Detecta y controla cualquier brecha de seguridad en tu red empresarial

Implanta medidas de ciberseguridad que exigen la LOPD, ENS e ISO 27001

- Registro de accesos realizados a archivos y aplicaciones
- Monitorización de la actividad de los usuarios
- Restricción de usos no autorizados del ordenador
- Función de cifrado para datos confidenciales
- Control de datos copiados a dispositivos extraíbles
- Supervisión dentro y fuera de la oficina

etseguridad
by edorteam

¿Por qué es fundamental monitorizar la actividad?

La ley exige registrar los accesos realizados a ficheros y programas que contengan datos de carácter personal

Registrar y limitar la actividad realizada en los equipos informáticos no es un gesto de desconfianza hacia tus trabajadores, es una de las **medidas de seguridad** que exigen la LOPD y el RGPD, así como también el **Esquema Nacional de Seguridad** (ENS) y el **estándar ISO 27001** para los Sistemas Gestión de la Seguridad de la Información (SGSI).

- **El art. 103.1 de la LOPD** establece que “de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o no”.
- **El art. 91**, por su parte, exige “limitar el acceso únicamente a aquellos recursos que los usuarios precisen para el desarrollo de sus funciones”.
- Sobre el transporte de datos de carácter personal, **el art. 92.3** establece que “se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte”.

¿Cumples con estas medidas de seguridad obligatorias?

Puede que ya cuentes con un servicio de protección de datos, pero si aún no aplicas en tu red empresarial **todas estas medidas de ciberseguridad** para la detección y control de brechas de datos, **estás incumpliendo la ley**:

Monitorización 24/7 de la actividad que realizan los usuarios en los equipos informáticos, dentro y fuera de la oficina.

Registro de los accesos realizados a archivos y aplicaciones. Control de usos no autorizados del equipo informático.

Herramienta para el cifrado seguro y eficaz de archivos, carpetas y dispositivos USB.

Registro y control de los datos copiados a **unidades extraíbles USB**.

¿De qué me sirven estas medidas de seguridad informática?

Estas medidas responden al **principio de responsabilidad activa:** todas las empresas que traten datos personales deben adoptar medidas de prevención suficientes para cumplir con los principios, derechos y garantías establecidos en la LOPD y el RGPD. Esto significa que, hoy en día, actuar en caso de incidencia es insuficiente. Debemos adoptar una serie de **medidas de prevención y buenas prácticas**.

A continuación hemos recopilado algunas **sentencias reales de empresas sancionadas** por la AEPD que **se podrían haber evitado de contar** con un software de monitorización y control de la actividad como ET Seguridad.

Que no te pase lo mismo que a estas empresas

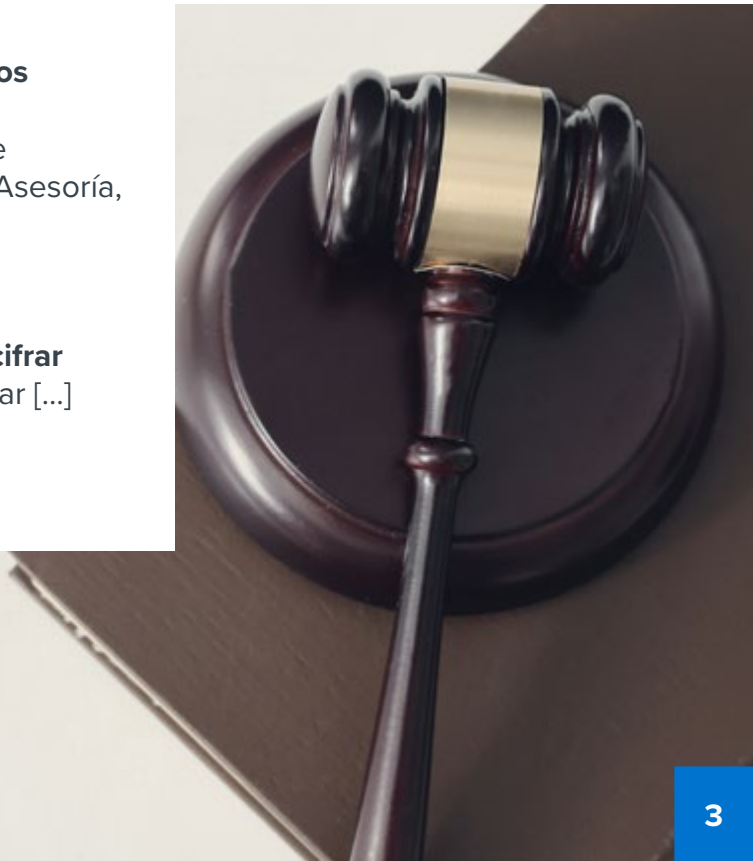
» **40.000€ a Vodafone España, por deficiencia en el registro y control de accesos**
"Consta acreditado que se produjeron accesos no autorizados por parte de terceros a los registros de llamadas (CDRs) [...] Asimismo, [...] no disponía de un sistema de logs para identificar los accesos a los CDRs..."
Enlace a la resolución >

» **20.000€ a Amazon España, por acceso no autorizado a datos de clientes**
"Utilizando la red corporativa, a la que se accedía con los valores de usuario y clave del servicio VPN, este usuario no autorizado se conectó al servidor [...] Una vez conectado el intruso al servidor [...], accedió a la base de datos de clientes de BUY VIP..."
Enlace a la resolución >

» **3.600€ a Efron Consulting, por deficiencia en el registro y control de accesos**
"Accesos injustificados [...] desde el usuario denominado "ADMINISTRADOR", que es utilizado por todas las personas que trabajan en dicha gestión..."
Enlace a la resolución >

» **3.000€ a Asesoría Alpi-Clúa por envío de datos personales de otro cliente sin cifrar**
"Aporta el email y un recibo de presentación de documentación ante Hacienda por parte de la Asesoría, con indicación de datos de otro cliente..."
Enlace a la resolución >

» **60.000€ a RTVE, por pérdida de un USB sin cifrar**
"Desaparición de dispositivos extraíbles sin cifrar [...] que contenían datos personales..."
Enlace a la resolución >



etseguridad
by edorteam

Protege tu negocio
y sus datos almacenados

Logra el cumplimiento total de los estándares de ciberseguridad

ET Seguridad es un **software de monitorización y productividad empresarial** diseñado para controlar la actividad que se realiza en los equipos informáticos de la empresa.

Seguridad y control de accesos

» Monitoriza quién **accede, elimina o modifica** archivos en todo momento.
» **Controla la navegación por internet** e impide usos no autorizados del equipo.
» Registra qué se copia en los **dispositivos extraíbles USB**.

Mejora la productividad de tu empresa

» Calcula el tiempo de uso real de las aplicaciones y detecta la **ausencia de actividad**.
» Programa la toma de **capturas de pantalla** periódicas.
» Obtén **informes de productividad** y justifica el tiempo invertido en proyectos de clientes.

Cumplimiento jurídico garantizado

» Al iniciar sesión, **muestra el aviso LOPD** para que el usuario dé conformidad.
» Los registros se almacenan en la nube durante **48 meses**, como exige la LOPD.
» Supervisión **dentro y fuera de la oficina**, en cumplimiento de la Ley del Teletrabajo.
» Incluye una **aplicación de fichaje** segura y eficaz (Ley de Registro Horario).
» Y además, **cifra archivos** con ET Encrypt, incluido con ET Seguridad.

Descubre todo lo que puedes hacer con ET Seguridad

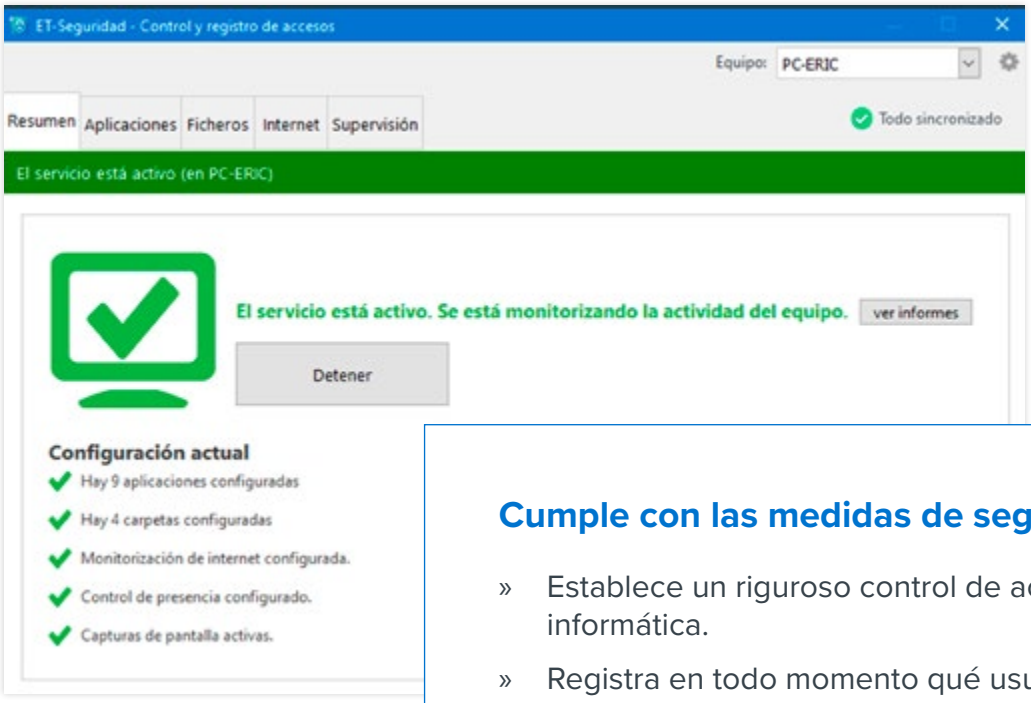
Acompáñanos por sus múltiples funciones en este breve recorrido

Instala el software en los equipos a monitorizar y gestiónalo todo desde la nube

» Una vez configurado, podrás gestionarlo todo desde tu panel de administración en la nube, tan solo necesitas conexión a internet.

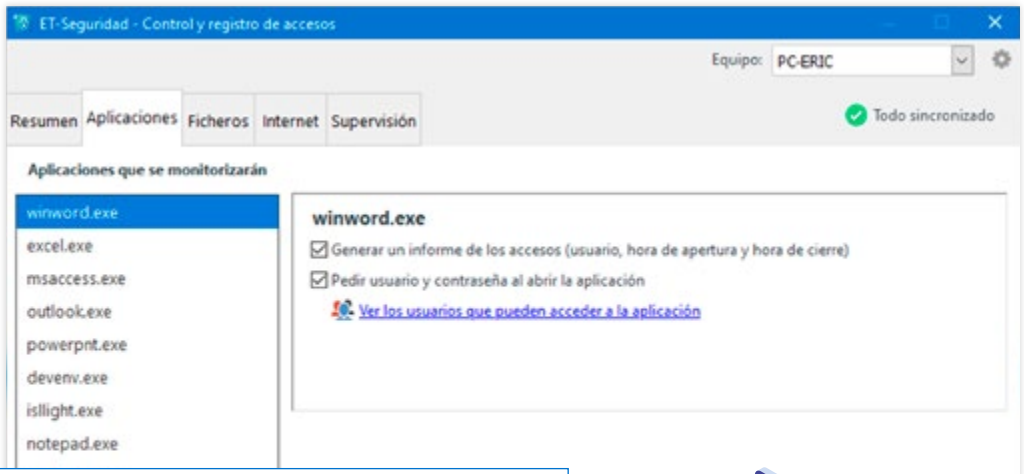
» El software muestra avisos si un equipo está fuera de conexión o en caso de incidencia.

» Aunque un equipo pierda la conexión a internet, **se seguirá monitorizando su actividad** y sus datos se actualizarán tras recuperar la conexión.



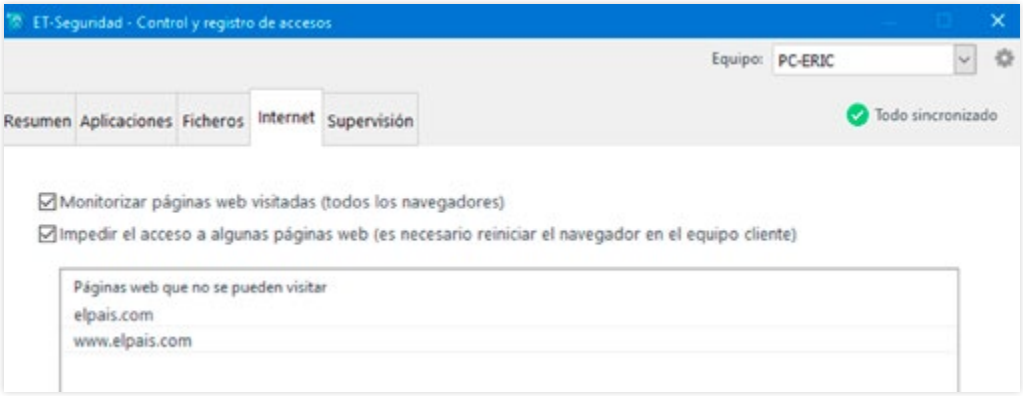
Cumple con las medidas de seguridad de datos

- Establece un riguroso control de accesos en toda tu red informática.
- Registra en todo momento qué usuario accede, elimina o modifica cualquier archivo.
- Controla también qué se copia a dispositivos USB.
- Los registros se mantienen durante 48 meses.
- Cada vez que un usuario inicia sesión, debe dar conformidad al aviso LOPD, que le **informa sobre la monitorización de su actividad** tal y como exige la ley.



Protege el acceso a aplicaciones y ficheros

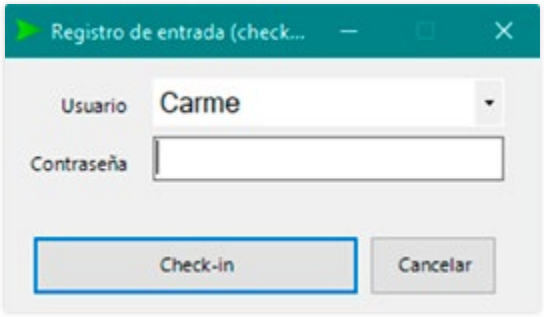
- **Impide el acceso a archivos y funciones** del equipo.
- Solicita contraseñas para abrir ciertos programas.
- Administra esos permisos según el usuario que inicie sesión en Windows (útil para equipos compartidos).

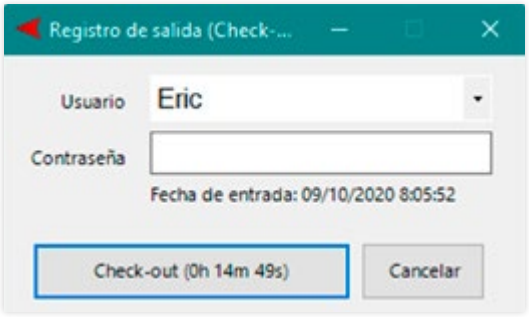


Navegando por internet puede instalarse *malware* que cause problemas en el equipo o, peor aún, una brecha de seguridad.

Controla la navegación por internet

- Limita el acceso a las páginas web que tú decidas.
- Revisa el historial de navegación **aunque se use la navegación privada.**
- Funciona con todos los navegadores.





Sácale partido a la función de registro horario

- Tus trabajadores podrán registrar el inicio y final de su jornada laboral en sus equipos informáticos.
- Establece horarios para que la ventana para fichar aparezca a las horas indicadas.
- Configura, si lo deseas, un *check-out* automático tras detectar varios minutos de inactividad en el equipo.
- Exporta el registro horario de cada trabajador y comprueba si cumplen con su jornada laboral.
- **Cumple con la Ley de Registro Horario**, obligatoria para todas las empresas.
- Incluido con ET Seguridad sin coste adicional.

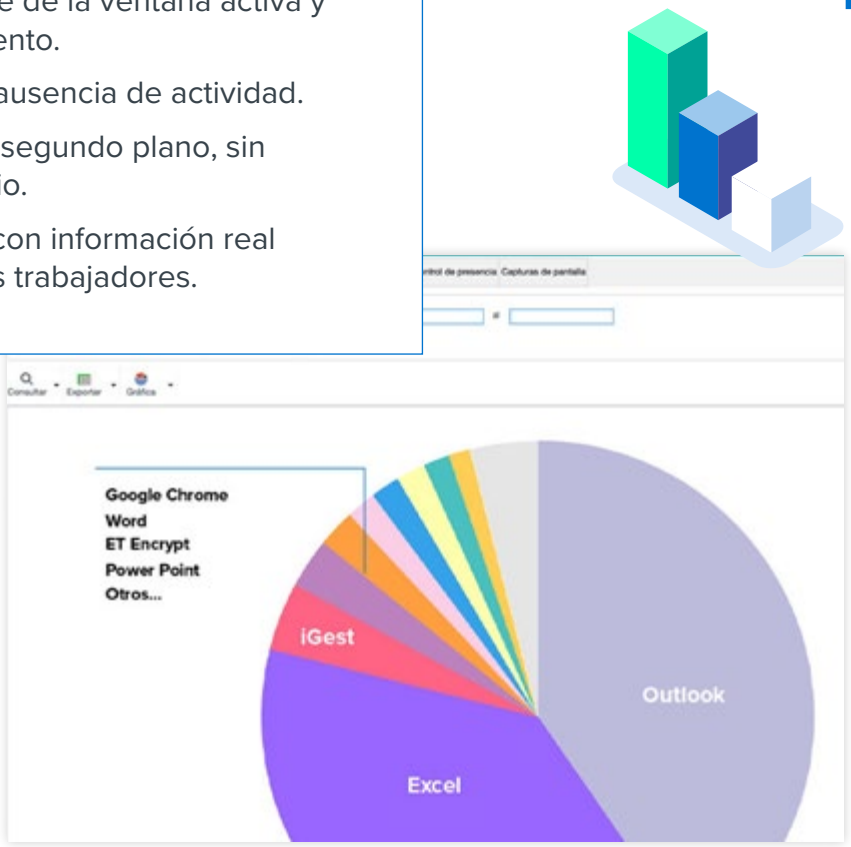
Supervisa la actividad laboral de tus trabajadores

» ET Seguridad registra el nombre de la ventana activa y el tiempo de uso en todo momento.

» También calcula el tiempo con ausencia de actividad.

» La monitorización se realiza en segundo plano, sin perturbar la actividad del usuario.

» **Genera informes estadísticos** con información real sobre la actividad laboral de tus trabajadores.



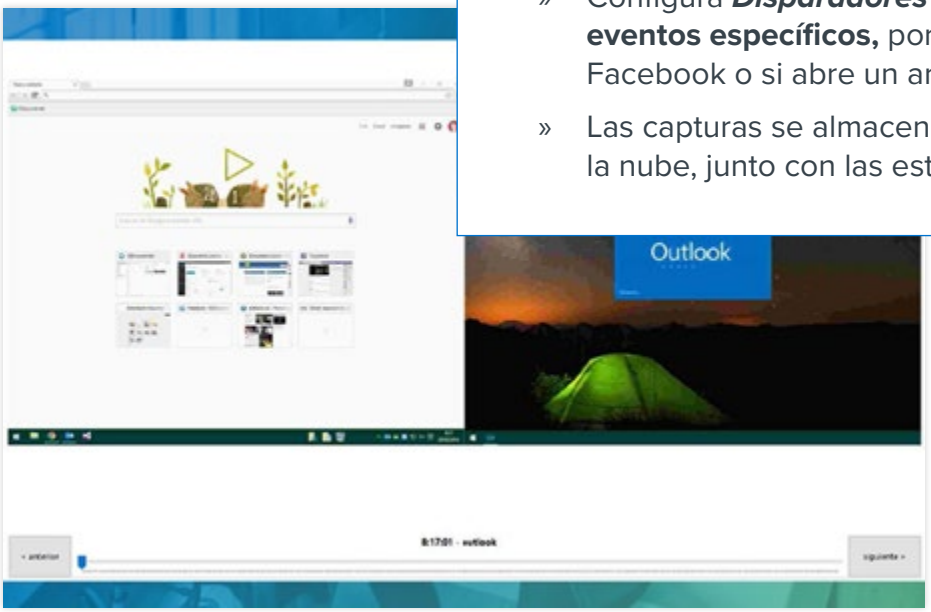
Gracias a los informes de productividad, el tiempo de dedicación de tu equipo al desarrollo de un proyecto quedará documentado.

Programa la toma de capturas de pantalla

» Configura la toma automática de capturas de pantalla con la periodicidad que desees.

» Configura ***Disparadores*** **que se activarán ante eventos específicos,** por ejemplo: si el usuario visita Facebook o si abre un archivo determinado.

» Las capturas se almacenan para su visualización en la nube, junto con las estadísticas de uso.



etencrypt
by edorteam

Y además... cifra ficheros y USB con ET Encrypt

Herramienta de cifrado AES 256, incluida con ET Seguridad

Cifra archivos y carpetas

- Protege con contraseña tus datos almacenados tal y como exige el **art. 34 del RGPD**.
- Cifra **cualquier tipo de archivo** que tengas en tu ordenador.
- **Cifra carpetas** y todo su contenido con una única acción.

Envía datos cifrados por internet

- Envía por internet documentos adjuntos que contengan **datos confidenciales**.
- Los archivos se pueden descifrar con nuestro **descifrador online**.
- **No es necesario** que el destinatario tenga instalado ET Encrypt.

Protege también unidades USB

- ET Encrypt permite cifrar dispositivos de **almacenamiento extraíble USB**.
- Descifra la información **en cualquier equipo**, tenga o no instalado ET Encrypt.
- **Si pierdes tu dispositivo**, nadie podrá acceder a la información.

¿Por qué debo cifrar los archivos y unidades USB con datos personales?

Porque podrías ser víctima de un **ataque informático o cometer un error humano** (como confundirse de destinatario de e-mail o perder el USB) y esa información caería en manos ajenas, ocasionando una **brecha de seguridad**. Por este motivo, si la información estaba cifrada, jamás podrán acceder al contenido.

Incidentes que pueden causar una brecha de datos personales y cómo evitarlos con ET Seguridad

La AEPD recoge en su *Guía para la notificación de brechas de datos personales* los incidentes que pueden causar de una brecha de seguridad.

INCIDENCIA GUÍA	¿CÓMO LA SOLUCIONA ET SEGURIDAD?
Modificación o eliminación no autorizada de datos personales	» Configura perfiles de usuario para limitar accesos y funciones del equipo informático. » En caso de incidente, el registro de actividad determinará quién y cuándo eliminó o modificó los datos.
Abuso de privilegios de acceso para extraer, reenviar o copiar datos personales	» Configura perfiles de usuario para limitar accesos y funciones del equipo informático. » Controla el acceso a ciertos ficheros con usuario y contraseña. » En caso de incidente, el registro de actividad determinará quién, cuándo y qué acciones realizó en el equipo informático.
Datos personales enviados por error de forma electrónica	» Usa la herramienta ET Encrypt para cifrar preventivamente cualquier documento con datos personales que vayas a enviar por internet. Así, en caso de error humano, evitarás que lean el contenido.
Dispositivo perdido o robado	» Usa la herramienta ET Encrypt para cifrar tus dispositivos extraíbles USB de forma preventiva. Así, en caso de pérdida o robo, evitarás que accedan a su contenido.
Ciberataque: acceso no autorizado a datos personales	» Configura perfiles de usuario para impedir accesos no autorizados a la información confidencial. » Controla el acceso a los documentos que contengan datos personales con usuario y contraseña, o almacénalos siempre cifrados.

Recuerda que, si siempre cifras preventivamente los documentos que contengan datos personales, no será necesario notificar a la AEPD en caso de producirse un ciberincidente o error humano.

Y además... La última capa de seguridad para el cumplimiento con ISO 27001

Cada vez es más frecuente que **el sector público y grandes empresas exijan** la certificación con ISO 27001 a sus proveedores.

Su cumplimiento garantiza que la gestión de la seguridad de la información de la empresa se efectúa **conforme a este estándar internacional.** Se prevé que este requisito será cada vez más demandado, ya que con la digitalización de las empresas **cada vez somos más dependientes de la tecnología** y de los datos que manejamos con ella. Por lo tanto, es lógico exigir a nuestros proveedores y colaboradores que demuestren una correcta y competente gestión de su ciberseguridad.

Cumple con la mayor parte de la ISO 27001 con ET Seguridad

Sus múltiples funciones otorgan **cumplimiento en 9 de las 14 secciones de la ISO 27001:**

- **Artículo 6: Organización de la seguridad de la información** (artículos 6.2.1 y 6.2.2).
- **Artículo 8: Gestión de activos** (artículos 8.2.2 y 8.3.1).
- **Artículo 9: Control de acceso** (artículos 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.1, 9.4.2, 9.4.3 y 9.4.5).
- **Artículo 10: Criptografía - Cifrado y gestión de claves** (artículo 10.1.1).
- **Artículo 12: Seguridad de las operaciones** (artículos 12.1.2, 12.4.1, 12.4.2, 12.4.3, 12.5.1, 12.6.2, y 12.7.1).
- **Artículo 13: Seguridad de las comunicaciones** (artículos 13.1.1 y 13.2.1).
- **Artículo 14: Adquisición, desarrollo y mantenimiento de los sistemas** (artículo 14.2.2).
- **Artículo 16: Gestión de incidentes de seguridad de la información** (artículos 16.1.2, 16.1.4, 16.1.5 y 16.1.7).
- **Artículo 18: Cumplimiento** (artículos 18.1.3, 18.1.4 y 18.1.5).

¿Empezamos?

Alcanza el cumplimiento total de los estándares de ciberseguridad

Solicita tu oferta personalizada aquí
www.edorteam.com/oferta-seguridad/

edorteam
DESDE 1992

Madrid
C/ Isabel Colbrand 6, 5º
28050 Madrid
91 344 69 10

Lleida
Avenida Madrid 38, 2º-2ª
25002 Lleida
973 248 601

info@edorteam.com

www.edorteam.com