

# **Ciberseguridad en el trabajo remoto.**

## **Claves para gestionar los riesgos.**

### **AUTOR:**

Torres Ponce, Mariano Enrique  
Abogado y Especialista en Derecho Informático  
*Universidad de Buenos Aires*

### **RESUMEN**

El trabajo remoto se ha consolidado como una forma habitual de operar en muchas organizaciones, modificando las condiciones en las que se gestionan la seguridad y el riesgo tecnológico. La descentralización del acceso, el uso de dispositivos y redes no controladas y la incorporación de servicios externos alteran las premisas sobre las que se apoyaban los modelos tradicionales de protección.

En este contexto, la ciberseguridad deja de ser una cuestión exclusivamente técnica. Pasa a depender, en gran medida, de cómo se gestionan los accesos, cómo circula la información y qué decisiones se toman en el día a día. La pérdida del perímetro como referencia obliga a centrar el control en la identidad, en las condiciones de acceso y en la visibilidad sobre el uso real de los sistemas.

Este trabajo aborda estos cambios desde un enfoque integrado, combinando la dimensión técnica con la jurídica. Se analizan los principales riesgos del trabajo remoto, los fallos

más frecuentes en la práctica organizativa y las limitaciones de los modelos tradicionales de seguridad. A partir de ahí, se revisa el marco regulatorio europeo como un conjunto de exigencias que condicionan la forma en que el riesgo debe gestionarse en entornos distribuidos.

Finalmente, se propone una guía práctica para evaluar la seguridad sobre la base de la operativa real de la organización. El objetivo es facilitar decisiones con criterio, de manera que los controles se ajusten a cómo se trabaja efectivamente y no a un modelo ideal que no se corresponde con la práctica. Ese ajuste entre modelo operativo y modelo de seguridad es, en definitiva, lo que determina si la protección es efectiva y sostenible.

## **ÍNDICE**

Resumen

A. Introducción

B. Fin del perímetro y pérdida de control directo

C. Superficie de ataque e identidad como eje de seguridad

D. Modelos de control en entornos distribuidos

E. Datos y responsabilidad en entornos remotos

F. Marco regulatorio aplicable en entornos remotos

G. Fallos frecuentes en entornos de trabajo remoto

H. Evaluación práctica del riesgo en entornos remotos

I. Responsabilidad organizativa y toma de decisiones

J. Guía práctica de revisión

K. Conclusión

Referencias

## **A. INTRODUCCIÓN**

La responsable de administración de una empresa pequeña abre el correo desde su portátil, en la cocina de su casa, porque hoy trabaja en remoto. Revisa facturas, descarga un Excel con datos de clientes para cruzarlo con el banco, y mientras tanto contesta por WhatsApp a un proveedor que le pide una copia del contrato. Todo funciona. Nadie está haciendo nada raro. Y, sin embargo, en cinco minutos, información que la empresa tiene obligación de proteger acaba de circular por cuatro entornos que la empresa no controla: un portátil personal, una red doméstica, una aplicación de mensajería y un correo sincronizado en un móvil.

Esta escena no tiene nada de excepcional. Es, cada vez más, la forma normal de trabajar.

El trabajo remoto dejó de ser, para muchas organizaciones, una solución puntual frente a una necesidad operativa y pasó a convertirse en una forma estable de funcionamiento. Este cambio no solo modificó la manera en que se desarrolla la actividad, sino también las condiciones en las que se protegen los sistemas y se gestiona la información. Lo que antes podía pensarse desde un entorno relativamente controlado hoy debe abordarse en un escenario distribuido, con accesos, dispositivos y servicios que no se encuentran dentro de un único espacio gestionado por la organización.

Durante años, la seguridad se estructuró sobre una lógica clara. Los sistemas críticos, los datos y los usuarios se ubicaban dentro de entornos administrados directamente por la organización, lo que permitía aplicar controles relativamente homogéneos. En ese modelo, la red corporativa funcionaba como punto de referencia para definir niveles de confianza y establecer mecanismos de protección. Ese esquema no desaparece, pero deja de ser suficiente cuando el acceso a los recursos se produce desde fuera de ese entorno y bajo condiciones que cambian de manera constante.

El trabajo remoto altera ese punto de partida. El acceso a sistemas corporativos puede producirse desde redes domésticas, dispositivos personales o servicios de terceros, muchas veces sin control directo por parte de la organización. En este contexto, la ubicación deja de ser un criterio fiable para determinar el nivel de seguridad, y el acceso autenticado deja de ser una garantía suficiente por sí misma (Rose et al., 2020).

En la práctica, esto implica que el riesgo deja de estar concentrado y pasa a distribuirse a lo largo de toda la operación. La seguridad ya no depende únicamente de proteger la

infraestructura central, sino también de cómo se gestionan los accesos, de qué herramientas se utilizan y de qué nivel de visibilidad existe sobre el uso real de los sistemas. Este cambio no introduce únicamente nuevos puntos de exposición, sino que modifica la forma en que debe entenderse la protección en entornos distribuidos (Anderson, 2020).

Además, los incidentes de seguridad no suelen originarse en fallos técnicos complejos, sino en situaciones cotidianas vinculadas al uso de credenciales, configuraciones incorrectas o accesos otorgados en condiciones inadecuadas (ENISA, 2023). En entornos remotos, donde la interacción digital es constante y la supervisión directa es menor, este tipo de situaciones adquiere mayor relevancia.

Este escenario tiene una consecuencia organizativa clara. La ciberseguridad deja de ser una cuestión exclusivamente técnica. Las decisiones sobre accesos, dispositivos, herramientas y circulación de la información tienen un impacto directo en el nivel de exposición de la organización. Por eso, la seguridad no puede evaluarse únicamente en función de las herramientas implementadas, sino en función de su adecuación a la forma concreta en que se trabaja.

Desde el punto de vista jurídico, este cambio no reduce las obligaciones, sino que las hace más exigentes en la práctica. El Reglamento General de Protección de Datos establece que deben adoptarse medidas técnicas y organizativas adecuadas al riesgo, sin diferenciar el entorno desde el cual se accede a la información (Reglamento (UE) 2016/679). Esto implica que el trabajo remoto no flexibiliza los requisitos de seguridad, sino que obliga a adaptarlos a un contexto más complejo.

Este documento no pretende convertir al lector en especialista en ciberseguridad ni en normativa europea. Busca algo más concreto: aportar criterio para tomar decisiones razonables sobre cómo se protege la información cuando el trabajo se hace fuera de la oficina. Tanto si el rol es definir políticas, administrar sistemas o autorizar herramientas, la pregunta de fondo es siempre la misma. Lo que se está haciendo debe tener sentido desde el punto de vista del riesgo, y ese juicio no se puede delegar en la herramienta.

En muchas organizaciones se observa una situación recurrente. Se incorporan nuevas herramientas, se habilita el acceso remoto y se amplía el uso de servicios externos, pero los criterios de seguridad continúan respondiendo a un modelo anterior. No

necesariamente faltan controles, pero sí suele existir una desconexión entre cómo funciona la organización y cómo se intenta protegerla (Schneier, 2018).

El problema, en este contexto, no es la tecnología en sí misma, sino el desajuste entre el modelo operativo y el modelo de seguridad. Ese desajuste no se resuelve comprando más herramientas. Se resuelve entendiendo cómo se trabaja realmente y decidiendo, con criterio, qué proteger y cómo.

## **B. FIN DEL PERÍMETRO Y PÉRDIDA DE CONTROL DIRECTO**

Durante mucho tiempo, la seguridad se organizó alrededor de una idea relativamente estable. Existía un entorno que podía considerarse propio de la organización y, por lo tanto, más confiable. Ese entorno estaba compuesto por redes internas, dispositivos gestionados y sistemas accesibles desde ubicaciones definidas. Sobre esa base se diseñaban los controles y se tomaban decisiones de protección.

Ese modelo no desaparece, pero pierde capacidad para explicar lo que ocurre en la práctica. El trabajo remoto introduce un escenario en el que el acceso a los sistemas deja de depender de una ubicación controlada. Un mismo usuario puede conectarse desde su casa, desde una red pública o desde un dispositivo personal, utilizando herramientas corporativas junto con servicios externos. En este contexto, la distinción entre lo interno y lo externo deja de ser suficiente para definir niveles de confianza (Rose et al., 2020).

Un ejemplo permite visualizar este cambio. Un empleado que gestiona pedidos trabaja desde casa con el portátil de la empresa y accede al sistema mediante usuario y contraseña. Un viernes por la tarde recibe una consulta urgente de un cliente, pero el portátil corporativo está sin batería. Decide acceder desde su ordenador personal, descarga el listado de pedidos en una hoja de cálculo y lo envía por correo. El sistema registra el acceso como correcto y, desde el punto de vista técnico, la operación es válida. Sin embargo, la organización pierde visibilidad sobre esa información, ya que no puede determinar en qué dispositivo quedó almacenada ni durante cuánto tiempo permanecerá allí.

Este tipo de situaciones refleja un cambio en la lógica del control. En modelos anteriores, gran parte de la seguridad se apoyaba en restringir el acceso desde fuera de la organización. En entornos remotos, el acceso es en muchos casos legítimo desde el inicio.

El problema deja de centrarse en quién intenta entrar y pasa a incluir las condiciones en las que se accede y lo que ocurre una vez que ese acceso se produce.

En la práctica, la organización deja de tener control directo sobre elementos clave. No controla completamente la red desde la que se accede, no siempre controla el dispositivo utilizado y, en muchos casos, tampoco controla todas las herramientas que intervienen en la operación diaria. A pesar de ello, mantiene la responsabilidad sobre los sistemas y sobre la información que gestiona.

La pérdida de control directo no implica una reducción de esa responsabilidad. Las obligaciones de seguridad se mantienen, pero deben aplicarse en un entorno heterogéneo y cambiante. Esto obliga a revisar los criterios sobre los que se diseñan los controles, ya que confiar en el origen del acceso deja de ser suficiente (Anderson, 2020).

Este escenario también introduce situaciones que no eran habituales en modelos perimetrales. Un acceso legítimo puede convertirse en un problema si se realiza desde un dispositivo comprometido o desde una red insegura. De la misma forma, una credencial válida puede utilizarse en un contexto distinto al esperado sin generar señales evidentes de alerta. En estos casos, el riesgo no proviene de un acceso no autorizado, sino de un uso válido en condiciones inadecuadas (ENISA, 2023).

La detección de estas situaciones resulta más compleja cuando los controles siguen diseñados para un modelo basado en el perímetro. La seguridad deja de depender de un punto de entrada claramente identificado y pasa a construirse a partir de múltiples factores que deben evaluarse de manera conjunta. La identidad del usuario, el estado del dispositivo y el contexto del acceso adquieren mayor relevancia que la ubicación desde la que se realiza la conexión (Rose et al., 2020).

Desde el punto de vista organizativo, este cambio también afecta a la forma en que se toman decisiones. Prácticas que podían ser tolerables en un entorno controlado adquieren un impacto distinto cuando el acceso es distribuido. Compartir credenciales, reutilizar accesos o utilizar herramientas no previstas pueden parecer decisiones menores, pero incrementan el nivel de exposición en este tipo de entornos (Schneier, 2018).

Cuando los controles no están alineados con la forma real de trabajar, es habitual que los usuarios busquen alternativas para sostener la operativa. Estas soluciones no suelen responder a una intención de incumplir, sino a la necesidad de resolver tareas concretas.

Sin embargo, introducen nuevos riesgos que no están contemplados en el modelo de seguridad.

Mantener un enfoque basado exclusivamente en el perímetro puede generar una sensación de control que no se corresponde con el riesgo real. Puede haber medidas implementadas, pero no necesariamente están actuando sobre los puntos donde se produce la exposición.

El desafío no consiste en eliminar el perímetro, sino en dejar de depender de él como único mecanismo de protección. En entornos de trabajo remoto, la seguridad requiere asumir que el acceso es distribuido, que el control es necesariamente parcial y que las condiciones cambian de forma constante. A partir de este reconocimiento, los controles pueden diseñarse de manera más coherente con la realidad operativa de la organización.

### **C. SUPERFICIE DE ATAQUE E IDENTIDAD COMO EJE DE SEGURIDAD**

En entornos de trabajo remoto, la seguridad deja de estar centrada exclusivamente en la infraestructura y pasa a depender, en gran medida, de la forma en que se gestionan los accesos. Este desplazamiento no implica que los sistemas pierdan relevancia, sino que el punto más frecuente de compromiso ya no suele encontrarse en fallos técnicos complejos, sino en el uso de accesos válidos bajo condiciones inadecuadas.

La superficie de ataque no desaparece, pero cambia de naturaleza.

En modelos tradicionales, podía identificarse con cierta claridad a partir de sistemas expuestos y puntos de entrada definidos. En entornos distribuidos, esa superficie se vuelve más amplia y difícil de delimitar. Incluye no solo los sistemas, sino también las identidades digitales, los dispositivos utilizados, las aplicaciones conectadas y las relaciones entre todos estos elementos. Cada acceso representa, en la práctica, un punto potencial de exposición (Anderson, 2020).

En este contexto, el acceso legítimo se convierte en el canal habitual de interacción con los sistemas. Plataformas cloud, herramientas de colaboración y servicios accesibles desde internet forman parte del funcionamiento normal de la organización. Esto implica que los mecanismos de protección no pueden basarse únicamente en impedir el acceso, sino en controlar las condiciones en las que ese acceso se produce (Rose et al., 2020).

Los datos disponibles muestran que una parte significativa de los incidentes se vincula con credenciales comprometidas, reutilización de contraseñas o permisos excesivos (ENISA, 2023). En estos casos, no es necesario vulnerar la infraestructura. El acceso ya existe y es válido desde el punto de vista del sistema, lo que dificulta su detección.

Este cambio obliga a replantear el enfoque.

La pregunta deja de ser únicamente quién puede acceder y pasa a incluir qué puede hacer una vez dentro, desde qué entorno lo hace y bajo qué condiciones se mantiene ese acceso. Un usuario legítimo con permisos excesivos o accediendo desde un entorno inseguro puede representar un nivel de riesgo equivalente al de un acceso externo no autorizado (Schneier, 2018).

En este escenario, la identidad digital se convierte en el eje de la seguridad.

Cada usuario, cada cuenta de servicio y cada integración entre sistemas representan un punto de acceso que debe ser gestionado de forma consciente. Esto incluye no solo la autenticación, sino también la asignación de permisos, la duración de las sesiones y la capacidad de supervisar la actividad. La seguridad ya no depende únicamente de proteger sistemas, sino de gestionar quién y cómo interactúa con ellos (Rose et al., 2020).

Uno de los problemas más frecuentes es la acumulación de privilegios. A lo largo del tiempo, los usuarios adquieren accesos que responden a necesidades puntuales, pero que no siempre se revisan posteriormente. En entornos remotos, donde la visibilidad es menor, estos accesos pueden mantenerse activos sin justificación clara, ampliando el impacto potencial de un incidente (Anderson, 2020).

Un caso habitual ilustra este patrón. Una persona entra en una empresa como comercial y, con el tiempo, rota a facturación, luego colabora temporalmente con el equipo de compras y termina pasando a operaciones. En cada movimiento, alguien del equipo técnico le da los accesos que necesita para su nueva función. Nadie le retira los anteriores, porque revisar qué se le puede quitar requiere tiempo y genera rozamientos si después resulta que lo necesitaba para una consulta puntual. Cinco años después, esa persona tiene acceso a sistemas que ya no utiliza desde hace años, a datos que no son de su responsabilidad actual y a permisos que ningún rol razonable justificaría por sí solo. No hay ninguna decisión explícita detrás de esa situación. Es el resultado acumulado de decisiones pequeñas, cada una razonable en su momento.



Algo similar ocurre con las cuentas técnicas y las integraciones entre sistemas. Las aplicaciones se conectan entre sí mediante credenciales o tokens que, en muchos casos, no están sujetos a los mismos controles que las cuentas de usuario. Estas credenciales pueden permanecer activas durante largos períodos, con permisos amplios y sin una supervisión adecuada. Si son comprometidas, el acceso resultante puede ser difícil de detectar y de contener.

Además, el uso intensivo de servicios externos introduce una complejidad adicional. La seguridad no depende únicamente de la infraestructura propia, sino también de cómo se configuran y utilizan plataformas de terceros. En muchos casos, la organización asume que el proveedor garantiza la seguridad, cuando en realidad una parte significativa del control sigue dependiendo de cómo se gestionan los accesos y permisos (ENISA, 2023).

Esto se traduce en una situación concreta. Un sistema puede funcionar correctamente desde el punto de vista técnico, pero estar expuesto si los accesos no están adecuadamente gestionados. La disponibilidad y el rendimiento no son indicadores suficientes de seguridad si las condiciones de uso no son las adecuadas.

En este tipo de entornos, los problemas no siempre se presentan como fallos visibles. El acceso funciona, las herramientas responden y la operación continúa con normalidad. Sin embargo, las condiciones en las que se produce ese acceso pueden no ser seguras, lo que dificulta la identificación temprana del riesgo.

Por eso, la seguridad no puede evaluarse únicamente en términos de funcionamiento técnico, sino en términos de control efectivo sobre las identidades y los accesos. En entornos de trabajo remoto, donde el acceso es el punto de entrada natural al sistema, la forma en que se gestionan las identidades determina en gran medida el nivel real de exposición de la organización.

## **D. MODELOS DE CONTROL EN ENTORNOS DISTRIBUIDOS**

Cuando el acceso a los sistemas deja de depender de un entorno controlado y comienza a producirse desde múltiples ubicaciones y bajo condiciones variables, el modelo de seguridad debe ajustarse a esa realidad. Este ajuste no consiste únicamente en incorporar nuevas herramientas, sino en revisar los criterios con los que se toman las decisiones de control.

En modelos tradicionales, gran parte de la seguridad se apoyaba en la red como punto de referencia. El acceso desde el entorno corporativo se asociaba a un mayor nivel de confianza, lo que permitía simplificar la gestión. Este enfoque funcionaba en contextos relativamente estables, pero pierde validez cuando el acceso se distribuye y deja de estar vinculado a una ubicación concreta.

En el trabajo remoto, la ubicación deja de ser un indicador fiable. El acceso legítimo puede producirse desde cualquier lugar, lo que obliga a desplazar el foco hacia otros elementos. La identidad del usuario, el estado del dispositivo, el contexto del acceso y el tipo de operación pasan a tener mayor relevancia que el origen de la conexión (Rose et al., 2020). Este cambio no elimina la necesidad de proteger la infraestructura, pero sí modifica el punto desde el cual se ejerce el control.

En la práctica, ningún acceso debería considerarse confiable únicamente por su origen. La validación de credenciales sigue siendo necesaria, pero deja de ser suficiente por sí sola. Resulta necesario evaluar de forma continua las condiciones en las que se produce el acceso y ajustar los niveles de control en función de ese contexto (Anderson, 2020).

La asignación de permisos adquiere un papel central en este escenario. En entornos distribuidos, otorgar más acceso del necesario incrementa el impacto potencial de cualquier incidente. Un usuario con privilegios excesivos o una cuenta técnica con acceso amplio pueden convertirse en puntos críticos si son comprometidos. Limitar el alcance de cada acceso no responde a una cuestión administrativa, sino a una estrategia directa de reducción de riesgo (Saltzer & Schroeder, 1975).

La visibilidad sobre la actividad se vuelve igualmente relevante. Cuando el acceso es legítimo desde el inicio, la detección de problemas depende de la capacidad de observar lo que ocurre dentro del sistema. Esto requiere contar con registros adecuados, mecanismos de monitoreo y criterios que permitan identificar comportamientos que se desvíen de lo esperado. Sin esta visibilidad, muchas situaciones de riesgo pueden desarrollarse sin generar señales evidentes (ENISA, 2023).

Los controles no pueden diseñarse de forma aislada respecto de la operativa. Los mecanismos de seguridad deben integrarse con la forma en que la organización trabaja. Cuando los controles resultan excesivos o no se ajustan a la realidad operativa, tienden a generar fricción. En esos casos, es habitual que los usuarios busquen alternativas para

mantener la productividad, lo que introduce nuevos riesgos que no estaban contemplados en el diseño original (Schneier, 2018).

El diseño de los controles requiere, por tanto, un equilibrio. Por un lado, es necesario reducir el riesgo mediante la validación de accesos, la limitación de permisos y la supervisión de la actividad. Por otro, estos controles deben ser operativamente viables y no generar comportamientos que los debiliten en la práctica.

Desde el punto de vista jurídico, este equilibrio también resulta determinante. El Reglamento General de Protección de Datos no exige la implementación de medidas ideales en abstracto, sino medidas adecuadas al riesgo y al contexto (Reglamento (UE) 2016/679, art. 32). Esto implica que la organización debe ser capaz de justificar no solo qué controles implementa, sino por qué esos controles son razonables en función de su actividad y de su forma de operar. La ausencia de una justificación clara sobre cómo se toman estas decisiones puede resultar tan relevante como la ausencia de medidas.

La evolución de los modelos de control responde a una necesidad práctica más que a un cambio teórico. Mantener esquemas diseñados para entornos cerrados puede generar una apariencia de seguridad que no refleja el riesgo real. En entornos de trabajo remoto, el control efectivo surge de la combinación de decisiones que determinan cómo se accede a los sistemas, qué acciones están permitidas y cómo se supervisa ese uso. La cuestión no pasa por incorporar más controles, sino por asegurar que los controles existentes sean adecuados a la realidad operativa.

## **E. DATOS Y RESPONSABILIDAD EN ENTORNOS REMOTOS**

En entornos de trabajo remoto, la gestión de datos deja de ser una cuestión puramente técnica y pasa a convertirse en un problema operativo y jurídico que atraviesa toda la organización. La información ya no circula únicamente dentro de sistemas controlados, sino que se mueve entre dispositivos, redes y servicios externos bajo condiciones que no siempre son homogéneas ni plenamente visibles. Este desplazamiento obliga a revisar cómo se entiende la protección.

Los datos ya no se encuentran solo en servidores corporativos. También están presentes en herramientas de colaboración, correos electrónicos, aplicaciones cloud y, en muchos casos, en dispositivos que no son gestionados directamente por la organización. Cada uno

de estos puntos introduce condiciones distintas de acceso y, en consecuencia, niveles de riesgo diferentes (ENISA, 2023). En la práctica, la seguridad de la información deja de depender únicamente de su ubicación y pasa a depender de la forma en que se utiliza.

El acceso remoto amplía las situaciones en las que la información puede ser visualizada, modificada o transferida, muchas veces sin supervisión directa. Esto genera escenarios en los que los datos permanecen formalmente protegidos en su origen, pero se dispersan en su uso cotidiano. Un ejemplo ilustra bien este desplazamiento. Una empresa almacena contratos en una carpeta compartida de un servicio cloud. Un responsable revisa uno desde su móvil durante el fin de semana. Al día siguiente envía un fragmento por correo a un colaborador externo, quien a su vez lo reenvía para una segunda opinión. En pocos días, la organización pierde visibilidad sobre la información, aun cuando el documento original sigue en su ubicación inicial.

Esta dinámica muestra que un sistema puede estar correctamente protegido desde el punto de vista técnico y, sin embargo, exponer información si el acceso se produce en condiciones inadecuadas. El uso de dispositivos no gestionados, redes inseguras o herramientas externas sin control suficiente puede comprometer la confidencialidad sin que exista una falla en la infraestructura central (Anderson, 2020).

Desde el punto de vista jurídico, este escenario está claramente contemplado. El Reglamento General de Protección de Datos exige garantizar la confidencialidad, integridad y disponibilidad de los datos mediante medidas adecuadas al riesgo (Reglamento (UE) 2016/679, art. 32). Esta obligación no depende del lugar desde el cual se accede a la información, sino de las condiciones en las que ese acceso se produce. En entornos remotos, esto implica que la organización debe comprender y controlar cómo circulan los datos en la práctica.

Ese control incluye conocer quién accede a la información, desde qué entorno, con qué finalidad y bajo qué condiciones. Sin esta visibilidad, se dificulta tanto la detección de incidentes como la capacidad de respuesta. También se compromete el cumplimiento de obligaciones concretas, como la notificación de violaciones de seguridad dentro del plazo de setenta y dos horas (Reglamento (UE) 2016/679, art. 33). Para cumplir con este requisito es necesario poder reconstruir lo sucedido, identificar los datos afectados y determinar el alcance del incidente, lo que solo es posible si existe trazabilidad previa.

La trazabilidad se convierte así en un elemento central. La capacidad de reconstruir el recorrido de la información y de identificar accesos concretos permite sostener el control en entornos donde los datos se desplazan entre múltiples herramientas y dispositivos. Cuando esta capacidad no está presente, la organización pierde margen de acción tanto para prevenir como para responder.

A esto se suma el uso intensivo de servicios externos. Las herramientas cloud forman parte del funcionamiento habitual de muchas organizaciones y generan una relación de corresponsabilidad en materia de seguridad. El proveedor puede garantizar determinados niveles de protección sobre la infraestructura, pero la organización sigue siendo responsable de la configuración de accesos, del tipo de datos que incorpora y del uso que hace de esos servicios (ENISA, 2023). Externalizar no elimina el riesgo, sino que lo redistribuye.

En este contexto, configuraciones inadecuadas, permisos excesivos o integraciones no controladas pueden generar exposición de información sin que exista ningún fallo en el proveedor. El problema no radica en la tecnología utilizada, sino en la forma en que se gestiona su uso dentro de la operación diaria.

Otro aspecto relevante es la minimización del dato. En entornos distribuidos, cuanto mayor es la cantidad de información accesible y mayor es el número de ubicaciones en las que se encuentra, mayor es la superficie de exposición. Limitar los datos disponibles y restringir su acceso a lo estrictamente necesario no solo responde a una exigencia normativa, sino que reduce de forma directa el impacto potencial de cualquier incidente (Schneier, 2018). El principio de minimización recogido en el artículo 5.1.c) del RGPD cumple esta doble función al disminuir tanto la exposición regulatoria como el impacto material.

Este enfoque permite sostener un nivel de protección razonable incluso cuando no es posible controlar completamente todos los entornos de acceso. En este sentido, la gestión de datos no puede separarse del modelo operativo ni de la gestión de accesos. La forma en que se trabaja determina cómo circula la información, y esa circulación define el nivel real de riesgo.

Desde una perspectiva práctica, el objetivo no es alcanzar un control absoluto, sino mantener un nivel de control suficiente para comprender qué ocurre con los datos y poder actuar cuando algo no funciona como debería. En entornos de trabajo remoto, la seguridad

de la información depende menos de dónde se almacenan los datos y más de cómo se utilizan en la práctica cotidiana.

## **F. MARCO REGULATORIO APLICABLE EN ENTORNOS REMOTOS**

El trabajo remoto no introduce un vacío normativo ni un espacio de excepción. Las obligaciones en materia de ciberseguridad y protección de datos se mantienen plenamente vigentes, aunque deban aplicarse sobre un entorno más complejo. En la práctica, esto implica que las organizaciones no pueden reducir sus niveles de control por operar en remoto, sino que deben adaptarlos a una realidad en la que el acceso es distribuido y las condiciones cambian de forma constante.

El marco europeo aplicable no se articula en una única norma, sino en un conjunto de instrumentos complementarios que se superponen. Desde una perspectiva práctica, puede entenderse como una arquitectura por capas. Una primera capa se ocupa de la protección de los datos personales. Una segunda capa se centra en la seguridad de los sistemas y servicios. Una tercera, específica para determinados sectores, incorpora exigencias adicionales vinculadas a la resiliencia operativa. Estas capas no se excluyen entre sí, sino que se acumulan, de modo que una misma organización puede estar sujeta a varias de ellas de forma simultánea.

El punto de partida lo constituye el Reglamento General de Protección de Datos. Esta norma establece que deben aplicarse medidas técnicas y organizativas adecuadas al riesgo, teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza del tratamiento (Reglamento (UE) 2016/679, art. 32). Esta exigencia no distingue entre entornos presenciales o remotos. Lo relevante es la coherencia entre las medidas adoptadas, la forma en que se accede a los datos y los riesgos asociados a ese acceso. Su aplicación alcanza a cualquier organización que trate datos personales, con independencia de su tamaño o sector.

En entornos de trabajo remoto, este criterio obliga a ampliar el foco. La protección no puede limitarse a la infraestructura central, sino que debe considerar cómo se accede a la información desde fuera de ese entorno, qué dispositivos se utilizan, qué herramientas intervienen y qué grado de control existe sobre esos elementos. La adecuación de las medidas no se evalúa en abstracto, sino en función de las condiciones reales de uso.

A esta base se suma una evolución normativa en materia de ciberseguridad. La Directiva NIS2 amplía el alcance de las obligaciones de seguridad y establece requisitos más exigentes en relación con la gestión de riesgos, la notificación de incidentes y la responsabilidad de la dirección (Directiva (UE) 2022/2555). A diferencia del RGPD, su aplicación se centra en entidades que operan en sectores considerados esenciales o importantes, como energía, transporte, banca, sanidad, infraestructura digital, administración pública o proveedores de servicios gestionados. También puede alcanzar a organizaciones que, sin pertenecer directamente a estos sectores, actúan como proveedores críticos dentro de su cadena de valor.

El valor de este marco no reside únicamente en su ámbito de aplicación, sino en la dirección en la que orienta la regulación. La seguridad deja de entenderse exclusivamente como una cuestión técnica y pasa a configurarse como un elemento de gestión organizativa, con implicación directa de la dirección. Esta orientación adquiere especial relevancia en entornos remotos, donde la dispersión del acceso y la dependencia de sistemas digitales vinculan de forma directa la continuidad operativa con la capacidad de gestionar el riesgo tecnológico.

En el ámbito financiero, el Reglamento DORA profundiza esta lógica al introducir obligaciones específicas sobre resiliencia operativa digital. Estas incluyen la gestión de riesgos tecnológicos, la supervisión de terceros proveedores de servicios TIC y la capacidad de recuperación ante incidentes (Reglamento (UE) 2022/2554). Su aplicación, vigente desde 2025, se extiende a entidades financieras y a proveedores tecnológicos considerados críticos. En contextos donde el trabajo remoto forma parte de la operativa habitual, estas exigencias inciden directamente en la gestión de accesos, en la dependencia de servicios externos y en la continuidad de los sistemas.

Un elemento común a estos marcos es el principio de responsabilidad proactiva. La seguridad no se limita a la implementación de medidas, sino que implica la capacidad de la organización para justificar sus decisiones. Esto incluye explicar por qué se han adoptado determinados controles, cómo se evalúan los riesgos y qué criterios se utilizan para ajustar las medidas en función del contexto.

En entornos distribuidos, donde el acceso se produce desde múltiples ubicaciones y bajo condiciones variables, esta exigencia se vuelve especialmente relevante. La organización debe ser capaz de demostrar que mantiene un nivel de control razonable sobre su

operativa. No se exige eliminar todos los riesgos, pero sí gestionarlos de forma coherente, proporcional y justificable.

También resulta importante comprender el alcance real de estas normas. No imponen soluciones tecnológicas concretas ni obligan a centralizar completamente los sistemas. Tampoco prohíben el trabajo remoto. Lo que exigen es que el modelo de funcionamiento sea compatible con un nivel adecuado de seguridad. Este enfoque deja margen de decisión, pero al mismo tiempo exige criterio.

En la práctica, muchas organizaciones logran cumplir formalmente con determinados requisitos sin trasladar ese cumplimiento a la operativa real. Las políticas existen, pero no reflejan cómo se trabaja. Los controles están definidos, pero no se aplican de forma consistente. Esta brecha entre lo documentado y lo efectivo constituye uno de los principales focos de riesgo.

En entornos de trabajo remoto, esta diferencia se vuelve más visible. La dispersión del acceso y la diversidad de herramientas obligan a que las decisiones sean más explícitas y a que los controles estén alineados con la realidad operativa. La normativa no debe entenderse como un conjunto de obligaciones aisladas, sino como un marco que permite evaluar si la forma en que la organización trabaja es sostenible desde el punto de vista de la seguridad.

El eje no está en el cumplimiento formal, sino en la capacidad de sostener, en la práctica, un modelo de trabajo coherente con el nivel de riesgo asumido y jurídicamente defendible.

## **G. FALLOS FRECUENTES EN ENTORNOS DE TRABAJO REMOTO**

En muchas organizaciones, los problemas de seguridad no se explican por la ausencia total de controles, sino por la forma en que esos controles funcionan en la práctica. En entornos de trabajo remoto, la distancia entre lo previsto y lo que efectivamente ocurre se vuelve más visible, ya que el acceso está distribuido y las condiciones en las que se produce cambian de manera constante.



Los fallos más habituales pueden agruparse en tres grandes líneas. La primera se relaciona con una interpretación incompleta del acceso. La segunda con una confianza excesiva en las herramientas. La tercera con el desajuste entre lo documentado y la operativa real.

En relación con el acceso, uno de los errores más frecuentes consiste en asumir que un acceso autenticado equivale a un acceso seguro. La validación de credenciales sigue siendo necesaria, pero deja de ser suficiente cuando el acceso se realiza desde entornos que no están bajo control directo. Un usuario puede autenticarse correctamente y, sin embargo, operar desde un dispositivo comprometido, una red insegura o un entorno compartido. Desde el sistema, el acceso es válido, pero desde el punto de vista de la seguridad puede no serlo (Rose et al., 2020).

A este problema se suma la acumulación progresiva de accesos y permisos. A lo largo del tiempo, usuarios y cuentas técnicas reciben privilegios que responden a necesidades puntuales y que rara vez se revisan. En entornos distribuidos, donde la visibilidad es menor, estos accesos pueden mantenerse activos sin una justificación clara, ampliando el impacto potencial de cualquier incidente (Anderson, 2020). Las cuentas técnicas y las integraciones entre sistemas presentan un riesgo particular, ya que operan con credenciales que no siempre están sujetas a los mismos controles que las cuentas de usuario, pueden permanecer activas durante largos períodos y, si son comprometidas, el acceso resultante puede pasar desapercibido al integrarse en el funcionamiento habitual del sistema.

La segunda línea de fallos se vincula con la relación entre la organización y sus herramientas. Es frecuente encontrar una dependencia excesiva de las soluciones implementadas. La incorporación de una plataforma de seguridad puede generar una sensación de control que no siempre refleja la realidad. Se asume que el problema está resuelto por el simple hecho de utilizar una herramienta determinada, cuando en realidad el nivel de riesgo depende más de cómo se configura y se utiliza que del producto en sí mismo. Configuraciones por defecto que no se revisan, permisos abiertos sobre recursos sensibles y ausencia de controles periódicos son situaciones habituales en entornos cloud (ENISA, 2023).

En el extremo opuesto, también es común el uso de herramientas no previstas. En entornos de trabajo remoto, los usuarios suelen resolver necesidades operativas con servicios externos que no forman parte del entorno definido por la organización.

Compartir archivos mediante plataformas personales, utilizar aplicaciones de notas en la nube para redactar documentos o abrir canales de comunicación fuera de los medios oficiales son prácticas frecuentes. Estas decisiones no suelen responder a una intención de incumplir, sino a la necesidad de mantener la operativa frente a controles percibidos como restrictivos. Sin embargo, el efecto es el mismo, ya que se generan circuitos de circulación de información que escapan al control y sobre los que no pueden aplicarse medidas coherentes (Schneier, 2018).

La tercera línea de fallos es más difícil de identificar porque no genera señales evidentes. Muchas organizaciones conocen su infraestructura, pero no tienen una comprensión clara de cómo se utilizan sus herramientas en la práctica diaria. Sin esa visibilidad, resulta complejo detectar comportamientos anómalos o evaluar si los controles existentes son adecuados. A esto se suma una situación habitual en la que las políticas y los procedimientos están definidos, pero no reflejan el funcionamiento real de la organización. El cumplimiento se vuelve formal, mientras que en la práctica persisten situaciones de riesgo que no son objeto de atención.

En conjunto, estos fallos comparten un rasgo común. No suelen originarse en errores aislados ni en decisiones claramente incorrectas, sino en la acumulación de decisiones que, consideradas individualmente, resultan razonables. Conceder un acceso adicional para resolver una necesidad puntual, permitir el uso de una herramienta externa en un caso concreto o postergar la revisión de una cuenta técnica son acciones que pueden parecer menores. Sin embargo, su acumulación configura un entorno con un nivel de exposición mayor al previsto.

El análisis de la seguridad, en este contexto, no puede limitarse a verificar la existencia de controles. Debe centrarse en cómo esos controles funcionan en la práctica y en qué medida están alineados con la forma real de operar. La diferencia entre ambos planos es, en muchos casos, la que separa una seguridad aparente de una seguridad efectiva.

## **H. EVALUACIÓN PRÁCTICA DEL RIESGO EN ENTORNOS REMOTOS**

Evaluar la seguridad en entornos de trabajo remoto no consiste en verificar la existencia de controles ni en comprobar el cumplimiento formal de políticas. En la práctica, el

problema es más exigente. Se trata de entender cómo funciona realmente la organización y qué riesgos se derivan de esa forma concreta de operar.

Muchas evaluaciones parten de un enfoque documental. Se revisan procedimientos, configuraciones y herramientas implementadas. Este análisis es necesario, pero no suficiente. En entornos distribuidos, la distancia entre lo definido y lo que ocurre en la práctica suele ser significativa. El riesgo no se encuentra únicamente en lo que falta, sino en lo que no se observa (Anderson, 2020).

Por eso, el punto de partida debe ser el uso real.

Es necesario comprender cómo se accede a los sistemas, qué recorrido sigue la información y qué decisiones se toman en el día a día. Quién accede, desde dónde, con qué dispositivo y bajo qué condiciones no es un dato accesorio, sino el núcleo del análisis. La seguridad no se define en la arquitectura formal, sino en la forma en que esa arquitectura se utiliza (Rose et al., 2020).

En este contexto, evaluar el riesgo implica reconstruir situaciones concretas. No en abstracto, sino en términos operativos. Cómo accede alguien del equipo comercial al CRM cuando está fuera de la oficina. Qué pasa con un archivo cuando se comparte con un proveedor externo para una revisión. Cómo se reemplaza el acceso de un empleado cuando deja la empresa, o cómo se revisa el de uno que cambia de puesto. Estas situaciones no siempre están reflejadas en las políticas, pero forman parte del funcionamiento habitual, y es ahí donde suele concentrarse el riesgo real.

El valor de este enfoque es que permite detectar riesgos que no aparecen en una revisión estática.

En muchos casos, los controles existen, pero no cubren todas las situaciones en las que se utilizan los sistemas. Una medida puede ser técnicamente correcta y, sin embargo, no ser suficiente en la práctica. Evaluar el riesgo implica identificar esas diferencias y entender su impacto.

Otro aspecto central es la coherencia.

No se trata solo de analizar cada control de forma aislada, sino de entender cómo se combinan entre sí. Un acceso puede estar correctamente protegido en términos de autenticación, pero ser excesivo en cuanto a permisos. Una herramienta puede estar bien configurada, pero utilizarse fuera de los canales previstos. El riesgo surge de la

interacción entre estos factores, no necesariamente de uno solo (Saltzer & Schroeder, 1975).

Además, la evaluación debe considerar la capacidad de respuesta.

En entornos remotos, es fundamental entender qué ocurre cuando algo no funciona como debería. Si se detecta un acceso inusual o una posible exposición de datos, la organización debe poder identificar el problema, limitar su impacto y reconstruir lo sucedido. Sin esta capacidad, incluso un entorno con controles adecuados puede volverse frágil (ENISA, 2023).

También conviene evitar un error frecuente: evaluar la seguridad desde un modelo ideal que no se corresponde con la realidad de la organización. Este enfoque puede generar diagnósticos correctos en teoría, pero difíciles de aplicar. La evaluación debe partir de cómo se trabaja realmente, no de cómo debería trabajarse en un escenario perfecto (Schneier, 2018).

Esto no implica aceptar cualquier situación, sino priorizar.

No todos los riesgos tienen el mismo impacto ni requieren la misma respuesta. En entornos distribuidos, donde el control nunca es absoluto, la gestión del riesgo consiste en identificar qué es crítico, qué es tolerable y dónde es necesario intervenir. Este criterio permite tomar decisiones razonables sin intentar aplicar el mismo nivel de control a todas las situaciones.

Desde el punto de vista organizativo, este proceso no puede quedar limitado a un área técnica. Las decisiones que afectan a la seguridad involucran distintas áreas y niveles de la organización. La definición de qué información es crítica, qué herramientas se autorizan o qué nivel de riesgo se acepta son decisiones que trascienden al equipo de IT. Por eso, la evaluación del riesgo debe incorporar una mirada transversal, entendiendo cómo interactúan los distintos actores en la práctica.

En términos concretos, las evaluaciones más útiles no son las que generan mayor volumen de documentación, sino las que permiten identificar con claridad dónde están los problemas y qué decisiones pueden mejorar la situación. Esto implica traducir el análisis técnico en escenarios comprensibles y en acciones concretas.

En entornos de trabajo remoto, donde el riesgo es dinámico y se distribuye en múltiples puntos, la evaluación no es un proceso puntual, sino una forma continua de observar,

ajustar y tomar decisiones sobre cómo se trabaja. La guía que se presenta a continuación ofrece un conjunto de preguntas para realizar esa observación de forma estructurada, partiendo de la práctica concreta de la organización y no de un modelo ideal.

## **I. RESPONSABILIDAD ORGANIZATIVA Y TOMA DE DECISIONES**

En entornos de trabajo remoto, la seguridad no puede entenderse como un resultado automático de la tecnología ni como una función aislada. Es, en última instancia, el resultado de decisiones. Cada acceso habilitado, cada herramienta incorporada y cada nivel de control definido determinan las condiciones en las que se desarrolla la actividad.

Cuando ocurre un incidente, rara vez se explica por un único fallo técnico. Lo que aparece es el efecto acumulado de decisiones que definieron un determinado nivel de exposición. La tecnología puede fallar, pero lo que se analiza es si las condiciones en las que se operaba eran razonables en función del riesgo asumido (Anderson, 2020).

Desde el punto de vista jurídico, este criterio es consistente. La normativa no exige eliminar todos los riesgos, sino gestionarlos de forma adecuada, y que esa gestión pueda ser explicada. El principio de responsabilidad proactiva del Reglamento General de Protección de Datos (art. 5.2) obliga a la organización a ser capaz de demostrar el cumplimiento, no solo a cumplir. En el ámbito de la ciberseguridad, la Directiva NIS2 va en la misma dirección al establecer que los órganos de dirección de las entidades obligadas son responsables de supervisar la gestión del riesgo y de aprobar las medidas adoptadas (Directiva (UE) 2022/2555, art. 20). En ambos casos, la existencia de controles no es suficiente si no se puede explicar por qué son adecuados para la forma en que se trabaja.

Esto tiene una consecuencia que excede lo técnico.

Las decisiones que afectan a la seguridad involucran a distintos niveles de la organización. La definición de políticas, la asignación de recursos, la elección de herramientas y la gestión de accesos configuran el nivel real de seguridad, y su efectividad depende de la coherencia con la que se adoptan y se sostienen. La seguridad deja así de ser un problema operativo aislado y pasa a integrarse en la gestión de la organización.

En la práctica, esto se traduce en una exigencia concreta. La organización debe tener claridad sobre cómo toma decisiones en materia de seguridad. No se trata de generar estructuras complejas, sino de poder explicar criterios: por qué se habilitan determinados accesos, por qué se utilizan ciertas herramientas, por qué se aceptan determinados niveles de riesgo. Esa capacidad de explicación es la que permite sostener las decisiones en el tiempo y defenderlas frente a un auditor, un regulador o un tribunal.

En entornos de trabajo remoto, donde las condiciones cambian con rapidez, esta claridad resulta especialmente importante. Las soluciones que funcionan en un momento pueden dejar de ser adecuadas si cambia la forma de trabajar o el contexto tecnológico. Sin un criterio definido, la seguridad tiende a ajustarse de forma reactiva, incrementando la probabilidad de inconsistencias (Schneier, 2018).

A esto se suma un problema frecuente: la falta de alineación entre lo que la organización declara y lo que efectivamente hace. Las políticas existen, pero no siempre reflejan la operativa real. Esa diferencia no solo afecta la eficacia de los controles, sino también la capacidad de justificar las decisiones. Cuando lo documentado no coincide con la práctica, la organización pierde consistencia y se expone a una situación particularmente incómoda: explicar un incidente apoyándose en políticas que el propio incidente demuestra que no se aplicaban.

El trabajo remoto no elimina esta responsabilidad. La hace más visible. Al distribuir el acceso y reducir el control directo, obliga a que las decisiones sean más explícitas y los criterios mejor definidos. En ausencia de ese marco, la organización tiende a operar por inercia, acumulando decisiones que pueden generar un nivel de exposición mayor al esperado.

En definitiva, la seguridad en entornos de trabajo remoto no se define únicamente por los sistemas que se protegen, sino por la forma en que se decide protegerlos. Y esa forma tiene que poder contarse. Una seguridad que no puede explicarse no es, en sentido estricto, una seguridad defendible.

## **J. GUÍA PRÁCTICA DE REVISIÓN**

Cuando un equipo de una empresa se plantea revisar la seguridad de su operación en remoto, suele ser útil bajar la discusión a preguntas concretas, de las que se hacen en una

reunión operativa. No se trata de una auditoría formal ni de un checklist de cumplimiento. Es una forma de observar la organización desde dentro, a partir de cómo efectivamente se trabaja.

Las preguntas se agrupan en cuatro bloques, siguiendo la lógica de las secciones anteriores de este documento: identidad y accesos, dispositivos e información, detección y respuesta, y gobierno. Si a una pregunta no se puede responder con claridad, eso ya es información útil: indica dónde conviene mirar.

#### Identidad y accesos

- ¿Sabemos qué sistemas y qué datos son accesibles en remoto, y qué personas tienen ese acceso hoy?
- ¿Los accesos remotos están protegidos con autenticación robusta, o dependen únicamente de contraseñas?
- ¿Los permisos que tiene cada persona se corresponden con lo que hace actualmente, o arrastran acumulaciones de funciones anteriores?
- ¿Tenemos control sobre las cuentas técnicas y las integraciones entre sistemas, sabiendo cuáles están activas, qué permisos tienen y si todavía se usan?

#### Dispositivos e información

- ¿Conocemos desde qué dispositivos se accede a nuestros sistemas, y hay criterios mínimos de seguridad para esos dispositivos?
- ¿Hay reglas claras sobre el uso de equipos personales y redes externas, especialmente cuando se accede a información sensible?
- ¿Las herramientas que se usan para compartir, almacenar o procesar información están definidas, o cada persona resuelve con lo que tiene a mano?
- ¿Sabemos por dónde circula realmente la información crítica, o solo sabemos dónde se supone que debería estar?

#### Detección y respuesta

- ¿Tenemos registros suficientes para saber qué ha pasado cuando algo sale mal, o nos quedamos sin información precisamente en el momento en que la necesitamos?

- ¿Sabríamos reaccionar ante incidentes comunes como un correo comprometido, un portátil extraviado o una exposición accidental de datos?
- ¿Podríamos reconstruir, en caso de incidente, quién accedió a qué, desde dónde y cuándo, sobre los datos más críticos?
- ¿Podríamos cumplir el plazo de 72 horas para notificar una violación de seguridad, si tuviéramos que hacerlo mañana?

#### Gobierno y decisiones

- ¿Las políticas y procedimientos reflejan cómo se trabaja realmente, o son un documento que solo se abre cuando hay una auditoría?
- ¿La dirección conoce los principales riesgos asociados al trabajo remoto y participa en las decisiones de seguridad, o lo delega por completo en el área técnica?
- ¿Podríamos explicar, frente a un auditor, un regulador o un cliente importante, por qué hemos tomado las decisiones de seguridad que hemos tomado?

Si estas preguntas no tienen una respuesta clara, lo más prudente no es añadir controles nuevos sino entender primero qué está pasando. Incorporar más herramientas sobre una base que no se conoce bien suele generar una sensación de progreso sin reducir el riesgo real. La seguridad efectiva, en entornos de trabajo remoto, depende menos de cuánto se implementa y más de cuánto se entiende de cómo se trabaja.

## K. CONCLUSIÓN

El trabajo remoto ha transformado las condiciones en las que las organizaciones gestionan la seguridad, desplazando el foco desde entornos controlados hacia un modelo distribuido en el que el acceso, los dispositivos y los servicios se encuentran fuera del control directo. Este cambio no introduce únicamente nuevos riesgos, sino que modifica la forma en que esos riesgos deben ser comprendidos y gestionados.

A lo largo del análisis se ha puesto de manifiesto que la seguridad ya no puede sostenerse sobre modelos perimetrales ni sobre la mera implementación de herramientas. La gestión de identidades y accesos, la visibilidad sobre el uso real de los sistemas y la coherencia



entre las políticas y la operativa se convierten en elementos centrales para determinar el nivel de exposición.

Asimismo, el tratamiento de datos en entornos remotos refuerza la necesidad de integrar la dimensión técnica con la jurídica. Las obligaciones normativas no se ven atenuadas por la descentralización del trabajo, sino que exigen una adaptación de los controles a un contexto más dinámico y menos homogéneo. En este sentido, la capacidad de justificar las decisiones adoptadas adquiere un papel clave.

En la práctica, los principales fallos no suelen derivarse de la ausencia de medidas, sino de la desconexión entre los controles definidos y la forma en que la organización opera. Por ello, la evaluación del riesgo debe centrarse en el uso real de los sistemas y en las condiciones efectivas de acceso, más que en el cumplimiento formal de estructuras predefinidas.

En definitiva, la seguridad en entornos de trabajo remoto no depende únicamente de la tecnología implementada, sino de la capacidad de la organización para alinear sus decisiones, sus controles y su modelo operativo con el nivel de riesgo que asume. Es en esa coherencia donde se determina si el modelo de trabajo puede sostenerse de forma segura y jurídicamente defendible.

## REFERENCIAS

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. *Diario Oficial de la Unión Europea*, L 333, 80–152.

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. *Diario Oficial de la Unión Europea*, L 119, 1–88.

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero. *Diario Oficial de la Unión Europea*, L 333, 1–79.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308. <https://doi.org/10.1109/PROC.1975.9939>

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W. W. Norton & Company.