ESTRATEGIAS DE PREVENCIÓN DE LA CIBERDELINCUENCIA PARA EMPRENDEDORES, EMPRESAS Y AUTÓNOMOS

Working Paper 25/2025

José Pablo Pérez

Telefónica Tech

Resumen: En este artículo se recoge una exposición integral sobre la evolución de la ciberdelincuencia y el incremento sostenido de los ciberataques, impulsados por la profesionalización del delito digital, la irrupción de la inteligencia artificial y la explotación de vectores como ransomware, infostealers y ataques a la cadena de suministro. Se analizan tendencias recientes, su impacto económico en organizaciones y la insuficiencia de enfoques tradicionales de seguridad basados únicamente en antivirus.

Se sistematizan riesgos críticos para empresas y usuarios —compromiso de credenciales, phishing (smishing y vishing), suplantación de marca y dominio, redes wifi públicas, QR maliciosos y abuso de permisos en aplicaciones— y se proponen medidas de mitigación: enfoque de "confianza cero", autenticación multifactor, gestión robusta de contraseñas, copias de seguridad, monitorización de presencia digital y uso de recursos institucionales como INCIBE, junto con verificación de enlaces y formación continua.

Palabras clave: Ciberseguridad; Phishing; Gestión De Credenciales; Ransomware; Identidad Digital; Concienciación Digital.

Códigos JEL: L86; O33; D83; M15; K24; G53.

José Pablo Pérez: Mi nombre es José Pablo Pérez. En Telefónica, dentro de este tipo de congresos, la mayoría de las personas me conocen como JP. Mi responsabilidad principal es el desarrollo de negocio de las soluciones de ciberinteligencia de la compañía. Asimismo, asumo parte de las funciones vinculadas al marketing, la generación de demanda, la organización de eventos y la gestión administrativa y financiera. Mi labor incorpora también una dimensión técnica, ya que trabajo directamente con clientes, les explico las distintas soluciones disponibles y les acompaño en la toma de decisiones más adecuadas en función de sus necesidades.

Teniendo en cuenta el ámbito de estudio en el que os estáis formando, es probable que en el futuro profesional terminéis incorporándoos a una empresa tecnológica. El desarrollo actual del sector exige, cada vez más, perfiles capaces de combinar competencias técnicas con habilidades para desenvolverse en entornos digitales y en redes orientadas a la captación de clientes.

Para la sesión de hoy he preparado un esquema que se estructura en varios bloques. En primer lugar, ofreceré un marco de contexto general. A continuación, analizaré los riesgos más habituales asociados al emprendimiento y a la exposición de una empresa en Internet, un planteamiento aplicable tanto a

pymes como a otros modelos de negocio. Evidentemente, existen distintos niveles de madurez en materia de ciberseguridad, pero el enfoque que propongo pretende ser útil y transferible a cualquier tipo de organización. Posteriormente, abordaré cómo proteger una empresa, presente o futura, y compartiré diversos recursos gratuitos que pueden resultar de utilidad. Finalmente, reservaré un espacio para preguntas, sin perjuicio de que podáis interrumpirme en cualquier momento si surge alguna duda o si algo no queda suficientemente claro.

Al adentrarnos en el ámbito del mundo digital, el primer paso consiste en comprender a qué tipo de amenazas podemos enfrentarnos. Cuando hablamos de ciberseguridad, solemos referirnos a los ciberataques que han causado daños significativos a grandes empresas y que han generado importantes pérdidas económicas. Sin embargo, esta realidad no es más que la versión digital de situaciones que también se producen en la vida cotidiana. Del mismo modo que puede producirse un robo de gran magnitud en el mundo físico, una organización puede sufrir en el entorno digital una filtración de datos u otros incidentes de gran impacto.

Resulta fundamental, por tanto, clarificar qué entendemos por ciberdelincuente, por ciberataque y por ciberseguridad. Los ciberdelincuentes son aquellas personas que realizan actividades delictivas en el entorno digital contra sistemas informáticos. Estas acciones pueden materializarse mediante ataques de diversa naturaleza: desde agresiones contra la reputación de una empresa, como la suplantación de marca o de identidad, hasta la filtración de información sensible o el ataque directo a los sistemas tecnológicos. El conjunto de estas acciones constituye lo que denominamos un ciberataque. La ciberseguridad, por su parte, tiene como objetivo proteger tanto a empresas como a personas frente a este tipo de amenazas, ya sea anticipándose a ellas o respondiendo una vez se han producido, mediante la contención del incidente y la realización de análisis forenses que permitan comprender qué ha ocurrido y cómo evitar que vuelva a repetirse en el futuro.

Existen múltiples tipologías de ciberataques, que varían en función de la tecnología empleada, del perfil de la víctima y del alcance de la acción. Pueden tratarse de ataques aleatorios, masivos o dirigidos específicamente contra un objetivo concreto, con una estrategia definida. Asimismo, el propósito del ataque puede diferir: desde el daño reputacional a una empresa, hasta la obtención de beneficios económicos mediante la comercialización de la información sustraída o su utilización con fines estratégicos por parte de organizaciones o incluso de Estados.

Si observamos la evolución histórica de los ciberataques, los primeros virus informáticos, como Creeper, surgieron principalmente como experimentos tecnológicos, con un carácter casi lúdico. No existía entonces una intención clara de destruir sistemas ni de obtener beneficios. Con el paso del tiempo, a medida que se intensificó la relación entre determinadas personas y la tecnología, y que aparecieron actores con intenciones más claramente maliciosas, la ciberdelincuencia comenzó a configurarse como un auténtico modelo de negocio. Se pasó de la experimentación a una actividad organizada y orientada a objetivos concretos.

En este contexto se sitúan algunos casos paradigmáticos, como el de Ross Ulbricht, creador de Silk Road, un mercado ilegal en la denominada web oscura. Este fue uno de los primeros ejemplos de plataformas de comercio ilícito en las que se ofrecían productos prohibidos. Estos antecedentes ilustran cómo la ciberdelincuencia fue evolucionando desde iniciativas aisladas hasta estructuras complejas con una clara orientación económica.

De manera progresiva, los ataques dejaron de ser inocentes y comenzaron a responder a objetivos definidos, como la sustracción de credenciales, el sabotaje de sistemas informáticos o la consecución de ventajas estratégicas. A lo largo de los años han aparecido amenazas relevantes a escala global, como determinados grupos de ransomware que, en momentos concretos, concentraron una parte significativa de los ataques a nivel mundial.

En la actualidad, con la incorporación de la inteligencia artificial, el ritmo de evolución de la ciberdelincuencia se ha acelerado notablemente. Anteriormente, el desarrollo de malware exigía un

esfuerzo considerable en programación y diseño. Hoy en día, existen herramientas basadas en inteligencia artificial que facilitan la creación de este tipo de código, lo que incrementa la velocidad y la sofisticación de los ataques.

Los datos oficiales del sistema estadístico de criminalidad del Ministerio del Interior muestran una tendencia claramente ascendente en el número de incidentes desde aproximadamente 2010. Aunque durante el año 2020 se observa una aparente estabilización, esta circunstancia no responde a una disminución real de los ciberataques, sino a las dificultades en el registro y la tramitación de denuncias durante la pandemia. Posteriormente, la gráfica experimenta un incremento notable, reflejo de una normalización en la recogida de datos y de la continuidad de la actividad delictiva en el ámbito digital.

Si se analizan los datos por comunidades autónomas, se aprecia una mayor incidencia en regiones como Cataluña, la Comunidad Valenciana, la Comunidad de Madrid y Andalucía. Este fenómeno puede estar vinculado tanto a la concentración de actividad empresarial y tecnológica como a los niveles de madurez en materia de seguridad digital y al uso intensivo de sistemas informáticos por parte de la población.

En 2024 se registró un incremento del 24 % en el número de incidentes respecto al año anterior, con una media aproximada de 26 ciberataques exitosos por organización a nivel mundial. Estas cifras se traducen en pérdidas económicas significativas, un aspecto especialmente sensible para quienes gestionan un negocio. Aunque en un primer momento estos datos puedan parecer lejanos, resulta fundamental tener presente el impacto que puede tener la falta de protección sobre un proyecto empresarial que se ha construido con esfuerzo y dedicación.

Hemos llegado a este nivel de impacto debido a varios factores: la creciente sofisticación de los ataques, la mayor organización de las redes criminales, la selección estratégica de los objetivos y la existencia de intereses geopolíticos que también se traducen en conflictos en el ciberespacio. Las perspectivas para 2025 no resultan más alentadoras. Entre los principales vectores de ataque actuales destacan los denominados infostealers, pequeños programas que se instalan en dispositivos como ordenadores o teléfonos móviles para exfiltrar información; el ransomware, que cifra los datos y exige un rescate económico para su recuperación; y las modalidades avanzadas de extorsión, que incluyen intentos de acceso a la cadena de suministro de las empresas para maximizar la presión sobre las víctimas. En este contexto, la realización de copias de seguridad en la nube, con la frecuencia adecuada al tipo de negocio, se convierte en una medida esencial de mitigación del riesgo.

La evolución de estas amenazas ha transformado profundamente la concepción tradicional de la seguridad informática. En el pasado, bastaba con instalar un antivirus en cada equipo para considerar que la empresa estaba protegida. Hoy en día, este enfoque resulta claramente insuficiente. La seguridad debe abordarse de manera integral: protección de la identidad digital, autenticación multifactor en los accesos, soluciones de detección y respuesta en los dispositivos, protección de los entornos en la nube, seguridad del correo electrónico y monitorización de la presencia de la empresa en Internet para detectar suplantaciones de dominio, duplicación de páginas web u otros usos fraudulentos de la marca. La protección ya no se limita a lo que ocurre dentro de la organización, sino que se extiende a todo el ecosistema digital en el que opera.

Llegados a este punto, resulta pertinente plantear una cuestión fundamental: ¿cuáles consideráis que pueden ser los riesgos más habituales que podrían afectar a vuestro proyecto empresarial o a vuestra futura actividad profesional? La identificación temprana de estas amenazas constituye un primer paso imprescindible para diseñar una estrategia de protección eficaz en el entorno digital.

Congresista: Uno de los principales riesgos que identifico es el acceso no autorizado a todos mis datos, especialmente a la información de mis clientes. Asimismo, tal y como se ha mencionado, el impacto sobre los proveedores constituye un factor crítico: si un ataque afecta a la cadena de suministro, las consecuencias se extienden de manera directa a la operativa del negocio. En definitiva,

la vulneración de estos elementos compromete la base misma sobre la que se sustenta la actividad empresarial.

José Pablo Pérez: El riesgo principal al que se enfrenta una organización es el acceso no autorizado a sus datos y a su infraestructura tecnológica, así como la sustracción de esa información. En efecto, se trata de una de las amenazas más críticas. A partir de esta constatación, resulta oportuno comenzar analizando el problema de las credenciales.

Las credenciales, en su forma más básica, están compuestas por un usuario y una contraseña. Se trata de los elementos de identificación que utilizamos para registrarnos y acceder a servicios digitales. En numerosas ocasiones, estas credenciales se ven comprometidas como consecuencia de filtraciones de datos. Si, por ejemplo, una persona se registra en una red profesional utilizando una dirección de correo electrónico y una contraseña que posteriormente reutiliza en otros servicios, una brecha de seguridad en una de esas plataformas puede permitir que terceros accedan al conjunto de sus cuentas. La reutilización de contraseñas convierte una única filtración en un riesgo sistémico para toda la identidad digital del usuario. De ahí la importancia de emplear contraseñas diferentes, robustas y, siempre que sea posible, direcciones de correo diferenciadas para servicios críticos.

En el ámbito corporativo, una parte significativa de las credenciales sustraídas acaba siendo comercializada en mercados clandestinos de la denominada web oscura. Conviene distinguir entre los distintos niveles de Internet: la web abierta, accesible de forma generalizada a través de buscadores; la denominada web profunda, que incluye contenidos no indexados y protegidos por mecanismos de autenticación; y, finalmente, la web oscura, que requiere herramientas específicas para su acceso y en la que proliferan actividades ilícitas. En estos entornos se negocia con credenciales robadas que posteriormente son utilizadas por actores maliciosos para extorsionar a las empresas, realizar ataques posteriores o facilitar el acceso no autorizado a sistemas corporativos. Este es el motivo por el cual las organizaciones establecen políticas estrictas de rotación periódica de contraseñas: no se trata de una medida arbitraria, sino de una respuesta necesaria ante la posibilidad real de que las credenciales hayan sido comprometidas.

En estos mercados ilícitos no solo se comercia con accesos a sistemas empresariales, sino también con cuentas de servicios digitales, medios de pago o datos financieros. Cuentas de plataformas de entretenimiento con saldo acumulado, así como tarjetas de crédito sustraídas tras ataques a páginas web vulnerables, se ofrecen a precios reducidos. No obstante, incluso en estos entornos predomina el fraude, ya que los compradores pueden no recibir nunca aquello que han adquirido, lo que evidencia el grado de degradación ética y de inseguridad que caracteriza a estos espacios.

Otro de los riesgos que afecta de manera directa a empresas y particulares es el phishing. Se trata de una modalidad de ataque en la que un ciberdelincuente suplanta la identidad de una persona o de una entidad legítima, con el objetivo de inducir al receptor a facilitar voluntariamente sus credenciales o datos sensibles, como contraseñas bancarias o accesos a servicios corporativos. Estos mensajes suelen presentarse con una apariencia verosímil, simulando comunicaciones oficiales de grandes proveedores tecnológicos o entidades financieras. En muchos casos, los atacantes cuidan incluso los detalles tipográficos o visuales para engañar al destinatario, introduciendo ligeras alteraciones en direcciones de correo o dominios que pasan fácilmente desapercibidas. Esta sofisticación creciente convierte al phishing en una de las amenazas más persistentes y eficaces en el panorama actual de la ciberseguridad.

Congresista: He conocido un caso cercano en el que una persona estuvo a punto de caer en este tipo de engaño. Recibió una comunicación que aparentaba proceder de su entidad bancaria, en la que se le advertía de la supuesta cancelación de su tarjeta y se le instaba a pulsar un enlace para resolver la incidencia. El mensaje resultaba verosímil y estaba diseñado para generar una reacción inmediata basada en la urgencia y el temor a perder el acceso a su cuenta. La intervención de un tercero, que le

aconsejó no interactuar con el enlace y contactar directamente con el banco por los canales oficiales, permitió evitar el fraude.

Este tipo de situaciones pone de manifiesto la importancia de la prevención y de la verificación de la información por vías seguras. Ante comunicaciones que apelan a la urgencia o al miedo, la pauta adecuada consiste en desconfiar, no interactuar con enlaces ni facilitar datos personales y confirmar siempre la autenticidad del mensaje a través de los canales oficiales de la entidad supuestamente emisora. La pregunta clave que debemos plantearnos es cómo identificar este tipo de comunicaciones fraudulentas. Reconocer los indicios de falsedad se convierte, en este contexto, en una competencia esencial para la protección de la identidad digital y del patrimonio económico.

José Pablo Pérez: A continuación abordaré algunas soluciones que pueden ayudar a identificar este tipo de situaciones. No obstante, el primer principio, y la base fundamental de mi trabajo, es interiorizar el concepto de "confianza cero". Este enfoque implica no otorgar credibilidad automática a ninguna comunicación recibida y examinar con detenimiento cualquier mensaje, notificación o solicitud de información. En el contexto actual, la principal línea de defensa sigue siendo el criterio propio, la capacidad de análisis y la atención consciente. Aunque existen herramientas tecnológicas que contribuyen a reforzar la protección, la primera barrera es siempre la actitud crítica ante cualquier estímulo digital.

Este tipo de mensajes fraudulentos no son situaciones excepcionales, sino experiencias habituales para la mayoría de los usuarios. Un ejemplo reciente lo ilustra con claridad: recibí en mi propio teléfono corporativo una notificación que aparentaba proceder de una entidad bancaria con la que no mantengo relación alguna. El mensaje estaba diseñado para generar una reacción inmediata y se presentaba con un formato aparentemente legítimo. Este tipo de intentos de fraude se producen de manera constante y no distinguen entre perfiles personales o profesionales.

Además, la sofisticación de estos ataques ha aumentado de forma significativa. En la actualidad, los ciberdelincuentes han conseguido integrarse en los mismos hilos de mensajes legítimos que utilizan las entidades financieras para el envío de códigos de verificación o notificaciones de autenticación en dos factores. De este modo, el usuario recibe mensajes fraudulentos intercalados con comunicaciones auténticas, lo que dificulta de manera notable la capacidad de discriminación. Este escenario refuerza la necesidad de aplicar de forma sistemática el principio de desconfianza razonable y de verificación por canales oficiales antes de interactuar con cualquier contenido recibido.

Congresista: Resulta especialmente preocupante comprobar hasta qué punto la sofisticación de los ciberataques ha alcanzado niveles en los que se replica incluso el número de teléfono de entidades bancarias u organizaciones legítimas, así como el de particulares. En algunos casos, la suplantación llega a incluir la imitación de la voz de la persona o de la entidad supuestamente emisora de la llamada. De este modo, el receptor puede recibir comunicaciones que aparentan proceder de una compañía de telecomunicaciones u otro proveedor de servicios, en las que se le ofrece, por ejemplo, una mejora de condiciones contractuales u otro tipo de beneficio aparente.

Este grado de realismo en la suplantación provoca una lógica sensación de desconcierto y vulnerabilidad, ya que los elementos tradicionales de verificación, como el número de origen o el tono de la comunicación, dejan de ser indicadores fiables de autenticidad. Ante esta realidad, la concienciación del entorno más cercano se convierte en una medida preventiva de gran valor. La transmisión de estas pautas de prudencia a familiares y personas con menor familiaridad con el entorno digital resulta esencial para reducir la probabilidad de que sean víctimas de este tipo de fraudes. La recomendación fundamental es no atender ni interactuar con llamadas o mensajes inesperados que soliciten información sensible, y contrastar siempre cualquier comunicación a través de los canales oficiales de la entidad correspondiente.

José Pablo Pérez: Es muy acertado adoptar una actitud preventiva ante este tipo de amenazas. Cuando recibáis una llamada de un número desconocido, resulta recomendable no responder

afirmativamente de manera automática. Existe una tendencia habitual a contestar con un "sí", pero conviene modificar ese patrón de respuesta y optar por fórmulas neutras que no confirmen de forma explícita la identidad. La razón es que una simple muestra de voz puede ser utilizada, con el apoyo de herramientas de inteligencia artificial, para generar grabaciones falsas que simulen comunicaciones realizadas por la propia persona. A partir de fragmentos mínimos de audio y de imágenes disponibles públicamente, es posible crear contenidos audiovisuales falsificados que imitan rostro y voz con un alto grado de realismo. Si, además, se produce la filtración de un documento de identidad, el nivel de suplantación puede alcanzar cotas especialmente preocupantes.

Dentro del ámbito del phishing, conviene distinguir sus principales variantes. Cuando el engaño se realiza a través de mensajes de texto se denomina smishing, mientras que cuando se ejecuta mediante llamadas telefónicas se conoce como vishing. En ambos casos, el objetivo es inducir al receptor a facilitar información sensible bajo pretextos aparentemente legítimos, como supuestas ofertas de empleo, comunicaciones de entidades financieras o notificaciones de servicios que el usuario no ha solicitado. La pauta esencial es mantener una actitud de desconfianza razonable ante cualquier comunicación inesperada y verificar siempre su autenticidad por canales oficiales.

Otro vector de ataque frecuente es la suplantación de marca combinada con la suplantación de dominio. Es habitual recibir correos electrónicos con supuestas ofertas de grandes descuentos en comercios reconocidos. Al acceder al enlace, la dirección web no corresponde a la página oficial de la empresa, sino a un sitio fraudulento que simula su apariencia. Estas páginas buscan que el usuario introduzca datos personales y financieros, lo que facilita la posterior suplantación de identidad. Por ello, resulta imprescindible comprobar siempre la URL y desconfiar de ofertas desproporcionadamente ventajosas que apelan a la urgencia o al atractivo económico inmediato.

El uso de redes wifi públicas constituye otro de los riesgos más comunes. Las conexiones en espacios abiertos, como cafeterías, estaciones o aeropuertos, facilitan ataques del tipo "intermediario", en los que un tercero intercepta las comunicaciones entre el dispositivo del usuario e Internet. A ello se suma la existencia de redes falsas creadas deliberadamente para engañar a los usuarios, conocidas como "gemelos maliciosos", que imitan el nombre de redes legítimas. Al conectarse a estas redes, el usuario expone sus datos sin ser consciente de ello. De igual modo, el uso de puertos USB públicos y el escaneo indiscriminado de códigos QR pueden conducir a páginas fraudulentas. Existen casos documentados en los que se han colocado códigos QR falsos en espacios públicos para simular sanciones o pagos urgentes, induciendo a las personas a realizar transferencias económicas bajo presión psicológica.

En el ámbito de la gestión de dispositivos y aplicaciones, es recomendable separar los entornos personal y profesional, evitando utilizar el mismo equipo para fines corporativos y privados. Asimismo, conviene extremar la precaución al almacenar datos bancarios en sitios web, compartir ubicaciones con aplicaciones o conceder permisos excesivos que no guardan relación con la funcionalidad del servicio. La concesión indiscriminada de permisos a aplicaciones que no los necesitan constituye una vía adicional de exposición al riesgo.

En cuanto a los recursos de apoyo, el Instituto Nacional de Ciberseguridad (INCIBE) representa un punto de referencia fundamental en el contexto español. A través de sus servicios gratuitos de asesoramiento, ofrece orientación tanto a particulares como a empresas sobre cómo implantar medidas de ciberseguridad, cómo actuar ante un fraude o cómo gestionar un incidente una vez se ha producido. Entre sus materiales se incluyen guías prácticas, políticas de seguridad, decálogos de buenas prácticas, orientaciones sobre protección de datos, cumplimiento normativo y planes de contingencia, así como herramientas para la elaboración de planes directores de seguridad que permitan estructurar la protección de una empresa desde sus primeras fases de desarrollo.

Entre las recomendaciones básicas destaca la correcta gestión de contraseñas. No deben almacenarse en soportes visibles ni en lugares accesibles para terceros. Las contraseñas deben ser memorizadas o,

en su caso, gestionadas mediante soluciones específicas de almacenamiento seguro. El uso de combinaciones predecibles, como nombres propios o referencias evidentes, incrementa de manera considerable la probabilidad de compromiso de los sistemas. Las contraseñas deben ser largas, complejas y únicas para cada servicio.

Existen asimismo recursos gratuitos que permiten comprobar si una dirección de correo electrónico ha sido incluida en alguna filtración de datos conocida. En caso afirmativo, resulta imprescindible proceder de inmediato al cambio de credenciales en todos los servicios afectados. De igual modo, pueden utilizarse herramientas para evaluar la fortaleza de una contraseña y generadores de contraseñas aleatorias que ayuden a crear combinaciones más robustas. Aunque estas contraseñas puedan resultar difíciles de memorizar, existen gestores específicos que permiten almacenarlas de forma segura, quedando en manos de cada usuario la decisión informada sobre su utilización.

En conjunto, la adopción de una cultura de ciberseguridad basada en la prevención, la verificación constante y el uso de recursos institucionales y técnicos disponibles constituye un elemento esencial para la protección efectiva de personas y empresas en el entorno digital.

Congresista: Existe un debate relevante en torno a la gestión de contraseñas, y es comprensible que genere dudas. Por un lado, se insiste en la necesidad de no reutilizar contraseñas y de crear combinaciones únicas para cada servicio. Sin embargo, en la práctica, una persona puede llegar a gestionar decenas o incluso cientos de credenciales, incluidas aquellas asociadas a servicios a los que se accede de manera muy esporádica. En este contexto, surge una dificultad real: la imposibilidad material de recordar contraseñas complejas para cada plataforma.

Ante esta realidad, los gestores de contraseñas se presentan como una solución funcional. Muchos usuarios emplean de forma habitual los gestores integrados en los navegadores, como el que ofrece Google, para almacenar de manera centralizada sus credenciales. La cuestión clave es si puede considerarse seguro delegar la custodia de las contraseñas en este tipo de herramientas. Desde un punto de vista de ciberseguridad, estos gestores incorporan mecanismos de cifrado y medidas de protección diseñadas para salvaguardar la información almacenada. No obstante, su nivel de seguridad está directamente condicionado por la robustez de la contraseña maestra asociada a la cuenta principal y por la correcta configuración de medidas adicionales de protección, como la autenticación multifactor. En consecuencia, el uso de gestores de contraseñas puede ser una práctica adecuada siempre que se acompañe de una gestión rigurosa de la cuenta principal que los protege y de hábitos de seguridad coherentes con el nivel de riesgo asumido.

José Pablo Pérez: En relación con la gestión de contraseñas, existe un debate abierto y legítimo. Por un lado, se promueve la creación de credenciales únicas y complejas para cada servicio, evitando su reutilización. Por otro, surge una dificultad práctica evidente: una persona puede acumular decenas de cuentas, incluidas aquellas a las que accede de forma muy esporádica, lo que hace prácticamente inviable recordar todas las contraseñas sin apoyo externo.

Existen sistemas de gestión de credenciales que no mantienen contraseñas estáticas, sino que las rotan de forma periódica y automatizada. En estos modelos, el usuario registra sus cuentas en una plataforma centralizada, que se encarga del proceso de autenticación y suele incorporar mecanismos de doble factor de verificación a través del teléfono móvil u otros dispositivos. Este tipo de soluciones, correctamente implementadas, ofrecen un nivel de seguridad elevado, ya que reducen el riesgo asociado a la exposición prolongada de una misma contraseña.

Desde una perspectiva más conservadora, conviene señalar que el almacenamiento centralizado de credenciales en un sistema estático introduce un riesgo agregado: si dicho gestor fuera comprometido, el impacto potencial afectaría de forma simultánea a un elevado número de cuentas. Esta circunstancia obliga a valorar cuidadosamente el equilibrio entre usabilidad y seguridad. En cualquier caso, resulta imprescindible que la cuenta principal que da acceso al gestor esté protegida mediante una contraseña robusta y autenticación multifactor.

Ante la dificultad de memorizar un gran volumen de contraseñas, algunas personas optan por estrategias de memorización selectiva o por métodos de custodia física de las credenciales, siempre que estos se mantengan fuera del alcance de terceros. Lo relevante, desde el punto de vista de la seguridad, es evitar prácticas que expongan de manera directa las contraseñas en entornos accesibles o visibles para otras personas, y adoptar un criterio consciente sobre el nivel de riesgo asumido en función del valor de los activos que se pretende proteger.

En lo que respecta a la verificación de enlaces y archivos potencialmente maliciosos, existen recursos que permiten analizar direcciones web sospechosas o ficheros descargados antes de interactuar con ellos. Estas plataformas contrastan el contenido con múltiples motores de detección y bases de datos de amenazas conocidas, lo que facilita identificar si una página o un archivo han sido catalogados como peligrosos. Esta práctica preventiva resulta especialmente útil cuando se reciben enlaces asociados a supuestas ofertas comerciales o comunicaciones que presentan indicios de suplantación de dominio, como variaciones mínimas en el nombre de una marca reconocida.

Asimismo, conviene apoyarse en fuentes de información especializadas para mantenerse actualizado sobre el panorama de amenazas. La difusión periódica de boletines de ciberseguridad, análisis de incidentes y comunicaciones sobre vulnerabilidades relevantes permite adquirir una visión más amplia del contexto de riesgo y refuerza la capacidad de anticipación frente a posibles ataques. La formación continua y el acceso a información contrastada constituyen, en este sentido, un complemento imprescindible a las medidas técnicas de protección.

Con todo ello, el conjunto de recomendaciones expuestas pretende ofrecer un marco práctico para la gestión responsable de la identidad digital, la protección de la información y la reducción del riesgo en el entorno tecnológico actual.