protegida por esas tres propiedades fundamentales. Adicionalmente, alrededor se aprecian capas que la rodean –comunicación, *hardware, software,* y, más externamente, seguridad física, personal y organizacional–, lo que indica que la seguridad de la información abarca múltiples dimensiones tecnológicas y administrativas.

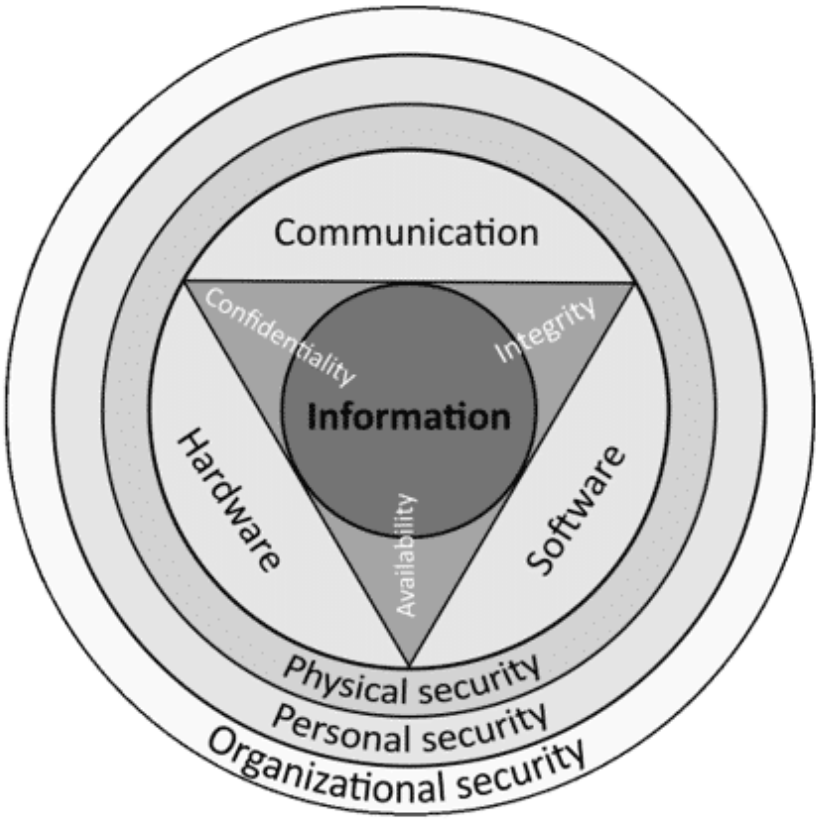
Además de CIA, otros atributos complementarios cobran importancia según el contexto:

Autenticidad: propiedad que garantiza que la identidad de usuarios y fuentes de datos es la que dicen ser. Implica mecanismos para verificar que alguien o algo es legítimo. Por ejemplo, al recibir

un correo electrónico importante, la autenticidad se comprueba verificando la firma digital o la procedencia real del remitente. También aplica a datos: asegurar que un documento es auténtico (no ha sido falsificado) o que un sitio web es el verdadero y no una copia falsa. La autenticidad es clave para prevenir suplantaciones de identidad.

No repudio: propiedad que asegura impedir que alguien pueda **negar su autoría o participación** en una transacción o evento. Este principio asegura que, una vez realizado algo, quede evidencia irrefutable de quién lo hizo, de modo que no pueda "repudiarlo" posteriormente. En términos prácticos, se logra mediante mecanismos como firmas digitales o registros (*logs*) robustos: por ejemplo, si un gerente aprueba una transferencia electrónica firmándola digitalmente, no podría después negar que la aprobó, pues la firma asociada a su identidad lo vincula de manera confiable. El no repudio suele ser muy importante en transacciones financieras o comunicaciones oficiales.

Figura 1: Representación de la tríada de seguridad de la información CIA



Fuente: [imagen sin título sobre tríada de seguridad de la información CIA] (s. f.). https://kaa.wikipedia.org/wiki/Fayl:CIAJMK1209-en.svg

Ejemplo práctico: aplicación de CIA y no repudio en una pyme

Imaginemos una pequeña clínica médica privada que maneja historiales de pacientes en formato digital. Para ellos, sucede lo siguiente:

- La **confidencialidad** es crítica. Solo el personal autorizado (médicos, enfermeros) debe acceder a los historiales. Se implementan contraseñas por usuario y cifrado de la base de datos para que ni siquiera un técnico de IT externo pueda leer datos sensibles sin permiso.

- La **integridad** es vital. Un error o alteración en un diagnóstico podría tener consecuencias graves. La clínica usa controles de acceso de solo lectura para ciertos archivos y registro de cambios (*log*) en el *software* de historias clínicas, de modo que, si alguien edita o borra información, quede constancia y se pueda revertir.
- La **disponibilidad** también es fundamental. Si el sistema donde se almacenan los historiales se cae por horas debido a un ataque o falla, la atención a pacientes se ve comprometida. Por eso mantienen ***backups* diarios** de los datos y un servidor de respaldo, además de un suministro eléctrico ininterrumpido para evitar cortes.
- Implementan medidas de **autenticidad y no repudio.** Los médicos deben iniciar sesión con autenticación de dos factores, asegurando que quien accede es quien dice ser (autenticidad). Cada acceso o modificación a un historial queda registrado con la identidad del profesional y marcado con hora/fecha (trazabilidad), de forma que posteriormente nadie pueda negar que ingresó cierta información en la ficha (no repudio). Por ejemplo, si un médico recetó un medicamento erróneo y trata de culpar al sistema, se puede verificar la cuenta usada y la firma digital del registro para confirmar quién hizo esa entrada.

Este ejemplo muestra cómo los **principios básicos** se aplican conjuntamente: la clínica protege la confidencialidad de los datos de pacientes, asegura su integridad y disponibilidad, y añade autenticidad/no repudio para robustecer la confianza en su sistema. Estos mismos principios aplican a cualquier organización: desde evitar que un competidor vea nuestros planes de negocio (confidencialidad) hasta garantizar que la página web de la empresa no sea alterada por un atacante (integridad) o que nuestros servicios en la nube no sufran interrupciones prolongadas (disponibilidad).

Activos son todos aquellos elementos de valor para una organización que deben ser protegidos. En seguridad suele hablarse de *activos de información*: pueden ser **datos** (p. ej., la base de datos de clientes, secretos industriales), **sistemas** (servidores, computadoras de empleados, dispositivos móviles corporativos), **infraestructura tecnológica** (redes, *routers*, almacenamiento en la nube), e incluso **personas o procesos** claves. Identificar los activos es el primer paso para saber **qué** debemos resguardar y cuáles serían los impactos si se ven comprometidos.

Por ejemplo, para una pyme comercial, sus activos principales podrían incluir: la lista de clientes y proveedores, su sitio web de ventas en línea, sus credenciales de banca electrónica, las computadoras de facturación, y la reputación/marca de la empresa.

Cada activo tiene cierto valor y, por ende, distintos niveles de protección requeridos. La seguridad se enfoca en proteger **la confidencialidad, integridad y disponibilidad de esos activos** (como vimos anteriormente).

Por otro lado, la **superficie de ataque** de una organización es el conjunto de todos los puntos potenciales de entrada o debilidades por donde un atacante podría intentar acceder sin autorización. En otras palabras, es la **suma de las vulnerabilidades y vías de ataque** que un adversario puede explotar para comprometer nuestros activos. Mientras más complejos y expuestos estén nuestros sistemas, más amplia será la superficie de ataque.

Algunos ejemplos de **componentes de la superficie de ataque digital** de una pyme típica:

- Los **sistemas expuestos a Internet**, como un servidor web corporativo, un portal de correo o una base de datos en la nube, son parte de la superficie de ataque porque están visibles para cualquier usuario (y potencial atacante) en la red.

- Las **computadoras y redes internas** también forman parte, ya que un atacante podría intentar introducir *malware* a través de ellas (por *phishing* a un empleado, por ejemplo).
- Las **contraseñas de usuarios** constituyen una superficie de ataque: si son débiles o reutilizadas, facilitan que un atacante fuerce su entrada.
- **Dispositivos o *software* mal configurados** (malconfiguraciones) amplían la superficie aprovechable; por ejemplo, si el firewall de la empresa tiene puertos abiertos innecesarios, esos puertos son puertas de entrada para quien las descubra.
- Las prácticas de los usuarios también cuentan: que un empleado conecte un *pendrive* USB desconocido o instale *software* sin autorización (lo que llamamos *Shadow IT* o TI en la sombra) añade caminos no controlados que un atacante podría aprovechar.

Una manera común de pensar la superficie de ataque es dividirla en categorías: **digital**, **física** y de **ingeniería social**:

- La **superficie digital** abarca los sistemas tecnológicos (servidores, aplicaciones, dispositivos conectados);
- la **superficie física** incluye accesos al espacio físico (equipos que pueden ser robados, documentos impresos, accesos a oficinas/servidores);

- y la **superficie de ingeniería social** se refiere al factor humano (empleados susceptibles a engaños o errores).

Para una pyme, esto significa que su superficie de ataque incluye **todos los puntos** donde guarda o procesa información (un servidor, una PC, un móvil corporativo), **todos los accesos físicos** (la puerta de la oficina donde hay archivos, la *laptop* que un empleado lleva fuera) **y todas las interacciones humanas** (personal que puede ser manipulado vía teléfono, *e-mail*, etc.).

¿Por qué es importante este concepto? Porque **reducir la superficie de ataque** es una estrategia clave de defensa. Entre menos "puertas" tengamos abiertas, menos oportunidades hay para el atacante. Por ejemplo, si en una empresa nadie usa escritorio remoto pero el puerto de *Remote Desktop* (RDP) quedó abierto a Internet por descuido, es una entrada innecesaria que conviene cerrar. Del mismo modo, dar de baja cuentas de empleados que ya no trabajan en la empresa, eliminar servicios no utilizados y mantener actualizado el *software* ayuda a disminuir la superficie de ataque vulnerable.

En el contexto de las pymes, un desafío común es el ***Shadow IT*** (TI en la sombra): el uso de sistemas o aplicaciones sin el conocimiento del área de TI. Muchas pymes no tienen un departamento de TI formal, o este no alcanza a controlar todo, así que los empleados instalan programas por su cuenta, usan servicios en la nube

gratuitos para compartir archivos o conectan dispositivos personales a la red de la empresa. Esto crea una zona fuera de visibilidad de los defensores. **Cada aplicación no autorizada o dispositivo no gestionado es parte de la superficie de ataque** y suele carecer de las medidas de seguridad corporativas. Por ejemplo, si un empleado usa su cuenta personal de Dropbox para transferir documentos de trabajo (porque quizás la empresa no se lo proveyó oficialmente), ese canal podría no tener los mismos controles de seguridad y podría exponer información sensible. Lo mismo si alguien instala una herramienta gratuita sin revisarla: podría contener *malware* o abrir una puerta de acceso. El *Shadow IT* **impide el control total** por parte de la empresa, y los atacantes buscan justamente esos puntos débiles fuera del radar. Por eso es importante educar a la plantilla sobre los riesgos de usar herramientas no autorizadas e intentar proveer alternativas seguras para que no sientan la necesidad de acudir a soluciones "en la sombra".

Resumen: identificar nuestros activos críticos y entender la superficie de ataque nos permite priorizar la protección. Una pyme debe preguntarse: "¿qué datos o sistemas no puedo permitirme comprometer?" (activos) y luego "¿por dónde podrían entrar a ellos?" (superficies/vectores de ataque: técnicas, físicas, humanas). Con esto claro, podemos aplicar medidas de seguridad en los puntos adecuados.

Estos tres conceptos están íntimamente ligados. En conjunto nos permiten evaluar y gestionar la **exposición al peligro** de nuestros activos:

Amenaza: es cualquier evento o agente potencial que podría causar daño a nuestros sistemas o datos. Una amenaza puede ser:

- una amenaza intencional (un *hacker* intentando robar información, un *malware* diseñado para cifrar archivos, un empleado deshonesto), o bien
- una amenaza no intencional/accidental (un incendio en el servidor, una inundación, un corte eléctrico prolongado, errores humanos involuntarios).

En seguridad de la información, con "amenaza" solemos referirnos tanto a los atacantes (ciberdelincuentes, virus, etc.) como a las posibles situaciones dañinas (un ataque DDoS, una intrusión, un fraude interno). Básicamente es lo malo que podría pasar.

Vulnerabilidad: es un fallo en nuestros sistemas, procesos o medidas de control, que puede ser explotado por una amenaza. En

otras palabras, es **una grieta en nuestra seguridad**. Las vulnerabilidades pueden ser:

- vulnerabilidades técnicas (un *bug* de *software* sin parche, una configuración insegura, una contraseña débil), o bien
- vulnerabilidades procedimentales/humanas (falta de capacitación, ausencia de políticas, descuidos).

Ejemplos:

- Una aplicación web con una falla de validación que permite SQL *Injection* es una vulnerabilidad.
- No tener copias de seguridad de datos importantes es otra vulnerabilidad (porque nos deja indefensos ante ciertos ataques).
- Usar la misma contraseña para todo es una vulnerabilidad personal.

Las amenazas aprovechan las vulnerabilidades: si hay una puerta abierta (vulnerable), eventualmente habrá alguien intentando entrar (amenaza). **Sin vulnerabilidad, la amenaza por sí sola no causa daño** –por eso es crucial reducir las vulnerabilidades.

Un concepto relacionado (pero distinto) con el de vulnerabilidades es el de **debilidad**. Una debilidad de un sistema, en relación con la

seguridad, es un aspecto del sistema que no ha sido diseñado para ser seguro, es decir, en el cual la seguridad no ha sido un requerimiento, pero que eventualmente puede ser explotado por una amenaza. Un ejemplo es el protocolo IP: es un protocolo en el que la seguridad no ha sido requerida en su diseño, y que aun sin tener fallos en su diseño y aun siendo correctamente implementado en un sistema, presenta debilidades relacionadas con la seguridad, ya que existen amenazas que pueden explotarlo.

Es por esto que en un análisis de seguridad hay que considerar tanto las vulnerabilidades como las debilidades de los sistemas.

Riesgo: es la *posibilidad* de que una amenaza explote una vulnerabilidad y cause un impacto negativo. En términos más formales, el riesgo se suele entender como la combinación de lo siguiente:

- la **probabilidad** de que ocurra un incidente y
- la **gravedad del impacto** que este tendría.

Si tanto la amenaza como la vulnerabilidad existen, hay un riesgo. El nivel de riesgo será mayor cuanto más probable sea el incidente y cuanto más severas sean sus consecuencias. El cálculo del riesgo se realiza multiplicando la **probabilidad de que ocurra un ataque** (la

posibilidad de que suceda) por la **gravedad del impacto** (la magnitud del daño que causaría) si ese ataque se materializa.

Riesgo = Probabilidad x Impacto

Esta fórmula permite a las organizaciones cuantificar y priorizar los riesgos para enfocar recursos de manera más efectiva. Un riesgo se considera alto si es **muy factible (muy probable)** que ocurra y **muy dañino (alto impacto)** si ocurre.

En resumen: *amenaza* es lo que nos puede atacar o afectar, *vulnerabilidad* es por dónde puede hacerlo, y *riesgo* es la exposición resultante, es decir, la chance de que pase algo malo y sus consecuencias.

Formalmente, podemos decir que **el riesgo está asociado a la posibilidad de que amenazas exploten vulnerabilidades y, por lo tanto, causen daño a la organización**. Una organización debe gestionar sus riesgos analizando escenarios de amenaza-vulnerabilidad. Por ejemplo, consideremos una pyme que almacena todos sus documentos críticos en una sola computadora sin copias de seguridad:

- Amenazas: fallo del disco duro o ataque de *ransomware* que cifre los archivos.

- Vulnerabilidades: no tener *backups* (y posiblemente, un antivirus deficiente).
- Riesgo: **pérdida permanente de datos**. La probabilidad podría ser moderada (no es seguro que se infecte o falle el disco, pero es bastante posible con el tiempo), y el impacto sería catastrófico (perder todo). Por tanto, el riesgo es alto.

Tras evaluar, la empresa debería **tratar el riesgo**: por ejemplo, mitigarlo haciendo copias de seguridad externas regularmente (así elimina la vulnerabilidad "no hay *backups*") y reduciendo drásticamente tanto la probabilidad de pérdida total como el impacto.

Otra relación útil: una **amenaza sin vulnerabilidad** posiblemente no logre dañarnos (p. ej., un *hacker* quiere atacar nuestra web, pero si está bien parcheada y sin fallos, sus intentos no prosperarán). Una **vulnerabilidad sin una amenaza que la explote** tampoco causa daño por sí misma (p. ej., tenemos un servidor sin parches –vulnerable –, pero si nadie lo ataca, puede que nada malo ocurra… aunque confiar en eso sería imprudente). El **riesgo surge cuando ambos se combinan** y puede materializarse en un incidente.

La gestión de riesgos es el proceso continuo de identificar, evaluar y priorizar riesgos, para luego aplicar controles que los mitiguen. En pequeñas empresas esto puede ser informal, pero igualmente necesario. Implica preguntarse: *¿qué amenazas son más probables y podrían hacernos más daño?* y *¿qué podemos hacer al respecto?*

Las opciones típicas para tratar un riesgo son:

- **Mitigar:** implementar medidas para reducir la probabilidad o el impacto. Por ejemplo: ante riesgo de *phishing*, dar capacitación a empleados y usar filtros de *spam* (reduce probabilidad de que caigan). Ante riesgo de pérdida de datos, tener respaldos (reduce impacto).
- **Evitar:** directamente eliminar la actividad de riesgo. Por ejemplo: si una aplicación es demasiado vulnerable y no es esencial, desconectarla del todo evita el riesgo asociado.
- **Transferir:** pasar el riesgo a un tercero, típicamente contratando un seguro o tercerizando cierta operación. Por ejemplo: un seguro cibernético puede cubrir costos de incidentes, o almacenar datos en un servicio confiable en la nube transfiere parte del riesgo de infraestructura al proveedor (aunque nunca al 100 %).

- **Aceptar:** asumir el riesgo tal cual si se considera bajo o inevitable, teniendo planes de contingencia. Ninguna empresa puede eliminar todos los riesgos, así que se aceptan los menores (consciente y documentadamente).

Ejemplo práctico: caso de amenaza, vulnerabilidad y riesgo en acción

Una *startup* de *e-commerce*, **TechGoods**, maneja un pequeño sitio web de ventas y la información de sus clientes (pedidos, direcciones, pagos). Analicemos un riesgo concreto:

- **Activo:** base de datos de clientes con información personal y registros de pedidos.
- **Amenaza:** un atacante externo (ciberdelincuente) interesado en robar esa base de datos para venderla o extorsionar a la empresa. Alternativamente, amenaza interna podría ser un empleado descontento intentando filtrar datos.
- **Vulnerabilidades:** TechGoods identificó varias: (1) su base de datos no está cifrada en reposo, (2) usan cuentas de usuario compartidas para acceder a ella, (3) la aplicación web tiene una interfaz de administración accesible por Internet con una contraseña débil. Estas debilidades serían vías para que la amenaza acceda a los datos.

- **Riesgo: filtración de datos de clientes**. Probabilidad: con las vulnerabilidades presentes, un ataque *es probable* (*automated bots* pueden explotar contraseñas débiles, o alguien puede aprovechar credenciales expuestas). Impacto: *alto*, pues la filtración de datos traería sanciones (ley de protección de datos), daño reputacional y pérdida de confianza de clientes. Conclusión: riesgo **crítico**.

¿Cómo debe actuar TechGoods? Primero, tienen que mitigar las vulnerabilidades: establecer contraseñas fuertes y únicas, restringir el acceso a la interfaz *admin* (por IP o VPN), habilitar cifrado de la base de datos o al menos de campos sensibles, y crear cuentas individuales para trazabilidad (evitar usuario compartido *admin* genérico). También podrían implementar monitoreo de accesos y detección de intrusos para reducir la ventana de explotación. Cada acción disminuye la probabilidad de éxito del atacante o el impacto en caso de ocurrir (por ejemplo, si la base de datos estuviera cifrada, aun robándola, el atacante no podría leerla fácilmente, lo que reduce el impacto).

TechGoods podría, además, transferir parte del riesgo contratando un seguro de ciberriesgo que ayude con los costos si ocurre una brecha, pero la prioridad es mitigar. Tras aplicar controles, reevaluarían el riesgo de filtración: con contraseñas robustas, cifrado y monitoreo, la probabilidad disminuye a *baja o moderada*, y el

impacto potencial también disminuye (menos datos accesibles). El riesgo pasaría a un nivel aceptable para la empresa.

Este caso demuestra la interacción: la amenaza de robo siempre existirá (no podemos controlarla del todo, los atacantes seguirán intentando), pero podemos **reducir nuestras vulnerabilidades** y, por tanto, **el riesgo** a niveles manejables. En ciberseguridad, casi todo es cuestión de gestionar este triángulo amenaza-vulnerabilidad-riesgo de forma continua.

Nota: Es aconsejable que incluso las pymes pequeñas realicen un **inventario de activos y evaluación de riesgos básica**. No requiere herramientas sofisticadas: basta listar qué información/sistemas son cruciales, qué podría pasarles, y tomar medidas razonables. Recordemos que más del 60 % de las pymes que sufren un ataque grave terminan cerrando en los siguientes meses debido al impacto financiero y de operaciones que conlleva. (Esta estadística alarmante, citada a menudo en la industria, subraya la importancia de prevenir incidentes antes de que sea tarde). La **cultura de seguridad** empieza por reconocer riesgos y responsabilidades desde el inicio.

CONTINUAR

Unidad 2: Riesgos típicos y pymes

Ahora que manejamos los conceptos básicos, pasamos a los **riesgos concretos más comunes** que afrontan las pymes en el mundo digital actual. Las pequeñas empresas suelen ser objetivo de ciertos tipos de ataques motivados por su información financiera, sus sistemas menos maduros en seguridad o simplemente por ataques masivos oportunistas.

Aquí describiremos cuatro categorías principales de amenazas actuales:

- *Phishing* **(y en particular el fraude tipo BEC)**
- *Ransomware* **(y extorsión)**
- **Malconfiguraciones y** *Shadow IT* (problemas de configuración y TI en la sombra que abren brechas)
- **Ataques vía terceros y cadena de suministro**

Por cada tipo, explicaremos de qué se trata, daremos ejemplos reales y sugeriremos medidas de protección enfocadas en pymes.

Phishing y BEC (Business Email Compromise)

El *phishing* es quizás la amenaza más difundida y con mayor éxito contra todo tipo de organizaciones, incluidas las pymes. Consiste en estafas mediante engaños digitales, típicamente correos electrónicos fraudulentos que aparentan provenir de fuentes confiables, con el fin de engañar al destinatario para que revele información sensible o realice alguna acción que beneficie al atacante. Los atacantes de *phishing* se hacen pasar por bancos, proveedores, compañías conocidas o incluso compañeros de trabajo, para solicitar credenciales, números de tarjeta, o inducir la descarga de *malware*.

Algunos indicadores clásicos de un correo de *phishing* incluyen:

- mensajes urgentes o alarmistas (“¡Su cuenta será suspendida, actúe ahora!”);
- remitentes que imitan organizaciones legítimas pero cuyo correo real es sospechoso (dominio extraño o con errores ortográficos);

- saludos genéricos (“Estimado usuario” en lugar de su nombre);
- errores de ortografía/gramática; o
- enlaces adjuntos que no coinciden con la URL legítima al pasar el cursor.

Las campañas de *phishing* pueden enviarse masivamente (*phishing* tradicional) o personalizarse a un blanco específico (*spear phishing*).

Dentro del *phishing*, un tipo muy dañino para empresas es el conocido como **BEC (*Business Email Compromise*)** o **fraude del CEO**. En estas estafas dirigidas, el atacante **se hace pasar por el CEO/gerente o un alto ejecutivo** de la empresa (o alguien de confianza, como un proveedor habitual), y envía un correo engañando a un empleado con acceso a finanzas o datos sensibles. El correo suele tener tono urgente y **confidencial**, pidiendo, por ejemplo, que se realice una transferencia de dinero a cierta cuenta, o que se envíe información financiera de inmediato, *sin seguir los procedimientos normales “por ser una situación especial”*. Los estafadores aprovechan la autoridad de la figura del jefe y la urgencia para que el empleado no dude.

Un caso real ilustrativo es el de **una clínica de fisioterapia en Cantabria (España)**: los propietarios (Aurora y Sergio) se ausentaron simultáneamente por motivos laborales y dejaron la clínica a cargo

del personal. Un atacante aprovechó para enviar un correo a un administrativo, Alfonso, **haciéndose pasar por Aurora (la CEO)**. Le pidió con urgencia que asistiera en una *operación financiera confidencial*. Alfonso, creyendo que su jefa real le escribía, respondió dispuesto a colaborar. En el siguiente mensaje, el impostor (aún como "Aurora") le solicitó datos bancarios y el saldo de la cuenta de la empresa para completar una supuesta compra de equipamiento, insistiendo en que no hablara de ello con nadie por ser confidencial. Afortunadamente, en ese momento Alfonso notó cosas extrañas (la clínica no tenía planeada ninguna compra de maquinaria y nunca se le habían pedido ese tipo de datos por *e-mail*) y decidió telefonear a Aurora para confirmar. Así **descubrieron el fraude antes de que se consumara**.

En este caso, la **señal de alarma** fue la petición inusual y el secretismo. El error inicial de Alfonso fue **no verificar la dirección de correo remitente**: de haber revisado, seguramente habría notado que, aunque el nombre decía "Aurora X", el *e-mail* provenía de una dirección diferente a la corporativa real. Esta verificación sencilla es una de las principales recomendaciones para evitar BEC: siempre comprobar que la dirección (lo que va después del @) coincida exactamente con la oficial de nuestro jefe/compañero. Los atacantes suelen usar dominios parecidos (p. ej., *empresa.com* vs. *empressa.com*) o cuentas gratuitas con el nombre de la persona.

Otro ejemplo común de BEC es el **fraude del proveedor**: el atacante se hace pasar por un proveedor de confianza y envía a Cuentas por Pagar de la empresa un correo diciendo que han cambiado de cuenta bancaria, que por favor a partir de ese momento transfieran los pagos a una nueva cuenta (controlada por el delincuente). Si la empresa no verifica directamente con el proveedor, podría enviar pagos legítimos al estafador. Este timo ha costado millones a empresas de todos los tamaños.

En general, ***phishing* y BEC explotan el eslabón más débil: el humano,** mediante ingeniería social. Para pymes, que quizá no disponen de avanzados filtros de seguridad, la *concienciación del personal* es la defensa número uno. A continuación, algunas medidas concretas:

- **Dar capacitación regular** a todos los empleados sobre cómo identificar correos sospechosos. Que sepan los signos típicos y que, ante la duda, pregunten a TI o a un supervisor antes de clicar. Simulaciones internas de *phishing* pueden ser útiles para entrenar.
- **Establecer políticas claras** para transacciones. Por ejemplo, definir que *ninguna transferencia ni pago importante se hará únicamente basado en un* e-mail. Siempre debe haber una verificación adicional por otro canal (una llamada telefónica al ejecutivo/proveedor, o doble aprobación). Implantar la **regla de**

doble verificación para operaciones financieras puede frustrar un BEC, aunque alguien caiga inicialmente.

- **Realizar una verificación técnica del remitente.** Configurar los servidores de correo con medidas como SPF, DKIM y DMARC ayuda a bloquear correos "spoofeados" que fingen venir de nuestro propio dominio. Aunque no evita que usen cuentas de otros dominios, sí elimina intentos directos de suplantar nuestro correo corporativo. SPF, DKIM y DMARC son tres protocolos de autenticación de correo electrónico que, en conjunto, protegen un dominio contra la suplantación de identidad y mejoran la entregabilidad de los correos, permitiendo que solo servidores autorizados envíen mensajes en nombre de un dominio y que el contenido del correo no sea modificado. El **SPF** autoriza servidores de envío, **DKIM** firma digitalmente los mensajes para verificar su contenido, y **DMARC** indica a los servidores receptores qué hacer si los correos fallan las verificaciones de SPF o DKIM, como marcarlos como *spam* o descartarlos.
- **Mantener simples hábitos de comprobación.** Enseñar a los usuarios a inspeccionar la dirección completa del remitente y a desconfiar de solicitudes urgentes de secreto. Fomentar una cultura donde no esté mal visto *llamar para confirmar* peticiones anómalas, incluso si aparentemente vienen del jefe.
- **Protecciones técnicas.** Usar filtros *antispam* y *antiphishing* en el servicio de correo (muchos proveedores ya detectan y alertan

de *e-mails* potencialmente fraudulentos), mantener actualizado el antivirus (por si algún adjunto malicioso pasa el correo, que sea frenado al intentar ejecutarse), y, si es posible, soluciones de seguridad de correo corporativo que detecten patrones de BEC (algunas soluciones de seguridad detectan cuando un nombre interno es usado desde fuera, etc.).

En caso de recibir un correo sospechoso, **no hay que responder ni hacer clic en enlaces**. Lo indicado es reportarlo (si se tiene un área de TI o seguridad, o incluso al INCIBE en España mediante sus canales de ayuda), y borrar el mensaje. Si, por desgracia, se hizo clic en un enlace y se ingresaron credenciales en una página falsa, se debe **cambiar la contraseña de inmediato** y monitorear posibles accesos indebidos, además de informar para que tomen medidas (p. ej., avisar a clientes si corresponde).

Ejemplo práctico: phishing/BEC

A continuación, veremos un **correo electrónico real** utilizado en un intento de fraude tipo CEO (datos ligeramente anonimizados). Analizaremos sus características para aprender a detectarlos a tiempo.

En este mensaje, el atacante suplanta la identidad de la CEO (**Aurora**) para solicitar a un empleado (**Alfonso**) que le proporcione

información financiera de la empresa y realice una gestión confidencial. Nótese el tono urgente y la petición de secreto absoluto, típicos de este tipo de fraude.

Como se aprecia en la figura, el correo tiene asunto "RE: CONFIDENCIAL" y en el cuerpo dice, entre otras cosas: "Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie… Necesito que me indiques el saldo con el que contamos y el número de cuenta." Estos elementos son **señales de alarma**:

1. **Solicitud fuera de procedimiento:** pedir saldo de cuentas y mantenerlo en secreto no es una práctica normal. Los ciberdelincuentes buscan que la víctima *no consulte* con nadie más ("no hables de esto con nadie en la empresa") para aislarla y evitar que otro detecte el fraude. Un empleado entrenado sabría que una petición legítima de este estilo *siempre* se verificaría por otro medio.
2. **Urgencia y autoridad:** el tono da a entender que viene de la jefa (Aurora) y que es algo urgente en curso ("estamos efectuando una operación financiera…"). La víctima siente presión de cumplir rápido una orden del superior, pasando por alto medidas de comprobación.
3. **Remitente falsificado:** aunque en la captura no se ve la dirección, habría que revisar si el *e-mail* proviene del dominio

corporativo real o de uno simulado. Este es el paso crucial: al hacer clic en el nombre “Aurora X”, se revelaría la dirección, que en el caso real era algo como “aurora.<apellido>@gmail.com”, en lugar del correo corporativo de Aurora. Esa discrepancia confirmaría el intento de fraude.

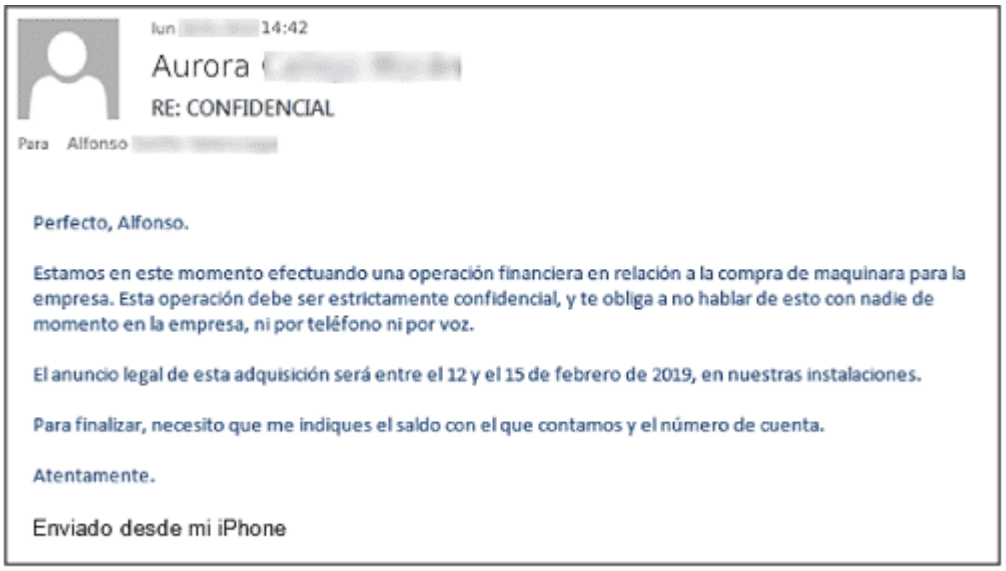
4. **Idioma/redacción:** en ocasiones, estos fraudes vienen en español correcto (más cuando el atacante investiga a la empresa objetivo), pero si fuera un *phishing* genérico, podría traer errores de idioma o expresiones extrañas. En este ejemplo, el correo estaba bien escrito en general, lo que lo hace más creíble. Aun así, se habla de “anuncio legal de la adquisición entre el 12 y 15 de febrero”: los atacantes a veces incluyen detalles así para sonar formales, pero, justamente, si no concuerda con la realidad de la empresa, es indicativo de engaño.

Lección

Para responder a un posible BEC, *siempre debemos verificar por un canal alternativo*. En la historia real, Alfonso llamó por teléfono a Aurora directamente y descubrió que el *e-mail* era falso. Esa simple acción evitó una posible pérdida financiera. Las empresas deben fomentar la confianza para que los empleados verifiquen órdenes inusuales sin temor. Mejor pasar cinco minutos confirmando que perder miles de euros por un fraude.

En conclusión, el *phishing* en todas sus formas (*e-mails*, SMS, *smishing*, llamadas, *vishing*) implica un riesgo **muy alto** para pymes porque **no requiere que el atacante "hackee" técnicamente nada; basta con engañar a alguien**. Y con técnicas cada vez más sofisticadas (correos muy verosímiles, incluso suplantación de dominios mediante caracteres Unicode, etc.), cualquiera puede ser víctima si no está alerta. Por eso, la inversión en **educación y procedimientos** *antiphishing* probablemente tenga el mejor retorno para la seguridad de una pequeña empresa.

Figura 2: Captura de un correo fraudulento de tipo BEC


lun 14:42

Aurora

RE: CONFIDENCIAL

Para Alfonso

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

Fuente: captura de pantalla de correo fraudulento de tipo BEC.

Ransomware y extorsión —

Otra amenaza gravísima y tristemente frecuente es el ***ransomware***. Se trata de un tipo de *malware* (*software* malicioso) que, una vez dentro del sistema de la víctima, **cifra (encripta) los archivos** o bloquea por completo el dispositivo, de forma que la víctima pierde el acceso a sus datos o sistemas. Acto seguido, el programa malicioso muestra un mensaje donde se exige el pago de un rescate (***ransom***, en inglés) a cambio de la clave para descifrar los archivos o restaurar el sistema. Es, esencialmente, un **secuestro digital**: los datos quedan "tomados como rehenes".

El *ransomware* puede ingresar por múltiples vías: adjuntos infectados en *phishing*, descargas ocultas al navegar por sitios comprometidos, vulnerabilidades en servicios expuestos (algunos gusanos de *ransomware* buscan servidores mal protegidos en Internet), memorias USB infectadas, etc. Una vez activa, la **capacidad destructiva** es enorme: en minutos puede cifrar documentos ofimáticos, bases de datos, fotos y cualquier otro archivo de valor, volviéndolos inútiles (quedan como garabatos irreconocibles). A menudo también **borra o cifra copias de seguridad locales** si las encuentra, y puede propagarse por la red a otros equipos compartidos. Finalmente, presenta la nota de rescate –por ejemplo, un archivo TXT o una pantalla– indicando cuánto dinero (usualmente en criptomonedas como bitcoin) se debe pagar y a dónde, para, supuestamente, recibir la herramienta de descifrado.

Para una pyme, un ataque de *ransomware* puede **paralizar completamente sus operaciones**. Imagina una asesoría contable que pierde todos los libros contables de clientes, o una empresa de logística que ve sus sistemas inaccesibles justo en temporada alta. Además, los rescates exigidos pueden ser cuantiosos –desde unos pocos cientos de dólares (en ataques masivos no dirigidos) hasta decenas o cientos de miles en ataques dirigidos a empresas con capacidad de pago.

En años recientes, los grupos de *ransomware* han añadido una táctica de **doble extorsión**: no solo cifran los archivos, sino que también **roban una copia de los datos** antes. Entonces, piden el pago no solo por la clave de descifrado, sino también con la amenaza de que, si no se paga, publicarán o venderán la información robada. Esto pone a las víctimas en una doble presión: incluso si tienen respaldos para restaurar sus sistemas, el atacante puede filtrar datos confidenciales (clientes, secretos comerciales, etc.) y provocar una brecha de datos. Un caso real ocurrió en Argentina en 2023: la **Comisión Nacional de Valores (CNV)** sufrió un ataque de *ransomware* donde los atacantes robaron más de 1,5 terabytes de documentación y exigieron USD 500 000 para no divulgarla. La entidad decidió no pagar alegando que eran datos públicos, pero días después los ciberdelincuentes comenzaron a filtrar documentos internos con información sensible (credenciales, actas, denuncias), evidenciando así la extorsión. Este es un ejemplo

de cómo el daño reputacional y legal puede ser serio aun si se logra restaurar todo desde *backups*.

¿Qué pueden hacer las pymes frente a esta amenaza?

PREVENCIÓN ANTE RANSOMWARE:	EJEMPLO PRÁCTICO: RANSOMWARE	MALCONFIGURACIONES Y SHADOW IT	EJEMPLO PRÁCTICO: SHADOW IT ABRE UNA BRECHA EN UNA EMPRESA DE MARKETING

- **Respaldos (*backups*) frecuentes y *offline***: la mejor póliza de seguro contra *ransomware* es tener copias de seguridad **desconectadas** de la red principal (para que el propio *malware* no las cifre). Se debe seguir la regla **"3-2-1"**: al menos 3 copias en 2 medios distintos, 1 de ellas fuera de sitio u *offline*. Por ejemplo, *backups* diarios automáticos a un servicio en la nube *con versionado* (que permita recuperar versiones antiguas de archivos, no solo sobrescribir), y *backups* semanales en un disco externo que luego se desconecta y se guarda aparte. Así, si ocurre un incidente, se puede restaurar la información con mínima pérdida.
- **Mantener sistemas actualizados**: muchas variantes de *ransomware* explotan vulnerabilidades conocidas del sistema

operativo o aplicaciones (un caso famoso fue WannaCry en 2017, que aprovechó una vulnerabilidad de Windows para propagarse a equipos no parcheados). Instalar las actualizaciones de seguridad en cuanto estén disponibles cierra puertas de entrada.

- ***Antimalware* y monitoreo**: usar un buen antivirus/*antimalware* actualizado en todos los equipos puede detectar *ransomware* conocido antes de que encripte (por firma), o incluso comportamientos típicos (por heurística, p. ej., actividad repentina de cifrado de muchos archivos). Hoy muchos antivirus tienen protección específica *antiransomware*. No es infalible, pero es una capa importante. También, si es posible, se debe monitorear la red local para ver actividad inusual (por ejemplo, herramientas de EDR –*Endpoint Detection & Response*– en empresas un poco más grandes).
- **Principio de menor privilegio**: los daños de *ransomware* se agravan si el usuario infectado tiene amplios accesos en la red. Es buena práctica dar a cada usuario solo los permisos necesarios. Por ejemplo, si el recepcionista solo necesita su carpeta y no accede al servidor de contabilidad, delimitar eso. Así, si su PC es infectada, el *malware* no podrá cifrar archivos en el servidor de contabilidad porque su cuenta no tiene permiso.
- **Segmentación de la red**: en lugar de una red plana donde cualquiera llega a cualquier recurso, segmentar (p. ej.,

separación VLAN o redes distintas para administración vs. empleados) puede frenar la propagación. Si un equipo de empleados se infecta, no alcanza automáticamente los servidores críticos.

- **Concienciación**: el *ransomware* suele entrar vía *phishing* (un adjunto de factura, CV, etc., malicioso). Capacitar a los empleados para no abrir archivos dudosos ni macros en documentos desconocidos es crucial (va de la mano con lo tratado en *phishing*). También es necesario evitar dispositivos USB de origen incierto.
- **Protección de RDP y accesos remotos**: muchas pequeñas empresas habilitan escritorio remoto (RDP) para que el dueño o soporte acceda. Los atacantes buscan servicios RDP expuestos y prueban contraseñas (fuerza bruta o credenciales filtradas). Es imprescindible poner contraseñas fuertes, limitar por *firewall* el acceso solo desde IP conocidas o activar autenticación multifactor. Mejor aún: usa una VPN segura para acceder a RDP, en lugar de exponerlo directamente.
- **Plan de respuesta**: tener un plan en caso de que, pese a todas las medidas, ocurra. Saber **qué hacer**: desconectar máquinas de la red al detectar un cifrado para aislar la infección, contactar a expertos/autoridades, no apagar la máquina (porque puede ayudar a análisis) y aprender a restaurar *backups* rápidamente para reducir el tiempo de inactividad.

¿Se debe pagar el rescate? La postura general de autoridades y expertos es **no pagar**, porque no garantiza recuperación (hay casos en que aun pagando no dieron la clave o esta no funcionó bien), incentiva a los criminales a seguir atacando, y en algunos países podría considerarse financiar actividad ilícita. Sin embargo, la realidad es que algunas empresas terminan pagando cuando se ven acorraladas (por ejemplo, si no tenían respaldos y su negocio está parado, o si la filtración puede ser ruinosa). Es una decisión difícil. Lo ideal es nunca estar en esa situación, gracias a las medidas preventivas mencionadas. Cabe notar que incluso pagando, si fue doble extorsión, la información pudo haber sido copiada; nada garantiza que no la vendan más adelante. Así que de nuevo: ***backups* + protección** para no depender de la "buena fe" de un delincuente.

PREVENCIÓN ANTE RANSOMWARE:	EJEMPLO PRÁCTICO: RANSOMWARE	MALCONFIGURACIONES Y SHADOW IT	EJEMPLO PRÁCTICO: SHADOW IT ABRE UNA BRECHA EN UNA EMPRESA DE MARKETING

Una pyme de diseño gráfico, StudioColor, es golpeada por *ransomware*.

StudioColor tiene 5 empleados, y almacenan todos los proyectos de clientes (archivos de imagen, Photoshop, ilustraciones) en una PC que hace de servidor compartido en la oficina. Un día, el encargado

descarga lo que cree que es un *pack* de fuentes tipográficas de un sitio web dudoso. Al abrir el ejecutable, no ocurre nada aparente… Hasta que, horas después, notan que **no pueden abrir ningún archivo** en la carpeta compartida: todos los nombres de archivos tienen ahora extensión *.locked y hay un archivo, *_LEAME.txt,* con instrucciones. El mensaje dice que sus archivos fueron cifrados y que envíen 0,5 bitcoins (unos €12 000) a una dirección para recuperarlos, y amenazan que, si no pagan en 72 horas, la clave se destruirá.

La empresa entra en pánico: **todos los trabajos de los últimos meses quedaron inaccesibles**, incluyendo proyectos en curso. ¿Tenían *backups*? Solo parciales y antiguos: el dueño hizo una copia de la carpeta compartida seis meses atrás en un disco USB, pero muchos archivos recientes no están respaldados. Evaluando el daño, ven que *todas las PC* de la oficina tienen archivos cifrados, no solo el servidor: el *ransomware* se propagó por la red local aprovechando que comparten todo sin segmentación, y posiblemente mediante credenciales administradoras comunes en todos los equipos.

- **Impacto:** negocio detenido, no pueden entregar trabajos a tiempo, reputación en juego con clientes. El rescate de 0,5 bitcoins es enorme para ellos, y no tienen garantía de que pagando recuperarán todo.

- **Respuesta:** deciden *no pagar* de entrada e intentan restaurar lo posible. Rescatan la copia de hace 6 meses para recuperar algo de los proyectos finalizados (perderán lo reciente). Contratan un servicio externo de respuesta a incidentes. Este les ayuda a **identificar la variante de *ransomware***; resultó ser una donde ya se conocía una herramienta de descifrado gratuita (no siempre ocurre, pero tuvieron suerte relativa). Logran restaurar parte de los archivos usando esta herramienta, aunque los más nuevos se pierden. Pasan semanas complicadas rehaciendo trabajo perdido y negociando con clientes plazos de entrega. Finalmente sobreviven, pero el dueño calcula que el incidente costó en total casi €15 000 entre días de productividad perdidos, servicios técnicos y descuentos a clientes insatisfechos.
- **Lecciones aprendidas:** StudioColor implementa inmediatamente un plan de *backups* 3-2-1, segmenta la red para que las PC de diseño no tengan acceso directo a la PC de administración, instala antivirus de mejor calidad en todos los equipos y refuerza la política de descargas (ahora solo se permite descargar *software* de fuentes verificadas). Un año después, sufren otro intento de *ransomware* vía un correo de *phishing*, pero el antivirus lo detiene y, además, los empleados ahora están conscientes y alertaron en seguida al ver algo sospechoso. El segundo incidente no causa daño gracias a las mejoras hechas.

El *ransomware* es un enemigo formidable, pero **podemos limitar su poder** con prevención y preparación. Para una pequeña empresa, **la diferencia entre un susto y la catástrofe** estará en si existen o no copias de seguridad viables y actualizadas. Ninguna empresa, por pequeña que sea, debería prescindir de *backups*, considerando la amenaza actual.

PREVENCIÓN ANTE RANSOMWARE:	EJEMPLO PRÁCTICO: RANSOMWARE	MALCONFIGURACIONES Y SHADOW IT	EJEMPLO PRÁCTICO: SHADOW IT ABRE UNA BRECHA EN UNA EMPRESA DE MARKETING

Este apartado cubre riesgos que podríamos llamar “de la casa”, es decir, fallos internos en cómo configuramos o gestionamos nuestra tecnología. Muchas brechas de seguridad no se deben a un *hacker* supersofisticado, sino a **errores simples en la configuración** de sistemas o a un **uso no controlado de tecnología** por parte de empleados. En pymes, donde a veces la infraestructura es instalada “rápido y como venga” y no siempre por expertos en seguridad, es **muy común** tener **malconfiguraciones** peligrosas sin saberlo.

Malconfiguraciones (*misconfigurations*) se refiere a cualquier configuración incorrecta o insegura de un sistema que lo deja vulnerable. Ejemplos típicos:

- Servidores o bases de datos expuestos a Internet **sin protección** (por ejemplo, instalar una base de datos MongoDB y no establecer contraseña de *admin*, algo que ha ocurrido miles de veces, dejando datos abiertos al mundo).
- **Puertos abiertos innecesarios** en un *firewall* o *router*. Quizá para una prueba se abrió el puerto 3389 (escritorio remoto) o 21 (FTP) y nunca se cerró; los atacantes escanean rangos de IP buscando justo esos servicios para explotar.
- **Uso de credenciales por defecto** o triviales: muchos dispositivos (*routers*, cámaras IP, NAS) vienen con usuario/clave conocidos ("admin/admin"). Si no se cambian, son invitaciones a intrusos. De hecho, hay *bots* automatizados que recorren Internet probando iniciar sesión con claves por defecto.
- **Configuraciones deficientes de seguridad web**: un ejemplo es no forzar HTTPS en un sitio web que maneja contraseñas, permitiendo que alguien en la misma red pueda interceptar credenciales (ataque *man-in-the-middle*). Otro ejemplo es no configurar correctamente los permisos en un almacenamiento en la nube: ha pasado que empresas suben información a un *bucket S3* de Amazon o a un Google Drive, pero lo dejan "público" por error, exponiendo así datos sensibles a cualquiera que encuentre el enlace.

- **Políticas laxas en servicios *cloud***. Por ejemplo, una malconfiguración en Azure AD o Google Workspace que permita que cualquier empleado pueda compartir datos externamente sin restricción, o que usuarios sin MFA puedan acceder a la consola de administración desde fuera.
- **Sistemas no actualizados** (falta de parches) a veces se consideran malconfiguración también, en el sentido de que no mantener un sistema al día "es configurar inseguridad". Muchas infecciones (como el gusano WannaCry) afectaron a empresas que no habían aplicado parches críticos disponibles desde hacía meses.

Las malconfiguraciones son peligrosas porque **son inadvertidas**: la empresa cree que todo funciona bien (y de hecho, funcionalmente el sistema anda), pero no se da cuenta de que hay una ventana abierta. Por ejemplo, un emprendedor instala él mismo la tienda *online* en un servidor AWS y, para probar, desactiva el *firewall*; luego se olvida de activarlo de nuevo. Todo marcha hasta que un día descubren que alguien encontró el puerto de base de datos abierto e hizo estragos.

En cuanto a ***Shadow IT***, ya lo explicamos anteriormente: es cuando empleados usan tecnología a espaldas o sin control del área de TI. Esto incluye *hardware* (dispositivos personales enchufados) y *software*/servicios (*apps* instaladas sin permiso, cuentas en la nube

no autorizadas). El *Shadow IT* **amplía la superficie de ataque** y genera malconfiguraciones por informalidad. Por ejemplo, si un empleado crea por su cuenta un formulario en un servicio web para recolectar datos de clientes, puede que lo configure mal y esos datos queden públicos; además, la empresa ni sabrá que esos datos están ahí, para protegerlos o integrarlos en sus políticas de privacidad. O un clásico, usar WhatsApp personal para enviar información de la empresa: se pierde control de esos mensajes, y aunque sea práctico, podría suponer compartir documentos internos en un medio no supervisado.

Tanto malconfiguraciones como *Shadow IT* suelen ser consecuencia de **falta de conocimiento o de prisa**: el sistema se pone a funcionar rápido para cumplir una necesidad, y la seguridad se deja "para después" (a veces nunca llega ese después).

¿Cómo mitigar estos riesgos en pymes?

- En primer lugar, **tomar inventario** de lo que se tiene: qué sistemas, dispositivos y aplicaciones hay en uso. Sin un inventario, es imposible saber qué puede estar mal configurado.
- Luego, aplicar **buenas prácticas básicas de configuración segura**: cambiar contraseñas por defecto en todo equipo/*software*, cerrar puertos no utilizados en el *router*/*firewall*, deshabilitar servicios que no se necesiten, revisar

periódicamente las cuentas de usuario (borrar las obsoletas), y seguir guías de endurecimiento (*hardening*) para los sistemas operativos y aplicaciones principales. Muchas veces basta con seguir listas de chequeo sencillas para mejorar significativamente la postura. Por ejemplo, Microsoft ofrece guías de seguridad para Windows Server, WordPress tiene recomendaciones de *hardening*, etc.

- De vez en cuando, **tener auditorías internas sencillas**: alguien (interno o un consultor externo si se puede) debe evaluar la configuración. Por ejemplo, probar si los servicios en nube de la empresa están compartiendo algo público sin querer (hay herramientas que escanean espacios *cloud* en busca de datos expuestos) o usar escáneres de vulnerabilidades gratuitos para la web corporativa y la red interna, que a menudo detectan configuraciones débiles (un escaneo podría alertar "el puerto tal responde, cuidado").

- Para el ***Shadow IT***, es más una cuestión de **políticas y educación**. Hay que recordar a los empleados que usar herramientas no aprobadas puede ser un peligro para la empresa; crear canales para que pidan soluciones (por ejemplo, si necesitan transferir archivos grandes, ofrecerles un servicio controlado por TI en lugar de que cada uno use lo que encuentre). Aun así, es difícil eliminar completamente el *Shadow IT*, por lo que también conviene **monitorizar**: existen

soluciones que detectan tráfico sospechoso saliente (por ejemplo, si muchos empleados están usando Dropbox, se puede notar en el tráfico y quizás oficializar una alternativa). También se puede implementar un *proxy* o *firewall* que limite descargas de ejecutables y acceso a ciertos sitios, y reducir así la instalación de *software* no autorizado.

- **Concienciación en protección de datos**: muchos casos de *Shadow IT* implican subir datos corporativos a servicios externos sin garantías. Enseñar sobre reglamentos (como GDPR para datos personales) puede hacer que los empleados piensen dos veces antes de, por ejemplo, mandar por Gmail personal una base de datos de clientes. Deben entender que hay implicaciones legales y de seguridad.

En definitiva, las malconfiguraciones y *Shadow IT* son fallos **evitables** si se presta un poco de atención. A veces la diferencia entre estar seguro o expuesto es solo marcar una casilla de "Requiere autenticación" en una herramienta o desactivar una opción. En pymes sin personal dedicado, puede ayudar apoyarse en consultores externos para una revisión inicial de seguridad de la configuración (muchas empresas de IT ofrecen "tuneo" de seguridad básico). Pero incluso sin eso, con curiosidad y voluntad, los propios dueños/empleados pueden leer las guías del fabricante y aplicar correcciones. **La seguridad no es solo comprar productos, es configurar bien lo que ya tenemos.**

CreativeCo es una agencia de *marketing* digital con 15 empleados. No tienen un departamento de TI formal; cada empleado administra más o menos su equipo. Uno de los diseñadores, para compartir archivos grandes con un cliente, decidió usar su cuenta personal de un servicio gratuito en la nube (porque el correo corporativo tenía límite de adjunto). Subió allí varias carpetas con materiales de campañas, incluyendo listas de contactos e imágenes no públicas. Lo compartió con el cliente vía un enlace. Meses después, tras finalizar el proyecto, olvidó eliminar esos archivos de su nube personal.

Mientras tanto, la misma persona instaló por su cuenta un *software* de edición de video descargado de una página poco confiable (versión *crackeada* para no pagar licencia). Ese *software* resultó tener *spyware*. El atacante obtuvo información del sistema de la víctima y encontró en un archivo de texto una nota con contraseñas (otro mal hábito). Con un poco de ingeniería social, descubrió que las credenciales eran del correo corporativo del diseñador. Accedió al correo y desde ahí buscó más información de la empresa.

No halló mucho, pero vio referencias a la carpeta en la nube (por el enlace compartido). Probó acceder, y efectivamente el enlace seguía activo con todo el material. Entre los datos encontró un Excel con una lista de *leads* (potenciales clientes) de un proyecto, con nombres, *e-mails*, presupuesto estimado, etc. Esa información podría venderse a competidores. Antes de que el atacante hiciera algo más, afortunadamente el Departamento de Ventas descubrió que alguien estaba enviando correos sospechosos a esos *leads* haciéndose pasar por CreativeCo (posiblemente el atacante intentando estafar). Investigando, detectaron la cadena de fallos: *software* pirata -> robo de credenciales -> exposición de datos en nube personal.

Este incidente *no debería haber ocurrido*:

- Si CreativeCo hubiese provisto un método seguro para compartir archivos (por ejemplo, OneDrive/Google Drive corporativo con políticas), el diseñador no habría recurrido a su cuenta personal.
- Si hubiesen tenido una política de "nada de *software* no autorizado", o al menos antivirus activo, el *spyware* se habría detectado.
- Si las contraseñas no hubiesen estado guardadas en texto plano, el atacante no habría escalado.
- Si se revisaran los accesos a datos, podrían haber invalidado ese enlace de nube una vez terminado el proyecto.

Después del incidente, la agencia tomó varias medidas: compraron suscripciones empresariales de almacenamiento en la nube y prohibieron usar cuentas personales para temas de trabajo (y lo monitorean); concientizaron sobre no instalar *software* pirata y pasaron un antivirus a todos los equipos; forzaron un cambio de todas las contraseñas y activaron autenticación en dos pasos en los correos; implementaron una *policy* donde cualquier herramienta nueva debe ser consultada antes con el encargado TI *freelance* que contratan. Desde entonces, no han tenido más sustos de este tipo.

Moraleja: muchas brechas se dan **sin un *hacker* directo**, por configuraciones débiles o prácticas inseguras internas. La seguridad es tan fuerte como el más débil de nuestros eslabones mal configurados. Una pyme debe esforzarse en cerrar esos huecos obvios: son arreglos de coste bajo (a veces es solo educar o apretar un botón en una configuración), pero con alto impacto en reducir riesgo.

Terceros y cadena de suministro —

Para terminar, un tipo de riesgo que ha cobrado relevancia en años recientes: los ataques a través de **terceros**. Las pymes, igual que las

grandes empresas, dependen de proveedores y socios de negocio para numerosas funciones (servicios de TI, *software* de terceros, empresas de logística, consultores, etc.). Esta **cadena de suministro** digital u organizativa puede convertirse en una vía de ataque. Es decir, aunque tu empresa tenga las puertas cerradas, *¿qué pasa con las puertas de tus proveedores?* Si alguien entra por allí y tú estás conectado, puedes salir perjudicado.

Un **ataque a la cadena de suministro** ocurre cuando los atacantes comprometen a una organización a través de vulnerabilidades en sistemas de un tercero confiable que se integra con la organización. En otras palabras, "*hackean* al vecino para llegar a ti". Veamos algunos ejemplos:

- Caso *software*: en 2020, la compañía SolarWinds (proveedora de un popular *software* de monitoreo usado por miles de empresas y gobiernos) fue comprometida, y los atacantes alteraron una actualización de su *software*, la cual se distribuyó automáticamente a todos los clientes. Esto permitió espiar redes de muchísimas organizaciones que confiaban en SolarWinds. Cada cliente tenía su seguridad, pero confiaron ciegamente en el *software* del proveedor –allí estuvo el talón de Aquiles.
- Caso servicios administrados: un ejemplo más cercano a pymes es el ataque a **Kaseya** en 2021. Kaseya provee herramientas de administración de TI usadas por proveedores de servicios

administrados (MSP) que atienden a muchas pymes. Los atacantes encontraron un fallo en la plataforma VSA de Kaseya y lo explotaron para distribuir *ransomware* disfrazado de actualización de *software* a los clientes de Kaseya. En efecto, *hackearon* al proveedor para hacer llegar *malware* a cientos de empresas gestionadas por esos MSP en todo el mundo. Muchas pymes sufrieron cifrado de datos vía este vector de confianza.

- Caso proveedores físicos: no todo es *software*. Recordemos cuando **Target** (grande minorista en EE. UU.) fue *hackeada* en 2013 a través del sistema de HVAC (aire acondicionado) que era mantenido por un proveedor. Los atacantes robaron credenciales de ese proveedor externo y mediante la VPN de mantenimiento entraron a la red de Target y extrajeron millones de tarjetas de crédito. Esto ejemplifica que un socio con pobre seguridad puede ser la brecha.

Para pymes, los riesgos de terceros pueden ser:

- ***Software* de terceros comprometido.** Usan algún *plugin*, sistema de gestión o incluso una página web de un socio que, si es atacado, expone datos de la pyme. Ejemplo: una aplicación SaaS donde suben información de clientes; si esa SaaS es *hackeada*, los datos quedan expuestos.
- **Proveedores con acceso a sistemas/datos.** Por ejemplo, un estudio contable externo que lleva tu contabilidad quizá tiene

credenciales para acceder a tu sistema de facturación en la nube; si ese estudio sufre *phishing* y le roban la contraseña, un extraño podría entrar a tus finanzas. O una agencia de *marketing* que lleva tu sitio web tiene las claves del servidor: si la agencia es comprometida, el sitio corre peligro.

- ***Hardware* o productos que compras con *malware* de fábrica.** Ha habido incidentes de dispositivos USB regalados en ferias que traían virus, o de *laptops* nuevas infectadas en la cadena de distribución. Es menos común, pero un riesgo al fin.
- **Ataques a proveedores críticos que impactan indirectamente.** Imagina que tu pyme depende 100 % de la plataforma de Shopify para vender. Un ataque a Shopify te deja sin operar, aunque tú no sufras intrusión directa. O si usas un servicio de correo transaccional y este es atacado, puede filtrarse tu base de datos de clientes porque estaba alojada allí.

¿Cómo mitigar estos riesgos? No es fácil, porque uno no controla las medidas de los demás, pero se pueden tomar acciones:

- **Diligencia debida al seleccionar proveedores:** incluir la seguridad como criterio al contratar servicios. Preguntar (o investigar) si el proveedor tiene certificaciones, políticas de seguridad, historial de incidentes. Por ejemplo, si vas a usar un sistema en la nube para datos sensibles, prefiere uno con buena reputación y medidas de cifrado, autenticación robusta, etc.

- **Cláusulas contractuales de seguridad:** aunque a veces las pymes no tienen poder de negociación, cuando sea posible, debes establecer acuerdos de confidencialidad y seguridad con los terceros, que se comprometan a notificar incidentes, a proteger apropiadamente tus datos, etc. Por ejemplo, si contratas a un desarrollador *freelance*, debes asegurarte contractualmente de que no se llevará tu código fuente a lugares inseguros y que borrará copias cuando termine.
- **Control de accesos de terceros:** no dar más acceso del necesario. Si un proveedor necesita entrar a tu sistema, créale un usuario específico con permisos limitados y ojalá temporales (que caduquen tras su trabajo). Hay que revocar accesos cuando ya no sean necesarios. Mantén un registro de "¿quién externo tiene llaves de qué?".
- **Segmentar integraciones:** si tienes integraciones con sistemas de proveedores (API, conexiones), intenta segmentar esos accesos en la red. Por ejemplo, si tu servidor se conecta con la API de un socio comercial, podría limitar esa comunicación a solo ese servidor, en lugar de tener toda tu red expuesta a la del socio.
- **Monitorear actividad anómala:** si un usuario de proveedor hace algo inusual (p. ej., tu contable externo descargando toda la base de clientes a medianoche), debería saltar una alarma.

Requiere herramientas o al menos revisión manual de *logs* de vez en cuando.

- **Plan de contingencia:** asume que un proveedor crítico puede caer. Tener un plan B si mañana tu *hosting* se cae por ataque, ¿tienes *backups* para migrar a otro? Si tu herramienta SaaS está fuera, ¿puedes operar manualmente un tiempo? Esto cruza con la continuidad del negocio.
- **Mantener *software* de terceros actualizado:** a veces la pyme usa *software* de terceros en casa (p. ej., un ERP local). Hay que aplicar parches de ese *software* también, no solo del SO. Los atacantes suelen apuntar a *software* popular sabiendo que muchos tardan en actualizar (p. ej., vulnerabilidad en *plugin* de WordPress, lo que deja a millones de sitios en riesgo).

En definitiva, **la confianza es un riesgo**. Hoy se habla de la **"confianza cero" (*Zero Trust*)** incluso hacia dentro de la empresa. De igual modo, hacia terceros debemos tener confianza cero por defecto. No hay que dar por sentado que "porque trabajamos con X, nuestros datos con X están a salvo". Debemos preguntar, verificar y limitar. Un dicho en seguridad: "Confía, pero verifica". En contexto de terceros, quizás sería "No confíes hasta verificar, y aun así, mantente alerta".

Ejemplo práctico: pyme textil afectada por proveedor de IT inseguro

Una fábrica textil, TelaFina S.A., con 80 empleados, contrató a una pequeña empresa de servicios de IT para que les administrara su red y sistemas (tercerizaron porque no tenían personal propio de IT). Esta empresa de servicios tenía otros clientes y usaba herramientas de acceso remoto para gestionar todos. Un día, TelaFina descubre que su servidor de archivos fue cifrado por *ransomware* **a pesar de tener políticas estrictas con sus usuarios internos**. Investigando, hallan que el punto de entrada fue la cuenta VPN del técnico de la empresa de IT: el técnico fue víctima de un *phishing*, los atacantes robaron sus credenciales y entraron por VPN como "usuario de soporte", y se movieron luego dentro de la red hasta instalar el *ransomware*.

Aquí, TelaFina sufrió por un **fallo de seguridad del proveedor**. ¿Qué podrían haber hecho?

- De entrada, exigir MFA en esa VPN (posiblemente hubiera evitado el uso de credenciales robadas).
- O bien, limitar la VPN del proveedor a ciertos horarios o servicios necesarios, no a toda la red.
- También se dieron cuenta de que el contrato con la empresa de IT no contemplaba responsabilidades en caso de incidentes; ahora están renegociando para incluirlo.

Veamos otro ejemplo: CasaElectro. Esta tienda minorista *online* utiliza una **plataforma de *e-commerce* de terceros** para su web. Un atacante no pudo *hackear* CasaElectro directamente, así que apuntó a la plataforma (que aloja cientos de tiendas). Consiguió explotar una vulnerabilidad en el código común de la plataforma y obtuvo números de tarjetas de miles de clientes de todas las tiendas. CasaElectro se enteró por las noticias. Tuvo que informar a sus clientes, sufrir inspecciones legales por fuga de datos, etc., **debido a una falla en su proveedor de *software***. Después de esto, decidieron migrar a otra plataforma con mejores prácticas de seguridad y reconocimientos en el mercado, aunque implicó costos.

Estos casos subrayan que **la ciberseguridad no termina en los límites de tu empresa**. En un mundo interconectado, hay que mirar más allá: nuestros aliados y proveedores pueden sin querer convertirse en amenazas si no gestionan bien su propia seguridad. Por eso, las pymes deben incluir en su matriz de riesgos los riesgos de terceros: tienen que evaluar con quién comparten datos o sistemas y cómo minimizan el daño en caso de que ese tercero sea comprometido.

Conclusiones:

Hemos cubierto los principales frentes de riesgo para las pymes: engaños dirigidos a personas (*phishing*/BEC), *malware* devastador (*ransomware*), fallos internos (configuración/*Shadow IT*) y debilidades en la cadena de confianza (terceros). Aún hay otros riesgos (fraudes bancarios, robo físico de dispositivos, etc.), pero muchos de esos se evitan aplicando las mismas buenas prácticas ya discutidas.

El mensaje clave es que, a pesar de contar con menos recursos, **una pyme puede y debe mejorar su seguridad de forma proactiva**. Con conocimiento fundamental (como el brindado en este módulo), pequeñas inversiones en tecnología adecuada y, sobre todo, la creación de una *cultura de seguridad* entre sus empleados, se pueden reducir en gran medida las probabilidades de ser víctima y limitar el impacto de los incidentes. En módulos posteriores, profundizaremos en cómo implementar medidas técnicas y de gestión para construir esa protección en capas.

Lecturas recomendadas y referencias

LISA Institute. (s. f.). *Diferencia entre Ciberseguridad y Seguridad de la Información.*

https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

(Se da una explicación detallada de estos conceptos y sus áreas de competencia).

Pallero, M., y Heguiabehere, J. M. (s. f.). *Seguridad de la información y ciberseguridad*. Fundación Sadosky (Argentina). https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

(Describe las propiedades de seguridad —confidencialidad, integridad, disponibilidad, autenticidad, no repudio— y fundamentos de gestión de riesgos).

IBM. (s. f.). *¿Qué es una superficie de ataque?*. https://www.ibm.com/es-es/think/topics/attack-surface

(Introduce la idea de superficie de ataque digital, física y de ingeniería social, con ejemplos de vectores comunes [contraseñas débiles, puertos mal configurados, etc.]).

INCIBE. (2024). *Shadow IT: lo que hay en la sombra de tu organización".* **https://www.incibe.es/empresas/blog/shadow-it-lo-que-hay-en-la-sombra-de-tu-organizacion**

(Explica qué es el *Shadow IT*, por qué surge, y los riesgos que conlleva para las empresas, así como recomendaciones para gestionarlo).

INCIBE. (2019). *Historias reales: el fraude del CEO.* **https://www.incibe.es/empresas/blog/historias-reales-el-fraude-del-ceo**

(Es un relato de un intento de fraude del CEO en una clínica [Auri y Alfonso] y la forma en que se detectó a tiempo. Incluye consejos para evitar caer en estos engaños de *Business Email Compromise*).

INCIBE. (2023). L*as principales vulnerabilidades de una pyme en materia de ciberseguridad.* **https://www.incibe.es/empresas/blog/las-principales-vulnerabilidades-de-una-pyme-en-materia-de-ciberseguridad**

(Resume las amenazas más frecuentes para pymes: *phishing*, *ransomware*, cadena de suministro, falta de formación, contraseñas débiles, falta de actualizaciones. Es una buena referencia para entender el panorama de riesgos en pequeñas empresas).

Hackmetrix Blog. (2025). *Ciberataques en empresas de Latinoamérica: Casos reales y cómo evitarlos.* **https://blog.hackmetrix.com/ciberataques-empresas-latinoamerica-casos-reales-como-evitarlos/**

(Describe, entre otros, el caso del ataque a la Comisión Nacional de Valores (AR) donde combinaron *ransomware* con extorsión de publicación de datos. Resulta útil para comprender la tendencia de la doble extorsión).

National Cybersecurity Alliance. (2023). *Cómo prevenir y recuperarse del ransomware.* **https://www.staysafeonline.org/es/articles/how-to-prevent-and-recover-from-*ransomware***

(Recurso práctico con pasos para prevenir infecciones de *ransomware* y cómo responder si ocurre una, orientado a

empresas y ciudadanos).

INCIBE. (s. f.). *TemáTICas Ransomware*. https://www.incibe.es/empresas/tematicas/*ransomware*

ISO 27001 y Gestión de Riesgos. (s. f.)

(Si se desea profundizar en estándares, se recomienda investigar la norma ISO/IEC 27001 [Sistemas de Gestión de Seguridad de la Información] e ISO 27005 [Gestión de Riesgos de SI]. Aunque quizás avanzadas para una pyme pequeña, dan un marco de referencia de buenas prácticas).

Sitio web de INCIBE Empresas: https://www.incibe.es/empresas .

(Contiene numerosos artículos, guías y herramientas gratuitas [como el "Kit de concienciación o Hazard": juego de mesa de ciberseguridad] diseñados para mejorar la seguridad en pymes. En particular, el "MOOC de ciberseguridad para pymes" es muy pertinente para complementar este curso).

CONTINUAR

Referencias

[Imagen sin título sobre tríada de seguridad de la información CIA]. (s. f.). https://kaa.wikipedia.org/wiki/Fayl:CIAJMK1209-en.svg

CONTINUAR