Operación diaria y respuesta básica

CÓRDOBA CREA FUTURO

Introducción

En este módulo abordaremos las prácticas cotidianas de seguridad y la respuesta inicial ante incidentes en una pyme. Los ciberataques contra pequeñas y medianas empresas van en aumento; un informe reciente reveló que 6 de cada 10 pymes argentinas sufrieron al menos un ataque en el último año, y la mayoría de los incidentes ni siquiera se detectaron a tiempo (Mercado, 2025). Esta realidad evidencia la importancia de estar preparados en el día a día: por un lado, fomentar la concientización en los empleados para prevenir amenazas comunes, como el *phishing*; y por otro, establecer procedimientos básicos de respuesta, o *playbooks* mínimos, para manejar alertas e incidentes cuando ocurran.

A continuación, en la unidad 1 nos enfocaremos en la concientización y el anti-*phishing*, proporcionando herramientas prácticas para que el personal identifique intentos de estafa y se mantenga alerta.

En la unidad 2 profundizaremos en *playbooks* mínimos de seguridad, es decir, procesos fundamentales de *triage* (evaluación y priorización de alertas), escalamiento de incidentes, documentación y lecciones aprendidas, adaptados a las capacidades limitadas de una pyme típica.

Con un enfoque pedagógico y ejemplos prácticos, buscaremos dotarnos de conocimientos para mantener la guardia en la operación diaria y reaccionar eficazmente ante amenazas básicas, asegurando la continuidad operativa y minimizando daños.

CONTINUAR

Lección 2 de 4

Unidad 1. Concientización y antiphishing

La primera línea de defensa en ciberseguridad es el usuario bien capacitado. En las pymes, donde el personal técnico suele ser reducido, concientizar a todos los empleados sobre las amenazas comunes —especialmente el *phishing*— resulta fundamental.

En esta unidad exploraremos los indicadores comunes de correos maliciosos para que cualquier empleado pueda reconocer señales de alerta. También veremos cómo implementar simulaciones básicas de phishing —incluso con herramientas gratuitas o de bajo costo— para entrenar al personal de forma práctica, y cómo medir su eficacia mediante métricas que nos permitan identificar mejoras. Por último, destacaremos la importancia de establecer un canal de reporte seguro en la organización, de modo que los empleados sepan cómo y a quién reportar un posible incidente o correo sospechoso.

Todo esto contribuye a crear una cultura de seguridad proactiva: cada empleado se convierte en un «sensor» capaz de detectar amenazas y activar la respuesta adecuada a tiempo.

Un correo de *phishing* es un mensaje fraudulento diseñado para engañar al destinatario y robarle datos sensibles —como credenciales o información financiera— o instalar *malware*. Estos mensajes suelen disfrazarse como comunicaciones legítimas de empresas conocidas —bancos, proveedores, sitios populares— para ganar la confianza de la víctima. Por suerte, la mayoría de los intentos de *phishing* contienen señales sutiles que podemos detectar si sabemos qué buscar.

A continuación, resumimos los **indicadores comunes** que delatan a un correo electrónico sospechoso:

- **Remitente extraño o dirección sospechosa**. Siempre debemos revisar quién envía el correo. ¿Es un remitente desconocido o un nombre familiar, pero desde una dirección inusual? Muchas veces el atacante falsifica el nombre mostrando, por ejemplo, «Banco X», pero la dirección real —lo que aparece tras el símbolo

<@>— no coincide con el dominio legítimo de ese banco. Por ejemplo, un correo que pretende ser del Banco Nación, pero proviene de notificaciones@bancoNacion.seguridad.ru es claramente malicioso. Del mismo modo, si proviene de alguien interno (un colega, el jefe), pero con un estilo de comunicación inusual o desde una cuenta personal, debemos desconfiar.

- **Destinatarios inusuales o genéricos**: los *phishers* a menudo envían correos masivos. Si el mensaje no está dirigido específicamente a nosotros —por ejemplo, si estamos en copia junto a personas que no conocemos, o si el saludo es genérico, como «Estimado cliente» en lugar de nuestro nombre—, podría tratarse de una estafa. En algunos casos, el campo «Para:» incluye expresiones como «Destinatarios no revelados», lo que también indica un envío masivo.

- **Asunto y contenido urgentes o alarmantes**: crear urgencia o miedo es una táctica común en el *phishing*. Frases como «¡Último aviso: su cuenta será suspendida!» o «Acción inmediata requerida por seguridad» buscan que reaccionemos sin pensar. Un asunto alarmante o amenazante, que apela al pánico, es un fuerte indicio. También es frecuente que indiquen que debemos actuar en un plazo muy breve —24 horas o «inmediatamente»— para evitar consecuencias. Este lenguaje apremiante casi nunca se encuentra en correos legítimos de empresas serias.

- **Errores de ortografía o gramática, formato poco profesional**: muchos correos de *phishing* contienen errores evidentes de redacción. Algunos ejemplos comunes son faltas de ortografía, frases traducidas de forma extraña, uso incorrecto de mayúsculas o minúsculas, entre otros. Las empresas cuidan mucho la calidad de sus comunicaciones, por lo que un texto descuidado es sospechoso. Estos errores, junto con logotipos de mala calidad o diseños inusuales, son señales de advertencia.

- **Enlaces sospechosos o archivos adjuntos extraños**: nunca debemos hacer clic sin revisar antes adónde lleva un enlace. Un truco útil es pasar el cursor por encima (sin hacer clic) para ver la URL de destino; muchas veces revela un dominio que no coincide con el de la empresa supuestamente emisora (por ejemplo, http://seguridad-bancoXYZ.com/actualizar en lugar del sitio web oficial). Asimismo, debemos tener cuidado con archivos adjuntos inesperados, ya que pueden contener *malware*. Si recibimos un correo con un adjunto en formato .zip, .exe, .docm u otro no habitual —especialmente si proviene de alguien que normalmente no nos envía archivos—, conviene desconfiar. Un caso común es el de correos que simulan contener una factura o comprobante, pero el PDF adjunto es falso o incluye macros maliciosas. Nunca debemos habilitar contenido externo ni macros en documentos de origen dudoso.

- **Solicitudes de información confidencial**: ninguna entidad legítima solicita por correo electrónico datos sensibles, como contraseñas, números de tarjeta o códigos de verificación. Si el mensaje pide que «confirme sus credenciales» o que envíe información personal, casi con certeza se trata de un intento de *phishing*. Este es un indicador claro mencionado en numerosas guías.

Ejemplo de correo de *phishing* (simula provenir de PayPal)

Pensemos en un correo que aparenta ser de PayPal: el asunto dice que la cuenta fue «limitada temporalmente» y se le pide al usuario que verifique sus datos con urgencia. El mensaje tiene un saludo genérico, un tono alarmante y un enlace disfrazado. Aunque incluye el logotipo de PayPal, tanto el remitente como el enlace de «Verificar cuenta» no pertenecen al dominio oficial. Un usuario entrenado detecta estas señales, evita hacer clic y reporta el correo al área de TI.

En situaciones como esta, conviene aplicar la regla mnemotécnica «SLAM»: *sender*, *links*, *attachments*, *message*. Es decir, revisar quién envía el correo, inspeccionar los enlaces y archivos adjuntos antes de interactuar, y prestar atención al contenido en busca de urgencia o errores sospechosos. Si uno solo de estos elementos resulta dudoso, lo más seguro es desconfiar.

La teoría por sí sola no basta para cambiar comportamientos. Por eso, muchas organizaciones implementan simulaciones de *phishing* como herramienta de concientización activa. Una simulación consiste en enviar correos señuelo a los empleados, imitando campañas reales, para evaluar quiénes caen en la trampa —haciendo clic o ingresando datos— y reforzar su entrenamiento en el momento. Estas prácticas permiten exponer al personal a ataques ficticios en un entorno controlado, generando información valiosa sobre el nivel de riesgo humano.

Actualmente, existen múltiples soluciones para realizar simulacros de *phishing*, desde servicios comerciales hasta herramientas gratuitas o de código abierto. Pensemos, por ejemplo, en Gophish, una plataforma *open source* muy popular que permite crear campañas personalizadas sin coste de licenciamiento. Con Gophish, una pyme con algo de conocimiento técnico puede instalar su propio servidor y enviar correos de prueba que simulan ataques, aunque esto requiere cierto esfuerzo inicial.

Otras alternativas gratuitas incluyen pruebas limitadas de suites comerciales —muchas ofrecen *free trials*— o incluso

funcionalidades integradas en plataformas existentes. Por ejemplo, si se cuenta con Microsoft 365, es posible usar «Attack Simulation Training» en Microsoft Defender para orquestar simulaciones de *phishing* dirigidas a usuarios de Outlook, aunque suele requerir licencias específicas.

La clave es empezar de forma simple. Una simulación básica podría consistir, por ejemplo, en un correo falso que simula provenir del área de TI y solicita «actualizar la contraseña» mediante un enlace. Antes de lanzar cualquier simulación, es importante informar a la dirección de la empresa, obtener su apoyo y comunicar al personal que se realizan ejercicios de seguridad periódicos (sin brindar detalles específicos), para no generar desconfianza innecesaria.

Luego, se puede utilizar una herramienta adecuada para diseñar el correo señuelo. Entre los recursos disponibles, se encuentran los siguientes:

- **Plantillas prediseñadas**. Muchas plataformas incluyen modelos de correos de *phishing* ya elaborados, como notificaciones de bancos, avisos de entrega de paquetes, ofertas de premios, entre otros. Se recomienda elegir un tema que sea relevante para la empresa. Por ejemplo, si se utiliza frecuentemente Dropbox, una simulación podría simular un aviso de «Archivo compartido pendiente».

- **Envíos graduales**: conviene iniciar con campañas pequeñas —por ejemplo, entre 10 y 20 empleados— y luego ampliarlas. Esto permite familiarizarse con la configuración de la herramienta y controlar el impacto. Además, es recomendable autorizar el dominio de envío de la simulación en los filtros de correo de la empresa, para que los mensajes de prueba no sean bloqueados automáticamente por el sistema antispam. Según la plataforma elegida, habrá instrucciones específicas para hacerlo.
- **Retroalimentación inmediata**: idealmente, la simulación debería ofrecer una respuesta educativa al usuario que interactúe con el enlace falso. Por ejemplo, si alguien hace clic, se le puede redirigir a una página de aviso que indique que se trató de una simulación y resalte los indicadores de *phishing* que no detectó. Algunas plataformas, como SMARTFENSE, permiten implementar estos «Momentos Educativos» emergentes, transformando el error en una oportunidad de aprendizaje.

Plataformas como Guardey permiten armar una campaña en pocos minutos: se elige una plantilla, se cargan los destinatarios y se envía

el correo. Tras el envío, la herramienta realiza un seguimiento de quién interactúa con el mensaje.

Realizar simulaciones periódicas —por ejemplo, una vez por trimestre— es una práctica recomendada para mantener a los usuarios en estado de alerta. Diversos estudios indican que la práctica sostenida mejora la capacidad de detección y reporte de amenazas por parte del personal. Eso sí, estos ejercicios deben manejarse con tacto: no se trata de «atrapar» ni sancionar a individuos, sino de recolectar métricas que permitan orientar mejor la capacitación.

De hecho, muchas organizaciones combinan las simulaciones con programas de formación continua. Por ejemplo, si un empleado hace clic en un enlace malicioso, se le puede asignar un breve curso adicional de seguridad ese mes. También puede resultar útil gamificar el proceso, reconociendo a quienes reportan correctamente las simulaciones o mantienen una tasa de clics nula. Algunos sistemas otorgan puntos e insignias a los empleados más atentos, fomentando una competencia saludable.

En síntesis, las simulaciones de *phishing* son una herramienta efectiva y accesible para pymes. Ayudan a mantener la atención de los usuarios, permiten evaluar la exposición real de la organización y refuerzan la formación en los casos donde más se necesita. El objetivo final es construir una verdadera «resiliencia al *phishing*»:

que, ante un ataque real, la mayoría del personal lo detecte a tiempo y actúe de forma adecuada.

Métricas y mejoras

Como en todo proceso de seguridad, «lo que no se mide, no se mejora». Después de implementar actividades de concientización —como charlas, simulaciones o capacitaciones—, es fundamental medir los resultados para entender el estado de la cultura de seguridad en la empresa y orientar los esfuerzos hacia la mejora continua.

En el contexto de campañas anti-*phishing* y concientización, algunas métricas clave a monitorear son las siguientes:

- **Tasa de apertura y clic en simulaciones**. Si se realizan campañas de *phishing* simulado, conviene registrar cuántos empleados abren el correo, cuántos hacen clic en el enlace y cuántos llegan a introducir datos en la página falsa (en caso de que incluya un formulario). Estos datos permiten estimar el nivel de susceptibilidad del personal. Por ejemplo, «campaña X: 80 % abrió el correo, 30 % hizo clic, 5 % ingresó credenciales». Un porcentaje alto de clics indica que el engaño fue efectivo y que se necesita reforzar la capacitación. La buena noticia es que

estas métricas suelen mejorar con el tiempo si se entrena regularmente: se espera que, en campañas sucesivas, el porcentaje de clics disminuya, reflejando mayor escepticismo y conciencia por parte de los usuarios.

- **Índice de reporte de *phishing***: tan importante como evitar clics es lograr que los empleados reporten los intentos sospechosos. Muchas simulaciones permiten medir cuántos usuarios identificaron el correo falso y lo reportaron al equipo de seguridad. Un aumento sostenido en la tasa de reporte es señal de una cultura de seguridad más proactiva. Por ejemplo, la plataforma SMARTFENSE incluye en sus estadísticas qué usuarios reconocieron la simulación y la reportaron mediante el botón de *phishing*, integrando ese dato a la evaluación general.
- **Métricas de formación**: si se imparten cursos o microcapacitaciones, se pueden medir tasas de finalización, resultados de cuestionarios o evaluaciones, entre otros indicadores. También es útil aplicar encuestas antes y después de la capacitación para cuantificar el aumento en el nivel de conocimiento o confianza del personal sobre temas específicos.
- **Incidentes reales evitados o detectados**: en la operación diaria, conviene llevar un registro de cuántos incidentes o intentos reales de *phishing* fueron reportados por empleados, en comparación con los que pasaron inadvertidos o se detectaron tarde. Un incremento en los reportes tempranos de

situaciones sospechosas puede estar relacionado con los esfuerzos de concientización. De igual manera, si luego de una campaña disminuye la cantidad de infecciones por *malware* proveniente de correos electrónicos, es una señal positiva (aunque estos datos pueden ser más difíciles de atribuir de forma directa).

Los informes detallados de las herramientas de simulación facilitan este seguimiento. Por ejemplo, la plataforma Guardey ofrece paneles desde los cuales es posible visualizar rápidamente los resultados de cada campaña: cantidad de correos enviados, porcentaje de aperturas, clics y datos ingresados por los usuarios. Incluso permite identificar qué personas hicieron clic, lo que posibilita focalizar los refuerzos de capacitación en aquellos individuos o departamentos más vulnerables.

Informe de resultados de una simulación de phishing —

Aquí, se observan métricas agregadas de una campaña: porcentaje de usuarios que abrieron el correo, los que hicieron clic en el enlace malicioso y aquellos que llegaron a ingresar datos en la página falsa —lo cual indica un nivel de compromiso mayor—. También se refleja cuántos usuarios reportaron activamente el correo simulado. Este tipo de paneles convierte la intuición en datos concretos,

permitiendo comprender qué tan expuesta está la organización ante intentos de *phishing*.

Con estos datos en mano, el responsable de seguridad puede proponer mejoras específicas. Por ejemplo, si se detecta que cierto departamento suele hacer clic en los enlaces de simulaciones —quizá porque, por la naturaleza de su trabajo, recibe muchos correos externos y está más expuesto—, se podría planificar una capacitación especial para ese equipo. O, si nadie reporta los intentos de *phishing*, tal vez sea necesario comunicar mejor el procedimiento de reporte o implementar una herramienta más accesible, como un botón de «Report Phishing» en el cliente de correo.

Además, las métricas pueden influir en decisiones de política interna. Por ejemplo, si a pesar de los esfuerzos muchos usuarios siguen ingresando contraseñas en sitios falsos, podría ser el momento de activar la autenticación multifactor (MFA) en las cuentas críticas, incorporando una capa adicional que mitigue el impacto de credenciales comprometidas.

Otra práctica de mejora continua es comparar las métricas a lo largo del tiempo. Una opción es mantener un cuadro de mando trimestral con indicadores como la tasa promedio de clics y la tasa de reporte en las simulaciones. El objetivo sería observar una disminución de clics y un aumento de reportes. Cualquier

desviación —como un pico de clics al introducir una plantilla nueva — puede ofrecer pistas sobre los tipos de ataque que resultan más convincentes, lo que, a su vez, indica qué contenidos reforzar en las próximas capacitaciones.

Un programa de concientización maduro incluye este ciclo de mejora continua: formar → simular → medir → retroalimentar el plan de formación. De hecho, varios estándares y regulaciones en materia de seguridad —como ISO 27001:2022— exigen contar con métricas y evidencias que demuestren la eficacia de las acciones de concientización, como parte del cumplimiento normativo.

En síntesis, como mencionamos, medir nos permite mejorar. Al cuantificar el comportamiento de los usuarios frente a amenazas simuladas o reales, podemos enfocar los esfuerzos donde más se necesitan y evidenciar el retorno —en términos de reducción de riesgo— de invertir en concientización. Incluso en una pyme pequeña, llevar una hoja de cálculo sencilla con estos datos y revisar las lecciones aprendidas tras cada simulación o incidente real puede marcar una diferencia significativa para fortalecer, de forma progresiva, la cultura de seguridad.

Reporte y canal de seguridad —

Para que la concientización sea efectiva, no alcanza con que el empleado detecte un correo malicioso: también debe saber cómo actuar a continuación. Aquí cobra importancia contar con un canal de reporte de seguridad claro y accesible. Muchas empresas adoptan la política de «si ves algo, di algo». Es decir, instruyen al personal para reportar de inmediato cualquier correo o actividad que parezca sospechosa, en lugar de ignorarla. De este modo, el equipo de TI o seguridad puede investigar a tiempo y tomar medidas preventivas antes de que la amenaza escale.

¿Cómo debería ser ese canal de reporte? En una pyme con poco personal técnico, lo más simple suele ser designar una dirección de correo interna —por ejemplo, seguridad@tuempresa.com o soporteTI@empresa.com— a la que los empleados puedan reenviar mensajes sospechosos o enviar avisos. Como alternativa o complemento, también puede habilitarse un grupo de mensajería corporativo o un número de interno telefónico para urgencias de seguridad. Lo fundamental es que todas las personas en la organización conozcan dónde y cómo reportar. Idealmente, el canal debe estar atendido por la persona responsable de TI o por alguien con conocimientos en ciberseguridad, que pueda recibir la alerta y darle seguimiento adecuado.

En entornos basados en Microsoft, existe la opción de añadir un botón de «Report Phishing» en Outlook. Muchos proveedores —

incluido el propio Microsoft— ofrecen *add-ins* que integran ese botón en el cliente de correo, permitiendo que el usuario marque un mensaje como *phishing*. Esta acción notifica automáticamente a los administradores y envía el correo para su análisis.

En Google Workspace (Gmail), también existe la función «Reportar *phishing*», integrada en el menú de opciones de cada mensaje. Incluir estas herramientas gratuitas facilita el acto de reportar —es solo un clic— y deja registro del incidente.

Para pymes que no utilizan estas *suites*, el método universal sigue siendo reenviar el correo sospechoso a la casilla designada de seguridad, preferentemente como archivo adjunto para conservar sus encabezados. Reforzar este procedimiento contribuye a que el canal de reporte sea realmente útil y efectivo.

¿Por qué es tan crítico fomentar el reporte?

Fomentar el reporte de correos sospechosos es fundamental por varias razones. En primer lugar, permite ganar visibilidad: si nadie reporta, la empresa podría estar bajo ataque sin saberlo, ya que muchas brechas comienzan con un mensaje de *phishing* que pasa desapercibido. Además, reportar empodera al empleado, que se siente parte activa de la protección colectiva y se involucra más en la estrategia de seguridad de la organización. Finalmente, permite activar una respuesta temprana. Si el equipo de seguridad recibe a

tiempo el aviso de un intento de *phishing*, puede bloquear al remitente en los filtros, alertar al resto del personal, escanear equipos en busca de *malware* y tomar medidas antes de que el incidente escale. En definitiva, un empleado alerta puede evitar un problema mayor.

Es recomendable que el proceso de reporte incluya algún tipo de retroalimentación para quien notificó el incidente. Si una persona se tomó el tiempo de reportar un correo sospechoso, es importante agradecerle y, si corresponde, confirmar si efectivamente se trataba de un intento de *phishing*. Algunas soluciones automatizadas envían un mensaje de respuesta como «Gracias por mantenernos seguros. Hemos recibido tu reporte», e incluso aplican mecanismos de gamificación otorgando puntos al usuario. En contextos manuales, el responsable de seguridad puede enviar un breve correo de agradecimiento y refuerzo, por ejemplo, «efectivamente, era un intento de *phishing*. Hiciste lo correcto al avisar. Notamos que provenía de un dominio ruso y prometía un pago pendiente, señales claras de fraude». Esta retroalimentación refuerza la conducta positiva y anima a otros a reportar también.

Por supuesto, habilitar el canal no es suficiente: también hay que capacitar sobre su uso. Es fundamental incluir en las inducciones al personal un módulo sobre cómo reportar incidentes, y reforzar periódicamente el mensaje en los comunicados internos. Por

ejemplo: «Ante cualquier duda de seguridad, reenvía el correo a seguridad@empresa.com o comunícate al interno 123». Incluso se puede simular el uso del canal durante campañas de *phishing* controlado: si un empleado reporta correctamente una simulación, en lugar de caer, ¡es motivo de felicitarlo públicamente! Este tipo de reconocimiento contribuye a consolidar la cultura de seguridad. En cambio, si alguien detecta algo sospechoso, pero no sabe a quién avisar, se pierde una oportunidad valiosa. Por eso, debemos eliminar cualquier barrera que dificulte el reporte.

Un caso concreto lo encontramos en la universidad ITESO, en México. Allí, se instruye a toda la comunidad académica para que, si reciben un correo con señales de *phishing*, no interactúen con él y lo reporten directamente a su Mesa de Servicios Informáticos. Esta indicación clara —«no respondas, no hagas clic, repórtalo al soporte»— ha demostrado ser una medida efectiva para prevenir incidentes mayores y mantener a la comunidad protegida.

En Argentina, también es clave conocer los canales externos disponibles. Si se trata de un incidente grave, es posible escalar el reporte al CERT Argentina o a organismos como la Dirección Nacional de Ciberseguridad. Sin embargo, en el día a día de una pyme, el primer aviso siempre debe canalizarse internamente.

En resumen, en una operación segura, todos los empleados actúan como sensores. Al capacitarlos para identificar amenazas y

ofrecerles un canal claro para reportarlas, se multiplica la capacidad de defensa de la organización. Un programa de concientización eficaz siempre cierra el ciclo con el reporte: concientizar es detectar y reportar. Para el operador de ciberseguridad en una pyme, recibir estos avisos y actuar en consecuencia será parte de su rutina diaria, un tema que abordaremos en la próxima unidad al hablar de *triage* y respuesta básica.

CONTINUAR

Unidad 2. Playbooks mínimos

Incluso en las empresas más concientizadas pueden ocurrir incidentes de seguridad: un descuido de un empleado, un ataque novedoso que evade los filtros o simplemente un evento inesperado —como una laptop robada o un *malware* en un equipo—.

¿Cómo reaccionar cuando la prevención no alcanza? En esta unidad desarrollaremos *playbooks* mínimos de respuesta: procedimientos básicos que una persona a cargo de la seguridad en una pyme debe seguir ante una alerta o incidente.

Comenzaremos por el proceso de *triage*, es decir, la evaluación y priorización inicial de alertas para distinguir rápidamente cuáles requieren atención urgente. Luego abordaremos el escalamiento: cuándo y cómo derivar un incidente a un nivel superior, ya sea interno —jefatura o dirección— o externo —proveedores, fuerzas del orden, CERT

—. También veremos la importancia de documentar el incidente durante y después de su gestión: llevar registros claros es clave para entender qué ocurrió y cumplir posibles obligaciones legales. Finalmente, cerraremos con las lecciones aprendidas, integrando la mejora continua en la respuesta a incidentes.

Estos *playbooks* serán mínimos, pero efectivos, y estarán adaptados a la realidad de una pyme —con recursos limitados y pocos especialistas—. El objetivo es que, ante un problema de seguridad, la organización sepa cómo actuar sin improvisar, conteniendo los daños y recuperándose lo antes posible.

Proceso fundamental para evaluar y priorizar alertas e incidentes de seguridad (*triage*). Alertas

En ciberseguridad, el *triage* es el proceso de analizar rápidamente las alertas o eventos de seguridad y clasificarlos según su gravedad y urgencia, para decidir qué atender primero. El término proviene del ámbito médico: así como en una sala de emergencias se atiende antes al paciente en estado crítico que al que presenta una herida leve, en seguridad informática debemos identificar qué alerta es

realmente crítica —por ejemplo, un servidor comprometido — y cuál representa un riesgo menor —como un escaneo de virus que fue bloqueado correctamente.

Un *triage* eficaz permite optimizar los recursos disponibles —a menudo escasos en una pyme— y reducir el tiempo durante el cual una amenaza grave puede permanecer activa sin ser atendida.

¿Cómo se realiza el triage?

Supongamos que en la consola del antivirus aparecen 50 alertas y, además, un empleado reporta un correo sospechoso. El operador de seguridad debe filtrar el ruido y enfocar los esfuerzos donde realmente importa. Para ello, los pasos fundamentales son los siguientes:

1. **Detección y recolección de datos**

   Todo comienza con la detección de un evento inusual. Puede tratarse de una alerta automatizada —proveniente del antivirus, el *firewall* o un sistema de monitoreo— o de un aviso manual —como el reporte de un empleado—. El primer paso consiste en reunir la información disponible sobre ese evento: ¿qué ocurrió exactamente?, ¿en qué equipo o cuenta?, ¿a qué

hora?, ¿qué síntoma se observó (archivo infectado, intento de acceso fallido, etc.)?

En esta etapa, es útil apoyarse en herramientas centralizadas, si se cuenta con ellas, como un registro de *logs* o un panel SIEM, que permita ver eventos correlacionados. En pymes más simples, esto puede ser tan básico como revisar el mensaje emergente del antivirus en la PC afectada y anotar lo que dice.

2. **Análisis inicial y clasificación**

Con los datos en mano, el siguiente paso es preguntarse: ¿esto representa realmente un incidente de seguridad o se trata de un falso positivo o evento benigno? Muchas alertas pueden descartarse tras una rápida verificación. Por ejemplo, si aparece una alerta de «*malware* detectado y eliminado», es posible que el antivirus ya haya resuelto el problema y no se requieran más acciones —aunque siempre conviene dejar constancia del caso—. En cambio, si el mensaje indica «conexión a sitio malicioso bloqueada», será necesario investigar qué programa originó esa conexión.

El objetivo del *triage* es responder a preguntas clave: ¿qué pasó?, ¿cómo pasó?, ¿a quién o a qué afecta?, ¿cuán grave puede ser? Para esto, es útil aplicar criterios de clasificación.

Muchas organizaciones utilizan categorías de severidad, como crítico (P1), alto (P2), medio (P3) o bajo (P4).

Un enfoque práctico consiste en asignar prioridad 1 (P1) a eventos que comprometan datos sensibles, servicios críticos o afecten a un número significativo de usuarios. Estos casos requieren atención inmediata, incluso fuera del horario habitual. En cambio, si el impacto es limitado o ya está mitigado, puede clasificarse como P3 o P4 y resolverse más adelante. En caso de duda, siempre es preferible sobrestimar la gravedad inicial: «si dudas, marca el incidente como crítico y luego ajusta la clasificación si corresponde».

3. **Correlación y contexto**

Una alerta aislada puede no decir mucho, pero varias en conjunto pueden revelar un incidente mayor. Por eso, durante el proceso de *triage* conviene verificar si hay eventos relacionados. Por ejemplo, si se detecta un *malware* en la PC del área de contabilidad, podría ser útil revisar si días atrás ese mismo usuario recibió un correo de *phishing*. También vale la pena verificar si otros equipos en la red presentan comportamientos anómalos, como picos inusuales de uso de CPU o tráfico sospechoso.

Además, es fundamental considerar el contexto del negocio. Un mismo evento —como cinco intentos fallidos de inicio de sesión— puede ser irrelevante si ocurre en la cuenta de un empleado, pero podría ser crítico si afecta a la cuenta del administrador del servidor financiero. Un *triage* eficaz no se basa solo en datos técnicos, sino que incorpora el conocimiento del entorno y la estructura de la empresa.

En una pyme, el operador de seguridad suele tener una idea clara de qué sistemas son más sensibles o críticos. Esa intuición también ayuda a priorizar. Por ejemplo, una alerta en el servidor de facturación merece más atención inmediata que una en una PC de uso común.

4. **Decisión de acción inicial**

Finalmente, luego del análisis preliminar, llega el momento de decidir cómo proceder: ¿se trata de un incidente confirmado que requiere activar una respuesta?, ¿es un falso positivo?, ¿o aún falta información para evaluar adecuadamente? En esta etapa, muchas organizaciones siguen un criterio —formal o informal— para orientar la acción.

Si el evento se clasifica como un incidente grave (por ejemplo, prioridad 1), debe activarse de inmediato el protocolo de respuesta para contener el daño lo antes posible. Si se trata de

> un incidente menor —de prioridad media o baja—, puede documentarse y atenderse durante el horario habitual, sin urgencia. Incluso si se determina que no hay incidente —es decir, se trata de una falsa alarma—, conviene registrar que se investigó y descartó, para mantener trazabilidad y evitar dudas futuras.

Un aspecto fundamental del *triage* es la velocidad. Esta evaluación debe realizarse rápidamente tras la detección del evento, ya que, en incidentes reales, cada minuto cuenta para contener los daños. Según el NIST, el *triage* se ubica entre la fase de detección y la de respuesta activa, funcionando como un puente que evita desperdiciar recursos en alarmas irrelevantes mientras, quizás, algo crítico ocurre en otro frente.

En entornos con un volumen elevado de alertas, parte del *triage* suele automatizarse mediante sistemas *SIEM* o *SOAR*, que filtran eventos y asignan puntuaciones de riesgo. Sin embargo, en una pyme es común depender del criterio humano. Incluso con poco personal, es posible aplicar *triage* de forma efectiva: un solo analista puede revisar su «bandeja de alertas» cada mañana, priorizando primero aquellas de mayor impacto potencial.

Para facilitar este proceso, es recomendable contar con criterios predefinidos. Una herramienta útil puede ser una matriz simple de impacto y probabilidad: se evalúa el impacto (bajo, medio o alto) y la

probabilidad de que el evento sea real, y con esa combinación se decide la prioridad. También resulta valioso utilizar taxonomías comunes para clasificar los tipos de incidentes —como *phishing*, *ransomware*, fraude interno, entre otros—, lo cual contribuye a sistematizar la respuesta y mejorar la comunicación interna.

En resumen, el *triage* es tanto un arte —porque requiere criterio y experiencia— como una ciencia —porque se apoya en procesos y herramientas—. En una empresa pequeña, es vital entrenar ese «sexto sentido» que permite distinguir la alerta que importa de la que puede esperar. Un *triage* bien hecho puede marcar la diferencia entre contener a tiempo una amenaza o sufrir una brecha seria.

Ejemplo práctico

Supongamos que, al mediodía, el operador de seguridad recibe dos notificaciones:

1. El antivirus en la PC de recepción puso en cuarentena un archivo EICAR (archivo de prueba para verificar el funcionamiento del antivirus).
2. Un empleado del área de ventas informa que abrió un archivo adjunto de Excel proveniente de un remitente desconocido y, desde entonces, su equipo «anda lento».

¿Cuál debería atenderse primero? En este caso, el segundo evento representa una posible infección activa —posiblemente un *malware* real en ejecución—, mientras que el primero fue bloqueado exitosamente por el antivirus y, además, involucra un archivo inofensivo diseñado para testeo.

Aplicando el *triage*, el evento (b) se clasifica como crítico: incidente sospechado de *malware* en un equipo de ventas, prioridad P1. Se procede a responder de inmediato. En cambio, el evento (a) puede clasificarse como no incidente —un falso positivo o archivo de prueba—, o en todo caso, como prioridad P4, sin urgencia.

Este ejemplo muestra cómo un *triage* eficaz permite enfocar los recursos en la alerta que realmente importa, evitando perder tiempo en eventos sin impacto mientras una amenaza potencial requiere atención urgente.

Escalamiento

El escalamiento se refiere al proceso de elevar un incidente al siguiente nivel de respuesta cuando supera la capacidad o autoridad del nivel actual. En una pyme, es común que el primer respondedor sea un analista de TI —o incluso el único responsable de sistemas—, quien realiza el *triage* y toma las acciones iniciales. Sin embargo, si la situación se vuelve más compleja o crítica, será

necesario involucrar a otras personas dentro de la organización o incluso recurrir a asistencia externa.

Saber cuándo y a quién escalar es fundamental para gestionar un incidente de manera eficaz. Existen dos tipos principales de escalamiento, que veremos a continuación:

- **Escalamiento horizontal (funcional)**. Consiste en involucrar a otras áreas o roles que tienen experiencia en aspectos específicos del incidente. Por ejemplo, si el caso afecta datos personales de clientes, además del personal técnico, puede ser necesario escalar a legales o a relaciones públicas, para abordar la comunicación externa y el cumplimiento normativo —como el RGPD—. Si se sospecha de un delito, se debe escalar a la dirección para evaluar la necesidad de notificar a las autoridades. En una pyme con estructura reducida, esto puede implicar simplemente llamar al gerente general para informarle y tomar decisiones en conjunto, o contactar al proveedor externo que brinda soporte en ciberseguridad.
- **Escalamiento vertical (jerárquico)**: se refiere a derivar el incidente a un nivel superior de experiencia o autoridad. Por ejemplo, si el técnico de primera línea no logra contener el ataque o no cuenta con las herramientas necesarias, debe escalar a un especialista —si existiera en la empresa— o a una empresa externa dedicada a la respuesta a incidentes. En términos generales, puede pensarse en niveles: nivel 1 (soporte básico de TI), nivel 2 (especialista o analista de seguridad), nivel 3 (equipo externo o autoridad competente). Aunque muchas pymes no cuenten con estos niveles formalmente definidos, al

menos deberían tener claro hasta dónde puede llegar cada persona y en qué momento se debe pedir ayuda.

Un *playbook* mínimo de escalamiento para pymes debería incluir ciertos elementos esenciales. En primer lugar, es importante contar con **criterios claros para decidir cuándo escalar.** Por ejemplo, si un incidente afecta a más del 15 % de los sistemas o usuarios, se debería escalar de inmediato a la dirección. Si hay datos de clientes comprometidos, la situación debe elevarse a gerencia y, si corresponde, al área legal. Otro criterio útil puede ser el tiempo sin resolución: si han pasado determinadas horas sin contener el incidente, conviene escalar para obtener más recursos o apoyo.

También es fundamental tener definidos de antemano los **contactos clave y los roles de decisión.** Antes de enfrentar un incidente, la organización debería identificar quién es el contacto de emergencia en cada área. Por ejemplo, tener a mano el teléfono móvil del gerente para fuera del horario laboral, el contacto de un proveedor de ciberseguridad o consultor externo con el que se tenga un acuerdo, o el número del CERT nacional o de la policía especializada en cibercrimen, en caso de que sea necesario hacer una denuncia. Además, es clave determinar con anticipación quién tiene autoridad para tomar decisiones críticas, como apagar un servidor, desconectar Internet en toda la empresa o responder a una demanda de rescate en caso de *ransomware*. Por lo general,

estas decisiones corresponden a la alta dirección, por lo que en incidentes graves se debe escalar a ese nivel.

Por último, es esencial que los **canales de comunicación estén definidos y probados**. Cuando se escala un incidente, la información debe llegar de forma rápida y directa. No sirve enviar un correo electrónico que la persona leerá al día siguiente. En una situación crítica, es preferible usar un canal más inmediato, como una llamada o un mensaje directo.

Algunas empresas pequeñas crean grupos de mensajería entre el equipo técnico y los responsables de la empresa, reservados exclusivamente para emergencias de seguridad. Así, ante una palabra clave, todos los involucrados se activan de inmediato. En una crisis, no es momento de improvisar canales: este detalle debe planificarse con antelación.

Cuando se decide escalar un incidente, es fundamental comunicar la situación de forma clara y concisa a quien recibirá el caso. Si se informa a gerencia, lo ideal es hacerlo en términos no técnicos. Por ejemplo, «tenemos un virus activo en tres equipos que está cifrando archivos. Ya aislamos las máquinas, pero necesitamos decidir si apagamos los servidores de forma preventiva. También requerimos su aprobación para notificar a los clientes potencialmente afectados». En el caso de escalar a un externo —como un proveedor de ciberseguridad—, puede ser necesario compartir *logs*, muestras

del *malware* o detalles técnicos que ayuden al análisis y resolución del incidente.

Como parte del registro del caso, es importante documentar a quién se escaló, en qué momento y qué información se compartió. Esto forma parte de la trazabilidad del manejo del incidente.

Un caso particular es el escalamiento a equipos externos como el CERT. En Argentina, se puede contactar a cert.gob.ar o al CSIRT de Ciberseguridad de la Policía ante incidentes graves, como fraudes o ataques de *ransomware* con pedido de rescate. La colaboración con estos organismos puede aportar experiencia y facilitar la coordinación en casos que afecten a múltiples actores. Eso sí, estos canales se utilizan generalmente cuando el incidente excede la capacidad local o tiene impacto público o nacional. Por ejemplo, el INCIBE-CERT en España recomienda escalar a sus equipos cuando el incidente sobrepasa las capacidades internas o afecta infraestructuras críticas.

En el caso de una pyme, escalar a un CERT suele reservarse para situaciones excepcionales: un ataque particularmente complejo, una campaña dirigida que pueda afectar a otras empresas, o un incidente que requiere alerta temprana a nivel sectorial o nacional.

Ejemplo

Retomemos el caso del incidente de *malware* en la PC del área de ventas. El técnico realiza el *triage* y ejecuta la primera acción de contención: aísla el equipo de la red. Al analizar más a fondo, descubre que se trata de un *ransomware* que está encriptando archivos compartidos. La situación escala automáticamente a crítica. Ante este escenario, decide escalar: llama al dueño de la empresa, ya que podrían tener que tomar decisiones importantes, como pagar o no un rescate o notificar a los clientes si hay datos inaccesibles. También contacta al proveedor externo de IT para que colabore en la recuperación de los respaldos. Este caso muestra claramente un escalamiento jerárquico —hacia la dirección— y funcional —hacia un especialista en recuperación—.

Dado que se trata de un delito, el dueño y el proveedor acuerdan notificar al CERT o a la policía especializada, presentando las evidencias correspondientes. Todo este proceso de escalamiento debe realizarse con agilidad, sin esperar autorizaciones formales que puedan demorar la respuesta. En una crisis, la regla es contener el daño primero; la documentación y las aprobaciones vendrán después, si son necesarias.

En definitiva, escalar a tiempo puede marcar la diferencia entre controlar un incidente o enfrentar una situación con consecuencias graves. Es preferible sobreactuar ante un falso incidente —lo peor que puede pasar es que se ejerciten los canales— que quedarse

> corto y enfrentar solos algo que nos supera. Un *playbook* sencillo debería ser claro: si ocurre X, contacta inmediatamente a Y. Con roles y contactos definidos de antemano, el operador sabrá cuándo levantar la mano y pedir refuerzos.

Durante la gestión de un incidente de seguridad, es común enfocarse solo en «apagar el fuego» y descuidar la documentación. Sin embargo, llevar un registro detallado es una parte esencial de la respuesta. ¿Por qué? Porque la documentación permite entender la secuencia de hechos más adelante, cumplir con requisitos legales o de auditoría, y extraer lecciones para el futuro.

¿Qué se debe documentar?

Idealmente, todo lo relevante. En la práctica, el responsable debería registrar al menos los siguientes aspectos:

- **Descripción inicial del incidente**. Qué se detectó y cómo. Por ejemplo, «fecha y hora tal, el usuario X reportó un correo sospechoso con adjunto malicioso; la PC Y presentaba alertas del

antivirus». Se debe incluir también quién (persona o sistema) detectó el problema.

- **Impacto y alcance conocidos**: detallar los sistemas o datos afectados. Por ejemplo, «equipo contabilidad-PC infectado; posible acceso a carpeta compartida Ventas; se identificaron tres archivos cifrados en el servidor». También se debe registrar la clasificación asignada (por ejemplo, prioridad 1, crítico).
- **Acciones realizadas y cronología**: es clave anotar, en tiempo real, cada acción tomada y su resultado. Por ejemplo, «14:05 – Se desconecta la PC de la red. 14:10 – Se inicia análisis antivirus. 14:30 – Se cambia la contraseña del usuario afectado. 15:00 – Se contacta al proveedor para soporte». Este registro cronológico permite revisar más adelante si se actuó a tiempo y qué medidas se implementaron. El NIST recomienda documentar desde el primer minuto, ya que es en el momento donde los detalles están más frescos. Con el paso de los días, es fácil olvidar información clave.
- **Evidencias recolectadas**: se deben conservar copias de archivos de *logs*, muestras de *malware*, capturas de pantalla de mensajes de error, cabeceras de correos, entre otros elementos técnicos. No basta con documentar en texto; es importante archivar las evidencias relevantes. Esto puede ser útil para un análisis forense posterior o en caso de realizar una denuncia formal del hecho.

- **Comunicación y escalamiento**: registrar a quién se notificó o se escaló el incidente, y en qué momento. Por ejemplo, «15:30 – Informado gerente general. 15:45 – Llamada al proveedor externo, caso #123 abierto». Esta trazabilidad permite demostrar que se cumplieron con las notificaciones internas o externas necesarias. Algunas normativas exigen reportar brechas en plazos específicos, por lo que contar con este registro facilita el cumplimiento. De hecho, la norma ISO 27001:2022 establece que deben conservarse evidencias de la gestión de incidentes, incluyendo documentación formal de cada caso.
- **Resolución y estado final**: al concluir el incidente, se debe dejar constancia de cómo se resolvió y cuál es el estado final. Por ejemplo, «16:30 – *Malware* eliminado, sistemas restaurados desde respaldo, servicio restablecido. Caso cerrado a las 17:00». Si queda algo pendiente —como un análisis forense más profundo o la notificación a clientes— también debe anotarse.
- **Lecciones aprendidas preliminares:** en algunos casos, se incluye en el informe del incidente un apartado con observaciones iniciales sobre fallas o aspectos a mejorar, aunque el análisis más profundo suele realizarse en una fase formal posterior. Aun así, quien gestionó el incidente puede registrar sus comentarios preliminares. Por ejemplo, «se detectó que el antivirus no estaba actualizado en ese equipo» o «El usuario

tardó dos días en reportar el correo, lo que permitió la propagación — se debe reforzar la concientización».

Un formato práctico para documentar incidentes puede ser un documento simple —un archivo Word, un formulario PDF o una plantilla en Notion o Excel— con los campos predefinidos para que quien responde solo tenga que ir completándolos. Lo importante es que esa plantilla exista antes de enfrentar un incidente, para no tener que empezar con una página en blanco bajo presión. Por ejemplo, se recomienda contar con un modelo de informe posincidente que incluya desde los datos básicos y la clasificación del incidente, hasta una sección de análisis y recomendaciones. En una pyme, puede ser suficiente con un documento estandarizado de «Reporte de incidente de seguridad» que incluya campos como fecha, responsable, descripción, impacto y acciones realizadas.

Además del informe formal final, también es útil mantener un registro en tiempo real durante la respuesta. Esto puede ser tan simple como una hoja y un lápiz o un archivo compartido, donde se va anotando la cronología minuto a minuto. Algunas metodologías sugieren asignar, en incidentes importantes, a una persona con el rol de «escriba», cuya única tarea es registrar todo lo que sucede. En un equipo reducido, probablemente el mismo analista deba hacerlo mientras actúa. Aunque puede resultar incómodo, este esfuerzo es

valioso: esa bitácora se convierte luego en una fuente clave para entender el incidente y mejorar la respuesta futura.

Beneficios de documentar

Documentar los incidentes trae múltiples beneficios. En primer lugar, permite contar con un registro histórico. Esto ayuda a identificar patrones —¿se repiten ciertos tipos de incidentes?, ¿cómo se resolvieron en el pasado?—, resulta útil para auditorías y es una excelente herramienta para capacitar a nuevo personal. En segundo lugar, facilita el análisis de lecciones aprendidas: sin documentación, todo queda en recuerdos imprecisos. Además, puede ser un requisito legal. Por ejemplo, si hubo una filtración de datos personales, la normativa puede exigir demostrar qué se hizo para mitigar el daño, y un informe formal permite acreditar la diligencia.

Otro beneficio es que fortalece el *triage* futuro. El NIST destaca que documentar cada incidente y revisar qué funcionó o no, mejora el proceso de respuesta en su conjunto. Tampoco hay que olvidar que la documentación incluye los formularios de notificación externa, si corresponden. Si la empresa debe comunicar el incidente a un regulador o a clientes, esas comunicaciones también deben archivarse (cartas, correos, acuses de recibo, etc.). En sectores regulados —como el financiero— se exige reportar dentro de ciertos plazos. Tener el informe interno preparado agiliza ese paso.

En la práctica pyme, lo esencial es anotar todo lo posible durante el incidente y elaborar un informe final sencillo. Aunque en medio del caos pueda parecer que «no hay tiempo para eso», registrar información crítica no es una pérdida de tiempo: ayuda a tomar mejores decisiones y deja evidencia útil. Al finalizar el incidente, conviene tomarse un momento para completar bien la documentación mientras los detalles aún están frescos; con el paso del tiempo, la memoria se vuelve imprecisa y se pierden datos clave.

Superado el incidente, cuando las aguas se calman, llega un paso que muchas veces se omite por la vorágine del día a día: el análisis de lecciones aprendidas, o *post mortem* del incidente. Cada incidente de seguridad es, en realidad, una oportunidad para fortalecer a la organización, siempre que se reflexione de manera sistemática sobre qué ocurrió y cómo evitar que vuelva a suceder.

Un ejercicio de lecciones aprendidas puede consistir en una reunión posincidente con todas las partes involucradas —el equipo técnico, representantes del área afectada y la gerencia, si correspondió— para analizar preguntas como las siguientes:

- **¿Se detectó a tiempo o hubo demorase en la detección o el reporte?** Es importante revisar si las alertas o reportes llegaron con rapidez o si falló algún mecanismo de detección temprana. Por ejemplo, «Juan recibió el correo de *phishing* el lunes, pero no lo reportó hasta el miércoles, cuando notó comportamientos extraños —necesitamos que los usuarios informen de inmediato». Esta observación puede derivar en acciones de mejora, como reforzar la concientización sobre el reporte oportuno.
- **¿El *triage* fue correcto?** Es necesario evaluar si la severidad del incidente se clasificó adecuadamente. Tal vez al principio se subestimó como P3 y resultó ser P1, ¿por qué ocurrió esa mala clasificación? O, por el contrario, ¿hubo falsas alarmas que hicieron gastar tiempo innecesario? Analizar estos casos ayuda a ajustar el proceso de *triage* para futuras situaciones.
- **¿Las medidas de contención fueron adecuadas y oportunas?** Conviene preguntarse qué se podría haber hecho mejor o más rápido. Por ejemplo, «debimos desconectar el servidor apenas detectamos el *ransomware*, pero tardamos una hora en decidirlo, y eso permitió que se cifraran más datos». Estas lecciones son fundamentales para actualizar los *playbooks* o protocolos: quizás establecer la regla de «ante un *ransomware* confirmado, aislar inmediatamente todos los sistemas críticos» sin tanta deliberación.

- **¿Hubo dificultades en el escalamiento o la comunicación?** Es importante revisar si todos sabían a quién avisar y si hubo confusiones en los roles. Por ejemplo, «no teníamos a mano el número del proveedor y se perdió tiempo buscándolo». La solución sería mejorar el directorio de contactos de emergencia. Otro caso podría ser el siguiente: «la jefa no entendió la gravedad porque le explicamos el incidente con demasiados términos técnicos». Esto indica que hay que ajustar cómo escalamos, explicando claramente el impacto en el negocio. Todo fallo en la coordinación debe identificarse para prevenirlo en el futuro.
- **¿Qué salió bien?** También es relevante destacar los aciertos. Por ejemplo, «gracias al respaldo nocturno, recuperamos los datos rápidamente», o «el empleado de recepción reportó el correo de *phishing*, evitando que otros cayeran». Reconocer estas buenas prácticas refuerza su continuidad y sirve como ejemplo para todo el personal.
- **¿Cuál es la causas raíz?** Analizar por qué ocurrió el incidente permite establecer acciones preventivas. Si se trató de un *phishing* exitoso, conviene preguntarse por qué tuvo éxito: ¿falta de entrenamiento del usuario?, ¿el filtro de *spam* no bloqueó el mensaje debido a una mala configuración de DKIM? Si fue un *malware*, ¿cómo ingresó al sistema, por un USB, falta de parches en Windows, o por otro vector? Una herramienta útil es el método de los «5 porqués», que ayuda a profundizar en la causa

subyacente: «Hubo infección» → ¿por qué? «El usuario ejecutó un adjunto» → ¿por qué? «Parecía legítimo / no sabía» → ¿por qué no sabía? «No tenía formación suficiente». Cada causa raíz idealmente debe derivar en una acción concreta: reforzar la capacitación, mejorar la gestión de parches o asegurar que el antivirus esté actualizado, según corresponda.

Actualización de documentación y controles

Con las lecciones aprendidas en mano, es necesario actualizar los *playbooks* y protocolos. El NIST y otros estándares recomiendan que, tras cada incidente, se ajusten los procedimientos y se documenten formalmente las lecciones para que no se pierdan con el tiempo. Por ejemplo, si se detectó que el tiempo de respuesta fue lento debido a fallas en la detección, se podría implementar un sistema de monitoreo más eficaz. O si una contraseña débil fue aprovechada por un atacante, la acción de mejora podría ser reforzar las políticas de contraseñas o activar la autenticación multifactor (MFA). Todas estas decisiones deben registrarse claramente y asignarse a responsables específicos, de manera que se asegure su ejecución y cierre el ciclo de mejora continua.

Las lecciones aprendidas cierran el ciclo de mejora continua en la gestión de incidentes. En ISO 27001, esto forma parte del ciclo PDCA (*plan-do-check-act*): después de actuar (*do*), es necesario revisar

qué sucedió (*check*) y aplicar mejoras para optimizar los procesos (*act*). La norma incluso exige evidenciar que los incidentes se revisan de manera eficaz y que las lecciones se documentan para no perderlas.

En una pyme, resulta muy valioso realizar, aunque sea de manera informal, una reunión posincidente. A veces, por la cultura de apuro, se tiende a decir «bueno, ya está resuelto, sigamos trabajando». Sin embargo, dedicar un momento a analizar el incidente con perspectiva ahorra problemas futuros. Puede tratarse de una reunión corta al día siguiente con las personas clave involucradas. Si la empresa es muy pequeña, el responsable de seguridad puede reflexionar por sí mismo y redactar un breve memo con las lecciones aprendidas y recomendaciones para la dirección.

Integrar a los empleados

Si el incidente afectó a usuarios finales —por ejemplo, empleados cuya máquina fue infectada—, también es recomendable comunicarles las lecciones aprendidas. Por ejemplo, «lo que ocurrió fue un *ransomware* a través de un correo engañoso. Aprendimos que debemos verificar siempre la dirección del remitente y no abrir adjuntos .ZIP inesperados. Por favor, refuercen esas precauciones». De esta manera, el incidente se convierte en una experiencia de

aprendizaje para todos, reforzando la cultura de seguridad sin señalar culpables y enfocándose en fortalecer los procesos.

Asimismo, conviene compartir información hacia el exterior cuando corresponda. Muchos CERT publican alertas y casos de los que otras organizaciones pueden aprender. Participar de esa comunidad —reportando indicadores del ataque o detalles relevantes— ayuda a prevenir incidentes en otras empresas y a recibir retroalimentación. Para una pyme, esto puede limitarse a notificar al proveedor de IT sobre lo ocurrido, de manera que esté al tanto y pueda aplicar medidas preventivas en otros clientes.

En conclusión, tras cada crisis es fundamental documentar las lecciones y ajustar los procedimientos. Las lecciones aprendidas son el paso que convierte un incidente en una mejora real de la postura de seguridad. Una empresa que aprende de manera iterativa se vuelve cada vez más resistente: los errores nuevos pueden ocurrir, pero rara vez se repetirá un mismo fallo grave. Como dice un experto, «cada incidente es una oportunidad para afinar el proceso», y aprovecharla nos hace más fuertes y mejor preparados para el futuro.

A continuación, integraremos los conceptos de las dos unidades, realizando ejercicios que abarcan desde la identificación de un correo de *phishing* hasta las acciones iniciales de respuesta. El objetivo es practicar de manera segura y sin costo, utilizando recursos disponibles en línea y herramientas de correo habituales. No se requiere *software* pago ni entornos especiales: solo un navegador web y una cuenta de correo electrónico (Gmail, Outlook o la que se use habitualmente).

Parte 1. Evaluando correos sospechosos con un quiz interactivo

1. **Accede al *Phishing Quiz* de Google/Jigsaw**: Google dispone de un examen interactivo gratuito de *phishing* (disponible en español). Abre el siguiente enlace en tu navegador: phishingquiz.withgoogle.com. Inicia el *quiz* ingresando un alias, como tu nombre de pila.
2. **Analiza los ejemplos propuestos:** el *quiz* mostrará ocho correos electrónicos de ejemplo y, tras cada uno, preguntará si se trata de *Phishing* o de un correo legítimo. Conviene dedicar tiempo suficiente a inspeccionar cada correo y aplicar los conceptos aprendidos en la unidad 1:

- Revisa el remitente colocando el cursor sobre el nombre para ver la dirección completa, función disponible en el *quiz*.
- Observa el saludo y el lenguaje utilizado.

- Coloca el cursor sobre los enlaces, sin hacer clic, para verificar la URL real a la que apuntan.
- Identifica cualquier urgencia sospechosa o errores ortográficos.
- Analiza si el correo solicita información inusual, como datos personales o la descarga de archivos.

Después de tomar una decisión, selecciona la respuesta. El *quiz* proporciona retroalimentación inmediata, indicando si la elección fue correcta y explicando las señales presentes en cada correo. Es importante revisar estas explicaciones para reforzar el aprendizaje.

3.

4. **Completa los 8 casos y anota tu puntaje:** al final del *quiz*, se debe anotar cuántos correos se identificaron correctamente. Si alguno resultó incorrecto, conviene revisar qué indicador pasó desapercibido. Por ejemplo, puede ocurrir que no se haya notado que el dominio del remitente era falso o que el enlace apuntaba a un sitio diferente. Registrar esos indicadores sirve como referencia para futuras evaluaciones.
5. **Reflexión rápida:** es útil considerar cuáles ejemplos resultaron más difíciles y por qué. ¿Eran correos muy sofisticados? ¿Qué acciones se tomarían si se recibe un mensaje similar en el

entorno laboral real? Esta reflexión prepara para la siguiente parte del laboratorio.

Parte 2. Inspección y reporte de un correo en tu entorno real

5. **Busca un correo sospechoso real (en un entorno seguro):** abre la bandeja de entrada personal o de trabajo y ve a la carpeta de *spam* o correo no deseado, donde la mayoría de los servicios filtra posibles intentos de *phishing*. Nota: no abras adjuntos ni enlaces de correos *spam*; solo visualízalos con precaución. Selecciona uno o dos mensajes que a primera vista parezcan intentos de phishing, como correos que indiquen «ha ganado un premio» o «actualice su cuenta bancaria».
6. Identifica los indicadores presentes en cada correo, sin salir de la vista previa:
    - Remitente: ¿es una dirección coherente o una extraña?
    - Asunto y contenido: ¿te genera urgencia inmotivada, ofrece algo demasiado bueno, o contiene amenazas de bloqueo de cuenta? ¿Está en español mal redactado o en inglés sin razón?
    - Enlaces: **sin hacer clic**, posiciona el *mouse* sobre cualquier botón o vínculo para ver la URL destino (en la esquina inferior del navegador/cliente de correo suele mostrarse). Anota si el dominio es sospechoso.

- Adjuntos: ¿tiene algún archivo? En Gmail/Outlook, no descargues nada, solo fíjate en la extensión (¿.pdf, .html, .exe, .docm?).

Anota todos los indicadores sospechosos que encuentras, como si estuvieras elaborando un pequeño análisis. Este es un ejercicio para afinar tu ojo con correos reales.

7. **Opcional – Ver encabezados completos:** si tienes conocimientos técnicos básicos, intenta ver los *headers* completos del correo (en Gmail: menú de tres puntos, «Mostrar original»; en Outlook: «Ver encabezados de mensajes»). En ellos pueden encontrarse datos como la ruta IP del servidor remitente o si el mensaje no pasó validaciones dkim o spf. Si no entiendes estos detalles, no te preocupes: el objetivo es mostrar dónde se encuentran más pistas técnicas.

8. **Realiza un reporte simulado**. Ahora actúa como si este correo fuera un caso real de *phishing* que debes reportar:
    - Si tu servicio de correo tiene una opción nativa como «Reportar phishing» o «Marcar como phishing», haz clic en ella. En Gmail, por ejemplo, esta acción envía el correo a Google para su análisis y lo mueve fuera de la bandeja de entrada.

- Si no existe esa opción, actúa como se haría en una empresa: reenvía el correo a la dirección de seguridad designada. Para este ejercicio, puedes reenviarlo a otra cuenta propia, simulando que esa segunda cuenta pertenece al «equipo de seguridad». En el mensaje de reenvío, escribe algo breve, por ejemplo: «Reporte: recibí este correo sospechoso que parece *phishing*. El remitente es extraño y solicita datos. Por favor, revisar». Este ejercicio sirve para practicar cómo se describiría un incidente al área de TI.

Después, observa si el cliente de correo muestra algún mensaje especial al realizar el reporte (por ejemplo, Gmail agradece el envío). En un entorno corporativo, en este punto, el equipo de seguridad ya tendría el correo reportado para su análisis, exactamente como se practica en este paso.

9. **Comprueba resultado:** si reportaste el correo como *phishing*, este debería haberse movido de tu bandeja de entrada, posiblemente a «Spam» o «Eliminados». Esto confirma que la acción se ejecutó correctamente. En un entorno real, el equipo de seguridad investigaría a partir de este punto. En este ejercicio, como se trata de un correo de *spam* cualquiera, no se espera más interacción. Sin embargo, habrás practicado el flujo completo: detectar → analizar → reportar.

10. **Conclusión de la parte 2.** Reflexiona sobre la experiencia: ¿fue fácil identificar los indicadores en un correo real? ¿Sentiste confianza al reportarlo? Si este hubiese sido un correo genuinamente malicioso dirigido a la empresa, es posible que hayas contribuido a prevenir un incidente. Por otro lado, si algún correo de *spam* resultó ser solo publicidad legítima mal clasificada, también aprendiste a diferenciar, lo cual es positivo: es preferible reportar de más que de menos.

Parte 3. Simulacro de respuesta inicial a un incidente

En esta parte final, se simula la respuesta básica a un incidente a partir de un escenario dado, siguiendo un pequeño *playbook*. No será necesario ejecutar acciones en sistemas reales; el objetivo es trazar mentalmente o en papel qué pasos se llevarían a cabo, de manera ordenada y segura.

11. **Lee el escenario**

Estás a cargo de TI en una pyme. Un martes a las 10 a.m., recibes una llamada de un empleado: «Abrí un correo que parecía de nuestro banco y descargué un adjunto. Ahora mi computadora está muy lenta y algunos archivos no abren». Al mismo tiempo, el gerente envía un mensaje de WhatsApp indicando que en el servidor de archivos compartidos observa documentos con extensiones .encrypted que antes no estaban así.

Claramente, este escenario indica un posible ataque de *ransomware* en progreso originado por *phishing*. Se tiene confirmación de:

- un usuario que ejecutó un archivo sospechoso, y
- signos de cifrado en archivos compartidos de la red.

12. **Aplica triage de inmediato.** En este escenario, identifica las prioridades:

- **Confirmación del incidente**: este no es un caso de alerta aislada; hay impacto tangible, con archivos cifrados.
- **Severidad**: alta (P1) — el *ransomware* afecta la disponibilidad de datos importantes y potencialmente compromete toda la red.
- **Alcance estimado**: al menos un PC infectado y un servidor afectado; la infección podría propagarse a otros sistemas.
- **Decisión**: se debe actuar de inmediato para contener el incidente. No se trata de un falso positivo; la amenaza es real.

13. **Esboza las acciones de contención (*playbook*).** Ante este escenario, las acciones se ordenan por prioridad:

- **Aislar el equipo infectado**. Desconéctalo de la red inmediatamente. Indica al empleado que apague el equipo o desenchufe el cable de red.
- **Desconectar temporalmente el servidor de archivos**: esto ayuda a frenar el cifrado en curso, si es posible hacerlo sin afectar otros sistemas críticos.
- **Escalar a dirección**: avisar a gerencia de inmediato sobre el impacto. Aunque el gerente ya contactó previamente, asegura que la dirección y todos los interesados estén informados de que el incidente es crítico.
- **Opcional: contactar al proveedor externo de soporte**: si la empresa cuenta con un servicio de TI externo, llamarlo para recibir asistencia especializada.
- **Identificar el ransomware**: revisar, si existe, el mensaje de rescate o los archivos .encrypted para determinar la cepa. No invertir demasiado tiempo en esta etapa, solo lo necesario para orientar la contención.
- **Preparar recuperación desde backups**: si existen copias de seguridad recientes, alistarlas para restauración. No reconectarlas hasta asegurar que la amenaza fue eliminada.
- **Cambiar credenciales comprometidas**: si se sospecha que contraseñas pudieron ser robadas (por ejemplo, si el correo

phishing buscaba credenciales), realizar el cambio de inmediato.

- **Documentar la acción**: registrar la hora de inicio del incidente y cada acción realizada. Aunque en este ejercicio sea mental, en la práctica se debe anotar todo para seguimiento y mejora futura.

14. **Decide sobre escalamiento externo:** en un caso de *ransomware*, ¿llamarías a las autoridades? Quizá luego, pero inicialmente tu prioridad es contener la amenaza. Suponiendo que la empresa es pequeña, primero se intentará resolver internamente y restaurar los sistemas. No obstante, anota «si datos de clientes están comprometidos, considerar notificar clientes y/o realizar denuncia policial». Para este ejercicio, evalúa primero el impacto del incidente antes de decidir si notificar a clientes o autoridades externas.
15. **Simula la comunicación.** Redacta (mentalmente o por escrito) un breve comunicado al equipo, por ejemplo:

«Equipo: Estamos experimentando un incidente de seguridad esta mañana. Por precaución, desconecten sus PC de la red y no abran archivos compartidos hasta nuevo aviso. TI está trabajando en ello. Les mantendremos informados».

Este mensaje sirve para practicar cómo notificar adecuadamente sin causar pánico, pero manteniendo al personal alerta y evitando que la infección se propague.

16. **Recuperación.** Piensa cómo restaurarías las operaciones. En este caso, lo lógico sería:

- Formatear la PC infectada desde cero para eliminar el *ransomware*.
- Restaurar los archivos del servidor desde la copia de seguridad más reciente (por ejemplo, del día anterior). Esto podría implicar pérdida de trabajo reciente, pero asegura la integridad de los datos.
- Mantener todos los sistemas desconectados de Internet mientras se actualiza el antivirus y se realiza un escaneo completo.
- Antes de restaurar, asegurarse de eliminar el ejecutable del *ransomware* en el servidor.

Este es un ejercicio teórico, así que describe mentalmente o por escrito los pasos que seguirías.

17. **Documentación rápida.** Anota los tiempos y la causa del incidente. Por ejemplo:

- «Incidente detectado 10:00»
- «10:05 – PC infectada aislada»
- «10:15 – Servidor desconectado»
- «10:30 – Comunicado a empleados»
- «11:00 – Iniciada restauración desde *backup*»

Causa: «*Phishing* con adjunto malicioso – el usuario abrió el archivo Factura.zip que contenía *ransomware*».

18. **Lecciones aprendidas (breve).** Identifica al menos dos mejoras que implementarías tras este incidente. Algunos ejemplos posibles podrían ser los siguientes:

- Capacitar al usuario que abrió el adjunto para que no vuelva a ocurrir; reforzar con todo el personal la política de no abrir adjuntos no solicitados.
- Asegurarse de que los antivirus estén activos y actualizados en todos los equipos; revisar por qué el de esa PC no detuvo el *ransomware* (¿estaba desactualizado?).
- Implementar segmentación de la red para que una PC no pueda afectar directamente al servidor de archivos, limitando la propagación.

- Verificar y mejorar la frecuencia de las copias de seguridad; considerar backups fuera de línea para evitar que también sean cifrados.
- Actualizar el *playbook* de respuesta incluyendo este tipo de ataque; ahora se sabe que desconectar rápidamente funciona, por lo que se debe formalizar ese paso para futuras ocasiones.

19. **Comparte la experiencia (si aplica):** en un entorno de capacitación, podrías comentar con colegas qué medidas se tomaron en este escenario simulado y comparar resultados. En el caso individual, simplemente concluye enumerando los puntos clave que experimentaste en esta simulación: detección temprana, acción decidida (aislar, desconectar), comunicación clara, ayuda externa cuando se requiere y aprendizaje posterior.

Con estos pasos, se recorre de forma guiada el flujo completo, desde la concientización (identificación de un *phishing*) hasta la respuesta básica a un incidente derivado de uno. Este laboratorio refuerza cómo ambas dimensiones —la prevención (usuario alerta) y la reacción (operador con plan)— se complementan para proteger a una organización pequeña.

Referencias:

- **Esta lectura se basa en incidentes comunes reportados por pymes, donde el phishing dirigido al área de finanzas constituye una de las amenazas más frecuentes. La importancia de la concientización en estos casos ha sido destacada por expertos: «invertir en prevención, concientización y tecnología de protección resulta clave para la continuidad operativa».**
- **Las guías utilizadas para el desarrollo de estos contenidos incluyen recomendaciones de INCIBE para la respuesta a incidentes, el estándar NIST SP 800-61 sobre manejo de incidentes, y buenas prácticas de concientización como programas continuos con simulaciones periódicas. Todas estas referencias se adaptan aquí al contexto de las pymes argentinas, considerando sus limitaciones, pero también su gran potencial para mejorar la seguridad mediante la cultura y la ejecución efectiva de procesos básicos**

CONTINUAR

Referencias

Google/Jigsaw. (s. f.). *¿Puedes detectar si eres víctima de phishing?* https://phishingquiz.withgoogle.com/

Guardey. (s. f.). *Ponga a prueba la concienciación de su equipo en phishing*. https://www.guardey.com/es/phishing-simulations/

INCIBE. (2019). *Respuesta a incidentes, ¿estáis preparados?* https://www.incibe.es/empresas/blog/respuesta-incidentes-estais-preparados

Malwarebytes. (s. f.). *7 ejemplos reales de phishing: estafas por correo electrónico que debe evitar*. https://www.malwarebytes.com/es/cybersecurity/basics/phishing-email

Mercado. (2025, noviembre). *El 60% de las PyMEs argentinas fue víctima de ciberataques en el último año*. Recuperado de https://mercado.com.ar/ruta-digital/el-60-de-las-pymes-argentinas-fue-victima-de-ciberataques-en-el-ultimo-ano/

Mutual de Seguridad. (s. f.). *Reporte de incidentes: Campaña altas temperaturas*. https://www.mutual.cl/portal/wcm/connect/7e670233-fbf3-48f4-b849-ab2968bf9f99/formato-reporte-de-incidente-campana-altas-temperaturas.pdf?MOD=AJPERES&CVID=oO7Q1eG#:~:text=,POTENCIALIDAD%20%28PRE

Nationwide. (s. f.). *Reconocer las señales de advertencia de phishing*. https://espanol.nationwide.com/lc/resources/cyber-resource-center/articles/recognize-phishing-red-flags

Oliva, D. (2025). *Triage informático: Guía práctica para priorizar incidentes*. OpenWebinars. https://openwebinars.net/blog/triage-informatico-guia-practica-para-priorizar-incidentes/

PowerDMARC. (s. f.). *Los 12 principales indicadores de phishing por correo electrónico que desenmascaran las estafas*. https://powerdmarc.com/es/common-indicators-of-a-phishing-attempt/

CONTINUAR