Automatización y eficacia: El camino de ITSAP hacia la ISO 27001

La empresa

Fundada en 1996, O2 ha crecido hasta convertirse en la principal empresa francesa de servicios personales, gracias en particular a su departamento de TI y a su software empresarial. En 2023, el departamento informático de O2, posteriormente rebautizado ITSAP, se convirtió en una **ESN, especializada en sistemas de información para servicios personales,** dentro del grupo Oui Care.

El CISO y sus retos

Dimitri Bouron lleva 10 años trabajando en ITSAP, inicialmente como técnico de soporte y administrador de sistemas y redes. Hace tres años y medio asumió el rol de CISO, coincidiendo con la creación del departamento de seguridad.

Dimitri se enfrentaba al reto de construir desde cero el departamento de seguridad y cumplir con estrictos requisitos normativos, todo ello con recursos limitados: un equipo compuesto únicamente por un estudiante a tiempo parcial y él mismo.

El sector sanitario está altamente regulado, destacando, por ejemplo, los requisitos HDS para los proveedores de alojamiento y gestión de instalaciones. En este contexto, ITSAP ha tomado medidas importantes para garantizar la fiabilidad de su SI y la confianza de sus clientes:

- **Creación de un puesto de CISO en 2021.**
- Lanzamiento de un proyecto de certificación ISO 27001 y HDS.

Dimitri necesitaba una solución integral que le permitiera:

- **Gestionar los objetivos de seguridad y cumplimiento de sus múltiples entidades**.
- **Implementar un SGSI** que incluyera toda la estructura y los procesos necesarios, especialmente en el contexto de la certificación ISO 27001.
- **Proteger** eficazmente su organización con **recursos limitados**.

La automatización y la **conformidad** eran, por tanto, los dos principales retos a los que se enfrentaba el CISO en su búsqueda.

La elección de Tenacy

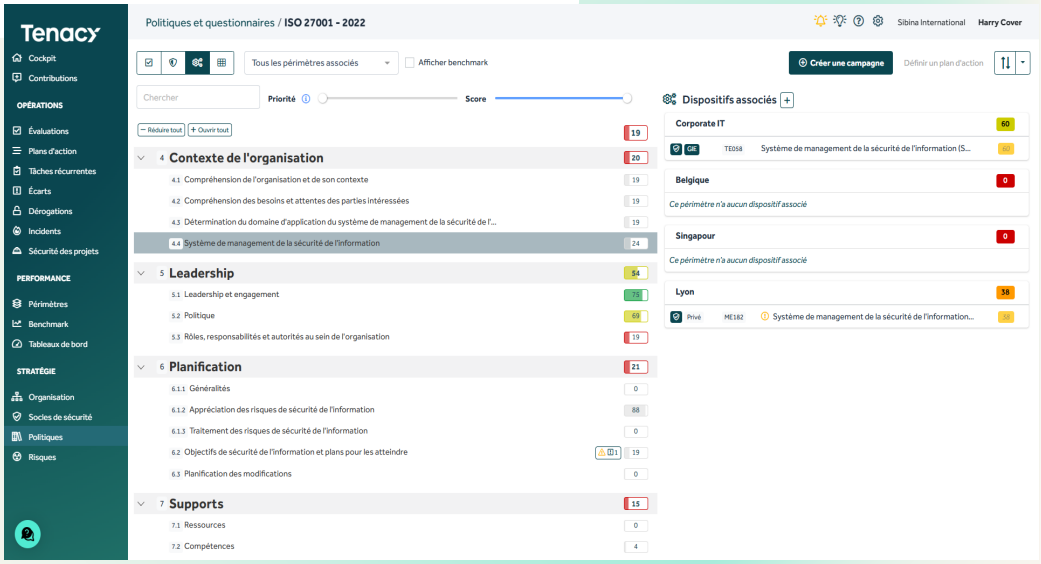
A finales de 2021, ITSAP identificó preocupaciones relacionadas con la norma HDS para la subcontratación. Dado que HDS requiere la certificación ISO 27001, Dimitri Bouron, CISO de ITSAP, tomó la decisión de **auditar su SI con el objetivo de obtener dicha certificación.**

Para ello, se llevó a cabo una auditoría previa que permitió **evaluar el nivel de madurez de la empresa frente a los requisitos de la norma**, lo que representó una inversión significativa, ya que un servicio de este tipo puede tener un coste de entre 5.000 y 10.000 euros.

Sin embargo, unos meses después de esta auditoría, **la versión de la norma ISO 27001 cambió**, haciendo imposible obtener la certificación con la versión de 2013. En consecuencia, ITSAP no pudo conseguir la nueva certificación HDS, ya que esta seguía requiriendo la ISO 27001:2013.

El CISO se vio obligado a empezar de cero, una situación complicada que le llevó a darse cuenta de la necesidad de una solución para **agilizar el cumplimiento normativo**. **Tenacy fue la solución elegida por Dimitri para satisfacer esta necesidad.**

> "Una auditoría previa HDS/ISO 27001 puede costar entre 5.000 a 10.000 euros, o incluso hasta 20.000 con apoyo adicional. **Gracias a Tenacy, pude realizar una autoevaluación guiada, reduciendo estos costes sin comprometer la eficiencia.**"



Etapa 1: autoevaluación

Dimitri no quería someterse de inmediato a una auditoría previa sin tener la garantía de que su contexto sería correctamente entendido ni de que recibiría las claves adecuadas para mejorar. Por ello, el CISO optó por **comenzar con una autoevaluación a través de Tenacy**, lo que le permitió evaluar su nivel de madurez respecto a los requisitos de la norma ISO 27001 y, además, **obtener un plan de acción adecuado** para guiar sus esfuerzos de cumplimiento y estructurar sus procesos.

> "Tenacy me permitió **crear y formalizar un SGSI completo desde cero en tan solo un año**."

> "Una de las ventajas clave de Tenacy es su capacidad para permitir una autoevaluación guiada. La plataforma muestra las medidas de seguridad asociadas a cada requisito, lo que permite comprender fácilmente tu nivel de cumplimiento sin depender de asesoramiento externo en cada etapa."

Bonus: Tenacy incluye ISO 27001, ISO 27002 y HDS (¡y muchas otras normas!). Cada texto se basa en un catálogo común de medidas de seguridad. Gracias a este enfoque de **multiconformidad**, cuando actualices un texto, solo necesitarás un minuto en para verificar con qué normas sigues cumpliendo y qué acciones aún te quedan por realizar.

Inicialmente, el CISO decidió basar su evaluación de madurez en la existencia (o ausencia) en ITSAP de las medidas de seguridad exigidas por la norma ISO 27001. Este inventario de medidas existentes le proporcionó a Dimitri **una puntuación inicial de conformidad en Tenacy**, así como un plan de acción claro para implementar las medidas de seguridad necesarias como parte del proceso de certificación.

Etapa 2: plan de acción

Al cabo de un año y medio, tras haber implantado todas las medidas de seguridad requeridas, Dimitri realizó una nueva autoevaluación. Su objetivo era evaluar la eficacia de las medidas de seguridad implementadas y obtener una puntuación de conformidad más precisa y fiable.

Basándose en estos resultados y en las sugerencias proporcionadas por la plataforma Tenacy, **desarrolló un plan de acción** para optimizar la eficacia de sus medidas de seguridad. Un ejemplo destacado de mejora fue el diseño de un nuevo método de gestión de riesgos basado en Ebios RM e ISO 27005, utilizando Tenacy como herramienta clave. Esto le brindó mayor flexibilidad en sus análisis, y le permitió cumplir con los requisitos de HDS desde el principio.

Los controles permanentes

La plataforma también se puede utilizar para supervisar los controles continuos (conocidos como tareas recurrentes) que **forman parte del proceso de cumplimiento**, suguiendo un conjunto claro de procedimientos:

- ¿Se ha completado la tarea?
- ¿Ha dado la comprobación el resultado esperado?

La **puntuación de cumplimiento se actualiza en tiempo real en función de los resultados** de estas comprobaciones. De esta forma, Tenacy ofrece a ITSAP una **visibilidad diaria de sus avances en materia de conformidad**. Además, el vínculo entre las operaciones diarias y las puntuaciones ayuda a evitar cualquier falsa sensación de seguridad, ya que no sólo se considera la existencia de la medidas, sino también su eficacia para proteger a la organización.

Bonus: el CISO puede colaborar con los equipos de infraestructura y soporte, quienes introducen algunas respuestas en Tenacy (por ejemplo, confirmando si se ha llevado a cabo la limpieza de las cuentas inactivas de Google). Dimitri puede, a partir de ahí, verificar las acciones realizadas, consultar el historial de cada elemento y realizar el seguimiento necesario.

Enfoque en la automatización

Supervisar el cumplimiento normativo implica gestionar un gran número de indicadores, que a menudo están dispersos en múltiples herramientas. Tenacy permite **centralizar estas métricas** e incluso **automatizarlas**, como lo ha hecho Dimitri utilizando la API de Tenacy. Al desarrollar varios scripts, el CISO ha automatizado la generación de informes de sus indicadores. Como resultado, **sus cuadros de mando en Tenacy se actualizan automáticamente**, sin necesidad de intervención manual.

Se trata de una función muy útil para las revisiones del SGSI que Dimitri presenta en las reuniones del comité de dirección. Antes de Tenacy, el CISO tenía que exportar los resultados brutos a Google Sheets, realizar los cálculos, formatear los datos y colocarlos en sus diapositivas, un proceso que podía llevarle hasta una semana. Ahora, todo lo que necesita hacer es copiar y pegar los gráficos generados por Tenacy en su presentación. **En tan solo 30 minutos, todo está listo.**

> “Gracias a Tenacy, he multiplicado casi por diez mi capacidad para obtener certificaciones. Lo que antes me llevaba días al introducir las métricas manualmente, ahora solo me lleva 30 minutos.”

De este modo, Dimitri puede dedicar su tiempo a analizar estos resultados (explicaciones, acciones a emprender, etc.), lo que constituye su verdadero valor añadido como CISO. El experto ahorra tiempo, tiempo que puede invertir en su “verdadero” trabajo.

> “La automatización en Tenacy me ha permitido **eliminar tareas repetitivas**. Donde antes realizaba todo manualmente, ahora puedo **dedicar mi energía a interpretar los resultados y tomar decisiones**.”

Etapa 3: certificación

¿El objetivo de Dimitri? **Solicitar una preauditoría ISO 27001 a finales de 2025**, con vistas a **obtener la certificación en 2026**. El CISO ya no necesita realizar preauditorías periódicas, ya que puede supervisar el progreso de sus esfuerzos directamente en Tenacy y elegir el momento en que todo esté listo.

Al mismo tiempo, Dimitri y su asistente están trabajando en la certificación HDS 2.0, publicada recientemente y que ahora exige la norma ISO 27001:2022. Gracias a la **modelización del marco** disponible en Tenacy y al enfoque de multiconformidad de la plataforma, el equipo de SSI puede visualizar fácilmente lo que queda por hacer una vez cumplidos los requisitos de la ISO 27001. **Con Tenacy, un equipo de dos expertos puede gestionar múltiples conformidades en varios perímetros.**

> "Personalmente, me resulta difícil imaginar cómo, por mí mismo, podría haber gestionado todo el trabajo que implica evaluar el rendimiento y dirigir el SGSI. **Tenacy simplifica y automatiza muchas tareas** que, de otro modo, habría tenido que gestionar manualmente en Excel, como los cuadros de mando y las evaluaciones de rendimiento, a la vez que guía el proceso."

Gracias a Tenacy, el CISO de ITSAP puede gestionar múltiples cuestiones de cumplimiento, elaborar informes precisos y ahorrar tiempo en el día a día. Una prueba de que se puede hacer mucho (en términos de protección) con poco (en términos de recursos humanos), siempre que se disponga de la herramienta adecuada. ¡Reserva una demostración y descubre más!