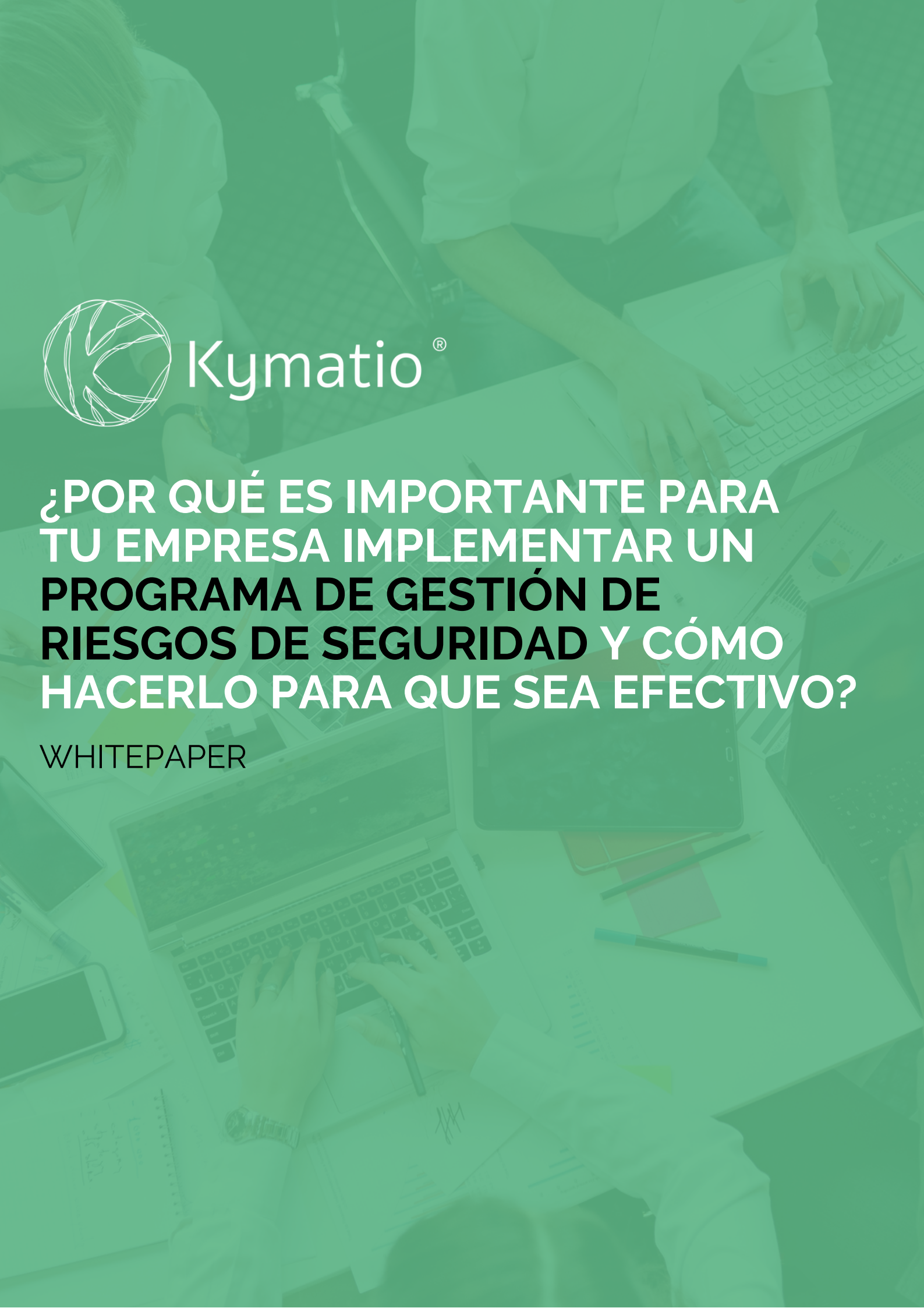


Kymatio®

¿POR QUÉ ES IMPORTANTE PARA TU EMPRESA IMPLEMENTAR UN PROGRAMA DE GESTIÓN DE RIESGOS DE SEGURIDAD Y CÓMO HACERLO PARA QUE SEA EFECTIVO?

WHITEPAPER

Las organizaciones, de manera constante, están expuestas a una serie de riesgos que pueden amenazarlas de diversas maneras, ya sea de manera económica, legal o reputacional, entre otras. En los casos más graves podrían impedir su continuidad e, incluso, afectar la integridad física de sus colaboradores.

A fin de cuentas, el riesgo podría definirse como la probabilidad de que ocurra un acontecimiento no deseado o desfavorable, en este caso, para la organización.

El riesgo se compone de varios factores, a saber:

- **Probabilidad:** los riesgos pueden ser muy variados, pero no todos tienen la misma probabilidad de ocurrencia. Mientras que hay algunos con alta probabilidad (por ejemplo, que un ciberdelincuente envíe correos fraudulentos a los empleados), otros son muy improbables (por ejemplo, que caiga un meteorito donde se encuentran todos los sistemas de información).

- **Impacto:** por otra parte, es necesario saber de qué manera afectaría a la organización en caso de que el riesgo se materializara. ¿Se trata de consecuencias menores o realmente se sufriría un gran daño? Tal y como se ha mencionado, estas consecuencias pueden ser de distintos tipos, como financieras, operativas, estratégicas, reputacionales o legales, entre otros.

- **Incertidumbre:** el riesgo implica un grado de incertidumbre, ya que no siempre es posible predecir con certeza si un evento adverso o una situación desfavorable ocurrirá o cuándo lo hará.

- **Contexto:** la percepción del riesgo y su importancia puede variar según el contexto y la perspectiva de las personas u organizaciones. Lo que una persona puede percibir como un riesgo, puede no serlo para otra, y lo que se considera como un riesgo en un contexto puede no serlo en otro.

- **Tolerancia:** muy ligado con el punto anterior tenemos lo que se suele denominar "apetito al riesgo". Mientras que hay personas u organizaciones muy conservadoras, que arriesgan poco, hay otras que deciden exponerse a una mayor probabilidad de sufrir un acontecimiento negativo ante la expectativa de una recompensa mayor si finalmente esta situación desfavorable no se llega a materializar. Un ejemplo muy claro se da en las inversiones.

En resumen, el riesgo se refiere a la posibilidad de que algo negativo suceda en el futuro, y su gestión implica tomar medidas para evaluar, mitigar o controlar esas posibilidades y su impacto para proteger los intereses y objetivos de la organización y sus colaboradores.

Para ello, es necesario conocer a qué riesgos se enfrentan. En función de su tipología, los riesgos se pueden clasificar en:

- **Riesgos financieros:** hacen referencia a todas las pérdidas que se pueden sufrir a nivel económico por distintos motivos.
- **Riesgos operativos:** son los que interfieren con el correcto funcionamiento de la organización, como aquellos relacionados con la seguridad o con los sistemas tecnológicos.
- **Riesgos estratégicos:** tienen que ver con la dirección y posicionamiento de la organización en el mercado.
- **Riesgos de cumplimiento:** aquí entrarían todos aquellos relativos al cumplimiento con la legislación vigente, así como con la ética de la propia organización.
- **Riesgos ambientales y sociales:** están relacionados con el impacto que tienen las actividades de la organización a nivel medioambiental y social.
- **Riesgos geopolíticos:** eventos políticos, conflictos internacionales y cambios en el entorno geopolítico que pueden afectar a la organización.

Es importante destacar que estos riesgos no son mutuamente excluyentes, y una organización puede enfrentar múltiples riesgos simultáneamente. Por esta razón es necesario tener un programa de gestión de riesgos que permita estar preparados ante los posibles peligros. En este documento se analizarán los conceptos básicos de un programa de gestión de riesgos, la importancia de contar con uno en cada organización y cómo implementarlo de manera exitosa, poniendo el foco en los riesgos de seguridad de la información.

PROGRAMA DE GESTIÓN DE RIESGOS: CONCEPTOS BÁSICOS

Lo primero que se debe conocer si se quiere implementar uno de estos programas es, precisamente, qué es. Se trata de un conjunto de procesos, políticas, procedimientos y estrategias diseñados para identificar, evaluar, mitigar y controlar los riesgos que pueden afectar a una organización en el logro de sus objetivos. El objetivo principal de un programa de gestión del riesgo es ayudar a la organización a anticipar y abordar los riesgos de manera proactiva para minimizar pérdidas financieras, daños a la reputación y otros impactos negativos.

Como ha quedado patente, los riesgos pueden ser múltiples y de distinta índole, por lo que se deberán elaborar estrategias específicas para cada uno. Para acotar y evitar quedarnos en la superficie, en este documento nos centraremos en la seguridad de la información, tal como se ha mencionado anteriormente.

Los elementos de los que se componen los distintos programas de gestión del riesgo son los mismos, aunque pueden contar con algunas variaciones en función de las características específicas de los elementos a controlar:

- **Identificación de riesgos**

Es obvio que, para poder manejar una situación peliaguda de manera eficaz y eficiente, es necesario saber a qué nos enfrentamos. Como se ha mencionado, puede que, por la naturaleza de las diversas organizaciones, algunas de ellas se encuentren con riesgos específicos. Sin embargo, hay otros que son comunes a todas ellas, independientemente de su tamaño, sector o actividad.

En el caso de la seguridad de la información, es imprescindible identificar cuáles son los activos más importantes, y para ello se utiliza la clasificación en función de tres parámetros: la confidencialidad, la integridad y la disponibilidad.
La confidencialidad hace referencia a las personas que pueden acceder a dicha información. No todas las personas deberían estar autorizadas a ver ciertos documentos o consultar determinados datos.
Por otra parte, la integridad tiene que ver con la modificación o borrado de información no autorizados. Por ejemplo, nadie debería alterar los números de un reporte financiero una vez han sido revisados y aprobados. Por último, la disponibilidad indica la necesidad de que la información en cuestión se encuentre disponible para su acceso en el momento necesario. Mientras que hay información que debe estar permanentemente accesible, como pueden ser las páginas web de empresas de venta online, otros simplemente deben estarlo en momentos concretos.

- **Evaluación de riesgos:**

Una vez se sabe qué es lo que se quiere mantener bajo control, cabe preguntarse la probabilidad de que ocurra y la gravedad de sus consecuencias en caso de darse. Esto lo que permitirá será una priorización en la posterior gestión de cada uno de estos riesgos: así, un evento con alta probabilidad de ocurrencia con un gran impacto tendrá mayor prioridad que uno con poca previsión de que suceda y con consecuencias poco significativas. En el caso del ciberriesgo también cabe preguntarse cuáles son las vulnerabilidades que se pueden encontrar en los sistemas, por lo que es necesario realizar pruebas de seguridad frecuentes, así como auditorías, que permitan comprobar que está todo en orden y solucionar los problemas identificados para reducir la superficie de exposición a un incidente.

- **Mitigación de riesgos:**

La mitigación no es otra cosa que reducir las probabilidades de que suceda el acontecimiento negativo en cuestión y/o el impacto que pueda tener. Para esto se deben seguir estrategias diferentes en función del tipo de riesgo al que nos estemos enfrentando. Es importante recalcar el término "reducción", ya que la completa eliminación del riesgo es, en la mayor parte de los casos, imposible, especialmente en el ámbito del ciberriesgo.

El factor humano es un elemento clave, ya que gran parte de los incidentes de seguridad que se producen involucran de alguna forma al personal de la organización, ya sea de manera voluntaria o involuntaria (siendo víctimas de un ataque de ingeniería social).

- **Comunicación:**

Estas medidas tomadas deben ser comunicadas apropiadamente para que todos los colaboradores sean conscientes de ellas y puedan cumplir con su parte si se precisa. Dependiendo de las acciones a realizar, esto también puede aplicar a terceros que trabajen con la organización.

- **Monitoreo y control:**

Cuando se implementan estas estrategias, es necesario llevar un seguimiento de ellas para comprobar que se están implementando de manera adecuada y que están surtiendo efecto.

- **Revisión y modificación:**

En caso de que las medidas tomadas resulten no ser óptimas, se deberán cambiar. También puede ocurrir que ciertas estrategias sean efectivas en un determinado momento pero que, con el tiempo, queden desactualizadas debido a cambios en el panorama cibernético, económico, político, social, etc.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: ¿QUÉ ESTRATEGIAS SEGUIR?

Cada organización tiene sus propias estrategias en función de sus características. Sin embargo, hay algunos puntos que suelen ser comunes a todos los programas.

- **Política de Seguridad de la Información:**

El elemento que debe encabezar el programa no es otro que la Política de Seguridad de la Información. Se trata de un documento general que define las pautas generales a seguir y las responsabilidades.

- **Control de accesos:**

Como se ha comentado anteriormente, no todo el mundo debería poder acceder a toda la información. Por eso es importante delimitar quién puede ver y/o editar los diferentes archivos y, posteriormente, restringir su acceso a los usuarios necesarios.
Además, también es importante mantener la información protegida de terceras partes que quieran visualizarla o modificarla con fines maliciosos. Por eso, normalmente se proponen métodos de acceso cada vez más seguros a medida que aumenta la sensibilidad de la información (por ejemplo, usuario y contraseña más un segundo factor de autenticación).

- **Monitorización:**

Es importante mantener un control sobre la actividad de los usuarios que interactúan con los diferentes activos de información. Para esto se recurre a diferentes soluciones, como aquellas que vigilan que los archivos no abandonan la ubicación designada o que controlan las intrusiones por parte de personas no autorizadas.

También es importante contar con un sistema de control de cambios que haga posible contar con un registro de cuándo y quién ha modificado los archivos que sean categorizados por la organización como confidenciales o, simplemente, importantes.

- **Protección de la información:**

Toda organización maneja datos sensibles de cualquier tipo, como pueden ser datos personales o propiedad intelectual. Por eso, se hace imprescindible especificar cómo debe ser su recopilación (en el caso de los datos personales), almacenamiento, procesamiento y protección. Para ello no solo se debe tener en cuenta el criterio de la propia organización, sino también la legislación vigente en cada territorio pertinente.

- **Copias de seguridad y recuperación de datos:**

La información puede ser alterada por accidente o por parte de un agente malintencionado, como es el caso de los ransomware. Por eso es necesario tener copias de seguridad y protocolos para la recuperación de datos en caso de incidente. Se debe establecer cuándo y cómo se realizan estas copias y cómo se debe proceder en caso de necesitarse esta recuperación. Además, las copias de seguridad deben almacenarse en un sistema fuera de línea si es posible o, al menos, separado del sistema principal de la organización. Esto debe ser así para que los ciberdelincuentes no puedan secuestrar también estas copias con facilidad.

- **Dispositivos:**

Las políticas respecto a los dispositivos utilizados con fines de trabajo pueden ser muy variados, pero siempre deben existir. Mientras que hay organizaciones que solo cuentan con un ordenador de mesa, hay otras que también hacen uso de ordenadores portátiles y móviles. Otras, incluso, permiten el uso de dispositivos personales para trabajar (BYOD por las siglas en inglés de "trae tu propio dispositivo"). Las estrategias a seguir incluyen la instalación de programas de seguridad, la manera de hacerlo, la restricción de visitas a determinadas páginas web, etc.

- **Gestión de incidentes:**

Es muy probable que cualquier organización sufra un incidente de seguridad de la información en algún momento. Estos se pueden considerar "grandes" o "pequeños" en función de su impacto, pero es necesario tener en cuenta que hay que gestionar incluso aquellos que, aparentemente, apenas supongan ninguna consecuencia.

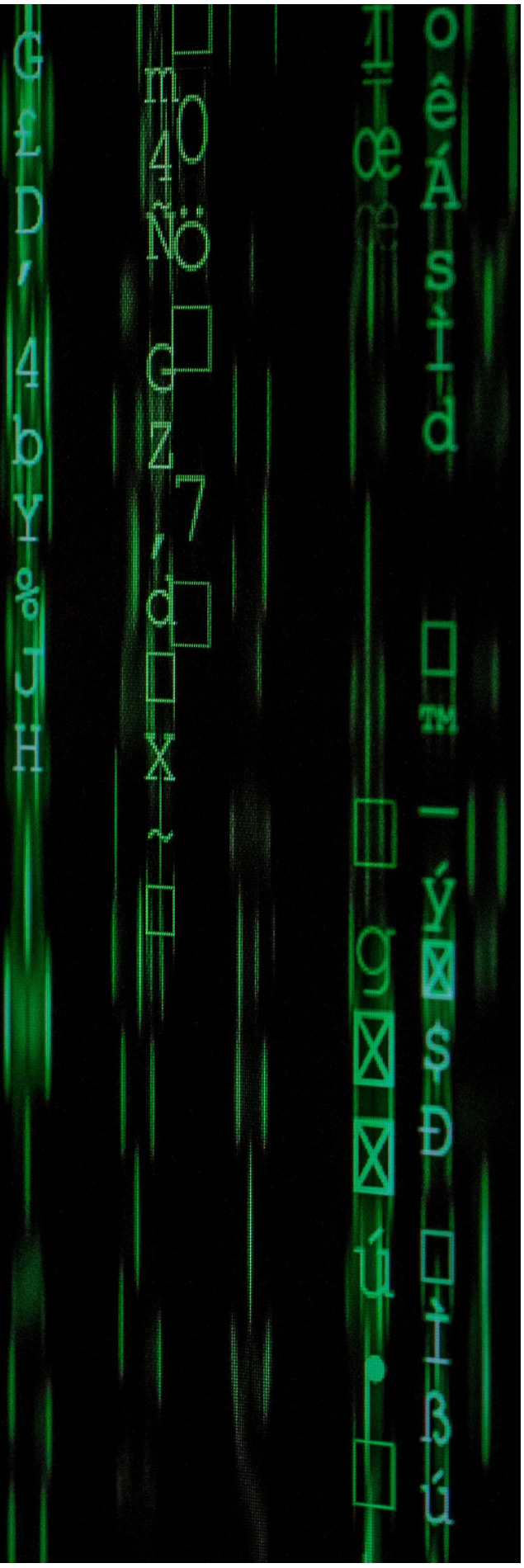
Para ello se deben establecer protocolos para el reporte de cualquier tipo de incidente por parte de los colaboradores y para responder a ellos por parte del equipo correspondiente en caso necesario. Es necesario hacer hincapié en la importancia de reportar cualquier cosa que les parezca susceptible de ser o convertirse en un incidente de seguridad, incluso si las sospechas son mínimas. A menudo, los colaboradores se sienten cohibidos cuando no están seguros por no querer molestar al equipo de Seguridad. Por esta razón es muy importante generar un clima de confianza en el que se fomente el reporte de cualquier sospecha que puedan tener, aun a riesgo de que se trate de una falsa alarma.

- **Seguridad de la red:**

Los dispositivos no son lo único que hay que proteger: también las redes de la organización, incluyendo la configuración de firewalls, detección de intrusiones, segmentación de redes y monitorización de tráfico.

- **Correo electrónico:**

Los correos electrónicos fraudulentos o phishing son uno de los principales vectores de ataque utilizados por los criminales. Ya sea a través de mensajes generales o personalizados (spear phishing), los ciberdelincuentes buscan manipular a los destinatarios para que les proporcionen información sensible o realicen transferencias bancarias. Contar con una solución que identifique y filtre este tipo de mensajes o, al menos, la mayor parte de ellos, ayudará a mantener la seguridad de la información, reduciendo las probabilidades de que los empleados caigan víctimas de estos engaños. Además, es muy recomendable que, dentro de la solución usada, se disponga de un software adecuado que se integre al cliente de correo utilizado y permita reportar un correo sospechoso con solo pulsar un simple botón.



- **Concienciación:**

Los ciberdelincuentes, cada vez con más frecuencia, están poniendo el foco de sus ataques en el factor humano. A través de ataques de ingeniería social intentan engañar a los colaboradores de una organización para que lleven a cabo acciones en contra de la misma, como conceder información sensible o realizar transferencias bancarias. Ya se ha mencionado que su método preferido para ello suele ser el phishing o spear phishing, pero no es el único medio que utilizan, sino que se valen de otros, como mensajes de texto (smishing), llamadas telefónicas (vishing) o códigos QR maliciosos.

Además, como humanos, es muy probable que se lleguen a cometer errores en un momento que deriven en un incidente de seguridad, o que no se sepan cuáles son las directrices a seguir en esta materia. Por todo esto, la concienciación es un punto indispensable en un programa de gestión del ciberriesgo.

- **Gestión de terceros:**

Las organizaciones a menudo colaboran con otras, ya sean proveedores, partners o cualquier otro tipo de relación. Cuando se realizan actividades conjuntas o se comparte información sensible entre ambas, es necesario definir unos requisitos de seguridad y firmar acuerdos de confidencialidad para evitar la filtración de información sensible.

Estas son solo algunas de las principales estrategias a seguir, pero existen incluso más. La manera de implantarlas y llevarlas a cabo depende de las características de cada organización y de sus necesidades. No obstante, hay ocasiones en las que lo que determina la forma final del programa de gestión de riesgos de seguridad de la información son otras razones distintas, generalmente afectando de manera negativa. A continuación explicamos cuáles son las principales dificultades a la hora de implantarlo.

PRINCIPALES DIFICULTADES:

- **Cultura organizacional inadecuada:** La seguridad de la información es un elemento que no todos los colaboradores consideran importante. No es extraño que opinen que se trata de un tema exclusivo del departamento de Seguridad o, incluso, el de IT. Sin embargo, no son conscientes de que se trata de un aspecto clave para la organización que necesita de la colaboración de todos. Por eso es necesario hacer hincapié en la importancia de que toda la organización, a cualquier nivel, esté involucrada en el proceso de fortalecerla.

- **Falta de compromiso de la Alta Dirección:** La cultura de seguridad empieza por la cúpula de la organización. Solo de esta manera se pueden llevar a cabo medidas que fomenten el cuidado de la seguridad de la información por parte de todos los colaboradores. Sin embargo, no es de extrañar que los directivos se desvinculen de esta tarea de mantener la seguridad de la información, a pesar de que son los perfiles que los ciberdelincuentes más buscan atacar. A menudo alegan no tener tiempo ni dinero que destinar a esto, delegándolo todo en un equipo de Seguridad que poco puede hacer sin presupuesto, y sin saber que su ejemplo e involucración son clave en el éxito de la estrategia.

- **Falta de recursos:** Se encuentra muy relacionado con el punto anterior. El éxito de las operaciones a nivel empresarial se considera según su retorno de inversión o ROI, y tiene un beneficio tangible; por ejemplo, el porcentaje en el que han aumentado las ventas tras introducir un producto nuevo es algo que se puede observar claramente después de un tiempo estipulado. Sin embargo, no ocurre lo mismo con la seguridad de la información, razón por la que se utiliza el ROSI.

En estos casos, el retorno de la inversión no es tan evidente, ya que no se está produciendo un aumento de las ganancias, sino una disminución de las pérdidas. Por tanto, en una sociedad centrada principalmente en las ganancias, no es extraño que la cúpula directiva considere que la inversión en seguridad está en la cola de las prioridades, dejando a un equipo de Seguridad con mucho que hacer con un presupuesto insuficiente y, a menudo, pocas manos.

- **Falta de concienciación:** Uno de los principales retos del equipo de Seguridad es el fomento de esa cultura que se comentaba en el primer punto. Para ello es necesario involucrar a todos los colaboradores, pero lo más común es encontrarse con una falta de concienciación en seguridad casi absoluta. Por eso es necesario establecer planes específicos para aumentar el estado de alerta de la plantilla. No obstante, este punto es algo que, desgraciadamente, pocos abordan de manera correcta. El mero hecho de dar un curso una o dos veces al año no funciona, y tampoco se tiene visibilidad sobre el estado de alerta de cada colaborador ni del riesgo humano al que está expuesta la organización, así como su evolución en el tiempo. Esta gestión suele consumir mucho tiempo del equipo de Seguridad, haciendo que el proceso no sea eficiente y, a pesar de los esfuerzos, a menudo tampoco eficaz. En este whitepaper detallamos por qué los enfoques actuales no funcionan y cómo cambiarlos para reducir verdaderamente el riesgo asociado al factor humano.

- **Resistencia al cambio:** Esto es algo muy común en los humanos. Tendemos a acomodarnos en los procedimientos a los que ya estamos acostumbrados y a tener cierta reticencia ante nuevas formas de hacer las cosas, rechazando el cambio por la incertidumbre que ello puede causar. Sin embargo, para poder perfeccionar el sistema de gestión de riesgos siempre es necesario ir modificando aquellas partes que no funcionan o que podrían ser mejoradas. La apertura al cambio por parte de todas las personas que conforman la organización es esencial para poder implantar soluciones y procedimientos nuevos que puedan ayudar a aumentar el nivel de seguridad de la misma.

- **Cumplimiento normativo:** Además de la importancia de la seguridad de la información per se, se debe sumar la legislación vigente. Cada territorio tiene sus propias regulaciones, y las organizaciones deben seguirlas para evitar sanciones y cualquier otro tipo de consecuencias que puedan derivar de su incumplimiento, como las legales.

- **Nuevas amenazas:** El cibercrimen se encuentra en constante evolución. Cada poco tiempo se desarrollan nuevas amenazas o se perfeccionan las existentes, de forma que las organizaciones son cada vez más vulnerables a ellas si no se hace nada para contrarrestarlo. Mantenerse al día de los últimos avances y soluciones no es tarea fácil, pero sí necesaria para evitar incidentes.

- **Complejidad del proceso:** Las funciones del equipo de Seguridad son amplias, por lo que también lo será el número de herramientas a utilizar. A este número elevado hay que sumarle, además, su complejidad, lo que hace que requieran de una gran inversión de tiempo por parte de quien las maneja.

Estas son solo las principales dificultades que suelen estar ligadas a la implantación de un programa de gestión de riesgos de seguridad de la información, pero pueden surgir muchas más. Esto hace que su implantación sea muy complicada, razón por la que, a menudo, estos programas no alcanzan la calidad que deberían tener.

Entonces, ¿qué hay que hacer para implantar un programa de calidad de manera exitosa?

01

Involucrar a la alta dirección

El primer paso para conseguir que el programa de gestión de riesgos de seguridad sea un éxito es involucrar a los perfiles directivos. Para ello será necesario educarlos sobre la importancia de la seguridad de la información y contar con suficientes recursos que destinar a un programa que involucre a todos los colaboradores. Comunicar los beneficios que tendrá para la organización será fundamental, apoyándose en datos como las últimas estadísticas, casos de incidentes recientes de otras organizaciones del sector o el ROSI estimado.

02

Crea una cultura de seguridad

Es importante que todos los colaboradores se sientan responsables de la seguridad de la información, ya que todos manejan información sensible en algún grado, o tienen conocimientos mínimos del funcionamiento de la organización.

03

Asignar recursos adecuados

Por supuesto, para que un programa tenga la fuerza necesaria, es preciso contar con recursos suficientes. La inversión en seguridad debe ir acorde a las necesidades de la organización y abarcar los distintos aspectos de un programa de gestión de riesgos sin dejar ninguno fuera.

04

Contar con soluciones completas que permitan automatizar los procesos.

Este punto está muy relacionado con el anterior. Uno de los recursos más valiosos de los equipos de Seguridad es el tiempo, que a menudo se ve ocupado por las diversas herramientas y tareas que, al final del día, terminan requiriendo una atención muy manual. Por eso, encontrar soluciones que engloben diferentes necesidades simplificará mucho su trabajo, máxime si son herramientas automáticas que requieran de poca interacción por parte de este departamento sin interferir de manera negativa en los resultados.

05

Desarrollar políticas y procedimientos claros

Un programa puede tener una gran calidad en la teoría, pero de nada sirve si los procedimientos a seguir no están suficientemente bien concretados y explicados.

06 Adaptar el programa a las necesidades de la organización.

Cada organización es diferente, por lo que los procedimientos tendrán que estar adaptados a las necesidades y la cultura de cada una. Por ejemplo, una empresa del sector logístico no tiene las mismas necesidades que una del sector legal.

07 Cumplir con las regulaciones

Cada territorio y sector cuenta con su propio marco normativo. Es necesario prestar atención a las que aplican a nuestra organización y actuar en consecuencia para cumplir con las necesidades legales.

08 Monitorización y mejoría continuas

Como se expresa anteriormente, un plan de gestión del riesgo no es estático, sino que debe estar en constante evolución. La monitorización de los procesos es necesaria para poder evaluar su efectividad y, a partir de ahí, mejorarlos en función de los elementos identificados y el desarrollo de nuevas amenazas.

09

Gestión de incidentes efectiva.

Una vez se ha producido un incidente es necesario responder ante él para minimizar su impacto. Para ello se debe contar con un plan sólido que se despliegue con rapidez en los casos necesarios. Por supuesto, cada incidente que ocurra es una oportunidad para mejorar tanto esta gestión de incidentes como el plan de prevención en general.

10

Poner a las personas en el centro

En muchas ocasiones, el enfoque de los planes de gestión del riesgo parece dejar a las personas a un lado, olvidando que son ellas las que manejan la información y los sistemas que la contienen. Relegarlas a un segundo plano y tratarlas como si fueran solo una máquina o un programa más de la lista es un error muy común que, a menudo, termina costando varios millones de euros a las organizaciones y/o destruyendo su reputación. Por eso es necesario reenfocar el programa para que los colaboradores, en lugar de un riesgo que gestionar, se conviertan en fuertes aliados para mantener la seguridad. Por ejemplo, si un mensaje de phishing consigue superar todas las barreras tecnológicas y finalmente alcanza la bandeja de entrada de un colaborador, será esencial que lo identifique y que lo reporte al equipo de Seguridad.

¿CÓMO PUEDE AYUDAR KYMATIO® A TU PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD?

Kymatio® es una solución que prepara a organizaciones y personas frente a las amenazas de ciberseguridad.

Se trata de un SaaS para la gestión del ciberriesgo humano que utiliza la neuropsicología y la ciberseguridad como base de su tecnología. La IA de Kymatio® automatiza el programa de concienciación en seguridad de la información de los empleados, la evaluación periódica de su estado de alerta, gestiona las simulaciones de ataque de phishing y proporciona el servicio de vigilancia y mitigación del riesgo de credenciales expuestas.

Utilizando la neuropsicología y la ciberseguridad como base de su tecnología, la IA de Kymatio® interactúa con las personas, ofreciéndoles una concienciación personalizada y adecuada a sus necesidades, manteniendo el nivel de alerta y fortaleciendo las áreas en las que pueden ser más vulnerables.

Al mismo tiempo, proporciona a las organizaciones visibilidad en tiempo real sobre el riesgo humano en función de distintas métricas como el nivel de concienciación, las funciones y acceso a la información, el nivel de bienestar, respuesta a simulaciones o análisis de cuentas expuestas en brechas.

Para saber más, contacta con nosotros en **contact@kymatio.com** o pídenos una reunión en **https://calendly.com/kymatio**

SOBRE LA AUTORA

Andrea Zamorano

Cyberpsychology Manager en Kymatio®, investiga el lado humano de la ciberseguridad y desarrolla los algoritmos necesarios para que la plataforma sea capaz de medir con precisión los factores implicados, de forma que se pueda evaluar el riesgo y presentar las recomendaciones personalizadas en función de las necesidades de cada uno. También es docente en la Escuela de Inteligencia Económica de la UAM (La_SEI) como experta en perfilado indirecto de personalidad. Es psicóloga de formación, habiendo estudiado en la Universidad Autónoma de Madrid, y posteriormente se graduó del Máster en Inteligencia Económica y Relaciones Internacionales por La_SEI. También cuenta con un título de Experto en Organización y Recursos Humanos por la Universidad Autónoma de Madrid.

Kymatio®

Activa tus firewalls humanos

www.kymatio.com