ACCOUNTANCY EUROPE.

GESTIÓN DE RIESGO EN LAS PYME

LISTA DE VERIFICACIÓN SOBRE RIESGOS CIBERNÉTICOS Y RESILIENCIA

DOCUMENTO INFORMATIVO **NOVIEMBRE 2022**

Traducido por: AUDITORES
Instituto de Censores Jurados de Cuentas de España

DESTACADO

Los incidentes cibernéticos pueden tener un alto impacto en la capacidad de una PYME para llevar a cabo su actividad y causan pérdidas económicas graves. Es crucial que las PYME identifiquen y mitiguen estos riesgos en un contexto en el que nuestras economías están cada vez más digitalizadas.

Los auditores/expertos contables son sus asesores de confianza y pueden jugar un papel clave para mitigar los riesgos cibernéticos de las PYME. Este documento, el más reciente de la serie de "gestión de riesgo en las PYME" de Accountancy Europe, proporciona una lista de verificación para mejorar la resiliencia cibernética de las PYME. Los propios despachos profesionales pueden también utilizar esta herramienta para evaluar su propia resiliencia cibernética.

INTRODUCCIÓN

Las empresas pequeñas y medianas (PYME) se enfrentan a nuevos riesgos que pueden tener un impacto significativo en sus negocios. Estos riesgos tienen su origen en las megatendencias globales, la crisis climática, la digitalización, la integración económica global o la COVID 19.

Accountancy Europe lanzó una serie de publicaciones sobre gestión de riesgo para informar a las PYME y a sus auditores/expertos contables que abarcan: la sostenibilidad (julio 2020), lista de verificación sobre sostenibilidad (2021), propiedad intelectual (2022 – en español) e insolvencia (2021-en español).

El sexto número de esta serie se centra en los riesgos cibernéticos. Explica el porqué y el cómo deben las PYME considerar y mitigar los riesgos cibernéticos y el modo en que el auditor/experto contable de la PYME puede ayudarla de la mejor manera. El documento incluye una lista de verificación que el auditor/experto contable puede utilizar para ayudar a sus clientes PYME a generar resiliencia en materia de riesgos cibernéticos.

La lista de verificación puede servir como base para la discusión o para la evaluación inicial de la resiliencia del cliente en materia cibernética y para que el propio auditor/experto contable conozca el riesgo cibernético en su despacho. Los auditores/expertos contables no necesitan tratar ellos mismos cada uno de los aspectos contemplados en la lista de verificación, pero deben poder reconocer cuándo han de referir a sus clientes al correspondiente experto técnico.

¿CUÁLES SON LOS RIESGOS CIBERNÉTICOS A LOS QUE SE ENFRENTAN LAS PYME?

El informe del Foro Económico Mundial (WEF por sus siglas en inglés): *2021 Global Risks Report* identifica los fallos de ciberseguridad como el cuarto riesgo claro y actual con potencial para causar una amenaza crítica al mundo. Ello lo sitúa justo después de riesgos tan críticos como un desastre climático o las enfermedades infecciosas.

Los riesgos cibernéticos surgen en las economías y modelos de negocio cada vez más digitales. Por ejemplo, en los procesos empresariales, pagos, listas de clientes y de contactos o diseños de producto o de servicios. Las PYME se pueden beneficiar de la mejora en la eficiencia, innovación, productividad y gestión que proporciona la tecnología pero, deben también conocer los riesgos que pueden acompañar a estas oportunidades y mitigarlos para acceder completamente al potencial que brinda la tecnología digital.

Los riesgos cibernéticos se encuentran entre los principales riesgos relacionados con la digitalización. Se pueden clasificar de manera aproximada entre errores humanos y ciberataques:

- Los errores humanos proceden de errores no intencionados de empleados, gerentes o socios empresariales con acceso a los flujos de trabajo digitalizados o a las bases de datos. Como ejemplos, se incluyen la publicación no intencionada de listas de clientes u otra información sensible, la pérdida de passwords, el borrado de contenido digital o el incumplimiento de legislación, como el Reglamento de Protección de datos de la UE (GDPR por sus siglas en inglés).
- Los ciberataques consisten en que partes maliciosas, que pueden ser terceros, socios empresariales o el propio personal de la PYME, perjudiquen, destruyan, espíen, compartan, publiquen o utilicen inadecuadamente y de manera intencionada el contenido digital y los procesos de la empresa (véase el cuadro de más adelante que incluye ejemplos específicos).

Una estrategia eficaz de mitigación del riesgo cibernético trataría ambas dimensiones porque están conectadas. Los errores humanos pueden exponer a las empresas a los ciberataques, mientras que los ciberataques generan una base para el error humano.

EJEMPLOS DE CIBERATAQUES

De conformidad con el informe 2021 de la Agencia Europea para la Ciberseguridad (ENISA, por sus siglas en inglés), los incidentes cibernéticos más comunes a los que se enfrentaron las PYME europeas fueron:

- 41% suplantación de identidad (phishing)
- 40% ataques basados en la web (web based attacks)
- 39% Software malicioso (malware) general
- 19% personal malicioso (malicious insider)
- 12% denegación de servicio (denial of service)
- 11% ingeniería social (social engineering)
- 7% dispositivos comprometidos o robados

El efecto multiplicador de la pandemia

Los riesgos cibernéticos se han visto amplificados por las tendencias recientes derivadas de la pandemia de COVID 19, que han empujado a las empresas a trabajar en mayor medida de manera remota y en línea. Por ejemplo, durante la pandemia se observó un incremento del 667% en el número de correos electrónicos de phishing.

¿CÓMO PUEDEN AFECTAR LOS RIESGOS CIBERNÉTICOS A LAS PYME?

Las PYME son un objetivo creciente de los atacantes cibernéticos. Es tres veces más probable que una PYME sea objeto de cibercriminales que una gran empresa.

Algunos ejemplos de consecuencias negativas de incidentes cibernéticos incluyen las siguientes:

- Pérdida económica: los incidentes cibernéticos, a menudo, tienen como resultado una pérdida económica.
  - robo de información de la empresa, información financiera, por ejemplo, detalles sobre bancos o tarjetas de pago o dinero;
  - interrupción de la actividad comercial, por ejemplo, imposibilidad de llevar a cabo transacciones en línea, interrupción grave u otros procesos dirigidos por la TI;
  - costes de reparación de los sistemas afectados, redes y dispositivos.
- Pérdida de negocio: la confianza es un elemento esencial de las relaciones empresariales. Los ataques cibernéticos pueden perjudicar la reputación de la PYME y mermar la confianza de los clientes y socios empresariales. Ello puede, posteriormente, derivar en una pérdida de clientes, socios empresariales y ventas.
- Consecuencias legales: las leyes de protección de datos y privacidad requieren que las empresas gestionen la seguridad de todos los datos personales que mantienen, sea de su personal, clientes o socios empresariales. Si estos datos se ven, accidental o deliberadamente, comprometidos, y la PYME no ha implementado medidas de seguridad adecuadas, puede enfrentarse a multas y sanciones.

¿CUÁLES SON LOS PRINCIPALES OBSTÁCULOS A LA RESILIENCIA DE LAS PYME?

Reforzar la ciberresiliencia es fundamental para que una PYME pueda mitigar los riesgos de incidente cibernético y el impacto negativo descrito más arriba. Existen ciertos obstáculos que pueden dificultar los esfuerzos que se hagan en esta área, tal y como resalta ENISA.

FALTA DE CONOCIMIENTO

Una falta de conocimiento y de compromiso de la dirección, es el obstáculo fundamental para mitigar los riesgos cibernéticos. En la práctica, ello supone destinar presupuesto y recursos e implementar procesos de seguridad cibernética.

Muchos propietarios de PYME están muy ocupados con el funcionamiento diario de la empresa y pueden no darse cuenta de la magnitud del riesgo que los errores y ataques relacionados con la ciberseguridad pueden suponer para su empresa. Por lo tanto, pueden no priorizar el tomar medidas preventivas para proteger su empresa y únicamente descubrir el coste tras la materialización de un riesgo de ciberseguridad.

Un bajo conocimiento del riesgo cibernético por el personal es también un problema. Todo aquel que tenga acceso a los sistemas de tecnología de la información puede, de forma no intencionada, provocar un incidente cibernético. Por lo tanto, es vital que todo el personal esté alerta ante potenciales problemas de ciberseguridad.

PROTECCIONES DÉBILES PARA INFORMACIÓN CRÍTICA Y SENSIBLE

Las PYME manejan una variada tipología de información tal como registros de personal, información de clientes, detalles relativos a producción y abastecimiento, datos financieros, políticas, procedimientos, etc. Esta información es esencial para la empresa. Las disposiciones legales, reglamentarias o los contratos pueden también requerir que la PYME proteja esa información.

La ausencia de una política de copias de seguridad, de actualización de soluciones anti-malware para todos los tipos de dispositivos o la utilización de software obsoleto o desactualizado puede poner en peligro gravemente información crítica y sensible de la empresa. Ello podría hacer que la PYME fuera un objetivo fácil a los ataques cibernéticos descritos más arriba.

PRESUPUESTO INSUFICIENTE

Los esfuerzos en ciberseguridad conllevan inversiones significativas, incluida formación, implementación de controles de ciberseguridad, contratación de expertos externos y formación especializada para miembros del personal. Muchas PYME ven la ciberseguridad como un coste, en lugar de verlo como una inversión esencial en su empresa. Las PYME deberían, por tanto, conocer mejor los problemas que los riesgos de ciberseguridad plantean a sus empresas y destinar presupuestos adecuados para invertir en los controles requeridos para proteger las áreas críticas de sus empresas.

FALTA DE ESPECIALIZACIÓN Y PERSONAL

Gestionar la ciberseguridad en una PYME supone una dificultad importante. La ciberseguridad es un tema que requiere de un conocimiento especializado. Sin embargo, es normal que dentro de una PYME el personal atienda múltiples tareas y que se le hayan asignado múltiples funciones. Como resultado, un empleado de una PYME puede ser responsable de la ciberseguridad y de otros procesos internos.

Muchas soluciones de ciberseguridad requieren de un conocimiento de TI especializado para su adecuada implementación y gestión. Es esencial reconocer las limitaciones potenciales del empleado responsable de la ciberseguridad y, por ejemplo, cuándo puede ser necesaria especialización adicional temporal.

A medida que la PYME crece y cambia, la tecnología que utiliza cambiará también. Ello significa que el panorama de las amenazas cibernéticas cambiará. Por lo tanto, las PYME necesitarán asegurarse de que sus esfuerzos para gestionar la ciberseguridad son continuos y coherentes. Si la empresa no tiene a un empleado con conocimientos especializados en Tecnología Informática y de la Información (TIC), lo cual es habitual en una PYME, se necesita invertir en soporte externo especializado.

FALTA DE ORIENTACIÓN ADECUADA

La disponibilidad y adecuación de orientación en forma de normas, libros blancos o similares es otra dificultad significativa. Dichos documentos existen, pero ENISA indica que la mayoría de ellos proporcionan información demasiado genérica o son en exceso complejos para las PYME, y requerirían que la PYME busque especialización específica en TI. Además, muchas PYME simplemente desconocen la existencia de tales guías, no saben cuál de ellas es mejor para su empresa o ni saben por dónde empezar.

¿PORQUÉ EL AUDITOR/EXPERTO CONTABLE ESTÁ BIEN POSICIONADO PARA AYUDAR?

Los auditores/expertos contables están bien posicionados para ayudar a las PYME a superar algunos de los obstáculos señalados en la sección anterior. La mayoría de los auditores o expertos contables no son expertos en TI. Sin embargo, están en una posición única para ayudar a las PYME a generar la resiliencia cibernética debido a que:

- Son asesores de confianza de las PYME.
- La mayoría de las PYME europeas ya confían en el auditor/experto contable para servicios de planificación empresarial, gestión económica o de flujo de efectivo, fiscalidad y cumplimiento, teneduría de libros y asesoría financiera.
- Los propietarios de PYME se reúnen regularmente con su experto contable y pueden ser su primera opción de contacto.
- Las PYME confían en los auditores/expertos contables para asesorar y cuestionar las hipótesis sobre el funcionamiento de su negocio.

Cualquier experto contable, auditor o firma puede tener cientos de clientes PYME. Por lo tanto, acumulan una amplia experiencia acerca de qué es lo que funciona en la empresa. Los auditores y expertos contables conocen los aspectos fundamentales subyacentes de la empresa a la que prestan servicios.

En concreto, en relación con la ciberseguridad, los expertos contables y los auditores pueden ayudar a:

- concienciar, entre la dirección y el personal de la PYME, acerca de la necesidad de mitigar los riesgos cibernéticos;
- asesorar acerca de en qué operaciones o prácticas empresariales es más probable que se origine un riesgo cibernético;
- identificar qué partes del negocio se “corresponden mejor” con las actividades diarias y, por lo tanto, precisan de atención especial y protección máxima. Por ejemplo, los sistemas de teneduría de libros deberían estar sujetos a copia de seguridad para asegurar una interrupción relativamente mínima, la interrupción de la producción impulsada por TI podría tener consecuencias mucho más graves para la PYME y debe ser protegida en consecuencia;
- presupuestar y planificar las inversiones en ciberresiliencia de la PYME, asesorar en las medidas críticas a tomar adaptadas a las características específicas de la empresa;
- identificar cuándo y dónde se va a necesitar experiencia especializada en TI para introducir medidas específicas y poner a la PYME en contacto con los expertos pertinentes de la red del auditor o del experto contable;
- informar a la PYME acerca de la legislación aplicable, como el Reglamento General UE de protección de datos (GDPR) y ayudarla con las medidas para su cumplimiento;
- proporcionar aseguramiento independiente sobre los sistemas de ciberresiliencia de la PYME, siempre que la persona y firma que proporcione aseguramiento sea distinta a la que ha asesorado a la PYME a establecerlos;
- asesorar acerca del desarrollo de planes de contingencia en caso de ciberataque.

En la siguiente sección se propone una lista de verificación sencilla para el auditor/experto contable como soporte de su trabajo para generar ciberresiliencia entre sus clientes PYME.

LISTA DE VERIFICACIÓN PARA AUDITORES Y EXPERTOS CONTABLES

Para una PYME, resulta caro contratar especialistas en TI internos o externos. Sin embargo, existen algunas medidas básicas que cualquier PYME puede tomar para generar ciberresiliencia.

Un auditor o el experto contable de la PYME puede utilizar esta lista de verificación para identificar la “situación” actual con respecto a los riesgos cibernéticos y ayudar a iniciar actuaciones donde sea necesario. El auditor o experto contable debería también poder evaluar y asesorar respecto a la necesidad de un especialista en TI.

APRENDER DE LA PRÁCTICA

No todos los despachos profesionales europeos están al mismo nivel en lo que se refiere a las capacitaciones en materia cibernética, el conocimiento de los ciberriesgos y la prestación de los correspondientes servicios. Cualquier despacho o profesional individual que esté interesado en prestar servicios de ciberresiliencia a clientes PYME debería empezar por su propio despacho o firma. Debe llevar a cabo una autoevaluación de su propio despacho o firma, por ejemplo, utilizando la lista de verificación como base y de manera gradual generar su propia ciberresiliencia.

Ello le ayudará a asegurarse de que su despacho o firma y sus datos están protegidos contra riesgos cibernéticos. Además, le ayudará a ganar experiencia y especialización en ciberresiliencia y a desarrollar una red de expertos a los que el experto contable o el auditor puede referir a sus clientes.

PASO 1 – LA RED

Los auditores/expertos contables deben empezar creando una red de expertos en los cuales pueden confiar para obtener mayor conocimiento y para referir a sus clientes PYME cuando lo necesiten.

El experto contable/auditor puede poner los riesgos cibernéticos en conocimiento de las PYME, convencerlas de tomar medidas y asesorarlas en algunos pasos iniciales sencillos. Sin embargo, la mayoría de los expertos contables/ auditores no tendrán la especialización en TIC necesaria para dar soluciones más sofisticadas en caso de que sean necesarias.

PASO 2 – EL CUADRO DE VALORACIÓN

Este cuadro se ha hecho sobre la base de una herramienta sencilla diseñada por SMESEC dirigida, de manera específica, a PYME con recursos. Completar el cuestionario y adoptar las primeras medidas de mejora debería ser sencillo y poco costoso para muchas PYME. El experto contable/auditor debería utilizarlo como base para su conversación con sus clientes PYME acerca de la ciberresiliencia de sus empresas.

La lista de verificación se puede utilizar también para generar ciberresiliencia y conocimiento sobre el propio despacho o firma. No es necesario que experto contable/auditor trate directamente todos los elementos de la lista, pero debería poder reconocer cuándo es necesario referir a sus clientes al correspondiente especialista técnico.

		SÍ	NO	NO SÉ
CONCIENCIACIÓN	¿Conocen los clientes de la PYME los riesgos cibernéticos y es poco probable que expongan a la PYME a amenazas cibernéticas?			
	¿Sabe el personal de la PYME cómo identificar y actuar ante correos electrónicos sospechosos o poco seguros, sitios web de hipervínculos e infracciones de hardware y actuar en consecuencia? *Por ejemplo, la utilización de memorias USB portátiles no seguras.*			
	¿Y los proveedores?			
	¿Recibe el personal de la PYME formación en ciberseguridad regularmente?			
	¿Ha establecido la PYME una política de seguridad de la información y la ha distribuido y explicado al personal?			
TAREAS Y RESPONSABILIDADES	¿Ha definido la PYME a una persona responsable de la ciberseguridad? *Es decir, el empleado de confianza al que informar acerca de fallos y errores cibernéticos, responsable de la actuación tras un ciberataque y de concienciar al personal.*			
	¿Tiene dicha persona el conocimiento y cualificaciones para responder a los tipos más habituales de ciberataques, tal y como se definen en este documento?			
	¿Tiene dicha persona la autoridad/poder dentro de la PYME para llevar a cabo actuaciones de mejora?			
	¿Tiene la PYME un plan para mitigar el impacto económico negativo en caso de que un ciberataque tenga éxito?			
PROTECCIÓN DE DATOS	¿Se almacena la información sensible y crítica encriptada, incluida la información en dispositivos móviles?			
	¿Maneja la PYME la información personal y sensible de conformidad con el Reglamento UE de protección de datos?			
	¿Protege la PYME el acceso físico a sus ordenadores, servidores y red?			
COPIAS DE SEGURIDAD	¿Tiene la PYME una copia de seguridad reciente de sus datos y sistemas?			
	¿Existe una copia de seguridad externa disponible o, como mínimo en un lugar desconectado completamente de sus sistemas?			
	¿Ha intentado la PYME restaurar una copia de seguridad de datos o sistema y comprobado que funciona?			

	RISK TYPE	YES	NO	DO NOT KNOW
ADMINISTRACIÓN DE PASSWORDS Y USUARIOS	¿Están las cuentas protegidas a través de autenticación multifactor (MFA)? *Por ejemplo, password combinado con un código pin o un token, por ejemplo, una tarjeta bancaria.*			
	¿Son las passwords de los empleados de la PYME fuertes y específicas para cada cuenta de usuario y sistema y se cambian periódicamente?			
	¿Puede cada empleado acceder únicamente a los sistemas que se supone que puede acceder?			
	¿Se bloquean adecuadamente del acceso a sistemas a los antiguos empleados?			
	Si un empleado ha sido objeto de un ciberataque ¿se ha cambiado su password?			
	¿Existe una rutina implementada de restricción y protección de uso de los privilegios de administrador de sistema?			
PROTECCIÓN ANTE SOFTWARE MALICIOSO	¿Está la PYME protegida por un cortafuegos que la proteja de ataques externos?			
	¿Están los dispositivos y aplicaciones de la PYME, protegidos contra software malicioso (por ejemplo, programas antivirus, protección contra secuestro de datos, filtros contra correo no deseado)?			
	¿Ha configurado la PYME su protección contra software malicioso para escanear los anexos en los correos electrónicos, las descargas, los ficheros recibidos de redes y sistemas de almacenamiento conectados?			
ACTUALIZACIONES	¿Se actualiza de manera regular todo el software de los dispositivos de los empleados (por ejemplo, las aplicaciones y los sistemas operativos)?			
	¿Se actualiza de manera regular la protección contra software malicioso (por ejemplo, programas antivirus y filtros de correo no deseado)?			
	¿Está todo el software en los servidores y en los dispositivos de la PYME actualizado de manera regular, incluidos los cortafuegos?			
COMUNICACIÓN SEGURA	¿Está todo el software en los servidores y en los dispositivos de la PYME actualizado de manera regular, incluidos los cortafuegos?			
	¿Se encriptan las passwords y los datos que se envían entre los clientes y el servidor?			
	¿Está la WLAN propiedad de la PYME encriptada y protegida y se exige a sus empleados que están en casa utilizar una VPN para acceder a los sistemas de la empresa?			
RESPUESTAS A UNA EMERGENCIA	¿Es la persona responsable de la ciberseguridad capaz de acabar con un ciberataque y limitar sus efectos?			
	¿Saben los directores y empleados de la PYME qué hacer ante un incidente cibernético? ¿Existen procedimientos y funciones asignadas de manera clara?			
	En el caso de que los clientes o vendedores de la PYME fueran atacados ¿informarían a la PYME si el ataque tuviera un efecto sobre ella?			
	¿Tiene la PYME un contacto de un experto en TIC que pueda darles soporte en caso de una necesidad urgente?			
	¿Tiene la PYME un seguro que cubra las disrupciones relacionadas con las TI que incluya ciberataques y el consiguiente impacto en el negocio?			
PARA PYMES QUE DESARROLLAN SOFTWARE O DISPOSITIVOS	¿La WLAN de los empleados está separada de la de los invitados?			
	¿Ha definido la PYME quién es el responsable de la seguridad de cada uno de los productos y servicios de software?			
	¿Ha hecho la PYME una inspección de códigos, especialmente para detectar vulnerabilidades y lagunas de seguridad?			
	¿Ha hecho la PYME comprobaciones de caja negra contra las amenazas de seguridad más comunes?			
RESULTADO	Indique el número de ocasiones en que ha respondido SÍ			

PASO 3 – ANALIZAR LOS RESULTADOS Y TOMAR LAS MEDIDAS ADECUADAS

0 - 10	Alerta roja La PYME es presa fácil. Ayuda a la PYME a determinar las respuestas **NO**/**NO SÉ** más fáciles de convertir en un **SÍ**.
11 - 24	Alerta naranja La PYME está en un punto de partida robusto, pero precisa de mayor progreso. Diseña un plan de cambio para alcanzar una puntuación de 24 o más en 6 meses.
25 - 30	Alerta verde La PYME ya realiza mucho en el ámbito de la ciberseguridad. Discutid acerca de qué más se podría hacer.
31 - 39	El club de los azules La PYME es un referente y ejemplo a seguir por otros.

CONCLUSIÓN

Las actividades y la supervivencia de las PYME pueden verse gravemente afectadas por los incidentes cibernéticos, tanto internacionales como debidos a un error humano. Es de gran importancia para los propietarios de PYME y sus empleados conocer los riesgos cibernéticos potenciales para ayudar a mitigarlos y para actuar de manera eficaz en caso de que se produzca un ciberataque.

El auditor/experto en contabilidad puede ayudar. Conoce las PYME y puede asesorarlas en áreas como la elaboración de un mapa de riesgos cibernéticos, medidas de mitigación, aumento del conocimiento y más. La lista de verificación que se incluye en este documento está diseñada para ayudar al experto a mantener una reunión inicial sobre el mapa de riesgos cibernéticos con sus clientes PYME.

Pero, a pesar de todos los esfuerzos para mitigar los riesgos cibernéticos, todavía pueden materializarse. Las PYME y los auditores/expertos en contabilidad deberían establecer procesos eficaces, copias de seguridad y sistemas que aseguren la continuidad del negocio y la recuperación de los sistemas cuando los riesgos se materialicen. La lista de verificación puede ser de ayuda aquí también.

ANEXO – DEFINICIONES Y TERMINOLOGÍA

Suplantación de identidad (phishing): es un tipo de ingeniería social por la que un atacante envía un mensaje fraudulento (por ejemplo, suplantado, falso o engañoso de otro modo) diseñado para engañar a una persona para que revele información sensible al atacante o para instalar software malicioso en la infraestructura de la víctima, como el secuestro de datos (ransomware).

Denegación de servicio: un ataque DoS que impide a los usuarios acceder a un servicio colapsando sus recursos físicos o sus conexiones de red.

Ataques basados en la web: cuando los criminales explotan las vulnerabilidades en el código para acceder a un servidor o base de datos, esas amenazas de vandalismo cibernético se conocen como ataques de capas de aplicación. Los usuarios confían en que la información sensible que divulgan en tu sitio web seguirá siendo privada y estará segura.

Software malicioso (malware): es el nombre genérico con que se conoce las diferentes variantes de software pernicioso, incluido virus, ransomware y programas espía. El software malicioso consiste habitualmente en código desarrollado por atacantes cibernéticos, diseñado para causar un daño extenso a los datos y sistemas o para obtener acceso no autorizado a una red.

Personal interno malicioso: también conocido como Turncloak es alguien que de manera maliciosa e intencional abusa de credenciales legítimas, habitualmente para robar información por incentivos económicos o personales.

Ingeniería social: es una manipulación técnica que se aprovecha del error humano para obtener información privada, acceso u objetos de valor.

Autenticación multifactor: la MFA (por sus siglas en inglés) es un método de autenticación electrónica en la que se facilita a un usuario acceso a un sitio web o a una aplicación solo después de presentar dos o más evidencias.

Secuestro de datos (ransomware): es un tipo de software malicioso que amenaza con publicar datos personales de la víctima o con bloquear permanentemente el acceso a menos que se pague un rescate.

Sistema de privilegios de administrador: es la capacidad de hacer cambios importantes en un sistema, habitualmente un sistema operativo. También puede significar grandes programas de software como un sistema de gestión de bases de datos.

Lista blanca, lista de permiso o de paso: es un mecanismo que permite explícitamente a las entidades identificadas acceder a privilegios, servicios, movilidad o reconocimiento específicos, es decir, es una lista de cosas que puedes hacer cuando todo está prohibido por defecto.

WLAN: Área de red inalámbrica.

Acerca de Accountancy Europe

Accountancy Europe reúne a 51 organizaciones profesionales de 37 países, que representan a 1 millón de profesionales de la contabilidad, auditores y asesores. Hacen que los números trabajen para las personas. Accountancy Europe traslada su experiencia diaria para informar al debate público en Europa y más allá.

Accountancy Europe está en el registro de transparencia de la UE (No 4713568401-18).

Esta publicación es la traducción de un documento publicado originalmente por Accountancy Europe en noviembre de 2022 bajo el título *SME Risk Management: Ciber risk and resilience checklist*. La traducción ha sido preparada bajo la responsabilidad única del Instituto de Censores Jurados de Cuentas de España. Accountancy Europe no se hace responsable del contenido del documento ni de la fidelidad de la traducción. En caso de duda los lectores deberán referirse al original en inglés que puede obtenerse gratuitamente del sitio web de Accountancy Europe website: https://www.accountancyeurope.eu.Los documentos de Accountancy Europe no pueden reproducirse total ni parcialmente en la versión original ni sus traducciones sin consentimiento escrito previo de Accountancy Europe info@accountancyeurope.eu