Co-funded by the European Union

GUÍA DE BUENAS PRÁCTICAS PARA PYMES

CYBER AGENT 06.2026

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Paquete de trabajo 6: Difusión y explotación

Entrega 6.4: Guía de buenas prácticas para pymes

Responsable del WP6: Fundación Women4Cyber

CONTENIDO

LISTA DE TABLAS

INTRODUCCIÓN

El proyecto CyberAgent se desarrolló a lo largo de tres años en ocho países europeos: Rumanía, Bélgica, Noruega, España, Turquía, Polonia, Lituania y Finlandia. CyberAgent se creó con el objetivo de desarrollar y poner a prueba un programa de formación en ciberseguridad modular y accesible dirigido a empleados de pymes, alumnos de formación profesional y estudiantes de educación superior. El resultado principal de este trabajo es el «agente de cambio en ciberseguridad»: un empleado formado, no especialista, que actúa como punto de referencia interno para la sensibilización sobre la ciberseguridad dentro de su organización.

Esta guía plasma la experiencia adquirida durante la ejecución del proyecto en orientaciones prácticas para las pymes. Explica en qué consiste la función del «agente de cambio», cómo identificar y designar a la persona adecuada, cómo apoyar su formación y cómo garantizar que la inclusión de género se integre en el proceso desde el principio. Una lista de verificación al final ayuda a las pymes a comprobar que se dan las condiciones adecuadas en cada etapa.

1. POR QUÉ LA CIBERSEGURIDAD ES IMPORTANTE PARA TODAS LAS PYMES

Según el informe «ENISA Threat Landscape 2025», los ciberdelincuentes están industrializando sus ataques, lo que convierte a las pymes en objetivos de gran valor, independientemente de su tamaño y sector. Las amenazas más comunes a las que se enfrentan hoy en día las organizaciones son el ransomware, el phishing y las filtraciones de datos. El ransomware y las filtraciones de datos representan por sí solos la mayor parte de los incidentes de ciberdelincuencia dirigidos a organizaciones de la UE, y el ransomware supone más del 80 % de los delitos. La industrialización de estos ataques, en particular el modelo «Ransomware como servicio», ha reducido las barreras para los atacantes, convirtiendo incluso a las organizaciones más pequeñas en objetivos viables.

Especialmente para las pymes, las consecuencias de un ciberataque no se limitan a interrupciones temporales. Según la ENISA, los ataques a la ciberseguridad tienen graves repercusiones negativas en la actividad empresarial del 90 % de las pymes una semana después de producirse. Sin embargo, a pesar de esta exposición, las pymes rara vez cuentan con personal dedicado a las tecnologías de la información o a la seguridad, y sus empleados rara vez reciben formación estructurada en materia de ciberseguridad. Las pymes europeas dan empleo a unos 100 millones de personas y representan más de la mitad del PIB europeo. Por lo tanto, la brecha de ciberseguridad en el sector de las pymes supone un riesgo económico y social.

La mayoría de los ciberataques tienen éxito debido a factores humanos, como hacer clic en un enlace de phishing, contraseñas débiles o correos electrónicos no verificados. Esto significa que la primera línea de defensa no es una herramienta técnica, sino un empleado informado y concienciado que sabe en qué debe fijarse y qué hacer cuando algo va mal. Este papel es precisamente el que desempeña el agente de cambio en ciberseguridad.

2. EL AGENTE DE CAMBIO EN CIBERSEGURIDAD

El concepto de «agente de cambio en ciberseguridad» constituye el núcleo del proyecto CyberAgent. En esta sección se explica en qué consiste esta función, por qué se ha desarrollado y cómo se aplica en la práctica en las pequeñas y medianas empresas (pymes).

2.1. ¿QUÉ ES Y POR QUÉ ES NECESARIO?

Las pymes son la columna vertebral de la economía europea, pero siguen siendo unas de las organizaciones más expuestas a las amenazas de ciberseguridad. A diferencia de las grandes empresas, la mayoría de las pymes no cuentan con departamentos específicos de TI o de seguridad, y sus empleados rara vez reciben formación estructurada en materia de ciberseguridad. Esto da lugar a una brecha persistente entre los riesgos cibernéticos a los que se enfrentan las pymes y la capacidad que tienen para hacerles frente.

El proyecto CyberAgent y la figura del «agente de cambio en ciberseguridad» se diseñaron para subsanar esta carencia mediante el desarrollo de un tipo diferente de capacidad dentro de los equipos existentes. El agente de cambio en ciberseguridad es un empleado sin perfil técnico que ha recibido formación y que actúa como referencia interna en materia de concienciación sobre ciberseguridad, fomentando comportamientos más seguros, identificando riesgos comunes e implementando mejores prácticas de ciberseguridad dentro de la organización. Esta figura también servirá de guía para que los compañeros puedan obtener el apoyo adecuado en caso de incidentes.

La necesidad de esta función queda confirmada por los datos recopilados a lo largo de la fase piloto de CyberAgent. En los ocho países socios, la formación llegó a 594 participantes inscritos, entre los que se encontraban empleados de pymes, estudiantes de instituciones de educación superior y alumnos de formación profesional. Los empleados de pymes suelen considerarse el grupo destinatario más difícil de alcanzar y retener en entornos educativos, principalmente debido a las limitaciones de tiempo y a las responsabilidades laborales. No obstante, la elevada tasa de finalización entre los empleados de pymes refleja la auténtica relevancia de la sensibilización sobre ciberseguridad en su trabajo diario.

2.2. RESPONSABILIDADES PRINCIPALES

El agente de cambio en ciberseguridad no es responsable de resolver por sí solo los problemas de ciberseguridad. Su función se centra en la sensibilización, la comunicación y la coordinación, siendo la persona de la organización que mantiene la ciberseguridad en la agenda y ayuda a sus compañeros a abordarla en su trabajo diario. Nada de esto requiere conocimientos técnicos especializados. Lo que se necesita es alguien de confianza, bien integrado en la organización y motivado para hacer de la ciberseguridad una parte habitual del funcionamiento del equipo.

En concreto, el papel se traduce en un conjunto de actividades recurrentes y sencillas que no exigen mucho tiempo, pero que tienen un impacto significativo en la cultura de seguridad de la organización:

- **Sensibilizar de forma periódica**. El agente de cambio comparte regularmente mensajes de sensibilización con sus compañeros sobre las amenazas más comunes, como los correos electrónicos de phishing, las contraseñas débiles, el manejo inseguro de datos o los enlaces sospechosos, manteniendo la ciberseguridad en primer plano sin convertirla en una carga. Esto puede ser tan sencillo como un mensaje mensual compartido en el chat del equipo, un breve recordatorio antes de un periodo de mucho trabajo o una nota sobre un nuevo tipo de estafa que circula en el sector. El formato importa menos que la constancia.

- **Mantener la ciberseguridad en la agenda de las reuniones**. El agente de cambio plantea temas de ciberseguridad durante las reuniones de equipo mediante debates breves y prácticos. Esto no implica presentaciones interminables ni sesiones de formación formales. Una conversación de cinco minutos sobre un intento reciente de phishing o un recordatorio sobre la actualización de contraseñas basta para mantener viva la concienciación y señalar que la ciberseguridad es una responsabilidad compartida de la organización, no algo delegado al personal técnico.

- **Fomentar la notificación de incidentes**. Una de las contribuciones más importantes del agente de cambio en ciberseguridad es crear una cultura en la que los empleados se sientan cómodos a la hora de informar de situaciones sospechosas, como un correo electrónico inusual, un sistema que se comporta de forma inesperada o un compañero que hace clic en algo que no debería. Muchos incidentes de ciberseguridad se agravan porque los empleados no informan de las primeras señales de alerta por miedo a la vergüenza o a que se les culpe. El agente de cambio ayuda a normalizar la notificación mostrándose accesible y explicando claramente el proceso.

- **Apoyar la incorporación**. Los nuevos empleados se encuentran entre los miembros más vulnerables de cualquier organización desde el punto de vista de la ciberseguridad, ya que no están familiarizados con los procedimientos internos, son más propensos a confiar en solicitudes inesperadas y, a menudo, aún no han recibido formación sobre prácticas básicas de seguridad. El agente de cambio desempeña un papel importante a la hora de introducir los conceptos básicos de ciberseguridad durante la incorporación, garantizando que se establezcan buenos hábitos desde el primer día, en lugar de tener que adaptarlos posteriormente.

- **Actuar como punto de contacto interno**. El agente de cambio en ciberseguridad es la persona a la que recurren los compañeros cuando tienen una duda sobre ciberseguridad o no están seguros de qué hacer ante una situación concreta. Esto significa que saben dónde encontrarlo, a quién remitir el asunto y cómo orientar a un compañero hacia el apoyo adecuado. En las pymes que carecen de personal de TI dedicado, esta función cubre un vacío que, de otro modo, dejaría a los empleados sin un punto de referencia claro.

- **Promover la formación y el aprendizaje continuo**. El agente de cambio anima a los compañeros a utilizar los recursos de formación disponibles, incluidos los módulos de CyberAgent, y se mantiene informado sobre las novedades en el ámbito de la ciberseguridad relevantes para el sector y las actividades de la organización.

- **Recopilar y transmitir los comentarios**. El agente de cambio recopila comentarios sobre las preocupaciones en materia de ciberseguridad dentro de la organización: qué aspectos resultan confusos para los empleados, qué prácticas no se están siguiendo y qué riesgos se perciben como más acuciantes, y transmite esta información a la dirección. Este ciclo de retroalimentación es lo que permite a la organización mejorar su cultura de seguridad con el tiempo.

Tabla 1. Distinción entre las tareas de los empleados técnicos y las del agente de cambio

ESPECIALISTA EN TI	AGENTE DE CAMBIO EN CIBERSEGURIDAD
Configura cortafuegos y sistemas de seguridad	Comparte mensajes de concienciación con sus compañeros
Gestiona las actualizaciones y los parches de software	Incluye la ciberseguridad en el orden del día de las reuniones
Responde a los incidentes cibernéticos activos	Anima a los compañeros a informar de los incidentes
Supervisa la seguridad de la red	Presta apoyo a los nuevos empleados durante su incorporación
Garantiza el cumplimiento de los requisitos técnicos	Recopila comentarios y los remite a la dirección

3. SELECCIÓN Y NOMBRAMIENTO DE UN AGENTE DE CAMBIO EN MATERIA DE CIBERSEGURIDAD

Identificar a la persona adecuada para el puesto de «agente de cambio en ciberseguridad» y proporcionarle las condiciones necesarias para que tenga éxito son decisiones cruciales a la hora de implantar este puesto dentro de una organización. El proyecto piloto «CyberAgent» demostró que el puesto funciona mejor cuando lo ocupa una persona que se percibe de confianza, que conoce bien los procedimientos de la empresa y que cuenta con el apoyo de la dirección. En esta sección se ofrecen orientaciones prácticas sobre cómo definir claramente el puesto para garantizar el éxito a largo plazo y cómo encontrar al candidato adecuado.

3.1. CÓMO IDENTIFICAR AL CANDIDATO ADECUADO

Según los resultados del proyecto piloto de CyberAgent, los agentes de cambio en ciberseguridad más eficaces no son necesariamente aquellos con formación técnica previa. En los ocho países participantes en el proyecto piloto, las pymes que se implicaron más activamente en la formación y mostraron mayor potencial fueron aquellas que combinaban el conocimiento de la organización con habilidades de comunicación y una motivación genuina por marcar la diferencia en su lugar de trabajo. Según la experiencia del proyecto piloto, las siguientes características suelen favorecer el éxito en este puesto:

- Familiaridad con los procesos internos de la organización y las prácticas de tratamiento de datos.
- Buenas habilidades comunicativas e interpersonales.
- Apoyo por parte de la dirección.

Es importante destacar que el puesto no requiere formación técnica ni en TI. Por lo tanto, los empleados que ocupan puestos administrativos, de RR. HH., de operaciones y de dirección pueden desempeñar eficazmente la función de agente de cambio, siempre que reciban la formación y el apoyo adecuados. La eliminación del requisito técnico previo es una elección de diseño deliberada que amplía significativamente el grupo de candidatos aptos y abre la puerta a la diversidad de género, tal y como demostró el proyecto piloto.

Una vez identificado el candidato, es necesario dar visibilidad y legitimidad a la función dentro de la organización. El alcance de la función debe darse a conocer en toda la organización y definirse con claridad: de qué es responsable el agente de cambio en ciberseguridad, a quién rinde cuentas y qué no se espera que haga.

3.2. PUESTA EN MARCHA DEL PUESTO

El siguiente paso es implementar el puesto dentro de una organización. Los pasos que se indican a continuación se basan directamente en las lecciones aprendidas del proyecto piloto «CyberAgent» en los países socios y están diseñados para adaptarse a pymes de cualquier tamaño.

3.2.1. SELECCIONAR Y FORMAR AL AGENTE DE CAMBIO EN CIBERSEGURIDAD

Identifica a la persona más adecuada de tu organización y ofrécele acceso al programa de formación de CyberAgent. El programa consta de nueve módulos que abarcan la gestión de programas de seguridad (M1), la administración de sistemas (M2), las herramientas analíticas (M3), las operaciones de seguridad (M4), la gobernanza y las políticas de seguridad (M5), la planificación de la ciberseguridad (M6), la gestión de riesgos (M7), la continuidad del negocio (M8) y el fomento de las carreras profesionales en ciberseguridad (M9). Estos nueve módulos se recogen formalmente en dos entregables oficiales del proyecto: el D3.1, que abarca el plan de estudios de la educación superior, y el D3.2, que abarca el plan de estudios de la formación profesional. Por lo tanto, los módulos a los que se hace referencia a lo largo de esta guía se corresponden directamente con el contenido descrito en D3.1 y D3.2, y se puede acceder a ellos a través de la plataforma CyberAgent, independientemente de la afiliación institucional del alumno. Además, el plan de estudios se ajusta a los niveles 4-6 del Marco Europeo de Cualificaciones (EQF) para empleados de pymes, proporcionando habilidades y conocimientos básicos en ciberseguridad con aplicación práctica en las áreas de competencia técnica, analítica, de gestión de riesgos y organizativa.

La formación se realiza al ritmo del alumno y está disponible en línea, lo que significa que el empleado seleccionado puede completarla de manera flexible, compaginándola con sus responsabilidades laborales actuales. Al completar un módulo y superar la prueba de evaluación de conocimientos con una puntuación mínima del 75 %, el «agente del cambio» recibe un certificado de finalización del curso para ese módulo, que constituye un registro formal de las competencias adquiridas y puede utilizarse para documentar la formación del «agente del cambio» dentro de la organización.

3.2.2. DEFINIR LAS RESPONSABILIDADES E INTEGRARLAS EN LAS ESTRUCTURAS EXISTENTES

Una vez que la formación esté en marcha o se haya completado, la organización debe definir formalmente las responsabilidades del agente de cambio en ciberseguridad e integrar la función en las estructuras existentes. Esto implica acordar qué hará el agente de cambio, cuánto tiempo dedicará a la función y con quién se coordinará, y comunicar todo ello a todo el equipo.

La fase piloto demostró que la función del agente de cambio en ciberseguridad resulta más sostenible cuando se vincula a algo que ya existe en la organización, en lugar de funcionar de forma aislada. Esto podría implicar incluirla como punto del orden del día en las reuniones periódicas del equipo o vincularla a una estructura existente de salud y seguridad o de cumplimiento normativo. El objetivo es que la concienciación sobre la ciberseguridad se convierta en una parte habitual del trabajo diario y en una responsabilidad organizativa compartida, y no en una actividad aislada.

3.2.3. FOMENTAR LA CONCIENCIACIÓN INTERNA EN TORNO A ESTA FUNCIÓN

El agente del cambio no puede actuar con eficacia si sus compañeros no saben quién es ni a qué se dedica. Para dotar al empleado seleccionado de la legitimidad organizativa que necesita para desempeñar su función, es necesario enviar una comunicación interna clara en la que se describan su papel y sus responsabilidades, así como organizar reuniones periódicas que permitan a los empleados plantear preguntas.

Más allá del anuncio inicial, se debe animar al agente del cambio a mantener la ciberseguridad en el punto de mira dentro de la organización mediante reuniones periódicas. Esto no implica largas sesiones de formación ni presentaciones formales. En el contexto de las pymes, esto podría hacerse mediante breves actividades directamente relacionadas con situaciones que los empleados reconozcan de su trabajo diario.

3.2.4. REVISAR PERIÓDICAMENTE Y MANTENER A LO LARGO DEL TIEMPO

Para que la función del agente de cambio en ciberseguridad genere un impacto duradero, la organización debe crear las condiciones necesarias para que continúe y evolucione. Esto implica incorporar un proceso de revisión al menos una vez al año, con el fin de evaluar qué está funcionando, qué carencias persisten y si el agente de cambio necesita formación o apoyo adicionales.

Los resultados de la fase piloto muestran que un compromiso sostenido requiere algo más que la formación inicial. Los participantes de las pymes necesitan sistemáticamente plazos flexibles, recordatorios y apoyo ocasional para mantener el impulso. Incorporar una sencilla revisión anual y garantizar que el agente de cambio tenga acceso continuo a los recursos son las condiciones mínimas para mantener la eficacia de esta función a lo largo del tiempo.

4. EQUILIBRIO DE GÉNERO E INCLUSIVIDAD

La ciberseguridad sigue siendo uno de los ámbitos más dominados por los hombres en la economía europea. Las mujeres representan aproximadamente el 20 % de la plantilla dedicada a la ciberseguridad en toda la UE, y la participación en la formación en ciberseguridad refleja el mismo desequilibrio. Debido a la brecha existente en materia de competencias y talento, un ámbito que solo recurre a una fracción del talento disponible tendrá dificultades para satisfacer la magnitud de la demanda que exige el panorama actual de amenazas.

El proyecto CyberAgent se diseñó con la inclusión de género como objetivo explícito, no como una idea de última hora. En un ámbito en el que las mujeres suelen constituir una pequeña minoría entre los participantes en la formación, el elevado número de mujeres que participaron en la fase piloto es un resultado significativo y fue fruto de estrategias de divulgación específicas y de un enfoque inclusivo.

4.1. POR QUÉ ES IMPORTANTE PARA LAS PYMES

Para las pymes en concreto, la dimensión de género de la ciberseguridad es tanto una cuestión de personal como de cultura organizativa. La mayoría de las pymes no cuentan con personal dedicado exclusivamente a la ciberseguridad. Su ciberresiliencia depende de la concienciación y el comportamiento de todos los empleados, especialmente de aquellos que desempeñan funciones administrativas, de recursos humanos, financieras y operativas. Por lo tanto, excluir a las mujeres de la formación en concienciación sobre ciberseguridad supone una brecha de seguridad.

Al mismo tiempo, la función de «agente de cambio en ciberseguridad» ofrece una oportunidad concreta para abordar el desequilibrio de género en la ciberseguridad desde el interior de las pymes. Dado que esta función se define por las habilidades de comunicación, la sensibilización organizativa y la mentalidad de gobernanza, más que por los conocimientos técnicos, se adapta bien a una amplia gama de perfiles profesionales y ofrece a las mujeres que ocupan puestos no técnicos una vía reconocida hacia responsabilidades en ciberseguridad que no requiere un cambio de carrera ni una cualificación técnica.

4.2. MEDIDAS PRÁCTICAS PARA LLEGAR A LAS MUJERES Y A LOS GRUPOS INFRARREPRESENTADOS

Las siguientes medidas prácticas se han extraído de la experiencia del proyecto piloto «CyberAgent» y están diseñadas para que puedan ser aplicadas por pymes de cualquier tamaño.

El proyecto piloto belga demostró que canalizar la divulgación a través de redes en las que las mujeres ya confían, como las asociaciones profesionales y las redes de mujeres empresarias, aumenta la participación femenina. En la práctica, esto significa que, cuando una pyme busca candidatas para el puesto de «agente de cambio en ciberseguridad», debe involucrar activamente a cualquier red profesional de mujeres relevante para su sector o región, en lugar de basarse únicamente en anuncios públicos.

Enmarcar el puesto en términos de impacto organizativo, no de conocimientos técnicos. Las mujeres que ocupan puestos no técnicos son más propensas a participar en la formación en ciberseguridad y a asumir la función de «agente de cambio» cuando el puesto se presenta en términos del valor organizativo que aporta, en lugar de en términos de competencias técnicas. El puesto puede enmarcarse como uno que protege la empresa, apoya a los compañeros y contribuye a la gobernanza. El lenguaje utilizado en las comunicaciones internas, las descripciones de los puestos y los materiales de selección de personal es importante.

5. BUENAS PRÁCTICAS

Nombrar a un agente de cambio en materia de ciberseguridad es un primer paso importante, pero esta función solo puede generar un impacto duradero si se desarrolla dentro de una cultura organizativa que la respalde activamente. Las siguientes prácticas recomendadas están diseñadas para ayudar a las pymes a crear las condiciones adecuadas para que el agente de cambio tenga éxito y para que la concienciación sobre la ciberseguridad se convierta en una parte habitual del funcionamiento de la organización.

- **Fomenta la comunicación abierta**. Los empleados deben sentirse cómodos a la hora de informar de errores, situaciones sospechosas o problemas de seguridad sin temor a ser culpados o a pasar vergüenza. En muchas organizaciones, los incidentes de ciberseguridad se agravan precisamente porque los empleados dudan a la hora de informar de algo de lo que no están seguros o por lo que se sienten responsables.

- **Que sea sencillo y se integre en las rutinas diarias**. La concienciación sobre la ciberseguridad no tiene por qué adoptar la forma de sesiones de formación formales o talleres prolongados. Los recordatorios breves y prácticos integrados en las rutinas existentes suelen ser más eficaces que una formación intensiva ocasional. El objetivo es convertir la ciberseguridad en un hábito de fondo, en lugar de un evento periódico.

- **Documenta cada paso del proceso**. Una de las medidas más prácticas que puede adoptar una pyme es plasmar por escrito sus prácticas básicas de ciberseguridad: cómo se gestionan las contraseñas, cómo se almacenan y comparten los datos sensibles, qué hacer cuando llega un correo electrónico sospechoso, a quién contactar en caso de incidente. No es necesario que sean documentos normativos formales. Basta con una referencia de una página accesible para todos los empleados.

- **Empiece por arriba**. Los comportamientos que se esperan de los empleados deben ser modelados de forma visible por los directivos y el equipo de liderazgo. Si la dirección no sigue las prácticas básicas de seguridad, transmite la idea de que estas prácticas son opcionales. La credibilidad del agente del cambio dentro de la organización depende, en parte, de si la cultura que le rodea respalda lo que está tratando de promover.

- **Haz que la sensibilización sea continua**. Las amenazas a la ciberseguridad evolucionan constantemente, y una única sesión de formación queda obsoleta rápidamente. La sensibilización debe tratarse como un proceso continuo, en lugar de como una actividad puntual. Esto implica puntos de contacto regulares, cursos de actualización periódicos y un agente de cambio en ciberseguridad que se mantenga informado y siga aportando información relevante a la organización.

-

5.1. APORTACIONES CUALITATIVAS DE LOS PROYECTOS PILOTO NACIONALES

Los comentarios cualitativos muestran que, en general, los participantes valoraron positivamente la formación, y muchos afirmaron que no se necesitaban mejoras importantes. Los temas más recurrentes en las respuestas de texto libre (D5.3 — Evaluación del programa de formación para la mejora de las competencias de los agentes de ciberseguridad) fueron: la usabilidad de la plataforma, la navegación o el flujo de evaluación; problemas técnicos de acceso o fiabilidad; valoración positiva en torno a la accesibilidad, la flexibilidad y la amplitud de conocimientos; peticiones de más casos prácticos, talleres prácticos o ejemplos reales de pymes; densidad del contenido, estructura o diferenciación de las rutas de aprendizaje. Cabe destacar que el tercer tema más mencionado (valor positivo en torno a la accesibilidad, la flexibilidad y la amplitud de conocimientos) refleja el reconocimiento de los participantes que afirmaron que no se necesitaban mejoras y destacaron los puntos fuertes del programa por iniciativa propia. Se trata de una señal significativa: en un campo de texto libre diseñado para recabar críticas, casi una cuarta parte de las respuestas cualitativas expresaron satisfacción con la accesibilidad y la amplitud de la formación.

5.2. MEDIDAS PARA LA IMPLEMENTACIÓN Y GESTIÓN DE LA FORMACIÓN EN LAS PYMES

La puesta a prueba a gran escala de la plataforma CyberAgent en ocho países europeos proporcionó información clave sobre cómo las pequeñas y medianas empresas asimilan y mantienen la mejora de las competencias en ciberseguridad. Basándose en los datos obtenidos mediante métodos mixtos y en las barreras a las que se enfrentan los alumnos documentadas en el informe final de evaluación de la formación (D5.3), se recomienda a los directivos de las empresas que adopten las siguientes medidas internas de gestión, técnicas y estratégicas para optimizar el impacto organizativo de la formación.

Consejos para la gestión de la calidad

Los materiales didácticos de CyberAgent presentan un volumen considerable de conocimientos operativos y estratégicos. Los responsables deben evitar asignar todo el plan de estudios de una sola vez; en su lugar, establecer un calendario modular evita la fatiga cognitiva y garantiza una transición más fluida de las capacidades a las rutinas diarias de la empresa.

Recomendaciones sobre integración técnica

Los datos iniciales de la fase piloto revelaron que las dificultades técnicas de incorporación, como los retrasos o el filtrado de los correos electrónicos de confirmación de registro en la plataforma, pueden obstaculizar la adopción temprana. Antes de poner en marcha la inscripción de usuarios, la dirección debería coordinarse con los responsables de los filtros de red para garantizar que las rutas de los dominios externos de aprendizaje electrónico estén totalmente permitidas y aconsejar al personal que revise las carpetas de correo no deseado.

Recomendaciones sobre la implementación estratégica

Los datos de la fase piloto nacional revelaron que los módulos estratégicos de nivel superior —concretamente el M6 (Planificación de la ciberseguridad) y el M8 (Continuidad del negocio)— requieren una sólida experiencia previa para poder aprovecharlos al máximo. Para maximizar el valor empresarial inmediato, estos módulos deberían dirigirse específicamente al personal con responsabilidades de gestión, operativas o de gobernanza empresarial.

5.2.1. LA OPINIÓN DE LOS AGENTES DEL CAMBIO

La fase piloto, que recopiló 272 respuestas exhaustivas a la encuesta en ocho países europeos, reveló tres repercusiones transversales en los grupos destinatarios.

Gran flexibilidad en la impartición y conciliación entre trabajo y estudios

Un significativo 86,0 % de los encuestados se mostró de acuerdo o muy de acuerdo en que el formato asíncrono y a ritmo propio era lo suficientemente flexible como para integrarse a la perfección en sus horarios profesionales y académicos, lo que permitía a los empleados de las pymes compaginar el desarrollo de competencias con sus tareas operativas diarias.

Relevancia metodológica para el personal no técnico

Los resultados de la fase piloto validan el diseño educativo básico del plan de estudios de CyberAgent, demostrando que una ciberresiliencia organizativa eficaz no requiere conocimientos técnicos avanzados ni habilidades de programación informática. Según los datos de la evaluación de impacto del documento D5.3, el 77,2 % de los participantes señaló que la formación les permitió comprender claramente cómo sus funciones profesionales específicas influyen en las prácticas de seguridad diarias de una empresa y contribuyen a protegerlas.

Progresión medible de los conocimientos partiendo de niveles iniciales de no expertos

Los análisis de la plataforma muestran que el 89,3 % de todos los participantes logró un aumento verificado de sus conocimientos en ciberseguridad. Es fundamental destacar que esta progresión fue más evidente entre los principiantes absolutos: el 90,9 % de los alumnos que evaluaron su comprensión inicial como «muy baja» antes del programa señalaron una mejora decisiva en sus conocimientos y en su confianza a la hora de reconocer los riesgos cibernéticos corporativos.

5.2.2. «QUÉ HACER Y QUÉ NO HACER»

Basándonos en los comentarios de los países piloto sobre la «diferenciación de las rutas de aprendizaje», presentamos las siguientes recomendaciones para las empresas:

Tabla 2 «Qué hacer y qué no hacer»

NO HACER (Errores comunes de las pymes)	RECOMENDADO (buenas prácticas)
Esperar que un empleado asista a los ocho módulos en un plazo poco realista y ajustado (por ejemplo, una semana o un mes). Los estudios piloto (D5.3) revelaron que la falta de tiempo debido a las responsabilidades laborales diarias era el principal obstáculo para los empleados de las pymes, lo que se traducía en una menor tasa de aprobados en las pruebas.	Crear un plan de aprendizaje flexible e individualizado basado en las necesidades y la disponibilidad del empleado, aplicando los principios del microaprendizaje. Permitir a los alumnos centrarse en los módulos que mejoran directamente su área específica de impacto en el lugar de trabajo.
Esperar que el «agente de cambio en ciberseguridad» formado sustituya a ingenieros informáticos especializados o resuelva de forma independiente incidentes cibernéticos complejos. Trasladar las expectativas relativas a la infraestructura técnica básica al personal no técnico genera una gran ambigüedad en las funciones.	Animar al agente de cambio a actuar como coordinador de seguridad interno y catalizador de la concienciación. Son más eficaces cuando impulsan la cultura de seguridad, recuerdan la formación interna y ofrecen breves actualizaciones durante las reuniones de equipo.
Dejar el proceso de aprendizaje electrónico sin ningún tipo de supervisión, para que se desarrolle de forma automática sin visibilidad por parte de la empresa. Un simple enlace de inscripción no garantiza un valor organizativo a largo plazo.	Utilizar un marco de seguimiento estructurado (como el de la Tabla 3) para realizar un seguimiento de los hitos y asignar mentores internos. Las indicaciones de la evaluación piloto (D5.3) confirman que contar con un responsable o mentor designado se correlaciona explícitamente con la finalización verificada de las pruebas.
Permitir que el estudio independiente se desarrolle de forma totalmente aislada, con el riesgo de que pasen desapercibidos los bloqueos de aprendizaje individuales o las dificultades técnicas ocultas. Sin interacción, los principiantes absolutos suelen estancarse y abandonar el programa en silencio cuando se atascan.	Integrar el estudio a ritmo propio con puntos de contacto operativos proactivos, como breves comprobaciones de progreso o recordatorios digitales. La alineación activa con la dirección elimina directamente las barreras de aprendizaje, lo que aumenta la motivación de los empleados y las tasas de finalización de los cursos.

6. HOJA DE RUTA PARA IMPLEMENTAR LA FIGURA DEL AGENTE DE CAMBIO EN CIBERSEGURIDAD

La implementación exitosa del papel de «agente de cambio en ciberseguridad» comienza mucho antes del propio nombramiento. Dedicar tiempo a evaluar la situación actual de la organización, generar apoyo interno y definir claramente el papel desde el principio aumenta significativamente las posibilidades de éxito a largo plazo. Los siguientes pasos están diseñados para guiar de forma práctica a las pymes a lo largo de esta fase de preparación.

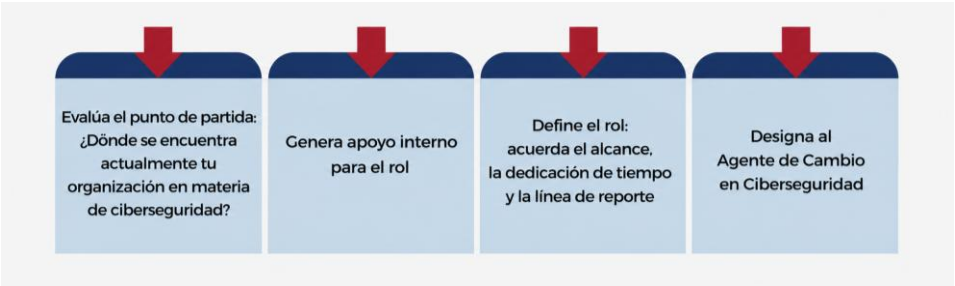
1. El primer paso consiste en evaluar la situación actual de la organización. Esto implica analizar con honestidad las prácticas de ciberseguridad ya implantadas o las que faltan. ¿Son conscientes los empleados de amenazas básicas como el phishing? ¿Existe un procedimiento para notificar incidentes sospechosos? ¿Se gestionan los datos sensibles de forma coherente en todo el equipo?

2. El segundo paso consiste en generar apoyo interno para el puesto. El agente de cambio no puede actuar con eficacia sin el respaldo de la dirección. Antes de seleccionar a un candidato, la decisión de introducir el puesto debe debatirse y acordarse a nivel directivo, con un compromiso claro de asignar tiempo, reconocer formalmente el puesto y apoyar activamente a la persona que lo asuma.

3. El tercer paso consiste en definir el puesto antes de cubrirlo. Esto implica acordar el alcance de las responsabilidades, el tiempo que se espera que dedique y cómo se integrará el puesto en la estructura organizativa existente. Un mandato claro, aunque sea una simple descripción de un párrafo, evita ambigüedades y otorga al futuro agente de cambio en ciberseguridad la legitimidad que necesita para actuar.

Solo una vez que se hayan dado estos tres pasos, la organización estará preparada para identificar y nombrar al candidato adecuado. En la siguiente sección se describe la lista de comprobación que servirá de guía para la implementación satisfactoria de la función.

Figura1 - Hoja de ruta visual para implementar el puesto de agente de cambio en ciberseguridad



7. LISTA DE COMPROBACIÓN

La siguiente lista de comprobación está pensada para verificar si se dan las condiciones clave para una implementación satisfactoria del agente de cambio en ciberseguridad. Se basa en las lecciones aprendidas del proyecto piloto CyberAgent.

7.1. DIRECCIÓN

[ ] Se ha acordado formalmente la función de agente de cambio y se ha presupuestado

[ ] Se ha definido un mandato claro: alcance, dedicación de tiempo y línea jerárquica

[ ] Se ha comunicado el nombramiento a toda la organización

[ ] Se ha programado una revisión de la función en los próximos 12 meses

[ ] El agente de cambio ha reservado tiempo en su agenda para desempeñar su función

7.2. RECURSOS HUMANOS

[ ] El proceso de selección estuvo abierto a todas las personas, independientemente de su género o procedencia

[ ] El puesto se describió en términos de impacto en la organización, no de conocimientos técnicos

[ ] Las responsabilidades del agente de cambio se han reflejado en su descripción de funciones u objetivos

[ ] A los nuevos empleados se les presenta al agente de cambio en ciberseguridad durante el proceso de incorporación

[ ] Se mantiene un registro de la formación y las certificaciones del agente de cambio

7.3. AGENTE DE CAMBIO EN CIBERSEGURIDAD

[ ] Registrado en la plataforma CyberAgent y ha acordado un itinerario de aprendizaje

[ ] Ha completado al menos un módulo y ha obtenido un certificado

[ ] Los compañeros saben cómo ponerse en contacto con el agente de cambio

[ ] Las prácticas básicas de ciberseguridad están documentadas y son accesibles para todo el personal

[ ] Se han establecido puntos de contacto periódicos para la sensibilización (reuniones, mensajes o recordatorios)

[ ] Existe un proceso claro para que los compañeros informen de situaciones sospechosas

[ ] Se recogen comentarios sobre cuestiones de ciberseguridad y se transmiten a la dirección de forma regular

8. CÓMO MEDIR EL ÉXITO DE LA IMPLEMENTACIÓN

La implementación de la figura del «agente de cambio en ciberseguridad» es un compromiso continuo. Los siguientes indicadores pueden ayudar a las pymes a evaluar si esta figura está teniendo un impacto real a lo largo del tiempo.

[ ] El número de empleados que participan en actividades de sensibilización sobre ciberseguridad ha aumentado desde que se nombró al agente de cambio

[ ] La ciberseguridad se aborda con regularidad en las reuniones de equipo y ya no se trata como un tema excepcional

[ ] Los empleados saben quién es el agente de cambio y se sienten cómodos acudiendo a él con preguntas o inquietudes

[ ] Ha aumentado el número de correos electrónicos sospechosos, incidentes o inquietudes notificados

[ ] El agente de cambio ha completado módulos de formación adicionales desde su nombramiento inicial

[ ] Se recogen periódicamente las opiniones del personal sobre la ciberseguridad dentro de la organización y se toman medidas al respecto

8.1. ORIENTACIONES DE GESTIÓN PARA LA ADAPTACIÓN Y PERSONALIZACIÓN DE LA PLANTILLA

Para garantizar que la mejora de las competencias de su «agente de cambio en ciberseguridad» se traduzca en una resiliencia corporativa a largo plazo, es esencial llevar a cabo un seguimiento estructural continuo. La tabla 3 ofrece una plantilla práctica de seguimiento diseñada para que los directivos de las pymes evalúen los niveles de referencia de la organización antes de la formación y midan el progreso concreto de la cultura de seguridad a los 6 y 12 meses tras el nombramiento.

Los directivos deben considerar esta plantilla como un marco dinámico. En función del tamaño de su empresa, el sector operativo y la infraestructura existente, se recomienda adaptar y ampliar esta matriz:

- **Personalización de las escalas**
  Las micro-pymes (menos de 10 empleados) pueden simplificar los indicadores basados en porcentajes y sustituirlos por recuentos directos de empleados para facilitar el seguimiento.
- **Ampliación de los indicadores**
  Se recomienda a las empresas que operan en entornos altamente digitalizados o de alto riesgo que añadan filas específicas para cada objetivo, como «% del personal que utiliza la autenticación multifactorial (MFA)» o «Tiempo medio de respuesta ante una amenaza simulada».

- **Adaptación local**

  Adapta la columna «Fuente de datos recomendada» a tus canales de comunicación internos específicos (por ejemplo, seguimiento a través de Slack, encuestas de MS Teams o registros físicos durante las reuniones informativas del equipo).

Tabla 3. Ejemplo de plantilla de seguimiento. Las pymes pueden adaptar esta tabla para supervisar los avances a los 6 y 12 meses tras el nombramiento de su agente de cambio.

Indicador de éxito	Unidad/Escala de medición	Antes del nombramiento	A los 6 meses	Tras 12 meses	Fuente de datos recomendada
Empleados que saben qué hacer cuando reciben un correo electrónico sospechoso	% del personal que se siente seguro a la hora de gestionar correos electrónicos sospechosos	%	%	%	Encuesta interna o datos de la plataforma CyberAgent
Se aborda el tema de la ciberseguridad en las reuniones de equipo	Número de reuniones de equipo en las que se ha abordado la ciberseguridad	N.º	N.º	N.º	Actas o órdenes del día de las reuniones de equipo
N. de incidentes sospechosos notificados al mes	Número de incidentes sospechosos documentados y notificados	N.º / mes	N.º / mes	N.º / mes	Registro interno de incidentes de seguridad o ciclo de retroalimentación de TI
% del personal que sabe quién es el agente de cambio	% del personal que sabe con certeza quién es el «Change Agent»	%	%	%	Breve cuestionario interno

CONCLUSIÓN

La ciberseguridad ya no es una preocupación exclusiva de las grandes organizaciones con departamentos de TI especializados. A medida que el panorama de amenazas sigue evolucionando y aumentan las exigencias normativas para las pymes, la pregunta es cómo pueden defenderse con los recursos de los que realmente disponen.

La figura del «agente de cambio en ciberseguridad» ofrece una respuesta práctica y proporcionada a esa pregunta. No requiere contratar a un especialista, invertir en herramientas costosas ni reformar los procesos existentes. Lo que sí requiere es identificar a la persona adecuada dentro de la organización, proporcionarle la formación y el mandato para actuar, y crear las condiciones para que la concienciación sobre la ciberseguridad forme parte de la vida laboral cotidiana.

El proyecto CyberAgent ha demostrado que esto es factible. En ocho países europeos, empleados de pymes sin formación técnica completaron la formación, asumieron el papel y comenzaron a marcar la diferencia en la forma en que sus organizaciones abordaban la ciberseguridad. Las pruebas son claras: cuando se reduce la barrera de entrada, cuando el papel se enmarca en la cultura organizativa en lugar de en los conocimientos técnicos, y cuando la inclusión se trata como un principio de diseño en lugar de como una idea de último momento, los resultados no se hacen esperar.

Esta guía es una invitación a dar ese primer paso. La hoja de ruta está ahí. Las herramientas están disponibles. El puesto está al alcance de cualquier pyme dispuesta a invertir en su personal.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau