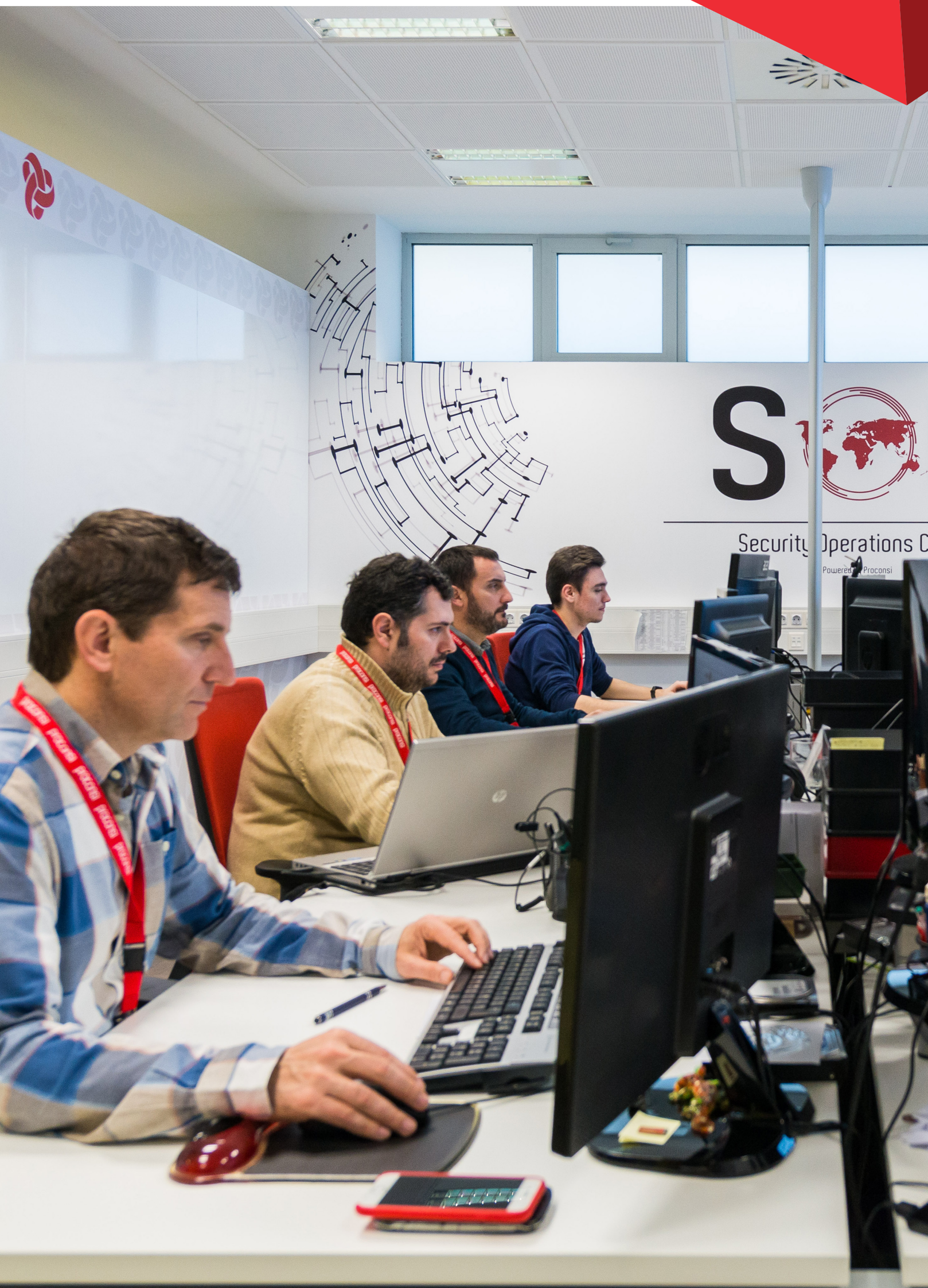
Soluciones en Ciberseguridad


Security Operations C
Powered by Proconsi

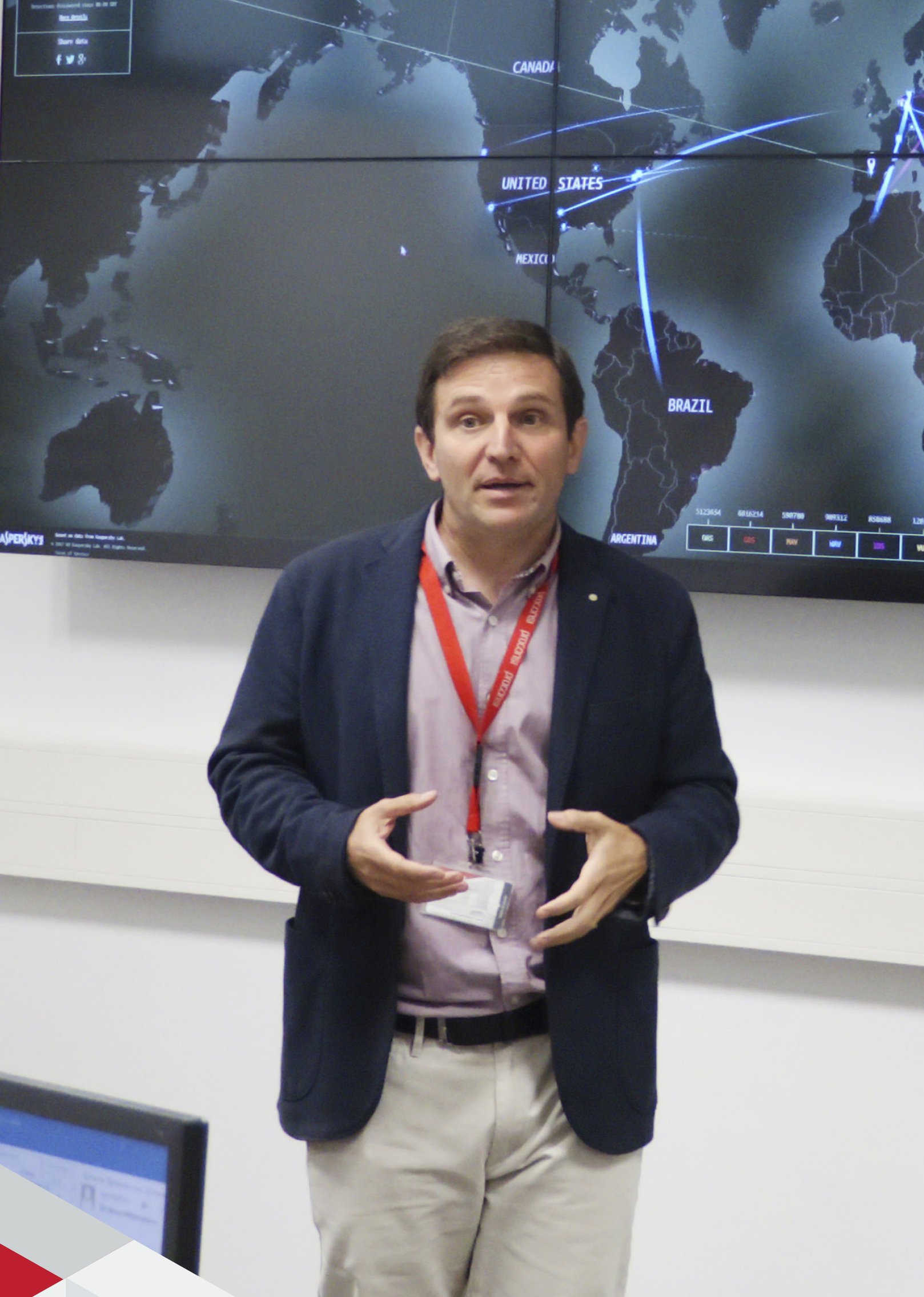
Ofrecemos un conjunto de soluciones en ciberseguridad adaptadas a su organización, para un seguro desarrollo de su actividad.

Nuestros profesionales dan respuesta a necesidades específicas aportando ideas e indicando las soluciones en ciberseguridad más adecuadas en cada momento, para que usted pueda centrarse en su actividad principal.

Hemos de tener en cuenta que uno de los valores principales de las organizaciones reside en la información. Por ello, la protección de la misma debe ser una de nuestras prioridades. Desde Proconsi, llevamos mucho tiempo involucrados en tareas de sensibilización y protección de los sistemas informáticos, por lo que disponemos de productos y servicios orientados a incrementar la seguridad, de forma que nuestros clientes puedan beneficiarse de todos los avances tecnológicos, a la par que disponer de las medidas de seguridad más adecuadas con el mínimo impacto posible para su trabajo diario.

Luis Ángel Martínez Cancelo
Director de Sistemas y Ciberseguridad de Proconsi

proconsi


CANADA
UNITED STATES
MEXICO
BRAZIL
ARGENTINA

Auditorías de Seguridad de la Información

¿Están sus sistemas correctamente securizados? Nuestro equipo de técnicos especializados en ciberseguridad, puede realizar una auditoría sobre sus sistemas, sometiéndolos a diferentes pruebas para verificar si están perfectamente configurados y actualizados.

Nuestras auditorías no sólo se centran en la parte técnica, también trabajamos la parte humana, ya que todas las medidas de seguridad que se implementen serán insuficientes si no sensibilizamos a las personas para minimizar el riesgo de ser víctimas de los cibercriminales.

¿Qué son las auditorías de seguridad informática?

Se conoce como auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) al estudio que comprende el análisis y gestión de los sistemas, llevado a cabo por profesionales externos con el objetivo de identificar las vulnerabilidades que pudieran encontrarse en los equipos de trabajo, redes de comunicación, servidores empresariales, etc.

¿Qué beneficios ofrecen las auditorías de seguridad?

- Reducción de impactos al conocer en profundidad las vulnerabilidades y, por tanto, los riesgos a los que está expuesta la empresa.
- Capacidad de ofrecer una mayor garantía y seguridad en el servicio a los clientes.
- Aumento del valor de imagen de empresa y marca.
- Aumento de la seguridad en la empresa, en cuanto a lo que procedimientos internos e información confidencial se refiere.

¿Qué tipos de auditorías de seguridad realizamos desde Proconsi?

Auditoría de caja gris:

En esta auditoría se realiza un análisis de vulnerabilidades, disponiendo de información facilitada por el cliente. En este caso, es interesante disponer de, por ejemplo, credenciales de usuario administrador y usuario estándar, para conocer las vulnerabilidades aplicables a cada escenario. El auditor realiza pruebas del manejo de tipo de datos, de los protocolos de comunicación, manejo de excepciones, etc., con el objetivo de conocer el estado y posibles amenazas del sistema.

Auditoría de caja negra:

En esta auditoría se realiza un análisis de vulnerabilidades para el cual, el equipo auditor cuenta con una visión ciega del sistema del cliente, debiendo recopilar todo tipo de información sobre ella, para la planificación de potenciales ataques. Estaríamos ante un escenario similar al que puede encontrarse el ciberdelincuente. El resultado de esta actividad es un informe en el que se plasman las vulnerabilidades encontradas, así como propuestas de medidas de seguridad a implantar para solventarlas o minimizarlas, según cada caso.

Auditoría de cumplimiento LOPDGDD/LSSICE:

Este tipo de auditorías son las encargadas de analizar el grado de cumplimiento y adaptación de una empresa, tienda online o servicio, a la nueva normativa de protección de datos RGPD y LOPDGDD, así como a la LSSICE, encargada de regular la prestación de servicios a través de internet y el comercio electrónico.

Consultoría Tecnológica ISO 27001 y ENS

Nuestro equipo de profesionales está especializado **en múltiples áreas de consultoría TIC**, generando de esta manera un gran valor en las organizaciones que contratan nuestros servicios al poder disponer de una **visión global de las tecnologías de la información.**

Mediante el **acompañamiento in situ** de nuestros consultores, el proceso de **adecuación a una norma, esquema o sello,** será rápido y sencillo. Además, la transferencia de conocimiento hacia el cliente será óptima.

Igualmente, si lo que desea es simplemente mejorar la ciberseguridad en su organización o está en **fase de transformación o mejora TIC**, podemos recomendar e implementar la solución que mejor se adapte a sus necesidades.

Consultoría para la implantación de un Sistema de Gestión de la Seguridad de la Información, conforme a la ISO 27001

Somos conscientes de que el **aseguramiento de la confidencialidad, la integridad y la disponibilidad de los datos** que maneja a diario su organización es vital para la continuidad de su negocio. Desde Proconsi (entidad certificada ISO 27001 desde 2010), ponemos a su disposición nuestra experiencia para que su organización pueda implantar la norma ISO/IEC 27001 de una manera ágil, alineando los procesos y metodologías de su organización con los requisitos de la norma.

Además, debido al gran conocimiento normativo en TIC, podremos asesorarle acerca de la **integración de la ISO 27001** con otras normas o reglamentaciones, como el Esquema Nacional de Seguridad o la RGPD.

Consultoría para la implantación de un Sistema de Gestión de la Seguridad de la Información, conforme al Esquema Nacional de Seguridad

Ofrecemos la posibilidad de conocer **el estado actual de cumplimiento** y realizar una **adecuación al ENS,** acompañándole durante todo el proceso, para que éste se realice de una manera ágil y directa.

Nuestros garantes son **nuestra experiencia como implantadores** y ser **una compañía certificada en el Esquema Nacional de Seguridad para nuestro sistema de información**, necesario para la correcta prestación de servicios profesionales de: “Diseño y desarrollo de software e integración de sistemas; Implantación y mantenimiento de soluciones hardware y software; Consultoría tecnológica y procesos de soporte”.

Obtención del Sello de Ciberseguridad de la AEI

El Sello de Ciberseguridad para Organizaciones de la AEI Ciberseguridad es un esquema de **certificación** que incluye los **requisitos de seguridad** que debe cumplir cualquier organización, así como cualquier entidad que **se relacione** con alguna de éstas a modo de proveedor, cuando necesite demostrar que dispone de los sistemas y medidas de **seguridad físicas y lógicas** necesarias para proteger sus activos de las distintas amenazas que puedan dañarlos y/o provocar daños en los servicios o capacidades de la organización.

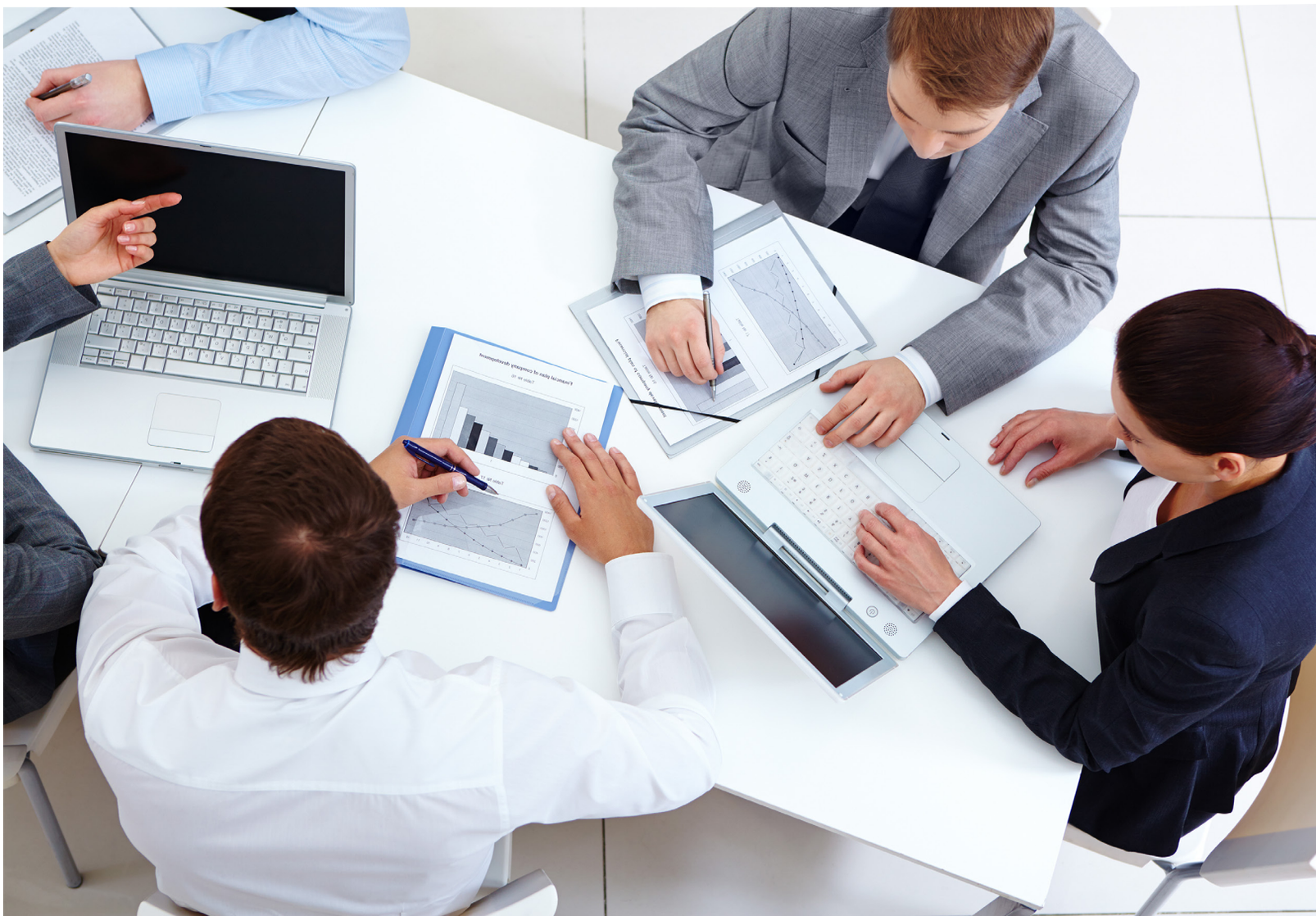
Las organizaciones que deseen obtener el **Sello de Ciberseguriad de la AEI** encontrarán en Proconsi, como **consultora calificada,** una forma eficaz de implantación del sello en sus instalaciones, de forma que el proceso de certificación posterior se produzca de manera ágil y sin contratiempos.

Implantación de un Sistema de Gestión de Seguridad de la Información (SGSI)

El propósito de una consultoría no siempre está enfocado a la obtención posterior de una certificación o a la adecuación para el cumplimiento de una reglamentación, como puede ser RGPD.

Si su organización está en cualquier fase de **transformación o mejora digital,** podemos ayudarle gracias a nuestra larga trayectoria como integradores de sistemas y comunicaciones.

En relación a la **ciberseguridad,** después de analizar personalmente los riesgos detectados en su organización, le recomendaremos e implantaremos o actualizaremos la solución de seguridad en los sistemas y las comunicaciones que mejor se ajusten a sus necesidades.



Seguridad Gestionada 24/7

Los avances tecnológicos de los últimos años suponen una gran ventaja competitiva para las empresas permitiendo que, determinados procesos de negocio esenciales sean más ágiles, eficientes y eficaces. Sin embargo, no es menos cierto, que estos mismos avances han puesto de manifiesto nuevas técnicas de ciberataque que están siendo profusamente explotadas por los cibercriminales.

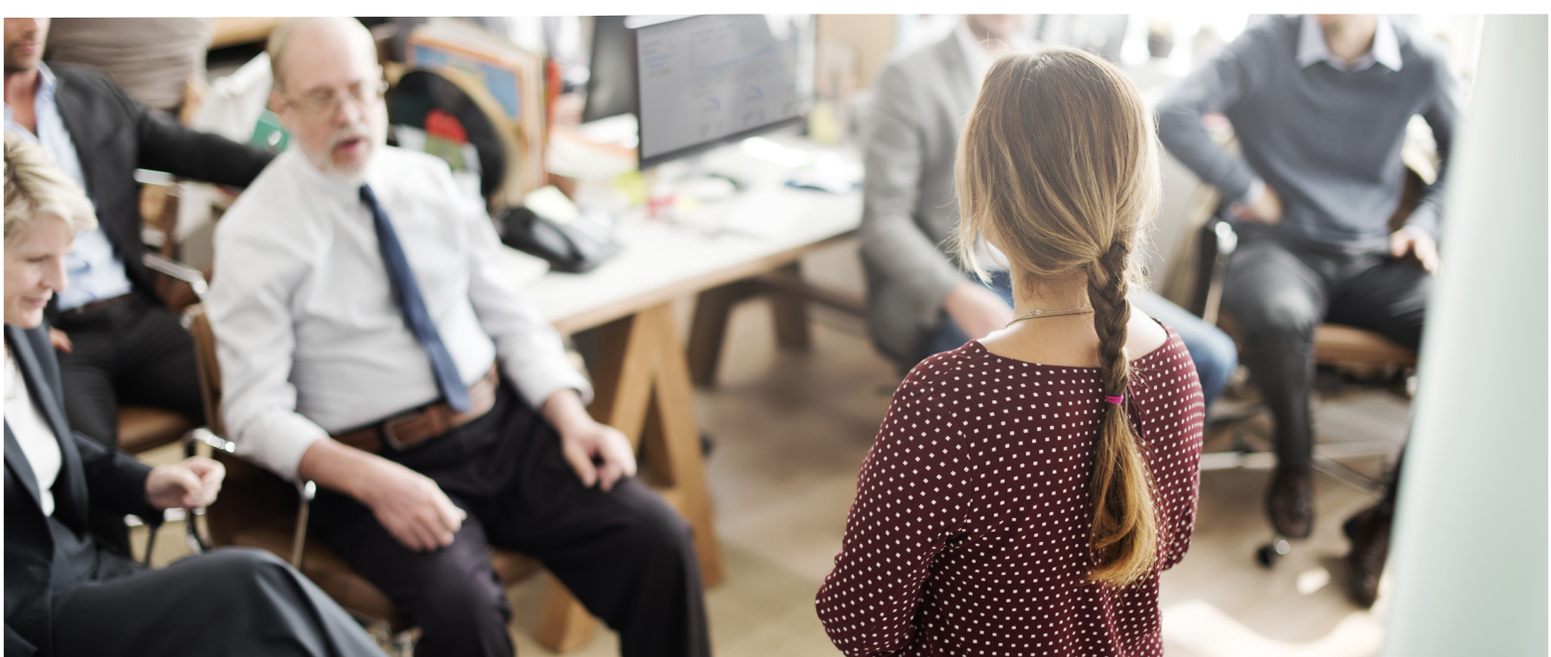
Ambos hechos, unidos al nivel de madurez alcanzado por las herramientas de monitorización y defensa ante las ciberamenazas, nos permiten proporcionar los servicios de seguridad gestionada tan necesarios para afrontar los nuevos desafios con unos costes asumibles por cualquier organización sea cual sea su tamaño.

Además, hemos de pensar también en la salud de los sistemas, no sólo en las ciberamenazas.



La detección temprana de un **disco duro a punto de fallar**, la **monitorización del consumo de ancho de banda** en las conexiones o el estado de las **copias de seguridad,** entre otras cosas, son claves para asegurar la continuidad del negocio y la minimización de los tiempos de parada ante los potenciales incidentes, tanto puramente técnicos, como de ciberseguridad.

Nuestros técnicos monitorizan los sistemas de información y actúan de forma proactiva para asegurar la salud de los mismos, a la par que trabajan sobre la capa de seguridad, reaccionando de igual modo ante los ciberataques, con el fin de mantener la integridad, disponibilidad y confidencialidad de la información, el elemento de mayor valor dentro de la empresa.



SIEM LOGPOINT

Los ciberataques son cada vez más habituales y sofisticados, de manera que los ciberdelincuentes consiguen sortear con frecuencia incluso las políticas y controles de seguridad más sólidos. Por ello, con el fin de minimizar los daños, es crucial actuar rápidamente una vez que los ciberatacantes han obtenido acceso a un sistema. Los equipos de operaciones de seguridad se enfrentan al desafío de gestionar miles de indicadores y múltiples herramientas de seguridad en un tiempo limitado, lo que dificulta la detección y respuesta a actividades maliciosas. La solución más efectiva consiste en la incorporación de un SIEM (Sistema de Información y Gestión de Eventos de Seguridad).

El servicio SIEM LOGPOINT de Proconsi es una plataforma de gestión de información y eventos de seguridad que ayuda a recopilar, analizar y responder a eventos de seguridad en tiempo real. Esta solución integral, ofrece una amplia gama de capacidades para monitorear y proteger los entornos de TI.

El SIEM de Proconsi emplea técnicas avanzadas de análisis y detección de amenazas para identificar patrones, correlaciones y comportamientos anómalos que pueden indicar actividades maliciosas. Esto permite la detección temprana de incidentes de seguridad, lo que a su vez facilita una respuesta rápida y efectiva.

VENTAJAS

· **Visibilidad y monitoreo centralizado**, lo que facilita la detección de amenazas y la respuesta a incidentes.

· **Detección y respuesta temprana a amenazas**: ayuda a identificar amenazas en las primeras etapas y a tomar medidas para mitigarlas antes de que causen un daño significativo.

· **Cumplimiento normativo**: pues ayuda a cumplir con los requisitos de seguridad y las regulaciones establecidas por organismos reguladores.

· **Análisis forense y de incidentes**: La capacidad de búsqueda y análisis avanzados de LOGPOINT permite realizar investigaciones forenses y análisis de incidentes de seguridad.

· **Optimización del rendimiento y la eficiencia**: ya que ofrece una amplia gama de paneles de control, informes y visualizaciones intuitivas que ayudan a comprender y optimizar el rendimiento de los sistemas y las aplicaciones.

· **Integración y automatización**: se integra con sistemas de seguridad y fuentes de datos de otros proveedores, lo que facilita la automatización de tareas y flujos de trabajo. Puedes conectarlo con sistemas de detección de intrusiones (IDS/IPS), firewalls, sistemas de gestión de vulnerabilidades y más, para obtener una imagen completa de la seguridad y mejorar la eficiencia operativa.

Desde Proconsi, te ofrecemos la posibilidad de realizar el despliegue, parametrización y monitorización continua de la solución desde nuestra central. De esta manera, no tendrás que preocuparte del seguimiento de las actividades e información que arroje el SIEM, ya que nuestro equipo de especialistas en ciberseguridad estará realizando el seguimiento continuo de tu infraestructura, protegiéndola frente a las ciberamenazas.

proconsi Tecnologías de la Información

info@proconsi.com www.proconsi.com
902 214 010 987 281 906

Análisis de Vulnerabilidades Web

El imparable avance de las comunicaciones y la tecnología asociada al mundo web, ha logrado que cada vez más empresas aprovechen sus ventajas para expandir y optimizar sus negocios.



Una **web corporativa básica, una tienda online** o incluso una **aplicación de gestión comercial (ERP) en la nube,** son sólo algunos ejemplos de las herramientas web más demandadas por las empresas, de cualquier tamaño y localización, llamadas a competir en el mercado global.

La deslocalización de los mercados, el acceso a un mercado global, la flexibilidad en los medios de pago y/o la reducción de costes, son sólo algunas de las ventajas que el "ecosistema en línea" proporciona a las empresas.

Una buena estrategia en línea puede permitir que incluso pequeñas empresas, algunas provenientes de un mercado tradicional muy local, hayan podido dar un giro, tanto cualitativo como cuantitativo, posicionándolas en el mercado global y haciendo crecer sus ventas y beneficios hasta límites que jamás hubieran imaginado sus fundadores.

Pero dentro de esta estrategia no puede quedar de lado el apartado de la ciberseguridad. Las aplicaciones de comercio electrónico, gestión empresarial,... pueden tener y de hecho tienen vulnerabilidades. Si éstas no son gestionadas a tiempo, pueden poner al descubierto información sensible o confidencial, lo cual, sin duda, impactará negativamente en la confianza, generando una pérdida de reputación y por ende una pérdida de clientes y beneficios. Además, no podemos olvidar los problemas legales que pueden derivarse del hecho de sufrir una brecha de seguridad, como consecuencia de ser explotada una vulnerabilidad.

Es por ello que resulta imprescindible realizar una auditoría de seguridad sobre este tipo de herramientas web antes de iniciar su ciclo de vida, así como llevar a cabo revisiones periódicas que nos permitan paliar el riesgo ante futuras vulnerabilidades que puedan aparecer en las mismas.

Detectar de forma temprana una vulnerabilidad permite aplicar medidas correctoras de forma proactiva, antes de que pueda producirse una brecha de seguridad.

Backup Online

Se denomina Backup online al servicio de copia de seguridad realizada en remoto, que permite al usuario almacenar sus documentos y archivos en un servidor online. Una forma segura y eficaz de mantener la integridad y disponibilidad de la información, frente a pérdidas o modificaciones indeseadas, provocadas por errores humanos o ataques malintencionados.

Principales ventajas del Backup Online:

- El hecho de que los datos se encuentren almacenados en una ubicación diferente al lugar de producción de los mismos, es decir, la oficina o fábrica en que se está generando la información, facilita su preservación frente a posibles robos o accidentes, como incendios, inundaciones, derrumbes, etc.

- Evita el engorroso proceso de copias de seguridad manuales en discos duros, DVDs, CDs, pendrives, etc., que requiere de una elevada inversión en tiempo y recursos, y está sujeta a la posibilidad de un olvido en su ejecución, que ponga en riesgo la preservación de los datos elaborados desde la última copia realizada.

- El Backup online copia datos, pero también puede copiar servidores completos o máquinas virtuales, favoreciendo una rápida restauración del sistema, de ser necesaria.

- Los datos son comprimidos y cifrados en origen, protegiéndolos de posibles robos o alteraciones.

- Es posible almacenar una copia local adicional además de la copia online.

¿Qué tipos de Backup Online existen?

- **Completo:** realiza copias del 100% de los datos, lo que ocasiona una mayor inversión en tiempo y espacio dedicados.

- **Incremental:** solo realiza copias de las modificaciones realizadas desde la última copia, registrando y comparando las fechas de modificación de los archivos para ello. Nuestra solución de Backup online utiliza además un sistema de duplicación profunda que copia únicamente la porción de archivo modificada en lugar del archivo completo, reduciendo de este modo los tiempos de copia.

- **Diferencial:** realiza el mismo proceso que el incremental, pero realizando la copia desde la última copia de seguridad completa.

Adecuación y auditorías de RGPD y LOPDGDD

Nuestros técnicos monitorizan y actúan de forma proactiva sobre la salud de los sistemas de información, a la par que trabajan sobre la capa de seguridad, reaccionando de igual modo ante el Reglamento (UE) 2016/679 de 27 de abril (RGPD) y la Ley Orgánica 3/2018 de 5 de diciembre (LOPDGDD), la normativa vigente relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de éstos, así como a la garantía de los derechos digitales de la ciudadanía.

En Proconsi ofrecemos los servicios de adecuación y auditoría a la RGPD y LOPDGDD, normativa vigente en protección de datos, así como el apoyo en la implementación de las medidas técnicas y organizativas requeridas para el cumplimiento de lo establecido.

Realización del proceso de adaptación conjuntamente con el cliente

- Análisis del sistema de tratamiento de datos y recogida de los datos requeridos.
- Establecimiento del nivel de riesgo.
- Evaluación de impacto sobre la protección de datos.
- Apoyo en la implantación del deber de información.
- Apoyo en el tratamiento de las solicitudes de los derechos de los interesados.
- Establecimiento de un procedimiento de tratamiento de las solicitudes relacionadas con los derechos de los interesados: acceso, rectificación, supresión, portabilidad, limitación y oposición.
- Establecimiento de un procedimiento de gestión de incidentes de seguridad en la protección de datos.
- Formación al responsable sobre la utilización de la documentación generada.
- Revisión / Adecuación de la página WEB.

Auditoría de los sistemas de seguridad implantados para cumplir con la normativa RGPD

- Apoyo en la adopción de las medidas de seguridad necesarias para cumplir con la normativa vigente.

Generación de la documentación requerida

- Contratos (personal, encargados de tratamiento, clientes y cesiones).
- Cláusulas legales, incluyendo aquellas requeridas para el tratamiento de las solicitudes de los derechos de los interesados y para la página web.
- Plantillas para facilitar el cumplimiento de las obligaciones establecidas.
- Documentación requerida para la ejecución de transferencias internacionales.


RGPD

Delegado de Protección de Datos

¿Qué es un DPD?

El Delegado de Protección de Datos (DPD o DPO en inglés) es una figura introducida por el Reglamento (UE) 2016/679 de 27 de abril (RGPD), cuya función principal es la de informar y asesorar a los responsables y encargados de tratamiento acerca de la normativa vigente en materia de protección de datos, contando con cualidades profesionales adecuadas y conocimientos especializados en derecho y la práctica en materia de protección de datos.

¿Qué servicios incluye?

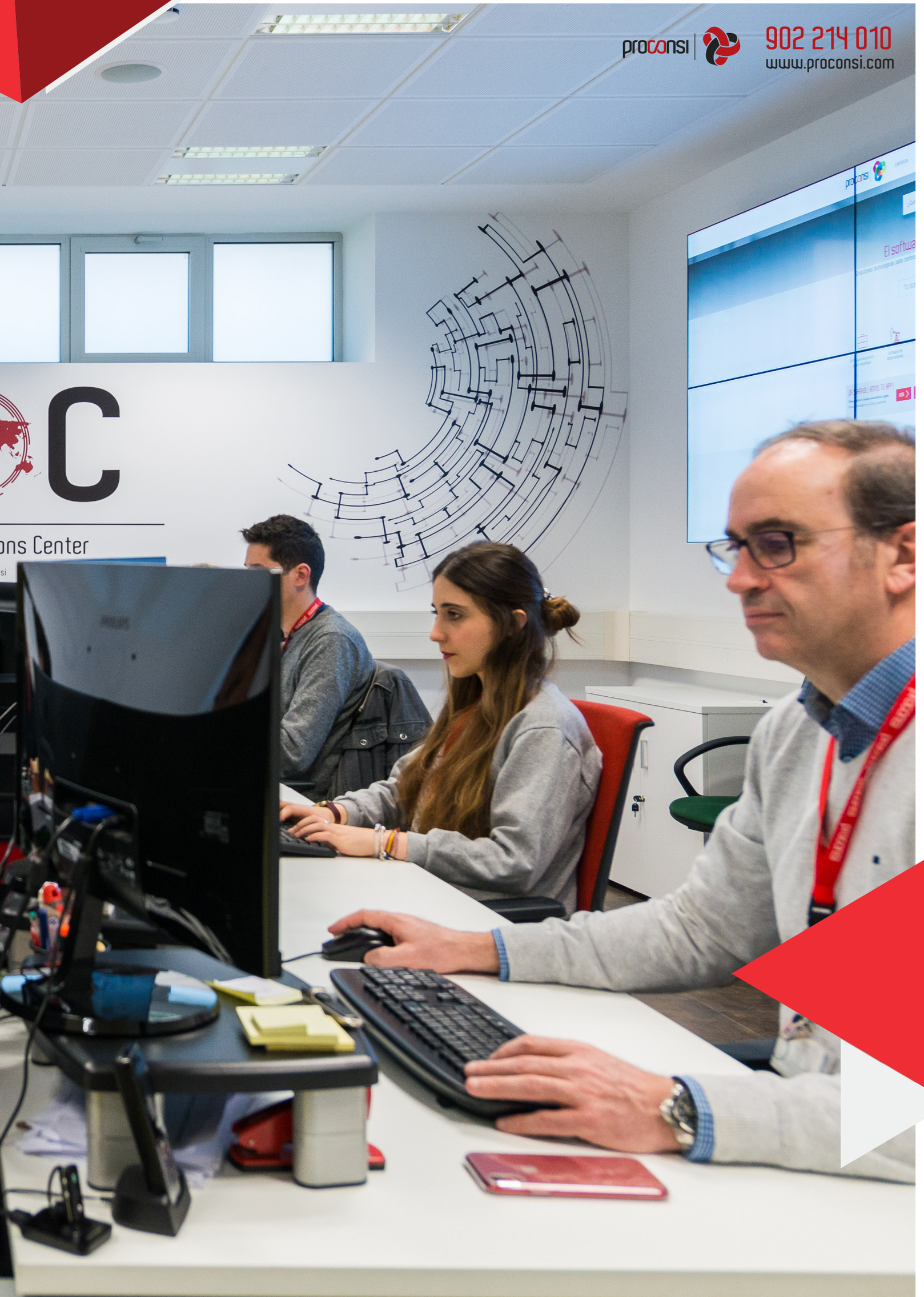
- Informar y asesorar al cliente y a sus empleados sobre las obligaciones que les incumben, relativas a las normativas de privacidad.
- Supervisar la asignación de responsabilidades entre los empleados del cliente.
- Supervisar la concienciación y formación de los empleados que participan en el tratamiento.
- Supervisar el cumplimiento de lo dispuesto en las normativas de privacidad vigentes.
- Supervisar las políticas en materia de protección de datos (responsabilidad proactiva, responsabilidades del tratamiento, política de información y política de seguridad).
- Supervisar las auditorías en materia de protección de datos personales.
- Asesorar al cliente acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación, si es el caso.
- Actuar como punto de contacto de la Autoridad de control y cooperar con ella en los requerimientos que le solicite.
- Actuar como punto de contacto con los interesados en lo que respecta al tratamiento de sus datos y al ejercicio de sus derechos.

¿Qué entidades requieren de un DPD?

- Autoridades u organismos públicos.
- Aquellas entidades cuyas actividades principales sean operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- Aquellas entidades cuyas actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

Concretamente:

- Colegios profesionales y sus consejos generales.
- Centros docentes.
- Entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- Entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Establecimientos financieros de crédito.
- Entidades aseguradoras y reaseguradoras.
- Empresas de servicios de inversión.
- Distribuidores y comercializadores de energía eléctrica y gas natural.
- Entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito.
- Entidades responsables de ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo (Ley 10/2010, de 28 de abril: fundaciones y asociaciones, auditores de cuentas, contables externos o asesores fiscales, notarios y registradores de la propiedad, abogados, procuradores, promotores inmobiliarios, agencias inmobiliarias, loterías, casinos de juego, joyerías, comerciantes de objetos de arte o antigüedades, entre otros).
- Entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o elaboren perfiles de los mismos.
- Centros sanitarios.
- Entidades que tengan como uno de sus objetos la emisión de informes comerciales acerca de personas físicas.
- Operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos.
- Empresas de seguridad privada. Federaciones deportivas cuando traten datos de menores de edad.
- Y por supuesto, cualquier entidad que voluntariamente quiera contar con esta figura.


C
ons Center

proconsi

Parque Tecnológico de León · C/ Andrés Suárez 5 · 24009 León
987 281 906 / 902 214 010 · info@proconsi.com
www.proconsi.com