GESTIÓN DE RIESGO EN CIBERSEGURIDAD

Introducción

Las empresas pequeñas y medianas (PYME) como la nuestra, 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. 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.

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.

Riesgos cibernéticos a los que nos enfrentamos

Los riesgos cibernéticos surgen en las economías y modelos de negocio cada vez más digitales. La empresa se puede 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.
- 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

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.

Afectaciones por los riesgos cibernéticos.

Empresas pequeñas como la nuestra 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 empresa 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 nosotros no hemos implementado medidas de seguridad adecuadas, podemos enfrentarnos a multas y sanciones.

Principales obstáculos a la resiliencia

Reforzar la ciberresiliencia es fundamental para 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:

- .Falta de conocimiento a nivel de dirección
  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.
- Bajo conocimiento del riesgo cibernético por el personal.
  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
  La empresa maneja 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.
- Ausencia de una política de copias de seguridad,
  La no 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 seamos un objetivo fácil a los ataques cibernéticos.
- 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.

- Falta de especialización y personal.
  La ciberseguridad es un tema que requiere de un conocimiento especializado; 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.

Lista de verificación para auditores y expertos contables

Enumeramos a continuación, las medidas básicas que debemos tomar para generar ciberresiliencia y que un auditor o el experto contable 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.

PASO 1 – **CUADRO DE VALORACIÓN**
Este cuadro se ha hecho sobre la base de una herramienta sencilla diseñada por SMESEC ("Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework") dirigida, de manera específica a PYMEs. Se debe completar el cuestionario y adoptar las primeras medidas de mejora. El experto auditor deberá utilizarlo como base para su conversación acerca de la ciberresiliencia de la empresa.
La lista de verificación se puede utilizar también para generar ciberresiliencia y conocimiento sobre el propio despacho o firma. No es necesario que el auditor trate directamente todos los elementos de la lista, pero debería poder reconocer cuándo es necesario referir a sus clientes al correspondiente especialista técnico.

	CUADRO DE VALORACIÓN	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 RESPONSABILIDA	¿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 SEGURIDA	¿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?			

	TIPO DE RIESGO	SI	NO	NO SÉ
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	¿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?			
PARAPYMESQUE ODISPOSITIVOS	¿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 2 – **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 la empresa puede verse gravemente afectadas por los incidentes cibernéticos, tanto internacionales como debidos a un error humano. Es de gran importancia para nostros 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 puede ayudar, conoce la empresa y puede asesorarla 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. La empresa y los auditores 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.

Control de cambios

ELABORÓ:	**REVISÓ**	**APROBÓ:**
Nombre: Ing. Enith Enilse Gustin **Cargo:** Asesor Externo **Fecha:** 10/02/2025	**Nombre:** Diego Córdoba **Cargo:** Gerente **Fecha:** 11/02/2025	**Nombre:** Diego Córdoba Z **Cargo:** Gerente **Fecha:** 11/02/2025

CONTROL DE CAMBIOS		
Versión No.1.0	2025/02/11	Creación del Documento