CENTRO DE CIBERSEGURIDAD INDUSTRIAL

CATÁLOGO DE SERVICIOS Y SOLUCIONES DE CIBERSEGURIDAD INDUSTRIAL **2021**

PRESENTACIÓN

El Centro de Ciberseguridad Industrial, CCI, en su compromiso por avanzar en el camino trazado por el "Roadmap de la ciberseguridad industrial en España 2019-2020", se complace en hacerle llegar la séptima edición de este "Catálogo de Servicios y Soluciones de Ciberseguridad Industrial". Este catálogo, primero en su género, recoge un completo inventario, que refleja la oferta existente en nuestro mercado, que queda organizada en diez categorías de servicios y ocho de soluciones. El Catálogo es fruto del trabajo de especificación, identificación y compilación llevado a cabo, conjuntamente, por CCI y los principales proveedores de "El Ecosistema CCI", sin cuya inestimable contribución la iniciativa habría sido inviable.

El Catálogo muestra, para cada servicio o solución registrados, información relativa a su nombre y descripción.

Asimismo, ofrece datos referidos al alcance geográfico y sectorial del servicio/solución; al número de profesionales cualificados para su prestación; a las certificaciones con que cuentan tales profesionales; y, finalmente, a las referencias reales de ejecución/despliegue que cada uno de los proveedores han declarado.

(Queda, en este sentido, CCI exento de toda responsabilidad sobre la veracidad de la información aportada).

Confiamos en que le resulte de utilidad.

El equipo CCI.

ÍNDICE

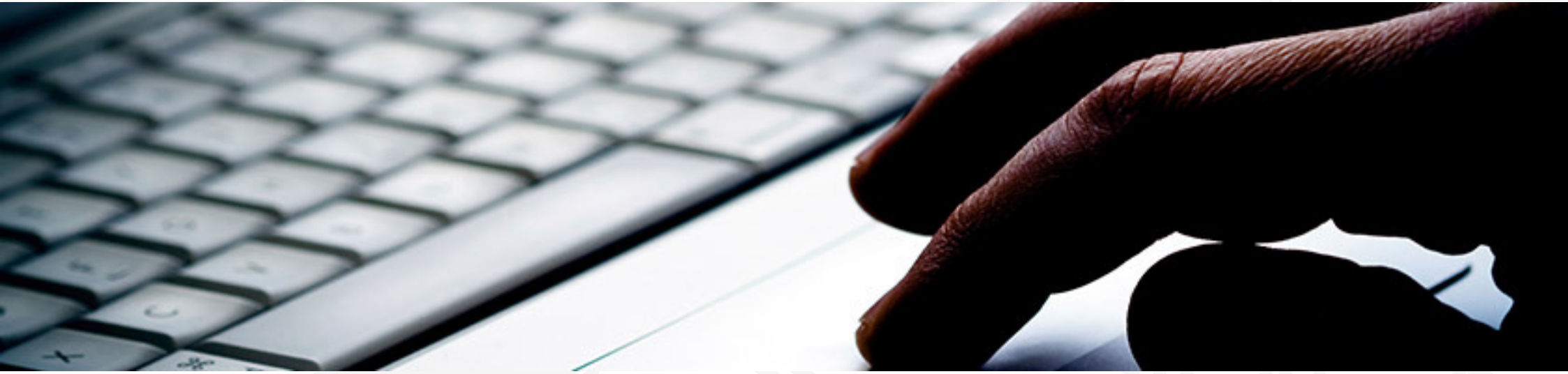
ÍNDICE

SERVICIOS

SOLUCIONES

ACCEDE A CADA APARTADO CON UN CLIC

SERVICIOS



ÍNDICE

ANÁLISIS E INVESTIGACIÓN DE MERCADO (1/3)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Ascent Look Out	Análisis en profundidad de las tendencias emergentes, las necesidades del negocio y las tecnologías que impulsarán la innovación en los próximos años.	ATOS	Todos	Global	70	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	10
Vigilancia tecnológica	Vigilancia en tecnologías en diversos ámbitos de la Ciberseguridad y Gestión de Riesgos. Análisis de mercado para desarrollar ideas y productos innovadores que permitan mitigar riesgos y reducir costes. Análisis de información, generación de material y propuestas de acciones de implantación.	ATOS	Todos	Global	10	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	5
BaaS/ISF	Análisis comparativo del nivel de seguridad de la información en comparación con el sector/mercado.	CALS	Todos	Global	20	N/A	150
Publicaciones especializadas en Ciberseguridad Industrial	Desarrollo de informes, análisis estratégicos, guías y herramientas de alta calidad centrados en la Ciberseguridad Industrial.	CCI	Todos	Global	7	CISA, CISM, CISSP, GICSP, CRISC, CGEIT	14
Investigación y Desarrollo de nuevos servicios de Ciberseguridad	Análisis y estudio de mercado de las mejores soluciones de CiberSeguridad.	ENTELGY SECURITY	Todos	Global	17	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	>35
BenchMarking de Soluciones	Estudio comparativo y análisis de la solución para despliegue en entornos concretos.	ENTELGY SECURITY	Todos	Global	25	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	>40
Roadmap de Ciberseguridad	Estudios orientados a analizar tendencias en materia de Ciberseguridad, e identificar buenas prácticas, recomendaciones y/o líneas de trabajo futura.	EVERIS	Todos	España, Europa y Latinoamérica	5	CISM, CRISC, CISSP	10
SIEM	Capacidades NOC + SOC. Gracias a su CMDB permite realizar la gestión del inventario activos, detectar cambios de configuraciones de cualquier elemento de red, así como monitorizar el rendimiento y disponibilidad de los mismos. Correlación de eventos de seguridad de todos los elementos conectados a la red. Monitorización de procesos críticos de negocio. También se integra con FortiGuard Labs para compartir Indicadores de compromiso y detectar cualquier actividad sospechosa en la red.	FORTINET	Todos	Global			

ÍNDICE

ANÁLISIS E INVESTIGACIÓN DE MERCADO (2/3)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Vigilancia Tecnológica	Detección y análisis de la mejor solución del mercado que cubra las necesidades del cliente.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, 166602, Lead Auditor 27001, 22301, 20000	>50
Innovación y Desarrollo	Análisis de tendencias y desarrollo de nuevas soluciones y servicios en Ciberseguridad. Identificación de buenas prácticas y recomendaciones.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, PMP, 166602, Lead Auditor 27001, 22301, 20000	>15
Seguridad IIoT - Vigilancia Tecnológica (Industrial Internet of Things)	Análisis de Servicios de seguridad para protección de proyectos IIoT, apoyado en el dpto. I+D+i de Inycom.	INYCOM	Todos	Global	>12	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	
Laboratorio Tecnológico	Identificar la mejor solución del mercado para cubrir las necesidades planteadas por el cliente.	ITS SECURITY	Todos	España	5		
Vigilancia Tecnológica	Estudios orientados a analizar tendencias, nuevas e identificar buenas practicas por sectores verticales.	ITS SECURITY	Todos	Iberia	3		5
Comparación de soluciones ICS (Detección de anomalías, Virtual Patching, IDS/IPS, Cortafuegos, etc.)	Análisis técnico de herramientas para su despligue en entornos industriales dentro de clientes. Dentro del análisis se ejecuta una comparativa de los dispositivos para revisar las capacidades que se adecuan más a los entornos que posee el cliente.	S21SEC	Cualquiera	España, Europa y Latinoamérica	10	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	4
Secure&Análisis	Análisis de soluciones de CiberSeguridad del Mercado.	Secure&IT	Todos	Global	>25	Lead Auditor ISO 20000/ISO 27001/ ISO23301, CISA, CISM, CISSP, CEH, OSCP, ITIL V3, Ldo. Derecho, Perito Informatico Judicial	>100

ÍNDICE

ANÁLISIS E INVESTIGACIÓN DE MERCADO (3/3)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Secure&PerJud	Peritajes Judiciales de CiberSeguridad.	Secure&IT	Todos	Global	3	Lead Auditor ISO 20000 / ISO 27001 / ISO23301, CISA, CISM, CISSP, CEH, OSCP, ITIL V3, Ldo. Derecho, Perito Informatico Judicial	>100
Secure&Estrategias CI	Diseño de Estrategias de Ciberseguridad en entornos industriales.	Secure&IT	Industria	Global	>5	Lead Auditor ISO 20000 / ISO 27001 / ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. Ldo. Derecho, Perito Informatico Judicial	
Industrial Security Monitoring SIEM	Análisis y Monitorización continua y transparente de la seguridad de red con SIEM. - SIEM es una solución técnica de análisis y monitorización de archivos y logs para detección e identificación de amenazas y eventos relevantes de seguridad. - Instalación y configuración de las aplicaciones SIEM y sus escenarios basados en un sistema de vectores que analizan amenazas e infraestructura ICS. - Monitorización continua y análisis seguridad base desde Centro de Operaciones de Ciberseguridad (Cyber Security Operation Center) CSOC. - Correlación con base de datos de "Global Threat Intelligence". - Notificación inmediata una vez detectadas amenazas y eventos de seguridad. - Visualización actual del estado de la seguridad mediante informes mensuales.	SIEMENS	Todos	Global			
Remote Incident Handling	Rápida reacción una vez se han detectado amenazas y eventos de seguridad mas relevantes. Siemens es experto en comportamiento de Seguridad Industrial y análisis de causa-efecto en eventos de seguridad. - Uso deThreat Intelligence Mechanisms, malware sandboxing and raw data gathering tool para investigación de causa-efecto en y análisis críticos. - Entrega de Informe que incluye propuesta con la estrategia para solución.	SIEMENS	Todos	Global			

ÍNDICE

CONCIENCIACIÓN (1/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Awareness (concienciación) en materia de Ciberseguridad Industrial	Acciones de concienciación y sensibilización corporativa y materia de Ciberseguridad Industrial. Campañas anti-phishing, E-learning, newsletters, security days, etc.	ATOS	Todos	Global	20	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	10
Infosecure	Planes de concienciación sobre seguridad de la información. Dispone de un gran repositorio de documentos gráficos y herramienta propia para adaptar y crear mensajes estándar.	CALS	Todos	Global	30	N/A	40
Concienciación en riesgos OT	Sesiones de concienciación personalizadas enriquecidas con la experiencia de nuestros expertos y colaboradores. Desde 30 min. y para diferentes roles (Gestores, técnicos, ingenieros…) de una organización industrial, ingeniería o proveedor.	CCI	Todos	Global	10	CISA, CISM, CISSP, GICSP, CRISC, CGEIT	14
Cibersospecha	Juego de mesa de Ciberseguridad, donde cada jugador asumirá el papel de un investigador de Ciberseguridad que debe utilizar sus facultades de deducción para descubrir donde, cómo, por qué y quién ha provocado el incidente de Ciberseguridad que ha paralizado una planta industrial.	CCI	Todos	Global	N/A	N/A	40
CiberDuelo	Juego de cartas donde se simula la gestión de un presupuesto para aplicar medidas de Ciberseguridad encaminadas a proteger una planta industrial.	CCI	Todos	Global	N/A	N/A	80
CyberPulze	CyberPulze es un innovador servicio de concienciación en seguridad cibernética remota científicamente probado que ayuda a proteger su organización de ataques cibernéticos con solo 3 minutos de esfuerzo a la semana por usuario.	CyberPulze	Todos	Global	N/A	N/A	N/A
Simulacro Spare Phishing	Realización de campañas de ataques dirigidos simulando un spare phishing, con el objetivo de medir el grado de resiliencia del factor humano ante un posible ataque real. Se medirá también el funcionamiento de los procesos de alerta y respuesta ante incidentes de la organización.	CIC Consulting Informático	Todos	Global	2	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	3
Sesiones de concienciación seguridad de la información e ICS	Sesiones de concienciación y divulgación para profesionales de redes de operaciones en materia de seguridad de la información.	DELOITTE	Todos	Global	20	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	5

ÍNDICE

CONCIENCIACIÓN (2/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Concienciación a entornos "VIP"	Sesiones de concienciación focalizadas a los riesgos de la alta dirección.	ENTELGY SECURITY	Todos	Global	9	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	> 15
Talleres de concienciación en Ciberseguridad	Formación orientada a toda la organización sobre riesgos en el puesto de trabajo y buenas prácticas. Riesgo en uso de Redes Sociales, uso Seguro correo electrónico, navegación segura, etc.	ENTELGY SECURITY	Todos	Global	20	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	> 45
Sinergias / Convergencia IT & OT	Talleres de definición de puntos clave de la seguridad en IT y OT.	ENTELGY SECURITY	Todos	Global	7	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	> 10
Campañas de concienciación en Ciberseguridad	Jornadas de concienciación para directivos sobre los riesgos de la ciberseguridad en la empresa y de buenas prácticas en el trabajo para empleados.	EURECAT	Todos	Global	6		> 10
Talleres de Continuidad de Negocio	Desarrollo de iniciativas encaminadas a fomentar la cultura de continuidad de negocio y la concienciación de los empleados respecto a la misma mediante actividades y talleres.	EVERIS	Todos	España y Latinoamérica	6	ISO22301 Lead Auditor, CISSP, CISM, CRISC	4
Talleres "Cultura de Ciberseguridad corporativa"	Charlas dirigidas a todo el staff de una compañía, orientadas a la concienciación en materia de Ciberseguridad.	EVERIS	Todos	España y Latinoamérica	6	CISA, CISSP, CISM, CEH	7
Sesiones de concienciación	Sesiones adaptadas a las necesidades del cliente que permiten mostrar los riesgos y beneficios asociados a contar o no, con medidas de protección en Ciberseguridad Industrial. Análisis inicial de riesgos y amenazas.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, CERT Lead Auditor 27001, 22301, MCSE	> 15
Formación a responsables	Sesiones de formación dirigidas a los responsables en diversos marcos: PRIVACIDAD, LOPD, ENS, ENI, NORMAS ISO, ITIL, INFRAESTRUCTURAS CRÍTICAS ETC...	GOBERTIS	Todos	Global			
Sesiones de sensibilización	Sesiones de sensibilización dirigidas a los empleados en diversos marcos: PRIVACIDAD, LOPD, ENS, ENI, NORMAS ISO, ITIL, INFRAESTRUCTURAS CRÍTICAS ETC...	GOBERTIS	Todos	España			

ÍNDICE

CONCIENCIACIÓN (3/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Desarrollo de planes de concienciación	De seguridad en dispositivos, en redes sociales y normativa, políticas y procedimientos internos a través de: Presentaciones, Cursos in-situ, cursos on-line, merchandising, multimedia, Desktop, Incluir cumplimiento regulatorio en materia de seguridad de la información, etc.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, CHFI, Comptia Security+	20
Concienciación - Ciberseguridad Industrial	Concienciación para la dirección y plantilla sobre buenas prácticas en el trabajo, evitar riesgos con herramientas ágiles como Gamificación (cybergames) que ayudan a evitar incidentes con formación específica y real.	INYCOM	Todos	Global	>12	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	
Sensibilización de la dirección	Sesiones orientadas a sensibilizar a la dirección y mandos intermedios sobre los riesgos en los sistemas OT.	ITS SECURITY	Todos	España	6	CISA, GICSP	3
Concienciación en Continuidad de Negocio	Jornadas de concienciación en la cultura de la Ciberseguridad y la Continuidad del negocio. Impacto sobre la productividad y la cuenta de resultados.	ITS SECURITY	Todos	España	2		1
Convergencia IT y OT	Trabajo en equipo entre los departamentos involucrados en la gestión de la Ciberseguridad IT y OT.	ITS SECURITY	Todos	España	2		1
Kaspersky Security Awaraness	Familia de productos de formación que emplea lo último en técnicas de aprendizaje (gamificación) y aborda todos los niveles de la estructura empresarial. - Plataforma de concienciación en seguridad - Enfocado a todos los trabajadores. Desarrolla habilidades relativas a la cultura cibernética individual. - Juegos de gestión de la ciberseguridad - Taller interactivo, enfocado a directivos para la comprensión sobre las medidas de ciberseguridad, así como un conjunto de acciones para su adopción en el lugar de trabajo. - Ciberseguridad para IT Online (CITO) - Enfocado para profesionales de TI generales. - Juegos de gestión de la ciberseguridad - Taller interactivo, enfocado a directivos para la comprensión sobre las medidas de ciberseguridad. - Evaluación de la cultura de la ciberseguridad.	KASPERSKY	Todos	Global			

ÍNDICE

CONCIENCIACIÓN (4/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Concienciación sobre riesgos para la ciberseguridad en entorno industrial	Jornadas orientadas a transmitir la importancia de la ciberseguridad a los ingenieros de planta/control, personal técnico y de gestión encargado de tratar habitualmente con los sistemas de control y automatización. Se exponen casos prácticos con soluciones de PHOENIX CONTACT para securización.	PHOENIX CONTACT	Todos	Global	8		
Concienciación en Ciberseguridad Industrial	Sesiones de concienciación empleando un entorno práctico con modelos realistas de sistemas de control industrial. Mediante este entorno se trasladan los modos en que la seguridad de la información que se maneja en los entornos industriales puede verse comprometida y cuáles pueden ser las consecuencias. De esta manera el personal involucrado en los procesos industriales toma conciencia no sólo de los riesgos derivados del uso de las TICs sino de cómo la combinación del conocimiento de expertos técnicos industriales y de expertos informáticos puede ser usado con malas intenciones para diseñar ataques específicos dirigidos contra este tipo de sistemas.	S2 GRUPO	Todos	Global	>15	ITIL, PMP, PRINCE2, CISA, CISM, CRISC, ISO 27001 Certified Lead Auditor, ISO 22301 Certified Lead Auditor, CISSP, GPEN, GICSP, APMG ISO 20000, APMG CMDB	>40
Curso de concienciación en entornos industriales	Curso adaptado a diferentes perfiles dependiendo del rol del empleado dentro de la organización y del sector al que pertenece la propia organización.	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC	>4
Sensibilización frente a phishing	Mediante sesiones de gamificación concienciar la dirección y la plantilla de las empresas sobre buenas prácticas en el trabajo.	SARENET	Todos	España	>5	N/A	N/A
Píldoras e-learning de concienciación en ciberseguridad Phosforea®	13 módulos de 10 minutos + 12 videos en 2 minutos cada uno sobre: contraseñas, virus y memoria USB, acceso a los datos, BYOD, e-mail: virus & phishing, ingeniería social, acceso físico escritorio limpio, movilidad profesional, incidentes de seguridad.	SCASSI CIBERSEGURIDAD	Cualquier	Global	6		70

ÍNDICE

CONCIENCIACIÓN (5/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Serious Game Infosentinel: dos juegos de rol online que abordan la seguridad informática en situación de movilidad profesional y al despacho	1 modulo de 15 min. para concienciar al conjunto de la plantilla de una empresa.	SCASSI CIBERSEGURIDAD	Cualquier	Global	6		70
Concienciación sobre RGPD	Jornadas orientadas a transmitir la importancia de la ciberseguridad a los ingenieros de planta/control, personal técnico y de gestión encargado de tratar habitualmente con los sistemas de control y automatización. Se trata de jornadas para explicar la importancia de concienciación a las empresas y portfolio y soluciones de SIEMENS para securización.	SIEMENS	Todos	Global	6		
Security Awareness Plan	Servicio para el diseño, implementación y ejecución de un Plan de Concienciación de 1-3 para mejorar el nivel de concienciación en seguridad de las compañías, formar a los empleados e inculcar habilidades y mejores prácticas	TELEFÓNICA - ELEVENPATHS	Todos	Nacional	Nacional / Internacional	CISSP, CEH, CCNA, CITRIX, COMPTIA	Más de 30
Formación a responsables	Sesiones de formación dirigidas a los responsables en diversos marcos: PRIVACIDAD, LOPD, ENS, ENI, NORMAS ISO, ITIL, INFRAESTRUCTURAS CRÍTICAS ETC...	TELEFÓNICA - GOVERTIS	Todos	Global	15	CISA, CISM, CDPSE, COBIT, CISSP, ISO 27001, ISO 22301, DPD	>25
Sesiones de sensibilización	Sesiones de sensibilización dirigidas a los empleados en diversos marcos: PRIVACIDAD, LOPD, ENS, ENI, NORMAS ISO, ITIL, INFRAESTRUCTURAS CRÍTICAS ETC.	TELEFÓNICA - GOVERTIS	Todos	Global	15	CISA, CISM, CDPSE, COBIT, CISSP, ISO 27001, ISO 22301, DPD	>25
Jornadas de concienciación	Servicio destinado a la sensibilización del personal de una organización en materia de ciberseguridad, mostrando las principales amenazas y riesgos existentes así como las posibles consecuencias en el caso de que estos sean aprovechados.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL	

ÍNDICE

CONCIENCIACIÓN (6/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Ti School - Jornadas de concienciación	Servicio destinado a la sensibilización del personal de una organización en materia de ciberseguridad, mostrando las principales amenazas y riesgos existentes así como las posibles consecuencias en el caso de que estos sean aprovechados.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE	
Ti School - Jornadas de concienciación On Line	Servicio destinado a la sensibilización del personal de una organización en materia de ciberseguridad, mediante el uso de una plataforma de formación On Line con la capacidad de programar campañas de Phishing y Ransomware	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE	
Programa para concienciación para ciberseguridad	Programa para concienciación para ciberseguridad.	TÜVIT	Todos	Global	>5	Ethical Hacker	>20

ÍNDICE

CONCIENCIACIÓN (7/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Concienciación para los Proveedores de Servicios Confianzas	Jornadas y seminarios sobre ETSI y nueva regulación eIDAS.	TÜViT	Proveedores de Servicios de Confianza, Hospitales, Empresas de seguros	Global	>5	ETSI Auditor y ISO 27001 Lead Auditor	>20
Centro de Procesamiento de Datos (CPD)	Jornadas sobre los Riesgos Físicos de CPDs.	TÜViT	Todos	Global	>8	TSI Professional	>200
ISO 27001	Introducción a ISO 27000. Actualización a ISO 27000:13.	TÜViT	Todos	Global	>15	ISO 27001 Auditor	>50
ISO 20000	Introducción a ISO 20000. Comparativa con ITIL.	TÜViT	Todos	Global	>8	ISO 20000 Auditor	>50
ISO 22301	Introducción a Continuidad de Negocio. ISO 22301. Seminarios y jornadas de concienciación.	TÜViT	Todos	Global	>5	ISO 20000 Auditor	>50
Análisis de Riesgos	Introducción a Análisis de Riesgos.	TÜViT	Todos	Global	>5	Ethical Hacker	>50
Concienciación para los Proveedores de Servicios Confianzas	Jornadas y seminarios sobre ETSI y nueva regulación eIDAS.	TÜViT	Proveedores de Servicios de Confianza, Hospitales, Empresas de seguros	Global	>5	ETSI Auditor y ISO 27001 Lead Auditor	>20
Centro de Procesamiento de Datos (CPD)	Jornadas sobre los Riesgos Físicos de CPDs.	TÜViT	Todos	Global	>8	TSI Professional	>200
ISO 27001	Introducción a ISO 27000. Actualización a ISO 27000:13.	TÜViT	Todos	Global	>15	ISO 27001 Auditor	>50
ISO 20000	Introducción a ISO 20000. Comparativa con ITIL.	TÜViT	Todos	Global	>8	ISO 20000 Auditor	>50
ISO 22301	Introducción a Continuidad de Negocio. ISO 22301. Seminarios y jornadas de concienciación.	TÜViT	Todos	Global	>5	ISO 20000 Auditor	>50
Análisis de Riesgos	Introducción a Análisis de Riesgos.	TÜViT	Todos	Global	>5	Ethical Hacker	>50

ÍNDICE

FORMACIÓN (1/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Formación en materia de ciberseguridad industrial	Acciones de formación en materia de Ciberseguridad Industrial. Planificación y desarrollo de material formativo. Cursos de gestión de seguridad, de riesgos y de continuidad de negocio para dirección de TI; cursos de normativas, legislación y estándares de seguridad para personal de TI; cursos de seguridad tecnológica (perimetral, hacking, desarrollo seguro, ...) para personal de TI y de seguridad; cursos de recomendaciones, buenas prácticas y responsabilidades en el uso de sistemas para usuarios. Diseño de paquetes formativos multimedia para formación online.	ATOS	Todos	Global	20	CISA, CISM, CRISC, CISSP, ITIL, PMP, ISO 27001/22301 LEAD AUDITOR, CobIT, PCI-DSS QSA, CDPP, CEH, SSCP	10
T01. Taller práctico de evaluación de madurez en el proceso de ciberseguridad en una organización industrial	Proporcionar a los profesionales de organizaciones industriales, ingenierías, integradores IT y OT el conocimiento necesario para determinar el grado de madurez en materia de Ciberseguridad de una organización industrial respecto a los requisitos de la organización, identificando las principales brechas de seguridad basado en C2M2. Permite también establecer comparaciones entre distintas organizaciones en cuanto a su madurez en capacidades de Ciberseguridad Industrial.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	8
T02. Taller Diagnóstico de ciberseguridad en un entorno de automatización industrial	Taller basado en un caso práctico para adquirir el conocimiento preciso acerca del estado de la ciberseguridad en una instalación industrial mediante la identificación de puntos débiles y la comprensión de los ciberriesgos que la instalación está afrontando; y la propuesta de acciones para mejorar su ciberseguridad.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	12
T03. Taller práctico Ciberseguridad en el Ciclo de Vida de un proyecto industrial	Proporciona a los profesionales de organizaciones industriales, ingenierías, integradores IT y OT los conocimientos fundamentales para aplicar la ciberseguridad en el diseño de la automatización industrial, analizando los riesgos e impacto en el negocio.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	11
T04. Taller práctico de aplicación de un sistema de gestión de ciberseguridad industrial (SGCI)	Taller donde se utiliza de forma práctica la guía para la construcción de un SGCI en la que se han aplicado directrices específicas de los estándares ISO27001 e IEC62443 para un tratamiento eficaz y continuado de los riesgos de las tecnologías industriales.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	4	CISM GICSP	11

ÍNDICE

FORMACIÓN (2/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
T05. Taller de Análisis Forense en un entorno de automatización industrial	Aprender a través de un caso práctico a realizar un análisis forense en un entorno de automatización y control industrial, aplicando la 'Guía de buenas prácticas' que forma parte del material del taller.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	2	CISM GICSP	4
C01. Curso multidisciplinar de Seguridad Digital en la Industria [4.0] y Protección de servicios esenciales	Este curso llevará a los participantes a través del estudio del estado del arte de la Protección de Servicios Esenciales y la Seguridad digital en la Industria [4.0], tanto en lo que a legislación y normativa se refiere, como a los estándares, iniciativas, marcos de gestión y tecnologías aplicables.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	19
C02. Curso Responsable de Ciberseguridad en IACS (Sistemas de Automatización y Control Industrial)	Curso práctico para implantar un sistema de Gestión de Ciberseguridad en un entorno IACS, basado tanto en un análisis de riesgos, como en un diagnóstico de ciberseguridad. Se utilizará de forma práctica la guía para la construcción de un SGCI y de diagnóstico de ciberseguridad en entornos industriales.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	5
M01. Máster Profesional Online de Ciberseguridad Industrial	Máster que permitirá analizar y comprender el riesgo asociado a las infraestructuras industriales y su relación básica con los Sistemas de Control Industrial. Conocimiento necesario para cualquier profesional de ingeniería industrial o informática relacionado con áreas como las TIC, energía, industria química y nuclear, agua, fabricación o transporte, entre otros.	CCI	Energía Transporte Agua Fabricación Salud Ingeniería	Global	5	CISM GICSP	4
CyberAcademy	Cursos de seguridad generales y específicos en entornos SCADA, incluyendo: - Investigaciones Forenses Avanzadas: Windows, Linux, Mac, Móviles. - Ataques dirigidos. - Desarrollo Seguro. - DDoS. - Hacking Etico: IPv6, Web, Red, Wifi y Sistemas. - Reversing. - Only Malware. - Tecnologías SIEM. - Seguridad en Dispositivos Móviles. - Ciberseguridad para no técnicos. - Ciber Inteligencia.	DELOITTE	Todos	Global	30	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	>20

ÍNDICE

FORMACIÓN (3/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Curso Sistemas Gestión Seguridad de la Información	Curso Sistemas Gestión Seguridad de la Información.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético	5
Curso normativa RGPD	Curso Reglamento General Protección de Datos.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético	8
Curso LOPD	Curso LOPD.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético	8
Formación especializada BLUE TEAM	Formación especializada en la defensa proactiva y reactiva en entornos CSIRTs.	ENTELGY SECURITY	Todos	Global	15	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	5
Formación especializada RED TEAM	Formación especializada en ataques avanzados para la consecución de un objetivo marcado.	ENTELGY SECURITY	Todos	Global	33	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	18
Curso de Gestión de incidentes de seguridad	Curso Básico / Avanzado en las buenas practicas Ciberseguridad para la gestión de incidentes.	ENTELGY SECURITY	Todos	Global	22	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	25
Formación en Normativas de aplicación Nacional o Internacional	Cursos de Formación en: ISO 27001, ISO 20000, ISO 22301, GDPR, ENS.	ENTELGY SECURITY	Todos	Global	8	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	

ÍNDICE

FORMACIÓN (4/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Formación Ciberseguridad Industrial (ICS / Scada)	Formación en materia de Ciberseguridad Industrial. Normativa NIST SP800-X, NERC-ZIP, IEC 62443, BSI-100.	ENTELGY SECURITY	Industrial	Global	4	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	
Formación Ley PIC	Formación adaptada a elaborar un PSO y un PPE según la ley PIC.	ENTELGY SECURITY	Industrial	Global	4	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH, CGIH, GREM	
Ciberseguridad en los vehículos conectados	Formación destinada a fabricantes y proveedores de vehículos conectados que les permitirá entender los riesgos de ciberseguridad que presentan sus productos y cómo estos deben ser protegidos.	EURECAT	Automoción	Global	4		4
Diseño del plan de seguridad para una infraestructura	Curso orientado a dar los conocimientos necesarios para diseñar un plan de seguridad para una infraestructura, detectando la situación actual, las necesidades de la organización y elaborando un plan de mejora para cumplir los objetivos deseados.	EVERIS	Todos	España, Europa y Latinoamérica	2	CISM, CRISC, CISSP	5
Análisis de Malware	Curso orientado a dar conocimientos para la gestión de malware. Detección, análisis y limpieza.	EVERIS	Todos	España, Europa y Latinoamérica	2	CEH, GCIH	4
Desarrollo Seguro de Software	Curso que tiene como objeto capacitar y concienciar al personal de una Organización sobre la importancia de incorporar la seguridad como un elemento clave dentro de las fases de desarrollo de un Sistema de Información.	EVERIS	Todos	España, Europa y Latinoamérica	2	CISSP, CSSLP	4
CONNtrol- Formación y Ciberseguridad	Curso presencial de seguridad en sistemas de control industrial. Dirigido a ingenieros, operadores o técnicos de Sistemas de Control Industrial.	GETRONICS	Todos	España, Europa y Latinoamérica	3	CISA, CISM, CISSP, Lead Auditor 27001, 22301	>10
Formación Ley PIC y adaptación a ENS	Formación adaptada a elaborar un PSO y un PPE según la ley PIC.	GETRONICS	Todos	España	3	CISA, CISM, CISSP, Lead Auditor 27001, 22301, MCSE	5
Formación NERC CIP	Formación adaptada al cliente basada en las mejores prácticas del NERC CIP.	GETRONICS	Todos	España	3	CISA, CISM, CISSP, Lead Auditor 27001, 22301	>10

ÍNDICE

FORMACIÓN (5/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Formación NIST 800-82, 53	Formación adaptada al cliente basada en las mejores prácticas del NIST 800-82, 53.	GETRONICS	Todos	España	3	CISA, CISM, CISSP, Lead Auditor 27001, 22301	>10
Formación especializada	Seguridad de la Información, contra-Inteligencia, reputación, estándares, cumplimiento regulatorio en seguridad de la información...	GRUPO SIA	Todos	Global	86	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI	17
Prevención de Riesgos Laborales - Ciberseguridad en la Industria Digital	Formación específica en riesgos laborales derivados de la seguridad cibernética industrial para el empleado como eslabón más débil. Formación en riesgos reales y las recomendaciones para responder ante incidentes en planta.	INYCOM	Industrial (Todos)	Global	>5	AENOR ISO 27001 Auditor, AENOR ISO 20000 Auditor, AENOR LOPD Auditor, Ethical Hacker, Especialista implantador de SGSTIC, ITIL, Lean IT	
Seguridad de la Información ISO 27001	Formación, Implantación y seguimiento de las distintas combinación de roles, normativas, procedimientos y elementos tecnológicos, permiten mantener los riesgos de la organización en niveles asumibles.	ITS SECURITY	Todos	España	3		10
Continuidad de Negocio ISO 22301	Formación, implantación y seguimiento que garantice la capacidad de gestionar la continuidad de negocio independientemente de los cambios que se produzcan en la organización: tecnológicos, organizativos o de entorno.	ITS SECURITY	Todos	España	3		3
Calidad de Gestión ISO 20000	Formación, implantación y seguimiento de la norma para garantizar la diferencia competitiva de las organizaciones.	ITS SECURITY	Todos	España	3		3
Curso intensivo en Ciberseguridad Industrial	Curso intensivo en nuestro laboratorio, aprovechando datos reales de producción. Permitirá entender el alcance, los riesgos y las amenazas que se están produciendo a día de hoy.	ITS SECURITY	Todos	España	3		2
LOPD alcance y riesgos	Proporciona un marco de trabajo para orientar adecuadamente el cumplimiento de la ley.	ITS SECURITY	Todos	España	3		100

ÍNDICE

FORMACIÓN (6/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Ciberseguridad en Smartgrid	Curso de los principios de seguridad en la smartgrid haciendo énfasis en las amenazas y salvaguardas en baja y media tensión, así como en la seguridad en su supervisión.	ITS SECURITY	Eléctrico	Global	3		5
Ciberseguridad en transporte ferroviario	Situación actual de la seguridad, cadena de valor, agentes, sistemas de control, sistemas safety y salvaguardas para asegurar el sistema ferroviario incluyendo metro.	ITS SECURITY	Ferroviario	España	3		2
Cursos de formación técnica y práctica avanzada	Enfocados a la protección de aplicaciones, sistemas, infraestructura y redes de control y automatización industrial. Temario adaptable al público asistente: iniciación, intermedio o avanzado. Sesiones prácticas acordes a los conceptos abordados.	ITS SECURITY	Industria, Energía, Transporte	España	6	CISA, GICSP	
Curso intensivo en Ciberseguridad Industrial. Conceptos, ataques, contramedidas y procedimientos	Curso modular de hasta tres días de duración y estructurado en 12 sesiones. Dirigido a clientes finales e integradores de sistemas donde permitirá a los asistentes entender el alcance de la ciberseguridad industrial, de los riesgos y amenazas que pueden sufrir en sus operaciones del día a día y ayudarles a poner en práctica las recomendaciones propuestas durante su desarrollo.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH	30
FEE(P) Cybertraining	Solución avanzada para la formación práctica, entrenamiento, experimentación, pruebas e investigación en ciberseguridad, ofreciendo a nuestros clientes un entorno avanzado con el cual mejorar sus capacidades de detección, reacción y respuesta ante ciberataques. Soporta cinco tipos de ejercicios, cada uno específicamente orientado a entrenar un conjunto particular de habilidades: Ciberguerra, Análisis Forense, Desarrollo Seguro, Ciberataque (incluye eventos "Capture the Flag") y Ciberdefensa. La plataforma permite configurar itinerarios formativos con los contenidos específicos de cualquier certificación a efectos de entrenamiento pero la certificación debería obtenerse en un centro de examen acreditado.	MINSAIT	Todos	Global	10	CISA, CISM, CISSP, CEH, CRISC, CGEIT, CCNP Security, Lead Auditor ISO 27001/20000, etc.	3
Formación ICS/SCADA	Generación de materiales formativos e impartición de sesiones de formación en ciberseguridad para sistemas de control industrial ICS/SCADA.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	12

ÍNDICE

FORMACIÓN (7/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Formación a directivos de IICC	Generación de materiales formativos e impartición de sesiones de formación a directivos de compañías de sectores catalogados como IICC.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	12
Ciberseguridad en Entornos OT	Formación sobre Ciberseguridad Industrial dirigida a los responsables de entornos de operación.	PHOENIX CONTACT	Todos	Global	10		
Formación para Protección de Infraestructuras Críticas	El contenido de los cursos está orientado a personal que desempeña su labor en Infraestructuras Críticas. El objetivo es mejorar el conocimiento en seguridad para incrementar la protección de dichas instalaciones. Con esa meta, las sesiones de adaptan para distintos perfiles de asistentes dentro de la organización.	S2 GRUPO	Todos	Global	ITIL, PMP, PRINCE2, CISA, CISM, CRISC, ISO 27001 Certified Lead Auditor, ISO 22301 Certified Lead Auditor, CISSP, GPEN, GICSP, APMG ISO 20000, APMG CMDB	FIRST, TF-CSIRT Trusted Introducer, ISO 9001, UNE 166002, ISO 27001, ISO 14001, ISO 20000-1	>10
Curso de estrategias de defensa frente a ciberataques industriales	Formación sobre aspectos generales de ciberseguridad industrial en cuatro módulos: i) aspectos introductorios de la ciberseguridad industrial (por ejemplo, TI vs ICS / OT ciberseguridad, tendencias, etc.), ii) técnicas utilizadas en ataques recientes contra ICS (ej. CrashOverride), iii) tecnología de seguridad para proteger Sistemas ICS (ej., cortafuegos industriales, solución de detección de anomalías, listas blancas de aplicaciones...), iv) mejores prácticas de seguridad cibernética para la seguridad ICS (ej. gestión de vulnerabilidades, gestión de parches, acceso remoto, protección de medios extraíbles, etc.).	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC	>10
Curso sobre cortafuegos e IDS/IPS industriales	Formación práctica sobre tecnologías como IDS/IPS industriales y cortafuegos industriales, incluidas sus versiones reforzadas (rugged), capacidades BDPI y DPI, etc.	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC	>6

ÍNDICE

FORMACIÓN (8/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Curso de gestión de redes y seguridad	Formación a la cartera de clientes sobre la gestión de riesgos en redes.	SARENET	Todos	España	>10	Certificación de fabricantes líderes en seguridad	N/A
Phosforea®: solución e-learning para la formación y concienciación en ciberseguridad	Mas de 600 módulos de formación en modalidad blended-learning sobre todos los temas de ciberseguridad: criptografía, seguridad en los proyectos, seguridad en los desarrollos web, hacking ético, análisis de código, seguridad de infraestructuras...	SCASSI CIBERSEGURIDAD	Todos	Global	15	No	>9000
Formaciones presenciales en Ciberseguridad Formaciones de grupo o In-Company	Formaciones sobre métodos de análisis y de gestión de riesgos (ISO 27005 Risk Manager, MEHARI Advanced Practitioner, EBIOS Advanced Practitioner Formaciones de continuidad de negocio (Elaborar y gestionar un Plan de continuidad, ISO 22301, ISO 24762 Implementar y gestionar la reanudación del negocio). Formaciones de gestión de la seguridad (Definir y controlar los indicadores y las hojas de ruta del SSI, Elaborar y gestionar una política de seguridad, Seguridad en los proyectos). Formaciones técnicas sobre seguridad (Principios básicos de la seguridad de la información, Auditoría de seguridad de las redes y los sistemas, Seguridad de la nube y virtualización, Seguridad de las aplicaciones, Auditoría de código, ISO 27034, CISSP) Ciberseguridad de OT (Seguridad de sistemas críticos (Scada, ICS, etc.).	SCASSI CIBERSEGURIDAD	Todos	Global	15	ISO27001, ISO 27005, MEHARI, ISO 22301, EBIOS, ISO 27034, CISA, CISSP	50
Seguridad de sistemas críticos (Scada, ICS, etc.)	A partir de la descripción de distintos tipos de sistemas críticos ilustrados con 3 ejemplos concretos procedentes directamente de la experiencia adquirida, esta formación trata los distintos aspectos de la seguridad de dichos sistemas (riesgos, medidas técnicas, etc.) en todas las fases de su ciclo de vida (concepción, despliegue, implementación y uso).	SCASSI CIBERSEGURIDAD	Sector industria	Global	6		5
Security Awareness Training	Transmisión de conocimiento para asegurar el "weakest link" - SITRAIN training. - Web-based, training de una hora. - Generar concienciación de seguridad en plantilla. Introducir escenario actual de amenazas, descripción de como manejar y ayuda en la identificación de incidentes de seguridad.	SIEMENS	Todos	Global			
Curso de Ciberseguridad en la smartgrid	Curso de ciberseguridad en la smartgrid sobre las instalaciones y laboratorios de Tecnalia y de forma remota.	TECNALIA	Smartgrid	Global	4		>10

ÍNDICE

FORMACIÓN (9/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Cyber exercises	CyberAcademy+ dispone de un servicio para el diseño, implementación, documentación y ejecución de ejercicios de simulación de incidentes de cibseguridad. Los ciber ejercicios permiten a las empresas evaluar el nivel de madurez de sus equipos, principalmente los equipo de respuesta de incidentes. Aportamos gran experiencia en el desarrollo de escenarios simulados tanto virtuales como estáticos que ponen a prueba, no solo los conocimientos técnicos de los equipos sino además ponen a prueba todos los sistemas internos de validación y procedimiento del cliente.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	Offensive Security Certified Professional Certified Professional Pentester (ICPP+) Certified Professional Web Applications Pentester (ICPWAP). CEH v8 ITIL Foundation v3 CompTia Security+ CRISC CISM CISA Offensive Security Certified Professional Offensive Security Advanced Web Attacks and Exploitation Offensive Security Wireless Attacks The CREST Practitioner Security Analyst CREST Registered Penetration Tester GIAC Gold Certification Program Offensive Security Web Expert Offensive Web Application Penetration Tester GIAC Certified Penetration Tester	Más de 5

ÍNDICE

FORMACIÓN (10/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Cyber Simulation (table top exercises)	CyberAcademy+ dispone de un servicio para el diseño, implementación, documentación y ejecución de ejercicios de simulación de crisis de ciberseguridad. Se construirán escenarios de crisis personalizados con múltiples líneas de decisión, posibles operativas, tácticas y estrategias. Plantean de manera realista y creíble situaciones críticas o de emergencia de carácter virtual a las que deben responder las distintas unidades y equipos de una organización.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	Offensive Security Certified Professional Certified Professional Pentester (ICPP+) Certified Professional Web Applications Pentester (ICPWAP). CEH v8 ITIL Foundation v3 CompTia Security+ CRISC CISM CISA Offensive Security Certified Professional Offensive Security Advanced Web Attacks and Exploitation Offensive Security Wireless Attacks The CREST Practitioner Security Analyst CREST Registered Penetration Tester GIAC Gold Certification Program Offensive Security Web Expert Offensive Web Application Penetration Tester GIAC Certified Penetration Teste	3

FORMACIÓN (11/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
CTF	Servicio Global para el diseño y creación de retos con el objetivo de desarrollar competiciones de Capture The Flag (captura la Bandera) en ciberseguridad. Permite medir conocimientos y habilidades de offensive, defensive y forensic, mejorar la concienciación en seguridad etc. Permite la réplica de situaciones reales de amenazas cibernéticas en las empresas. Uso de los frameworks MITRE y NICE para el diseño de retos. Los escenarios pueden proporcionar una simulación realista de los impactos de una amenaza cibernética en las empresas.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	Offensive Security Certified Professional Certified Professional Pentester (ICPP+) Certified Professional Web Applications Pentester (ICPWAP). CEH v8 ITIL Foundation v3 CompTia Security+ CRISC CISM CISA Offensive Security Certified Professional Offensive Security Advanced Web Attacks and Exploitation Offensive Security Wireless Attacks The CREST Practitioner Security Analyst CREST Registered Penetration Tester GIAC Gold Certification Program Offensive Security Web Expert Offensive Web Application Penetration Tester GIAC Certified Penetration Teste	Más de 5

ÍNDICE

FORMACIÓN (12/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Academia Virtual	Acceso a la Academia virtual para llevar a cabo los cursos que ofrece CyberAcademy+. La solución integra tanto teoría como práctica. Es posible llevar a cabo un control en todo momento sobre el progreso. Cursos y píldoras de aprendizaje bajo el framework NIST enfocados en las siguientes disciplinas: Certified Professional Pentester, Certified Studen Pentester, Digital Forensics Windows, Incident Responder, CREST Practitioner Security Analyst, CREST Registered Tester.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	Offensive Security Certified Professional Certified Professional Pentester (ICPP+) Certified Professional Web Applications Pentester (ICPWAP). CEH v8 ITIL Foundation v3 CompTia Security+ CRISC CISM CISA Offensive Security Certified Professional Offensive Security Advanced Web Attacks and Exploitation Offensive Security Wireless Attacks The CREST Practitioner Security Analyst CREST Registered Penetration Tester GIAC Gold Certification Program Offensive Security Web Expert Offensive Web Application Penetration Tester GIAC Certified Penetration Teste	Más de 6

ÍNDICE

FORMACIÓN (13/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Seguridad y continuidad	Formación en seguridad y continuidad, en las distintas áreas en las que la empresa presta sus servicios: ISO 27001; ISO22301; ISO9001; CSA-STAR.	TELEFÓNICA - GOVERTIS	Todos	Global	12	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP	>25
ISO 27001	Formación en materia de Seguridad de la Información. ISO 27001.	TELEFÓNICA - GOVERTIS	Todos	Global	12	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP	>25
ENS	Formación en sistemas y servicios afectados por el ENS: Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP	>25
ENI	Formación en los contenidos del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.	TELEFÓNICA - GOVERTIS	Todos	Global	12	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP	
Protección de Datos	Formación en el Reglamento Europeo de Protección de Datos. Formación Delegado Protección de datos (DPD)	TELEFÓNICA - GOVERTIS	Todos	Global	25	Acreditación DPD según esquema AEPD, CDPSE	>50

ÍNDICE

FORMACIÓN (14/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
Ti School - Introducción al hacking en sistemas de control industrial	El objetivo de esta formación es conocer las particularidades de los sistemas de control y cómo pueden ser aprovechadas por terceras partes maliciosas para interrumpir nuestros procesos industriales	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADAguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE	
Ciberseguridad en Entornos OT	Formación transversal en Ciberseguridad Industrial dirigida a los diferentes perfiles profesionales que intervienen en capa una de las fases del ciclo de vida de la planta (diseño, construcción y puesta en marcha y O&M).	TSK	Energía, Plantas industriales, Medio ambient	Global	1	Lead Auditor ISO 27000, Lead Auditor ISO 20000, CCNA, NS4, CISSP, CEH, ITIL SO	
Ciberseguridad SCADA	Seguridad en sistemas de Supervisory Control and Data Acquisition (SCADA).	TÜViT	Industria	Global	>5	Ethical Hacker	>10
Ciberseguridad Industrial	Concienciación para ciberseguridad en general.	TÜViT	Todos	Global	>5	Ethical Hacker	>20
Certificación de Ofrecedores de Servicios Confianzas	ETSI y nueva regulación eIDAS.	TÜViT	Ofrecedores de Servicios Confianzas	Global	>5	ETSI Auditor y ISO 27001 Lead Auditor	>20
Centro de Procesamiento de Datos (CPD)	Seminario especializado del Esquema de Trusted Site Infrastructure.	TÜViT	Todos	Global	>8	TSI Professional	>200
ISO 27001	Formación Lead Auditor, Formación implementación ISMS. Cursos on-line.	TÜViT	Todos	Global	>10	ISO 27001 Lead Auditor	>20

ÍNDICE

FORMACIÓN (15/15)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Número de referencias
ISO 20000	Formación Lead Auditor, Formación implementación ISMS. Cursos on-line.	TÜViT	Todos	Global	>5	ISO 20000 Lead Auditor	>20
ISO 22301	Formación Lead Auditor, Formación implementación ISMS. Cursos on-line.	TÜViT	Todos	Global	>5	ISO 22301 Lead Auditor	>20
IT Security Basics	IT Security Basics.	TÜViT	Todos	Global	>5	Ethical Hacker	>50
Formación de la seguridad de los sitios web	Formación de la seguridad de los sitios web.	TÜViT	Todos	Global	>5	Ethical Hacker	>20
Common Criteria (CC, ISO 15408)	Common Criteria (CC, ISO 15408) en general, CC Documentation Writing Workshop for Developers, CC Audit Workshop.	TÜViT	Todos	Global	>40	Evaluador de CC	>30
Esquema Nacional de Seguridad	Curso especializado sobre el Esquema Nacional de Seguridad.	TÜViT	Todos	Global	>2	ISO 27001 Lead Auditor	>30

ÍNDICE

TÉCNICO (1/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Implantación de tecnologías de seguridad	Diseño e implantación de arquitecturas de seguridad en entornos industriales.	ACCENTURE	Todos	Global	100	CISA, CISM, CISSP, ITIL, Certificaciones de fabricantes de ciberseguridad	ISO 900, ISO 27001, ISO 20000, ISO 14001, CMMI L5	100
Infraestructuras de Seguridad en entornos industriales	Análisis, Diseño, Implantación, Operación y Mantenimiento de plataformas de seguridad en entornos industriales.	ATOS	Todos	Global	40	CISA, CISM, CRISC, CISSP, SSCP, ITIL, PMP, ISO 27001/22301 LEAD AUDITOR, CobIT, PCI QSA, CDPP, CEH, CCNA, CCNP, CCSA, CCSE, CCNSP	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL	20
Implantación de sistemas de seguridad específicos para entornos industriales	Servicio de implantación que incluye el diseño de alto y bajo nivel, instalaciones piloto, pruebas de concepto, test de aceptación y despliegues generales.	AXIANS	Todos	Europa	5	CISA, CISM, ITIL, CISSP	9001, 166002, 27001, 14001, 20000	5
Centro de demostración y laboratorio	Laboratorio con entornos de networking, seguridad y movilidad, video IP, servicios gestionados, datacenter y virtualización y comunicaciones unificadas.	AXIANS	Todos	España	5	CISA, CISM, ITIL, CISSP	9001, 166002, 27001, 14001, 20000	N/A
Seguridad de red	Diseño, implantación y soporte de arquitecturas de seguridad de red: NG Firewall, IPS, SIEM, Proxy, WAF, ATP, VPN, DPI, Data diode.	CIC Consulting Informatico	Todos	Global	6	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	>25
Seguridad de servidores y end point	Diseño, implantación y soporte de arquitecturas de controles de seguridad en servidores y endpoints: bastionado, anti-malware, Advanced EndPoint Protection (AEP), whitelisting.	CIC Consulting Informatico	Todos	Global	3	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	12

ÍNDICE

TÉCNICO (2/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Control de Acceso	Diseño, implantación y soporte de arquitecturas de controles de seguridad para el control de acceso lógico en redes (cableadas y wifi) y aplicaciones: SSO, LDAP, NAC.	CIC Consulting Informatico	Todos	Global	3	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	4
SIEM	Diseño, implantación y soporte de arquitecturas de controles de seguridad para la monitorizacion de seguridad en redes IT y OT.	CIC Consulting Informatico	Todos	Global	4	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	1
Continuidad de negocio	Diseño, implantación y soporte de arquitecturas de sistemas para la continuidad de negocio apoyados en servicios cloud MS Azure (ASR) y AWS de Amazon.	CIC Consulting Informatico	Todos	Global	4	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	2
Operaciones de seguridad	Servicios de operación y mantenimiento de la seguridad de las infraestructuras tecnológicas del cliente: monitorización, gestión de vulnerabilidades y parcheado, actualización de firmas.	CIC Consulting Informatico	Todos	Global	10	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	5
Seguridad de Red	Diseño, instalación y gestión de tecnologías de seguridad de red, Firewall, IPS, SIEM, Proxy, VPN.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Monitorización y Gestión de Red	Monitorización de redes de comunicaciones e infraestructuras. Gestión de tráfico, anchos de banda. Control accesos. En redes cableadas e inalámbricas.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Instalación y configuración de Sistemas SIEM	Implantación y puesta en marcha de soluciones SIEM.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Hacking Ético	Test y pruebas de Seguridad en Red.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Test de Intrusión en entornos industriales	Análisis de vulnerabilidades en entornos industriales.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		

ÍNDICE

TÉCNICO (3/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Monitorización de la seguridad de las plantas industriales	Monitorización de la seguridad de los ICS en las plantas industriales a través de análisis en tiempo real de red, basado en reconocimiento de protocolos y tendencias.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Sistemas de autenticación biométrica	Diseño e implementación de sistemas de autenticación biométrica.	EURECAT	Todos	Global	4		ISO 9001	3
Sistemas de seguridad distribuidos	Diseño e implementación de sistemas de seguridad distribuidos basados en Inteligencia Artificial.	EURECAT	Todos	Global	4		ISO 9001	2
Ciberseguridad en dispositivos electrónicos	Evaluación de la ciberseguridad de dispositivos electrónicos y definición de requerimientos de seguridad.	EURECAT	Todos	Global	3		ISO 9001	3
CONNtrol - Securización de sistemas	Planificación, diseño, despliegue y configuración de la securización de sistemas de control.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
CONNtrol - Monitorización ciberseguridad de sistemas	Supervisión, gestión y monitorización de la seguridad de sistemas de control.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
CONNtrol - Mantenimiento ciberseguridad de sistemas	Mantenimiento preventivo y correctivo de seguridad en sistemas de control.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
Defensa en Profundidad	Medidas de modelado de zonas y defensa en profundidad.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30

ÍNDICE

TÉCNICO (4/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicios de VP Hardening y Bastionado en sistemas de control	Implantación de soluciones de bastionado para sistemas SCADA, White Listing, Checksum y parcheado virtual.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
Implantación de tecnologías de seguridad en OT	Tecnologías de seguridad para entrono Industrial (Diodo de datos, firewall DEP industrial, IDS/IPS, Anti APT, Anti Malware.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
Integración de soluciones de ciberseguridad en Centros de Control	Diseño, instalación, parametrización, soporte y mantenimiento de soluciones de ciberseguridad IT en Centros de Control Industrial y puntos de frontera entre redes OT e IT.	GMV	Todos	Global	7	CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, CEH, GCIH, GCFA, GREM y GSEC	ISO 9000, UNE 166002, ISO 14001, ISO 27001, ISO 20000, ISO 22301, CMMI L3	2
Benchmarking de soluciones de ciberseguridad	Comparativa entre distintas soluciones tecnológicas de ciberseguridad aplicadas a un entorno de pre-producción.	GMV	Todos	Global	7	CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, CEH, GCIH, GCFA, GREM y GSEC	ISO 9000, UNE 166002, ISO 14001, ISO 27001, ISO 20000, ISO 22301, CMMI L3	3
Auditorías de Ciberseguridad	Revisión del estado de seguridad del entorno tecnológico principal del cliente, de forma que permita detectar las vulnerabilidades y debilidades existentes, determinar la criticidad de las mismas en relación a los sistemas de producción y establecer tanto las medidas técnicas y organizativas que permitan prevenir/disminuir los riesgos asociados a las mismas, así como las posibles medidas adicionales que se consideren adecuadas para incrementar el nivel de seguridad.	GRUPO SIA	Todos	Global	50	CISA, CISM, CISSP CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad Mº Interior, Postgrado Análisis de Inteligencia	ISO 9001, ISO 14001, ISO 27001, ISO 20000, PCI-QSA, ISO 22301, ISO 15504 L3	>40

ÍNDICE

TÉCNICO (5/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Red Team	Análisis de seguridad por expertos en seguridad digital, física y social, que tienen por objetivo la realización de una intrusión real y controlada en una organización.	GRUPO SIA	Todos	España	5	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad Mº Interior, Postgrado Análisis de Inteligencia	ISO 9001, ISO 14001, ISO 27001, ISO 20000, PCI-QSA, ISO 22301, ISO 15504 L3	8
Pentest	Análisis de seguridad con el objetivo de realizar una intrusión a los sistemas del cliente.	GRUPO SIA	IT	Global	15	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad Mº Interior, Postgrado Análisis de Inteligencia	ISO 9001, ISO 14001, ISO 27001, ISO 20000, PCI-QSA, ISO 22301, ISO 15504 L3	40
Seguridad de dispositivos "endpoints"	Integración de servicios en los equipos finales (HMI) para la descarga de actualizaciones automáticas y centralizadas. Integración de los equipos SCADA en planes de Recuperación ante desastres. Integración técnica de monitorización de servicios de equipos finales.	INYCOM	Todos	Global	>20	Certified Ethical Hacking, AENOR ISO 27001 Auditor, AENOR ISO 20000 Auditor, AENOR LOPD Auditor	AENOR ISO27001, AENOR ISO20000-1	

ÍNDICE

TÉCNICO (6/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Seguridad de infraestructura lógica	Implementación de soluciones para segmentación lógica y segura en la red industrial. Implementación de Zonas seguras (DMZ) en planta. Implementación de servidores de control de acceso en la red industrial. Implementación de servidores de control de actualizaciones de sistema operativo y antimalware en planta. Implementación de servidores para copias de seguridad y Disaster Recovery en planta. Implementación de redundancia en enlaces de comunicaciones de planta industrial. Implementación de seguridad entre PCN (Process Control Network) y PIN (Plant Information Network). Implementación de seguridad para acceso remoto a redes SCADA. Control de operadores con Implementación de controladores de dominio independientes para usuarios de la red SCADA. Implementación de servicios de monitorización de la electrónica de comunicaciones en la planta. Implementación de redes inalámbricas seguras para entorno industrial.	INYCOM	Todos	Global	>20	CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU, AENOR ISO 27001 Auditor, AENOR ISO 20000 Auditor, AENOR LOPD Auditor, Ethical Hacker	AENOR ISO27001, AENOR ISO20000-1	
SEGURIDAD "IIoT"	Seguimiento de la arquitectura de referencia concreta para la seguridad IIoT (Industrial Internet of Things). Análisis e implantación de seguridad para cada dispositivo conectado, seguridad para la comunicación en la trasferencia de datos a cloud y seguridad en la administración de toda la infraestructura conectada en la planta industrial.	INYCOM	Todos	Global	>20	Certified Ethical Hacking, AENOR ISO 27001 Auditor, AENOR ISO 20000 Auditor, AENOR LOPD Auditor	AENOR ISO27001, AENOR ISO20000-1	
KICS - SECURITY	Integración Técnica de KICS: Protección Ciberseguridad Industrial (ICS). Control de integridad del Hardware y Software, Control de privilegios de aplicaciones, Control de acceso al dispositivo, Host-based Firewall y Prevención de intrusiones, Prevención automática de Exploit y Seguridad de SCADA, Comprobación de integridad del PLC, Avanzada protección anti-malware, Actualizaciones de confianza, Evaluación de la vulnerabilidad, La implementación centralizada, La gestión y el control centralizado de anomalías en redes de control de proceso.	INYCOM	Todos	España	1	Technical training #KL 038.10		

ÍNDICE

TÉCNICO (7/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Integración de soluciones de Ciberseguridad en Centros de Control	Diseño, implantación y gestión de los centros de control coordinando tanto la de IT como OT.	ITS SECURITY	Trasporte, Industria, Energía	Iberia	6	CISA, GICSP	ISO 27001	7
Firewalls industriales, Diodos de Datos, electrónica de red	Implantación y gestión de Firewalls Industriales, Diodos de Datos y Electrónica de Red en entornos OT.	ITS SECURITY	Trasporte, Industria, Energía	Iberia	10	CISA, GICSP	ISO 27001	2
Arquitecturas Resilientes	Diseño e implantación de arquitecturas resilientes en entornos industriales. Segmentación y fortificación de redes OT.	ITS SECURITY	Trasporte, Industria, Energía	Iberia	10	CISA, GICSP	ISO 27001	3
Test de Intrusión en entornos industriales	Análisis de vulnerabilidades en entornos industriales.	ITS SECURITY	Todos	Iberia	10	CISA, GICSP	ISO 27001	10
Pruebas de estrés y planes de disaster recovery	Diseño y realización de pruebas de estrés sobre los sistemas críticos, así como el desarrollo e los planes de disaster recovery.	ITS SECURITY	Todos	Iberia	4	CISA, GICSP	ISO 27001	6
Servicio de monitorización subestaciones	Servicio de monitorización de la seguridad del protocolo IEC-61850 y la monitorización de los dispositivos, IEDs que alberga la subestación en términos de seguridad y resiliencia.	ITS SECURITY	Eléctrico	Global	4	CISA, GICSP	ISO 27001	1
Evaluación de seguridad a endpoints (RTUs, PLCs, IEDs, dispositivos adhoc, etc.)	Hacking ético a dispositivos industriales (caja negra, caja blanca, caja gris).	ITS SECURITY	Todos	Global	4	CISA, GICSP	ISO 27001	5
Integración de sistemas criptográficos ligeros en sistemas industriales	Empleo de sistemas criptográficos ligeros en sistemas con restricciones de tiempo muy elevados como por ejemplo en la subestaciones con el IEC 61850.	ITS SECURITY	Todos	Global	4	CISA, GICSP	ISO 27001	5

ÍNDICE

TÉCNICO (8/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Monitorización de la seguridad de las plantas industriales	Monitorización de la seguridad de los SCI en las plantas industriales a través de indicadores sujetos a patrones de comportamiento.	ITS SECURITY	Todos	Global	10	CISA, GICSP	ISO 27001	2
Protección ante fuga de datos	Sistema de protección de fuga de datos en el entorno IT y OT.	ITS SECURITY	Todos	Global	5	CISA, GICSP	ISO 27001	6
Integración y soporte de soluciones de seguridad en entornos IACS	Planificación, diseño, despliegue y configuración de soluciones de seguridad tecnológicas para sistemas OT. Las soluciones incluyen antivirus, IPS/IDS, firewalls industriales, análisis dinámico, tecnologías de listas blancas, diodos de datos, etc.	ITS SECURITY	Industria, Energía, Transporte	España	4			
Instalación, despliegue y puesta en marcha de firewalls industriales DPI	Instalación, despliegue y puesta en marcha de firewalls industriales DPI.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		8
Instalación, despliegue y puesta en marcha de Diodo de Datos	Instalación, despliegue y puesta en marcha de Diodo de Datos.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2
Instalación, despliegue y puesta en marcha de dispositivos para la realización de whitelisting de protocolos	Instalación, despliegue y puesta en marcha de dispositivos para la realización de whitelisting de protocolos.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2
Despliegue, puesta en marcha y formación de tecnología antimalware para entornos OT	Despliegue, puesta en marcha y formación de tecnología antimalware para entornos OT.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2

ÍNDICE

TÉCNICO (9/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue, puesta en marcha y formación de tecnologías SNMP Monitor	Despliegue, puesta en marcha y formación de tecnologías SNMP Monitor.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		1
Despliegue y puesta en marcha de dispositivos de electrónica de red para acceso remoto seguro a entorno OT	Despliegue y puesta en marcha de dispositivos de electrónica de red para acceso remoto seguro a entorno OT.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		1
Instalación, despliegue y puesta en marcha de Diodo de Datos	Instalación, despliegue y puesta en marcha de Diodo de Datos.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2
Instalación, despliegue y puesta en marcha de dispositivos para la realización de whitelisting de protocolos	Instalación, despliegue y puesta en marcha de dispositivos para la realización de whitelisting de protocolos.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2
Despliegue, puesta en marcha y formación de tecnología antimalware para entornos OT	Despliegue, puesta en marcha y formación de tecnología antimalware para entornos OT.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		2
Despliegue, puesta en marcha y formación de tecnologías SNMP Monitor	Despliegue, puesta en marcha y formación de tecnologías SNMP Monitor.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		1

ÍNDICE

TÉCNICO (10/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue y puesta en marcha de dispositivos de electrónica de red para acceso remoto seguro a entorno OT	Despliegue y puesta en marcha de dispositivos de electrónica de red para acceso remoto seguro a entorno OT.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		1
Gestión de cambios	Despliegue de soluciones para la gestión de cambios en entornos OT.	LOGITEK	Todos	España, Portugal	3	IEC62443, CEH, CSSA, CCNA	ISO 9001	15
Implantación tecnologías tolerantes a fallos	Despliegue de sistemas de computación con tolerancia a fallos (99,999+% disponibilidad garantizada).	LOGITEK	Todos	España	2	IEC62443, CEH, CSSA, CCNA	ISO 9001	10
Soluciones de protección para infraestructuras de red y centros de datos	Diseño, implantación y soporte de arquitecturas de seguridad (NG Firewall, NG IPS, SIEM, Proxy e eMail, WAF, SSO, VPN, DDoS, APS's y Malware dinámico).	NTT	Todos	Global	73	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	
Soluciones de Control de Acceso	Diseño, implantación y soporte de soluciones de control de acceso tanto cableada como WiFi mediante NAC y BYOD.	NTT	Todos	Global	73	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	
Soluciones de seguridad para la Navegación y el correo electrónico	Diseño, implantación y soporte de soluciones de navegación mediante proxy, filtrado de URLs, AV de navegación y de soluciones de correo mediante antispam y malware en correo.	NTT	Todos	Global	73	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	
Oylo Senses	Servicio de Consultoría e implementación de soluciones del ámbito Industrial.	OYLO Trust Engineering	Industrial	España y Latinoamérica	25	14	ISO 27002/22301/ ENS/LEET SECURITY	38

ÍNDICE

TÉCNICO (11/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Diseño de topología de red segura	Soporte en diseño y puesta en marcha de una red de control segura. - Tecnologías y estándares de redundancia de red para mayor disponibilidad - Segmentación de celdas de red conforme a ISA99/IEC 62443 - Creación de zona desmilitarizada DMZ - Configuración adecuada de las reglas para Firewall perimetral. - Implementación de reglas de firewall DPI para protocolos Modbus TCP o OPC DA.	PHOENIX CONTACT	Todos	Global	6			
Firewalling avanzado en industria	Qué, cómo y dónde instalar de forma adecuada un firewall en industria. Como configurar adecuadamente reglas de firewall perimetral Inspección profunda de paquetes por protocolos industriales (Modbus TCP, OPC DA..). Securización de puntos de acceso remoto. Firewall dentro de las VPN VPN con Firewall interno implementado. Defensa Avanzada: Chequeos de Integridad en sistemas de archivos de IPC para protección de sistemas SCADA.	PHOENIX CONTACT	Todos	Global	4			
Despliegue de soluciones de segmentación de red	Servicios de implementación, configuración, mantenimiento y soporte de cortafuegos con capacidades de filtrado OT (por ejemplo, DPI de protocolos industriales como OPC, Modbus TCP, etc.).	S21SEC	Cualquiera	España, Europa y Latinoamérica	>14	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio (Fortinet, PaloAlto, Checkpoint, Stormshield, Cisco, F5)	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5

ÍNDICE

TÉCNICO (12/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue de soluciones de acceso remoto seguro	Servicios de implementación, configuración, mantenimiento y soporte de soluciones específicas para un acceso remoto seguro a PLC, RTU, etc., evitando una exposición real de los servicios a los que se accede.	S21SEC	Cualquiera	España, Europa y Latinoamérica	>14	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA Certificaciones de fabricantes relacionados con el servicio (Fortinet, PaloAlto, Checkpoint, Stormshield, Cisco, F5)	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
Despliegue de soluciones de protección de medios extraíbles	Servicios de implementación, configuración, mantenimiento y soporte de protección de medios extraíbles, que permiten protegerse frente a ataques de malware, ataques eléctricos (por ejemplo, USB Killer) y ataques de hardware (por ejemplo, BadUSB, ataque HID).	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5

TÉCNICO (13/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue de soluciones antimalware	Servicios de implementación, configuración, mantenimiento y soporte de soluciones antimalware para servidores SCADA y PC industriales.	S21SEC	Cualquiera	España, Europa y Latinoamérica	>14	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
Despliegue de soluciones de detección de anomalías	Servicios de implementación, configuración, mantenimiento y soporte de soluciones de detección de anomalías basadas en tráfico con capacidades BDPI para protocolos industriales, de detección de IoC, de identificación de vulnerabilidades, etc.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
Despliegue de soluciones de deception	Servicios de implementación, configuración, mantenimiento y soporte de soluciones de engaño basadas en honeypots de baja y alta interactividad para sistemas industriales, capaces de apuntar a grupos criminales concretos mediante el diseño de campañas específicas, etc.	S21SEC	Cualquiera	España, Europa y Latinoamérica	2	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	0

ÍNDICE

TÉCNICO (14/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue de soluciones de SIEM	Servicios de implementación, configuración, mantenimiento y soporte de soluciones SIEM con cuadros de mando preconfigurados y casos de uso para eventos provenientes de sistemas de automatización y de control industrial, así como de soluciones de seguridad industrial.	S21SEC	Cualquiera	España, Europa y Latinoamérica	>14	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
DFIR OT prebrecha	Conjunto de subservicios orientados a estar preparados ante un ataque: evaluación de preparación y detección de DFIR (mapa de calor de TTP), evaluación de BAS (por ejemplo, Cymulate), capacitación de DFIR y desarrollo del plan de respuesta a incidentes.	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	2

ÍNDICE

TÉCNICO (15/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Despliegue de soluciones de backup	Servicios de implementación, configuración, mantenimiento y soporte de soluciones de respaldo y restauración automatizadas dirigidas a la lógica de control de PLCs y programación SCADA/DCS para múltiples fabricantes.	S21SEC	Cualquiera	España, Europa y Latinoamérica	>14	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	2
DFIR OT bajo demanda postbrecha	Soporte con personal especializado (ej. certificación SANS GIAC Response and Industrial Defense) en un servicio DFIR donde los sistemas afectados incluyen sistemas ICS/OT. Las tareas abordadas por el personal de ICS incluyen: análisis forense de ICS, recopilación de tráfico y eventos de ICS, búsqueda activa de IoC y IoA en ICS, correlación y análisis de eventos.	S21SEC	Cualquiera	España, Europa y Latinoamérica	4	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	2
Seguridad de la lógica de red	Segmentación y separación entre redes Cloud/IT/OT/IIoT	SARENET	Todos	España	>10			
Seguridad IoT Industrial	Implementación de la seguridad de los dispositivos IoT en un entorno industrializado.	SARENET	Todos	España	>10			
Servicios de operación de red	Monitorización de eventos y fiscalización de tráficos en las redes de cliente.	SARENET	Todos	España	>10			
Ingeniería de clientes	Implementación de soluciones de seguridad y mantenimiento de activos de cliente.	SARENET	Todos	España	>10			

ÍNDICE

TÉCNICO (16/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
OPTIMIZE	Este servicio llave en mano permite racionalizar la infraestructura SSI de las organizaciones para optimizar su uso y reducir los costes relativos a la sobreutilización de recursos. Abarca tres etapas fundamentales: - Evaluación del estado de uso de la infraestructura en base a las necesidades reales de la organización. - Reconciliación de dichas necesidades con la infraestructura que realmente hace falta. - Reconfiguración del conjunto desde el punto de vista del mejor compromiso entre prestaciones, consumo y seguridad.	SCASSI CIBERSEGURIDAD	Todos	Global	6	CEH, CISSP		10
Secure&Guard	Análisis de Vulnerabilidades, es un servicio por medio del cual se comprueba la debilidad o fortaleza ante el conjunto de amenazas conocidas tanto para los elementos externos como para los elementos internos.	Secure&IT	Todos	Global	>5			1
Security Policy Consulting	Establecimiento de prácticas estándares de seguridad en Sistemas de Control Industrial (ICS). - Establecer nuevas o revisar las políticas de seguridad, procesos, procedimientos y trabajos existentes de base. - Integración con prácticas de ciberseguridad de la compañía. -Patch and backup strategy, handling of removable media…	SIEMENS	Todos	Global	7			
Network Security Consulting	Soporte en diseño y setup de seguridad de la red. - Cell segmentation en soporte de security cells basado en estandares IEC 62443 y SIMATIC PCS 7 & WinCC security concept. - Diseño y planificacion de red de proteccion perimetral: DMZ network (Desmilitarizada). - Establecimiento/revisión de las reglas para Firewall perimetral.	SIEMENS	Todos	Global				

ÍNDICE

TÉCNICO (17/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Perimeter Firewall Installation	Primera linea de defensa contra amenazas reveladas. - Basado en Automation Firewall Appliance. - Instalación, configuración, commissioning and test del sistema de firewall y reglas de trafico. - Configuration backup. - Consideracion aplicaciones especificas para cliente: (fine-tuning of intrusion detection/prevention system (IDS/IPS)).	SIEMENS	Todos	Global				
Clean Slate Validation	Validación “clean-slate”del status del entorno. - Identificación de brechas de seguridad gracias a virus scanning con dos motores de búsqueda diferentes. (McAfee Command Line Scanner and Kaspersky Rescue Disk). - Sin instalación.	SIEMENS	Todos	Global				
Anti Virus Installation	Protección antivirus y detección y prevención de malware. - Instalación y configuración de software Anti Virus. (McAfee Virusscan Enterprise Agents). - Instalación y configuración McAfee de una consola central para gestionar 10 agentes antivirus instalados. (ePO). - Compatibilidad con sistemas SIMATIC PCS 7.	SIEMENS	Todos	Global				
Whitelisting Installation	Protección antivirus y detección y prevención de malware. - Instalación y configuración de software Anti Virus. (McAfee Application Control). - Instalación y configuración McAfee de una consola central para gestionar 10 agentes antivirus instalados. (ePO). - Compatibilidad con sistemas SIMATIC PCS 7.	SIEMENS	Todos	Global				
System Backup	Sistema de Control Backup Industrial. - Performance of one-time backup of systems in plant environment -Symantec System Recovery software propiedad del cliente.	SIEMENS	Todos	Global				
Windows Patch Installation	Instalación de Microsoft OS Patches - Instalación de parches Microsoft OS via WSUS server en propiedad de cliente. - Consideración de compatibilidad: recomendación de parches compatibles tanto por proveedor como autorizado por el cliente.	SIEMENS	Todos	Global				

ÍNDICE

TÉCNICO (18/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Perimeter Firewall Management	Continua protección contra amenazas. - Monitoring, alarming and (monthly) reporting. - Management of Intrusion Detection / Prevention System (IDS/IPS). - Configuración y adaptación adaptions de politicas de firewall. - Backup / Upgrades del firmware y software del firewall.	SIEMENS	Todos	Global				
Anti Virus Management	Continua protección antivirus y estrategia de defensa up-to-date. - Update de firmas y licencias antivirus y scanning periódico de virus scanning. - Inclusión y tratamiento de Falsos positivos incluyendo cooperación para prevención de malware con proveedores de software. - Centralización y gestión a través de consola central (ePO). - Reporte mensual protección malware del entorno planta.	SIEMENS	Todos	Global				
Windows Patch Installation	Instalación de Microsoft OS Patches - Instalación de parches Microsoft OS via WSUS server en propiedad de cliente. - Consideración de compatibilidad: recomendación de parches compatibles tanto por proveedor como autorizado por el cliente.	SIEMENS	Todos	Global				
Perimeter Firewall Management	Continua protección contra amenazas. - Monitoring, alarming and (monthly) reporting. - Management of Intrusion Detection / Prevention System (IDS/IPS). - Configuración y adaptación adaptions de políticas de firewall. - Backup/Upgrades del firmware y software del firewall.	SIEMENS	Todos	Global				

TÉCNICO (19/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Anti Virus Management	Continua protección antivirus y estrategia de defensa up-to-date. - Update de firmas y licencias antivirus y scanning periódico de virus scanning. - Inclusión y tratamiento de Falsos positivos incluyendo cooperación para prevención de malware con proveedores de software. - Centralización y gestión a través de consola central (ePO). - Reporte mensual protección malware del entorno planta.	SIEMENS	Todos	Global				
Windows Patch Installation	Instalación de Microsoft OS Patches - Instalación de parches Microsoft OS via WSUS server en propiedad de cliente. - Consideración de compatibilidad: recomendación de parches compatibles tanto por proveedor como autorizado por el cliente.	SIEMENS	Todos	Global				
Perimeter Firewall Management	Continua protección contra amenazas. - Monitoring, alarming and (monthly) reporting. - Management of Intrusion Detection / Prevention System (IDS/IPS). - Configuración y adaptación adaptions de políticas de firewall. - Backup / Upgrades del firmware y software del firewall.	SIEMENS	Todos	Global				
Anti Virus Management	Continua protección antivirus y estrategia de defensa up-to-date. - Update de firmas y licencias antivirus y scanning periódico de virus scanning. - Inclusión y tratamiento de Falsos positivos incluyendo cooperación para prevención de malware con proveedores de software. - Centralización y gestión a través de consola central (ePO). - Reporte mensual protección malware del entorno planta.	SIEMENS	Todos	Global				

TÉCNICO (20/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Whitelisting Management	Continua protección whitelisting y estrategia de protección continua. - Update application control policy (excepto management) - Enforce application control policy con aprobación de cliente. - Centralización y gestión a través de consola central (ePO). - Reporte mensual application control del entorno planta.	SIEMENS	Todos	Global				
Patch & Vulnerability Management	Soporte para gestión de vulnerabilidades de software. - WSUS Server con información aprobada por Microsoft Security Patches para SIMATIC PCS 7. - Descarga automática y principal información en WSUS server de cliente.	SIEMENS	Todos	Global				
Arquitecturas resilientes	Diseño de arquitecturas resilientes y convergentes en entornos industriales.	TECNALIA	Eléctrica, Industria y Transporte	Global	7			>50
Evaluación de ciberseguridad de producto	Evaluación de ciberseguridad en productos y dispositivos como smartmeters, concentradores, IEDs, RTUs, PLC y otros dispositivos industriales.	TECNALIA	Eléctrica, Industria y Transporte	Global	10			>500
Adecuación de dispositivos de fabricantes de seguridad en entornos semi reales	Adecuación de los productos de fabricantes de seguridad en los laboratorios de Tecnalia para poder evaluarlos en entornos semi-reales o cuasi reales.	TECNALIA	Eléctrica	Global	3			>5

ÍNDICE

TÉCNICO (21/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Implantación de soluciones y tecnologías de seguridad	Diseño y despliegue de soluciones de seguridad en entornos industriales tales como firewalls, sondas de monitorizacion, TAPs, appliances de acceso remoto…	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 10	OPST, ACSA, Chief Auditor ISMS, FireEye Systems Engineer, FireEye Product Specialist, CISA, GCIH, GPEN, CEH, CISSP, OSCE, GXPN, CCNA, CPTE, ITIL Foundation v3, CCS-T, CCS-SP, Nozomi Networks Certified Engineer, Director de Seguridad, Investigador Privado, Information Security for Technical Staff, Fundamentals of Incident	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 5
Perimeter Protection - Protección perimetral	Perimeter Protection engloba todas las soluciones necesarias para mantener una red industrial protegida, segregándola, segmentándola y controlando el acceso de todos los dispositivos. Se basa en firewalls de nueva generación, diodos de datos, NAC y otras tecnologías.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE, Certificaciones fabricantes NGFW	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 20
Remote Access - Acceso remoto	Las soluciones de acceso remoto seguro son fundamentales en los entornos operacionales modernos. Permiten el acceso remoto cifrado, control de usuarios, gestión sencilla y trazabilidad de las acciones. Telefónica ofrece distintas tecnologías basadas en VPNs para dar la mejor solución para cada caso de uso.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE, Certificaciones fabricantes NGFW	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	

ÍNDICE

TÉCNICO (22/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Secure Credentials - Identificación/ autenticación de dispositivos	La identidad de un dispositivo IoT juega un papel crucial en el proceso de autenticación contra la plataforma de IoT. Secure Credentials automatiza el proceso de proporcionar una identida segura a los dispositivos IoT para acceder a los servicios para IoT en la nube pública.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	
Industrial Endpoint Protection - Protección de dispositivos industriales	Industrial Endpoint Protection engloba todas las tecnologías necesarias para mantener todos los equipos de la red industrial protegidos. Desde soluciones de EDR especializadas para industria hasta protección contra ataques eléctricos con USBs.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE, Certificaciones fabricantes EDR	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	3
OT&IoT Security Monitoring - Monitorización de seguridad en OT&IoT	OT&IoT Security Monitoring permite monitorizar la red industrial en busca de anomalías, malware, exploits e incluso problemas operacionales, generando a la vez un inventariado de todos los dispositivos. Cuenta con tecnologías especialistas para entornos OT, IoT y sanitarios.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE, Certificaciones fabricantes NBA/ IDS OT	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 5
Secure Factory of the Future - Fábrica del Futuro Segura	Secure Factory of the Future es un set de soluciones de seguridad a medida para redes industriales con conectividad 4G y 5G, ofreciendo protección de red, de dispositivos, análisis, auditoria y monitorización continuas con la mejor cobertura y latencia.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Nacional / Internacional	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE, Certificaciones fabricantes NGFW, NBA/IDS OT, EDR	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	
Infraestructuras críticas (IICC)	Integración de PSOs y PPEs para sector financiero con mejores prácticas internacionales.	TELEFÓNICA - GOVERTIS	Todos	Global	10	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		

ÍNDICE

TÉCNICO (23/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Unified Compliance Framework	Implantación de Marcos Unificados de Control sobre los que mapear distintas normas y estándares para simplificar las auditorías (normativa BCE, BdE, Secure Pay, PCI-DSS, auditoría interna, COBIT, 27002, CCM…).	TELEFÓNICA - GOVERTIS	Todos	Global	12	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		
Privacidad	Soporte jurídico + técnico. Reglamento Europeo de Protección de Datos. Expertos en legislación sobre Privacidad en LATAM.	TELEFÓNICA - GOVERTIS	Todos	Global	25	Acreditación DPD según esquema AEPD, CDPSE		100
Oficinas Técnicas de Ciberseguridad	Integración de personal experto IT/OT en los equipos de trabajo para dirigir o apoyar las tareas de ciberseguridad.	TELEFÓNICA - GOVERTIS	Todos	Global	20	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		20
Plan Director de Seguridad	Análisis de la situación de la compañía respecto a los estándares de seguridad (GAP Analysis), elaboración de un Análisis de Riesgos, evaluación del riesgo y planes de tratamiento de riesgos. Confección de un Roadmap de iniciativas en seguridad IT/OT.	TELEFÓNICA - GOVERTIS	Todos	Global	20	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		20
Pruebas de penetración	Comprobación de la fortaleza de su infraestructura IT con el fin de medir su grado de adecuación con su política de seguridad usando nuestros expertos y el software específico.	THALES	Todos	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	
Arquitectura IT	Evaluamos y redibujamos la arquitectura global de sus sistemas de información para mejorar su resiliencia.	THALES	Todos	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	
Gestión de crisis	Define escenarios de respuesta para crear un plan de acción creíble que abarque toda la compañía, con lo que se minimiza el impacto operacional, financiero y reputacional.	THALES	Todos	Global		CISM, ITIL Expert	ISO 27001	
Equipo de reacción rápida	Enviamos nuestros expertos en ciberseguridad in situ para responder inmediatamente a un incidente de seguridad.	THALES	Todos	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	

ÍNDICE

TÉCNICO (24/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Protección DDOS	Esta solución es operada desde Thales CSOC, que ofrece una gama completa de servicios que incluyen detección y respuesta 24/7 con monitorización, mitigación e informes de ataques DDoS, así como inteligencia de amenazas DDoS y gestión de cambios para asegurarse de que la solución se adapta continuamente a la configuración de red de clientes y el panorama actual de las amenazas.	THALES	Todos	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	
Consultoría técnica	Servicio orientado a la creación/adecuación de arquitecturas de seguridad basadas en el modelo de defensa en profundidad destinadas a proteger las infraestructuras y los sistemas de información de las organizaciones, mediante la aplicación tanto de conceptos como de soluciones de seguridad tecnológicamente avanzadas.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL		
Pre-certificación de sistemas y productos OT	Servicio orientado a la evaluación de sistemas y productos en base a un listado de controles de seguridad extraído de las principales guías de buenas prácticas y estándares de seguridad inherentes al sector industrial, con el objetivo de verificar que cumplen con un nivel de seguridad adecuado a su entorno de aplicación.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL		
Acompañamiento de ciberseguridad OT/IT	Servicio destinado al asesoramiento, planteamiento, diseño, ejecución y mantenimiento de un plan de proyectos de seguridad de forma evolutiva y controlada dentro de una organización, buscando el equilibrio entre seguridad y operatividad mediante la aplicación de "quick wins" en primera instancia.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL		
Integración de tecnologías de seguridad IT/OT	Diseño, configuración, despliegue y mantenimiento de soluciones de seguridad IT/OT (NGFW, IPS, Diodos de datos, SIEM, etc.) en la infraestructura de una organización, comprobando en todo momento que la solución seleccionada cumple con los requisitos necesarios para su integración.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL		
Servicio de laboratorio	Laboratorio industrial y centro demostrador destinado a la evaluación de tecnologías/productos y a la investigación de nuevas soluciones de seguridad aplicables al sector industrial.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	5	GICSP, CSSA, CISSP, ITIL		

ÍNDICE

TÉCNICO (25/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría técnica	Servicio orientado a la creación/adecuación de arquitecturas de seguridad basadas en el modelo de defensa en profundidad destinadas a proteger las infraestructuras y los sistemas de información de las organizaciones, mediante la aplicación tanto de conceptos como de soluciones de seguridad tecnológicamente avanzadas.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Acompañamiento de ciberseguridad OT/IT	Servicio destinado al asesoramiento, planteamiento, diseño, ejecución y mantenimiento de un plan de proyectos de seguridad de forma evolutiva y controlada dentro de una organización, buscando el equilibrio entre seguridad y operatividad mediante la aplicación de "quick wins" en primera instancia.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (26/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Ti Lab - Laboratorio Industrial	Laboratorio industrial y centro demostrador destinado a la evaluación de tecnologías/productos y a la investigación de nuevas soluciones de seguridad aplicables al sector industrial. Evaluación de sistemas y productos en base a un listado de controles de seguridad extraído de las principales guías de buenas prácticas y estándares de seguridad (IIC SMM, ETSI EN 303 645, OWASP Top 10 IoT, IEC 62443 for ICS), inherentes al sector industrial, con el objetivo de verificar que cumplen con un nivel de seguridad adecuado a su entorno de aplicación	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Virtualización de sistemas OT	Diseño, configuración, despliegue y mantenimiento de soluciones de virtualización OT (HMI, Historian, Aplicaciones industriales, etc.) en la infraestructura de una organización, comprobando en todo momento que la solución seleccionada cumple con los requisitos necesarios para su integración.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (27/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Networking (High Availability Industrial Routing and Switching)	Diseño, configuración, despliegue y mantenimiento de soluciones de red industrial (Alta disponibilidad de conmutación y enrutado en redes de control) en la infraestructura de una organización, comprobando en todo momento que la solución seleccionada cumple con los requisitos necesarios para su integración.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
NGFW (IT/OT Segmentation)	Diseño, configuración, despliegue y mantenimiento de soluciones de seguridad IT/OT (NGFW, IPS, Diodos de datos, SIEM, etc.) en la infraestructura de una organización, comprobando en todo momento que la solución seleccionada cumple con los requisitos necesarios para su integración.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (28/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Acceso remoto seguro a redes OT	Diseño, configuración, despliegue y mantenimiento de soluciones de acceso remoto seguro a la red OT (Jump Host, VPN, Password Vault, grabación de sesiones, etc.) en la infraestructura de una organización, comprobando en todo momento que la solución seleccionada cumple con los requisitos necesarios para su integración.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Bastionado de sistemas OT (Networking, OS, Apps,…)	Servicio destinado al asesoramiento, diseño, ejecución y pruebas de configuraciones mínimas en servidores de la red de control.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (29/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Controlador de dominio OT (Usuarios y Políticas de Seguridad)	Diseño, configuración, despliegue y mantenimiento de controladores de dominio de la red OT en la infraestructura de una organización, permitiendo la gestión unificada de usuarios y políticas de seguridad.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Gestión de parches en sistemas de control	Servicio destinado al diseño, ejecución y pruebas de las actualizaciones necesarias sobre los servidores de la red de control para mitigar vulnerabilidades.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (30/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión de vulnerabilidades en Sistemas OT	Servicio destinado a la gestión de vulnerabilidades de los diferentes elementos presentes en un ecosistema industrial (sistemas IT/OT, equipamiento embebido, redes de comunicaciones y electrónica de red, aplicaciones/servicios) mediante herramientas tanto de terceros como propietarias. Revisión periódica, diseño y ejecución de planes de mitigación e integración con la gestión de parches.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Titanium Honeypots	Diseño, configuración, despliegue y mantenimiento de señuelos en la red OT de la infraestructura de una organización, permitiendo la detección de intentos de intrusión y ataques a los sistemas.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (31/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
EPP (Endpoint Protection) / EDR (Endpoint Detection and Response)	Diseño, configuración, despliegue y mantenimiento de soluciones de protección ante Software malicioso centralizadas en la red OT, en función de las especificaciones de los fabricantes de sistemas de control.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Despliegue de soluciones de detección de anomalías en redes OT	Diseño, configuración, despliegue y mantenimiento de soluciones de detección de anomalías en el tráfico de red dn la red OT, propias y de terceros. (SilentDefense y Nozomi)	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (32/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Instalación y mantenimiento de soluciones SIEM OT	Diseño, configuración, despliegue y mantenimiento de soluciones de detección y correlación de eventos maliciosos en la red OT.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Backups (PLC, DCS, Robots, Engineering Workstations, HMI,…)	Diseño, configuración, despliegue y mantenimiento de soluciones de copias de seguridad centralizada de los dispositivos de la red OT, a distintos niveles (PLCs, DCS/SCADA, HMI, Historian, Servidores de aplicaciones industriales).	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (33/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Anti APT (Email, Network, Endpoint)	Diseño, configuración, despliegue y mantenimiento de soluciones de protección al correo electrónico y a los dispositivos finales de la red de control frente a Amenazas Avanzadas Persistentes.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Instalación y mantenimiento de Datadiode	Diseño, configuración, despliegue y mantenimiento de soluciones de conectividad unidireccional entre los dispositivos de la red OT, a distintos niveles (PLCs, DCS/SCADA, HMI, Historian, Servidores de aplicaciones industriales).	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

TÉCNICO (34/34)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Diseño e implantación de medidas de ciberseguridad en entornos y sistemas industriales	Fase de diseño de solución cibersegura y su implementación hardware/software en planta.	TSK	Energía, Plantas industriales, Medio ambiente	Global	4	Lead Auditor ISO 27000, Lead Auditor ISO 20000, CCNA, NS4, CISSP, CEH, ITIL SO	ISO9001, ISO14001, ISO27001, ISO45001, UNE166002	
Test de intrusión (hacking ético) en entornos y sistemas industriales	Test de intrusión y vulnerabilidades mediante técnicas no agresivas sobre sistemas industriales.	TSK	Energía, Plantas industriales, Medio ambiente	Global	4	Lead Auditor ISO 27000, Lead Auditor ISO 20000, CCNA, NS4, CISSP, CEH, ITIL SO	ISO9001, ISO14001, ISO27001, ISO45001, UNE166002	
Asesoría Técnica sobre Diseño de Redes IT	Identificación de los elementos vulnerables en las redes IT.	TÜViT	Todos	Global	>5	Ethical Hacker		

CONSULTORÍA (1/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cybersecurity Assesment	Evaluación del grado de madurez en ciberseguridad de un área de la compañía desde un punto de vista procedimental. Organizativo y tecnológico definiendo un roadmap de evolución.	ACCENTURE	Todos	Global	20	CISA, CISM, CISSP, ITIL, Certificaciones de fabricantes de ciberseguridad	ISO 9001 ISO 27001, ISO 20000, ISO 14001, CMMI L5	5
Plan de adecuación a LPIC	Análisis de situación y definición del plan de acción para la adecuación a la LPIC.	ACCENTURE	Todos	Global	30	CISA, CISM, CISSP, ITIL, Certificaciones de fabricantes de ciberseguridad	ISO 9001 ISO 27001, ISO 20000, ISO 14001, CMMI L5	0
Servicio de Identidades, Accesos, Firma Electrónica, Tarjetas Inteligentes y Biometría	Servicio de consultoría y asesoramiento tecnológico relativo a materias de Gobiernos y Administración de Identidades y Accesos, Federación de Identidades, Single Sign-On (Enterprise /Web), Gestión de Cuentas de Usuarios con Privilegios, Autenticación Fuerte, Firma Electrónica, Tarjetas Inteligentes y Biometría.	ATOS	Todos	Global	8	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	10
Servicios de Gestión de la Continuidad de Negocio (SGCN)	Diseño e Implantación de Sistemas de Gestión de la Continuidad de Negocio (SGCN) según ISO 22301. Realización de Business Impact Analysis (BIA), Diseño de soluciones de respaldo y de servicios de notificación de emergencia (EMNS), Diseño e implantación de los Planes de Continuidad, Diseño y ejecución de Planes de Pruebas, mantenimiento del SGCN a través de una herramienta (BCMP) propia.	ATOS	Todos	Global	15	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	30

ÍNDICE

CONSULTORÍA (2/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicios de Gestión de la Seguridad de la Información (SGSI)	Diseño e Implantación de Sistemas de Gestión de Seguridad de la Información (SGSI) según ISO/IEC 27001. Gestión del proceso de certificación de la norma ISO/IEC 27001.	ATOS	Todos	Global	15	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	15
Servicios de Análisis y Gestión de Riesgos	Análisis y Gestión de Riesgos de Seguridad y de TI. Diseño, implantación y gobierno de modelos de Gestión de Riesgos de TI (ITRM), basado en CobIT for Risk, ISO/IEC 27005 e ISO 31000.	ATOS	Todos	Global	40	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	20
Servicios de estrategia en seguridad	Planes Estratégicos y Directores de Seguridad de la Información, Planes de Seguridad de Operador de Infraestructuras Críticas. Assessments de Seguridad. Identificación de GAPs. Propuesta de Roadmap y seguimiento de su implantación.	ATOS	Todos	Global	30	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	20
Servicios de cumplimiento y homologación de proveedores	Servicios de adecuación y cumplimiento normativo y legal en materia de seguridad de la información (LOPD, PCI DSS, LPIC, ENS). Gestión, diseño, creación y revisión del cuerpo normativo en materia de seguridad de la información (Política, Normas y Guías de implantación). Servicios de homologación de seguridad de proveedores.	ATOS	Todos	Global	10	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	8

ÍNDICE

CONSULTORÍA (3/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Oficinas técnicas de seguridad	Servicios de apoyo y soporte al proceso de seguridad corporativo. Seguimiento de actividades y proyectos de seguridad, asesoramiento experto y dedicado al cliente, control de KPIs de seguridad, implantación y mantenimiento de cuadros de mando de seguridad	ATOS	Todos	Global	10	CISA, CISM, CISSP, ITIL, PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	15
Consultoría de ciberseguridad para entornos industriales	Servicio para la identificación y adecuación de los principales activos que componen los sistemas críticos.	AXIANS	Todos	Global	4	CISA, CISM, ITIL, CISSP	9001, 166002, 27001, 14001, 20000	3
Continuidad de negocio	Servicios de consultoría para el establecimiento de políticas, procedimientos y tecnologías para la continuidad de los procesos de negocio de nuestros clientes.	CIC Consulting Informatico	Todos	España	3	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	2
Plan de protección	Adecuación cumplimiento normativo (LPIC y otros) y mejores prácticas de seguridad en entornos ICS y TI.	DELOITTE	Todos	Global	15	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	10
Guías de bastionado y seguridad industrial	Elaboración de guías de configuración segura para entornos industriales.	DELOITTE	Todos	Global	20	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	10
Diseño de arquitecturas de protección industrial	Elaboración de arquitecturas seguras y asesoramiento para su implementación en redes de campo, operaciones e interconexión con redes corporativas u otras redes.	DELOITTE	Todos	Global	20	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	5
Ciber-ejercicios One to One o múltiples	Servicio de medición y entrenamiento de las capacidades técnicas, humanas y organizativas para responder y resistir ante ciberataques. Incluye personalización de malware y simulación de APT.	DELOITTE	Todos	Global	10	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	10

ÍNDICE

CONSULTORÍA (4/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión de Crisis	Servicio global de preparación y mejora de capacidades de respuesta ante crisis, escalada desde cualquier ámbito, ya sea tecnológico, humano, natural, etc., con coordinación entre diferentes áreas, tanto técnicas como organizativas y con soporte técnico, legal, financiero, etc.	DELOITTE	Todos	Global	5	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	5
Consultoría RGPD	Servicio de consultoría y asesoramiento en materia de adaptación al Reglamento General de Protección de Datos.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		30
Consultoría LOPD	Servicio de Consultoría en materia de Protección de Datos de cara a la adaptación la nueva LOPD.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		15
Consultoría Comercio Electrónico	Servicio de consultoría y asesoramiento en materia de Comercio Electrónico.	ECIJA	Todos	Europa	40	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		20
Consultoría RLOPD	Servicio de Consultoría en materia de Protección de Datos de cara a la adaptación la nueva RLOPD.	ECIJA	Todos	Europa	40	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Consultoría ISO 27001	Servicio de consultoría en materia de ISO 2700.	ECIJA	Todos	Europa	20	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8

ÍNDICE

CONSULTORÍA (5/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría Europrise Privacy Seal	Servicio de consultoría en materia de Europrise Privacy Seal.	ECIJA	Todos	Europa	20	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		6
Consultoría Sellos Privacidad	Servicio de consultoría y asesoramiento en materia de sellos de privacidad.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Consultoría DPO	Servicio de designación de Data Protection Officer	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		10
Análisis de riesgos ciberseguridad	Servicio de consultoría en materia de identificación, evaluación y clasificación de los principales riesgos y elaboración plan de acción.	ECIJA	Todos	Europa	6	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Análisis de riesgos ciberseguridad	Servicio de consultoría en materia de identificación, evaluación y clasificación de los principales riesgos y elaboración plan de acción.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Diseño	Diseño de soluciones de red con ciberseguridad aplicada siguiendo las mejores prácticas de los fabricantes de los equipos.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		
Asesoramiento	Identificación de las necesidades del cliente respecto a critérios de ciberseguridad, mapa de riesgo, y plan de implantación.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		

ÍNDICE

CONSULTORÍA (6/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Planes Estratégicos de Ciberseguridad	Elaboración de planes directores de seguridad a nivel sectorial, nacional y/o empresarial.	EVERIS	Todos	España, Europa y Latinoamérica	2	CISM, CRISC, CISSP	ISO 27001, ISO 9000, ISO 14000, CMMI v5, Oracle, PartnerNetwork	2
Sistemas de Gestión de Seguridad de la Información (SGSI)	Servicio orientado al diseño e implantación de un Sistema de Gestión de Seguridad de la información conforme a lo establecido en el estándar ISO/IEC 27001.	EVERIS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CRISC, CISSP, ITIL Expert	ISO 27001, ISO 9000, ISO 14000, CMMI v5, Oracle, PartnerNetwork	10
Adecuación Normativa Legal (LOPD, ENS, etc.)	Servicio cuyo objeto es la adecuación de una organización a los requerimientos normativos establecidos por alguna regulación.	EVERIS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CRISC, CISSP, ITIL Expert	ISO 27001, ISO 9000, ISO 14000, CMMI v5, Oracle, PartnerNetwork	>25
Seguridad en el Ciclo de Vida de los Sistemas de Información	Servicio orientado a la revisión y transformación de la metodología y/o procesos de una organización en materia de diseño y mantenimiento de Sistemas de Información, de forma que la seguridad se integre durante todo el ciclo de vida de un S.I. (concepción, análisis, diseño, implementación, pruebas y mantenimiento).	EVERIS	Todos	España, Europa y Latinoamérica	2	CISA, CISSP	ISO 27001, ISO 9000, ISO 14000 CMMI v5, Oracle, PartnerNetwork	2
Implementación de Sistemas de gestión de Identidades y/o Control de Acceso	Servicio de consultoría cuya finalidad es la definición, implantación y/o mantenimiento de la infraestructura tecnológica requerida en una Organización que proporcione un control de acceso centralizado a los Sistemas de Información y/o una gestión centralizada de la identidad de los usuarios que acceden a los mismos.	EVERIS	Todos	España, Europa y Latinoamérica	5	PMP	ISO 27001 ISO 9000 ISO 14000 CMMI v5, Oracle, PartnerNetwork	10
Implantación de Sistema de Gestión de Continuidad de Negocio	Realización del flujo de implantación completo del SGCN, desde la fase de análisis y contexto de la organización, la planificación de la implantación, diseño y análisis de resultados del BIA y AARR, selección de estrategia, planes, etc. en base a las buenas prácticas de referencia (Business Continuity Institute Guidelines) y la norma ISO 22301:2012.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead, Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10

ÍNDICE

CONSULTORÍA (7/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis de Adecuación conforme a la norma (ISO22301)	Ejecución de assessment con referencia a la norma ISO 22301 con la obtención de grado de cumplimiento, puntos de mejora, y plan de acción.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead, Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Planes de Continuidad	Realización de los planes de continuidad de negocio en base a los resultados del análisis de impacto en el negocio, la evaluación de riesgos y la estrategia de continuidad de negocio seleccionada, garantizando el correcto desarrollo de los procedimientos y tareas a poner en marcha en caso de contingencia.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead, Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Análisis de Impacto en el Negocio	Preparación, realización y extracción de resultados del Análisis de impacto en el negocio a través del cual se obtendrá la relación de los procesos de negocio/áreas/ actividades, su criticidad y las dependencias tanto internas como externas de los mismos.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead, Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Evaluación de Riesgos	Preparación, realización y extracción de resultados de la evaluación de riesgos, llevada a cabo con una aproximación hacia Continuidad de Negocio, de la mano de la Gestión de riesgos que pueda haber implantada, si la hubiera, y obteniendo resultados que permitan adecuar la respuesta y estrategia de continuidad de negocio.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead, Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Estrategia de Continuidad	Definición de la estrategia de continuidad de negocio acorde a las necesidades de continuidad del cliente tanto a nivel de TI como de negocio. Asesoramiento en las posibilidades de elección existente, implantación y seguimiento.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Pruebas de Continuidad	Desarrollo de planes de pruebas, incluyendo la preparación de las mismas, ejecución y obtención de lecciones aprendidas, con alcance tanto para pruebas globales como parciales y de escritorio.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000 CMMI v5	10

ÍNDICE

CONSULTORÍA (8/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Disaster Recovery	Orientado a los servicios e infraestructura IT, desarrollo de los planes acorde a la estrategia de continuidad y las necesidades técnicas de la misma (solución de TI alternativa), preparación y asistencia en pruebas, coordinación y alineamiento con las necesidades de negocio, etc.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Gestión de Crisis	Con el propósito de abarcar los objetivos del plan de continuidad de negocio se trabaja en la coordinación con el plan de emergencias, proveedores, y factores logísticos necesarios en caso de crisis buscando optimizar los tiempos de respuesta y recuperación. Diseño y propuesta de equipos tácticos, operativos y comité de crisis. Flujos de comunicación a establecer y reporte de los distintos equipos. Coordinación con el plan de comunicación.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Becnhmarking de Herramientas de CN	Realización de análisis de las distintas herramientas de continuidad de negocio presentes en el mercado tanto para la gestión previa a una crisis como para la gestión de la misma y el lanzamiento de comunicaciones orientado al cumplimiento de las necesidades del cliente.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Evaluación de la Cadena de Suministros	Ejecución de análisis y evaluación de la cadena de suministro con vistas a la garantía y fortalecimiento de la misma con la realización de un plan de acción como resultado.	EVERIS	Todos	España, Europa y Latinoamérica	6	CISA, CISSP, CISM, CRISC, ITIL Expert, ISO22301 Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	10
Inceptive Cybersecurity Assesment	Valoración de la situación inicial de una infraestructura, compañía o instalación en materia de Ciberseguridad.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
CONNtrol - Evaluación ciberseguridad	Evaluación de riesgos, obteniendo resultados que permitan adecuar la respuesta y estrategia de continuidad de negocio.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30

ÍNDICE

CONSULTORÍA (9/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
CONNtrol - Consultoría ciberseguridad	Consultoría de ciberseguridad de sistemas de control industrial y generación de un plan de acción.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
CONNtrol - Soporte ciberseguridad	Servicios de soporte técnico de gestión del nivel de riesgo de la organización.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30
Servicio Cumplimento Normativo	Adecuación al cumplimiento normativo motivado por las diferentes regulaciones existentes.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20001	ISO 27001, ISO 20000, CMMI	17
Creación Estrategia en Ciberseguridad	Elaboración de planes directores de seguridad, seguridad Industrial.	GETRONICS	Todos	España, Europa y Latinoamérica	5	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20001	ISO 27001, ISO 20000, CMMI	>20
Gestión de incidentes y plan de continuidad	Ciclo completo y continuidad del servicio en una compañía, infraestructura u organización con base OT instalada. - Análisis BIAS. - Diseño organización para la gestión de la continuidad de la producción y el negocio. - Procesos y procedimientos de respuesta a emergencias. - Plan de gestión de crisis. - Diseño del plan de pruebas del conjunto del BCP. - Diseño del plan de formación y capacitación del BCP. - Especificación de políticas y metodologías para la realización de auditorías con relación al BCP.	GETRONICS	Todos	España, Europa y Latinoamérica	6	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20001	ISO 27001, ISO 20000, CMMI	15

ÍNDICE

CONSULTORÍA (10/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cybersecurity Assesment	Consultoría cuyo alcance incluye: Análisis de ciberseguridad en redes OT y en Centros de Control, gap analysis con las buenas prácticas y estándares de ciberseguridad del sector, determinación de hoja de ruta de mejora, aplicación de contramedidas.	GMV	Energía y Espacio	Global	6	CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, CEH, GCIH, GCFA, GREM y GSEC	ISO 9000, UNE 166002, ISO 14001, ISO 27001, ISO 20000, ISO 22301, CMMI L3	4
Cyber risks management	Consultoría de análisis y gestión de riesgos tecnológicos aplicado al ámbito industrial.	GMV	Todos	Global	6	CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, CEH, GCIH, GCFA, GREM y GSEC	ISO 9000, UNE 166002, ISO 14001, ISO 27001, ISO 20000, ISO 22301, CMMI L3	2
Continuidad de Negocio	Solución que por medio de GAP Análisis, definición de políticas, evaluación de escenarios de continuidad, definición de estrategias de continuidad y la definición, desarrollo, implantación y pruebas de Planes de Continuidad de Negocio, permita garantizar su continuidad ante un incidente grave que impida la normal operación de los servicios e infraestructuras que sustentan el negocio.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	21
Protección de Infraestructuras Críticas	Solución encaminada a la correcta adecuación de la compañía a los requerimientos de la Ley de Protección de Infraestructuras Críticas (LPIC).	GRUPO SIA	Banca, Energético, Trasporte, Comunicaciones, Suministros, Salud	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor CEH, CPHE, CHFI, Comptia Security+	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	9

CONSULTORÍA (11/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis y gestión de riesgos TIC	Plan Director de Seguridad; Análisis de Riesgos; Sistemas de Gestión del Riesgo, SG de Gobierno de la Seguridad y SG de Cumplimiento basados en herramientas GRC.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, C|CISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor CEH, CPHE, CHFI, Comptia Security+	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	25
Desarrollo de Marco Normativo	Definición de los Marcos normativos aplicables en base a un Modelo Unificado de Controles requerido.	GRUPO SIA	Todos	Global	53	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, C|CISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Audito	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	20
Gobierno y gestión de la Seguridad Física	Se prestan servicios para la correcta divulgación de los servicios corporativos de seguridad al resto de la organización. El objeto principal del servicio es presentar el valor de seguridad corporativa aporta al resto de la organización y el negocio de la compañía. SIA dispone de Directores y Jefes de seguridad que asesoren a las empresas en la definición de los procedimientos de la seguridad integral de las mismas.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, C|CISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor CEH, CPHE, CHFI, Comptia Security+	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	4
Adecuación LOPD	Alineamiento de los diferentes procesos de tratamiento de datos a los requisitos legales, organizativos y técnicos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre, su Reglamento de desarrollo, y normativa complementaria.	GRUPO SIA	Todos	Nacional	>50	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, C|CISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor CEH, CPHE, CHFI, Comptia Security+	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	>100

ÍNDICE

CONSULTORÍA (12/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Contratación TIC	Asesoramiento y apoyo en los diferentes procesos que integran el ciclo de vida de la gestión contractual en materia de servicios IT y cloud computing (selección y evaluación de proveedores, negociación, contratación y supervisión).	GRUPO SIA	Todos	Global	15	CISA, CDPP, CISM, CISSP, ITIL, CICISO	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	10
Servicio de Asistencia Técnico Legal (SATEL)	Servicio especializado de asesoramiento legal y técnico en materia de cumplimiento regulatorio asociado a la seguridad y a las tecnologías de la información.	GRUPO SIA	Todos	Global	15	CISA, CDPP, CISM, CISSP, ITIL, CICISO	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	>15
Consultoría SGCI	Servicio de consultoría para Sistemas de Gestión de Seguridad en el entorno Industrial.	INYCOM	Industrial (Todos)	Global	>10	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	AENOR ISO27001, AENOR ISO20000-1	
Consultoría para infraestructura física	Consultoría para el diseño y la evaluación de elementos pasivos de la red de comunicaciones.	INYCOM	Industrial (Todos)	Global	>10	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	AENOR ISO27001, AENOR ISO20000-1	

ÍNDICE

CONSULTORÍA (13/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría para infraestructura lógica	Consultoría para el diseño y la evaluación de la lógica de red (redundancia, replicación, servicios, elementos activos.).	INYCOM	Industrial (Todos)	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/ Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	AENOR ISO27001, AENOR ISO20000-1	
Consultoría para equipos finales	Consultoría para la seguridad del equipo final de OT.	INYCOM	Industrial (Todos)	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/ Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	AENOR ISO27001, AENOR ISO20000-1	
Web Application Pen Test	Auditoría de seguridad aplicaciones web PHP, ASP, .NET, Web Services, etc, búsqueda de vulnerabilidades tanto en el desarrollo objetivo como en frameworks utilizados.	IOACTIVE	Todos	Global	>50	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Mobile Application Pen Test	Análisis de seguridad de aplicaciones para todo tipo de dispositivos móviles incluyendo sistemas Android, iOS, BlackBerry y Windows Phone.	IOACTIVE	Todos	Global	>30	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4

ÍNDICE

CONSULTORÍA (14/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Infrastructure Pen Test	Tests de intrusión para evaluar la seguridad de la infraestructura de red, aplicación de ataques reales y búsqueda de puntos débiles.	IOACTIVE	Todos	Global	>50	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Wireless Pen Test	Análisis de seguridad para sistemas wireless simulando ataques reales y búsqueda vulnerabilidades.	IOACTIVE	Todos	Global	>20	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Threat modelling	Evaluación e identificación de las diferentes amenazas y riesgos derivados de la seguridad de un sistema.	IOACTIVE	Todos	Global	>20	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Architecture review	Análisis de los diferentes componentes de una sistema como código fuente, librerías y ejecutables y sus diferente relaciones.	IOACTIVE	Todos	Global	>30	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Social Engineering	Aplicación de técnicas reales para la obtención de mayores privilegios dentro de la organización o información confidencial. Conseguir el objetivo mediante Ingeniería Social.	IOACTIVE	Todos	Global	>20	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Red Team Assessments	Test de intrusión simulando un ataque real, sin el conocimiento previo de gran parte de la organización.	IOACTIVE	Todos	Global	>15	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Hardware reverse engineering	Análisis con enfoque BlakBox de sistemas electrónicos. Identificación de buses de datos, componentes y sus conexiones. Extracción de firmware y/o claves criptográficas. Identificación de vulnerabilidades.	IOACTIVE	Todos	Global	>10	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Firmware reverse engineering	Análisis tipo BlackBox de firmware sin acceso al código fuente para la búsqueda de vulnerabilidades, extracción de claves criptográficas o analizar diferentes medidas de seguridad.	IOACTIVE	Todos	Global	>10	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4

ÍNDICE

CONSULTORÍA (15/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cloud security assessments	Auditoría de seguridad de sistemas desplegados en "la nube", búsqueda de vulnerabilidades y realización de ataques reales.	IOACTIVE	Todos	Global	>20	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Embedded security assessments	Análisis de seguridad con enfoque BlackBox de sistemas electrónicos incluyendo ingeniería inversa de Hardware y Firmware sin acceso a código fuente.	IOACTIVE	Todos	Global	>15	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Industrial Services Security Assessments	Análisis de seguridad de sistemas industriales, búsqueda de vulnerabilidades en sistemas aislados o despliegues completos, por ejemplo Smart Meters.	IOACTIVE	Todos	Global	>15	CISA, CISM, CISSP, PCI-QSA, PA-QSA, CobiT v4.1, ITIL V3, GPEN, CEPT, CEH		3 ó 4
Evaluación cuantitativa y análisis de riesgos.	Servicio orientado a identificar, evaluar y clasificar cuantitativamente y de forma periódica los principales riesgos físicos y lógicos, tanto IT como OT, que afectan a los procesos industriales y a los activos que los soportan dentro de una organización.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administación pública, TELCO	España	4	CISA, GICSP	ISO 27001	
Consultoría de cumplimiento	Servicio orientado a la identificación de brechas y debilidades de seguridad en sistemas de control y automatización industrial en base a los controles planteados en las principales guías y estándares de seguridad inherentes al sector, proponiendo una serie de recomendaciones sobre cómo abordar las vulnerabilidades para mejorar la visibilidad de la ciberseguridad en los activos IACS pertenecientes a las organizaciones.	ITS SECURITY	Industrial, Energía, Transporte	España	4	CISA, GICSP	ISO 27002	
Desarrollo y cumplimiento de cuerpo normativo: Evaluación de Cumplimiento LPIC	Evaluación de cumplimiento y desarrollo de plan de adecuación que permita: • Análisis de la Seguridad tanto a nivel físico como lógico. • Determinar las carencias. • Planificar la mejora y la fecha de cumplimiento.	ITS SECURITY	Industrial, Energía, Transporte	España	4	CISA, GICSP	ISO 27003	

CONSULTORÍA (16/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Desarrollo y cumplimiento de cuerpo normativo: Adecuación y despliegue LPIC	El servicio de adecuación a la LPIC proporciona a los clientes de ITS todo el soporte y asesoramiento necesario para guiarles en el cumplimiento y su mantenimiento: 1. Plan de Seguridad del Operador o Desarrollo de un Análisis de Riesgos. a) Identificación de las medidas de seguridad implantadas. b) Identificación de las medidas a implantar y el Plan de Acción para su implantación. c) Revisión y actualización con carácter anual. 2. Plan de Protección Específico. a) Desarrollo de Plan conjunto donde se incluye la seguridad física y lógica. b) Análisis de Riesgos. c) Medidas implantadas, permanentes y temporales. d) Plan de Acción. e) Revisión y actualización con carácter anual. Implantación de las medidas, tanto del PSO como de los PPE, a nivel técnico como organizativo.	ITS SECURITY	Industria, Energía, Transporte	España	4	CISA, GICSP	ISO 27004	
Diseño de arquitecturas de seguridad	Servicio orientado al diseño de arquitecturas de red seguras, aplicando una estrategia de defensa multi-nivel basada en segmentación mediante la inclusión de soluciones de seguridad tecnológicas como IDS/IPS, diodos de datos o cortafuegos industriales.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	2	CISA, GICSP	ISO 27005	
Laboratorio de análisis OT	Laboratorio en tiempo real de análisis de vulnerabilidades en entornos industriales.	ITS SECURITY	Trasporte, Industria, Energía	España	6	CISA, GICSP	ISO 27001	1
Diseño de arquitecturas resilientes	Diseño e implantación de arquitecturas resilientes en entornos industriales.	ITS SECURITY	Trasporte, Industria, Energía	España	10	CISA, GICSP	ISO 27001	20
Bastionado en entornos OT	Elaboración de guías de configuración segura en entornos Industriales.	ITS SECURITY	Trasporte, Industria, Energía	España	10	CISA, GICSP	ISO 27001	14

ÍNDICE

CONSULTORÍA (17/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Plan estratégico de Ciberseguridad	Para entornos específicos de OT (Operation Technology) en los que la disponibilidad prima sobre otros vectores de la seguridad, incorporamos diferentes capas de seguridad sobre los elementos a proteger apoyándonos en la experiencia en seguridad IT y la especialización en el ámbito OT.	ITS SECURITY	Trasporte, Industria, Energía	España	3	CISA, GICSP	ISO 27001	24
Análisis GAP de ciberseguridad industrial	Diagnóstico de Situación actual y plan de acción de mejoras.	ITS SECURITY	Todos	Global	3	CISA, GICSP	ISO 27001	2
Evaluación de centros de control	Evaluación de la relación entorno OT/IT en los centros de control.	ITS SECURITY	Todos	Global	4	CISA, GICSP	ISO 27001	2
Hacking ético a entornos industriales	Hacking éticos a los sistemas OT que comprenden las diferentes industrias con el fin de detectar vulnerabilidades y garantizar la disponibilidad de la planta.	ITS SECURITY	Todos	Global	4	CISA, GICSP	ISO 27001	5
Desarrollo de PSOs y PPE para cumplimiento Ley PIC	Desarrollo de los planes de seguridad del operador y los planes de protección específico para dar cumplimiento a lo establecido a la ley PIC.	ITS SECURITY	Todos	España	6	CISA, GICSP	ISO 27001	
Propuesta de arquitecturas de referencia	Diseño de la arquitectura OT segura que permita alcanzar niveles óptimos de rendimiento y que esté alineado con la idiosincrasia de la organización.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		10
Diseño de modelo de control	Diseño del modelo de control estructurado por dominios y teniendo en cuenta diferentes modelos de madurez.	LOGITEK	Todos	Global	2	ISA99, CSSA, CEH		1
Seguridad en redes Smart Metering	Diseño e implementación de especificaciones de ciberseguridad para toda la arquitectura smart metering con un enfoque global, de contador a centro de telegestión incluyendo concentradores y otros sistemas intermedios de transmisión y comunicaciones.	MINSAIT	Todos	Global	8			2

ÍNDICE

CONSULTORÍA (18/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cybersecurity Assesments	Evaluación técnica (en entornos de laboratorio y controlados) de Redes de campo (PICs), Evaluación técnica en entornos controlados de laboratorio de redes de supervisión con auditoría y tests de penetración. Evaluación de riesgos y gestión de crisis. Seguridad en los procesos de control industrial.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Aeronáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	7
Asesoramiento legal	Revisión y adecuación a requisitos legales LPIC y sectoriales.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Aeronáutico	Global	3	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	4
Security Architecture Assessment (SAA)	Arquitectura que permite desplegar servicios de consultoría de seguridad de forma flexible y orientados a negocio de forma consistente a nivel mundial. Consiste en tres niveles que son: 1. Entrevistas y workshops de negocio. 2. Revisión de la arquitectura existente. 3. Análisis Técnico detallado (opcional).	NTT	Todos	Global	60	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	
Tests de penetración	Servicio de hacking ético para evaluar las soluciones de seguridad existentes analizando hasta qué punto es posible entrar hasta los sistemas de negocio. Para los Tests de Penetración solemos usar una combinación de equipos externos internacionales de NTT y locales con personal de NTT España.	NTT	Todos	Global	60	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	

ÍNDICE

CONSULTORÍA (19/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión avanzada de firewalls industriales	Chequeo periódico de las reglas activadas de Firewall en OT. - Chequeo de vulnerabilidad de Firmware. - Verificación de las reglas de consistencia para la redundancia de firewall/router - Validación de la configuración del firewall contra el diseño de red ICS para asegurar el tráfico estrictamente funcional del control industrial. - Valoración de diferentes tecnologías de firewall a implementa.	PHOENIX CONTACT	Todos	Global	6			
Diseño de infraestructura segura de gestión remota	Soporte y configuración de una plataforma hardware propia para gestión segura y remota de activos.	PHOENIX CONTACT	Todos	Global	2			
Análisis de brecha y plan de acción de ciberseguridad industria	Análisis de brecha contra la serie de estándares IEC 62443 bajo la perspectiva de las personas, los procesos y la tecnología y considerando un nivel de madurez objetivo para las prácticas relacionadas. Como resultado se desarrolla un Plan de Ciberseguridad para sistemas OT.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>10
Análisis de riesgos y plan director de ciberseguridad industrial	Este servicio incluye el servicio análisis de brecha que se complementa con un análisis de riesgos para la definición de un plan director de ciberseguridad industrial que incluye un conjunto de proyectos priorizados según riesgos.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5

ÍNDICE

CONSULTORÍA (20/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Desarrollo de políticas y procedimientos	Desarrollo de políticas y procedimientos de seguridad enfocados en preocupaciones clave en la ciberseguridad industrial, como por ejemplo: gestión de vulnerabilidades, gestión de parches, acceso remoto seguro, manejo de incidentes, planes de recuperación ante desastres, especificación de seguridad de productos, etc.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
Rediseño de arquitectura de seguridad	Evaluación de mecanismos de segregación IT-OT, estrategia de segmentación OT, flujos de comunicación, etc., bajo el paradigma de zonas y conductos de seguridad definidos por la serie de normas IEC 62443. Asimismo, evaluación de endpoints, equipos de red, aplicaciones, bases de datos y medidas de seguridad de datos, abarcando todas las funciones del NIST. Como resultado del proyecto se realiza una propuesta de nuevas medidas de seguridad en múltiples niveles, desde una perspectiva teórica, como por ejemplo: nuevos diagramas de segmentación, nuevo conjunto de roles & usuarios y LDAP industrial, nueva arquitectura de firewalls IT-OT y OT, propuesta de soluciones antimalware, propuesta de solución para recuperación ante desastres, etc.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
Monitorizacion de Vulnerabilidades en la red IT/OT/IIoT	Monitorizacion del tráfico de red Cloud/IT/OT/IIoT para detectar amenazas o comportamientos anómalos. Supervisión continua de todos los elementos activos relacionados con la Ciberseguridad. Activos IP (routers, switches, PLCs, HMIs, SCADA, Disp IoT, impresoras, lectores código de barra, IoT, etc.). La información se recolecta para ser visualizada de forma centralizada (web). Se envía un reporte de los nuevos riesgos y de las nuevas alertas.	SARENET	Todos	España	>10			

ÍNDICE

CONSULTORÍA (21/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría para la Infraestructura de Comunicaciones	Facilitar ayuda al cliente industrial, ofreciendo protección en todo el ciclo de vida de una amenaza. Estableciendo distintas capas de seguridad, para todas las zonas de una superficie de ataque.	SARENET	Todos	España	>10			
Análisis de riesgos	Análisis de riesgos para nuestros clientes, basados en diferentes estándares y normas: ISO 27005, EBIOS, MAGERIT…	SCASSI CIBERSEGURIDAD	Todos	Global	6			30
Asesoramiento a la dirección y los equipos técnicos sobre sistemas de Detección de Intrusiones (IDS), SIEM (Security Information & Event Management), AV, Proxy	Asesoramiento a la dirección y los equipos técnicos sobre sistemas de Detección de Intrusiones (IDS), SIEM (Security Information & Event Management), AV, Proxy.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Asesoramiento sobre Plan de Continuidad de Negocio y Plan de Recuperación de Negocio	Asesoramiento sobre Plan de Continuidad de Negocio y Plan de Recuperación de Negocio.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Redacción de procesos operacionales de seguridad	Redacción de procesos operacionales de seguridad.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Apoyo a los equipos de desarrollo en temas de seguridad	Apoyo a los equipos de desarrollo en temas de seguridad.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10

ÍNDICE

CONSULTORÍA (22/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión de alertas e incidentes, gestión de crisis	Gestión de alertas e incidentes, gestión de crisis.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Despliegue de estrategias risk-driven para los equipos técnicos	Despliegue de estrategias risk-driven para los equipos técnicos.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Apoyo SSI en los procesos de certificación (DO 178, ECSS, ARINC,…)	Apoyo SSI en los procesos de certificación (DO 178, ECSS, ARINC,…).	SCASSI CIBERSEGURIDAD	Todos	Global	6			20
Homologación de seguridad de sistemas	Ayudamos a nuestros clientes a conseguir las homologaciones y a mantenerlas al nivel adecuado en su fase operativa, a través de actividades de gestión del sistema de información y de mantenimiento de la certificación. También ayudamos a garantizar la coherencia entre diferentes estándares (ISO 27001 y HDS por ejemplo).	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Gestión SSI / 2700x	Sistema de Gestión de la Seguridad de la Información (Information Security Management System).	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
Secure&LPIC	Consultoría de cumplimiento de la Ley de Protección de Infraestructuras Críticas (LPIC).	Secure&IT	Industria	Global	>5	LEAD AUDITOR ISO 20000/ISO 27001 /ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. LDO.DERECHO, PERITO INFORMATICO JUDICIAL		

ÍNDICE

CONSULTORÍA (23/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Secure&SGCI	Sistema de Gestión de Ciberseguridad industrial	Secure&IT	Industria	Global	>5			
Perimeter Firewall Review	Chequeo periódico de las reglas activadas del Firmware de Firewall. - Chequeo de vulnerabilidad de Firmware. - Chequeo redundante y en profundidad de las reglas de evaluación. - Validación de la configuración del firewall contra el diseño de red ICS para asegurar ICS para asegurara su precisión. - Amplio catálogo de tecnologías de firewall soportadas.	SIEMENS	Todos	Global				
Security Policy Consulting	Establecimiento de prácticas estándares de seguridad en Sistemas de Control Industrial (ICS) - Establecer nuevas o revisar las políticas de seguridad, procesos, procedimientos y trabajos existentes de base. - Integración con prácticas de ciberseguridad de la compañía. - Patch and backup strategy, handling of removable media…	SIEMENS	Todos	Global				
Network Security Consulting	Soporte en diseño y setup de seguridad de la red. - Cell segmentation en soporte de security cells basado en estandares IEC 62443 y SIMATIC PCS 7 & WinCC security concept. - Diseño y planificación de red de protección perimetral: DMZ network (Desmilitarizada) - Establecimiento/revisión de las reglas para Firewall perimetral.	SIEMENS	Todos	Global				
Proyectos de Adecuación Normativa y Gobierno de Seguridad	Proyectos de Adecuación e Implantación de Normativas, Buenas Prácticas y Estándares en materia de Seguridad de la Información: Privacidad, ISO 22301, ISO 27001, ISO 9000, ISO 14000, Esquema Nacional de Seguridad (ENS), Esquema Nacional de Interoperabilidad (ENI), Protección a Infraestructuras Críticas (LPIC), PCI DSS.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 10	CISA, CISM, CGEIT, CISSP, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Lead Auditor BS 25999, ITIL Foundation, ISO 20000 Practicione	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 50

ÍNDICE

CONSULTORÍA (24/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicios Profesionales de ciberseguridad industrial	Servicio de evaluación integral de la ciberseguridad en entornos industriales, incluyendo políticas, procedimientos, prácticas, contramedidas y tecnologías de seguridad. Evaluación del GAP frente a normativas, estándares y buenas prácticas de seguridad tales como ISA/IEC-62443, NIST SP 800-82. Propuesta e implementación de medidas para cubrir las debilidades y/o deficiencias de cumplimiento.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 5	GICSP, ISA/ IEC 62443 Fundamentals Specialist, CISA, CISM, CGEIT, CISSP, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Lead Auditor BS 25999, ITIL Foundation, ISO 20000 Practicioner, Nozomi Networks Certified Engineer	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 5
Ciberseguridad Industrial	Consultoría de Seguridad de los Sistemas de Control y Automatización Industrial (IACS), conforme a los criterios definidos en los principales estándares de Ciberseguridad Industrial.	TELEFÓNICA - GOVERTIS	Todos	Global	10	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		15
Análisis de Impacto en el Negocio	Servicio de análisis de Impacto en el Negocio (BIAs) conforme a ISO 22317.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		>25
Infraestructuras Críticas (II.CC.).	Integración de PSOs y PPEs para sector financiero con mejores prácticas internacionales.	TELEFÓNICA - GOVERTIS	Todos	Global	10	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		

ÍNDICE

CONSULTORÍA (25/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría normas ISO e ITIL	Auditoría interna normas ISO: 27001, 9100, 20000, 22301, 20000 e ITIL.	TELEFÓNICA - GOVERTIS	Todos	Global	15	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP, COBIT		>50
Planes de Recuperación de Desastres (DRPs)	Servicios de implementación de Planes de Recuperación de Desastres (DRPs) conforme a ISO 27031.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		>25
Elaboración de normas internas	Servicio consistente en elaboración de protocolos de uso de las TIC. Redacción de normas BYOD. Recomendaciones de uso de redes sociales, blogs.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		>50
Adecuación Esquema Nacional de Seguridad (ENS)	Servicio que permite la adecuación de una organización a los requerimientos normativos establecidos por la normativa del Esquema Nacional de Seguridad (ENS).	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		>50
Privacidad	Consultoría/Auditoría RGPD (Reglamento General de Protección de Datos de la Unión Europea) y LOPDGDD (Ley de Protección de datos y Garantía de los Derechos Digitales).	TELEFÓNICA - GOVERTIS	Todos	Global	25	Acreditación DPD según esquema AEPD, CDPSE		>50
Cumplimiento normativo IT/OT/IoT	Adecuación a los marcos normativosa de referencia: ISO 27001, ISA/IEC 62443, NIST CSF, LPIC…	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		15

ÍNDICE

CONSULTORÍA (26/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Consultoría	Proporcionamos asesoramiento ciber a las infraestructuras críticas para abordar los desafíos derivados del cumplimiento normativo, la implementación de la seguridad desde el diseño, la evaluación de riesgos y la realización de pruebas de penetración (PENTEST).	THALES	Infraestructuras Críticas	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	
Análisis y gestión de riesgos en entornos IT/OT	Identificación y clasificación de amenazas/vulnerabilidades y evaluación de los riesgos asociados a los diferentes activos tanto IT como OT de una organización, en base a métricas y controles de seguridad prestablecidos.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

CONSULTORÍA (27/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cumplimiento normativo OT	Servicio destinado a evaluar y adecuar a las organizaciones a los requerimientos fijados por las diferentes normativas de seguridad existentes aplicables a entornos industriales, como pueden ser la Ley de Protección de Infraestructuras Críticas, IEC-62443, NIST-800-82, NIST-800-53, NERC-CIP, etc.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Desarrollo de cuerpo normativo OT	Servicio destinado a la creación y desarrollo de políticas, procedimientos y plan director de seguridad aplicables a las diferentes organizaciones industriales dependiendo del entorno objetivo, entre los que se incluyen IEC-62443, NIST-800-82, NIST-800-53, NERC-CIP y la ley PIC en el caso de las infraestructuras críticas Españolas.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

CONSULTORÍA (28/28)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Redes y sistemas industriales	Diseño, adaptación, implementación y mantenimiento de redes de comunicaciones y sistemas de control industrial con criterios de ciberseguridad.	TSK	Energía, Plantas industriales, Medio ambiente	Global	3	CCNA	ISO9001, 14001, OSHAS 18001, UNE 166002	1
Elaboración del "Plan de Ciberseguridad Industrial"	Elaboración de planes de ciberseguridad industrial tanto integrales para toda una organización como específicos para áreas productivas concretas.	TSK	Energía, Plantas industriales, Medio ambiente	Global	3	CCNA	ISO9001, 14001, OSHAS 18001, UNE 166002	1
Consultoría de Ciberseguridad industrial	Servicios de consultoría para la elaboración, desarrollo, implementación y mantenimiento/revisión de planes de Ciberseguridad industrial.	TSK	Energía, Plantas industriales, Medio ambiente	Global	3	CCNA	ISO9001, 14001, OSHAS 18001, UNE 166002	1

ÍNDICE

AUDITORÍA (1/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría de cumplimiento	Auditorías de cumplimiento de estándares, normativas y legislación en materia de seguridad (LOPD, PCI DSS, LPIC, ENS, ISO/IEC 27001, ISO 22301). Obtención de no conformidades, recomendaciones, plan de acción.	ATOS	Todos	Global	100	CISA, CISM, CISSP, ITIL PMP, LEAD AUDITOR, PCI-DSS QSA, CRISC, SSCP, CEH	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	>50
Análisis de vulnerabilidades	Análisis externo de vulnerabilidades (caja blanca y caja negra) de aplicaciones web (hacking ético) siguiendo el estándar OWASP. Análisis interno de vulnerabilidades (tests de intrusión) de sistemas, servicios, aplicaciones, bases de datos, equipos y redes siguiendo, entre otros, el estándar OSSTMM. Servicios de revisión de código de aplicaciones. Red teaming.	ATOS	Todos	Global	20	CEHv7, CISA, CISM, SSCP, CRISC, CISSP, ITIL, PCI QSA, CDPP, 27001 Lead Auditor	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	20
Auditorías de seguridad	Servicio de auditoría técnica de infraestructuras de red y sistemas desde el punto de vista de arquitectura, controles existentes, vulnerabilidades y estado de operaciones.	CIC Consulting Informático	Todos	España	3	ITIL, PMP, vendor certifications	ISO 9001, ISO14001, ISO 27001, ISO 20000, CMMI L2	2
Revisión de seguridad ICS	Auditoría y revisión de seguridad de entornos ICS, a nivel tanto técnico como organizativo y procedimental. Incluyendo test de intrusión, análisis de vulnerabilidades, etc.	DELOITTE	Todos	Global	20	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	10
Auditoría RGPD	Servicio de Auditoría en materia de Protección de Datos de cara a la adaptación al nuevo RGPD.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		30

ÍNDICE

AUDITORÍA (2/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría LOPD	Servicio de Auditoría en materia de Protección de Datos de cara a la adaptación la nueva LOPD.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		20
Auditoría RLOPD	Servicio de Auditoría en materia de Protección de Datos de cara a la adaptación la nueva RLOPD.	ECIJA	Todos	Europa	25	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		10
Auditoría Comercio Electrónico	Servicio de auditoría en materia de Comercio Electrónico.	ECIJA	Todos	Europa	50	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		20
Auditoría Europrise Privacy Seal	Servicio de auditoría en materia de Europrise Privacy Seal.	ECIJA	Todos	Europa	20	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		6
Auditoría ISO 27001	Servicio de auditoría en materia de ISO 27001.	ECIJA	Todos	Europa	20	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Análisis de riesgos ciberseguridad	Servicio de consultoría en materia de identificación, evaluación y clasificación de los principales riesgos y elaboración plan de acción.	ECIJA	Todos	Europa	6	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Auditorías de Seguridad	Detección de vulnerabilidades, test de intrusión interno/externo, arquitectura y configuraciones para la determinación del grado de riesgo y afectación a producción.	ELECNOR	Todos	Global	5	NS4, CEH, CHFI		

ÍNDICE

AUDITORÍA (3/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría Aplicación Web	Análisis de seguridad que tiene como objeto identificar las vulnerabilidades existentes en un aplicativo web, conforme a los controles establecidos en la "Guía de Pruebas de OWASP versión 4". El informe resultante contemplaría tanto las pruebas realizadas, como evidencias y recomendaciones en relación a las deficiencias que pudieran haber sido detectadas.	EVERIS	Todos	Global	10	CISA, CEH, CISSP, GPEN, GCIH	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>25
Auditoría Interna de Seguridad	Análisis de seguridad que tiene como objeto identificar las vulnerabilidades que pudieran existir en la infraestructura tecnológica de una organización.	EVERIS	Todos	España, Europa y Latinoamérica	5	CISA, CEH, CISSP, GPEN, GCIH	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>25
Auditoría de Código Fuente	Análisis de seguridad orientado a la identificación de vulnerabilidades en un aplicativo, empleándose para ello una revisión en profundidad del propio código fuente.	EVERIS	Todos	Global	2	CISA, CEH	ISO 27001, ISO 9000, ISO 14000, CMMI v5	5
Test de Penetración	Análisis de seguridad cuyo objeto es la identificación de deficiencias en una organización, que permitan ganar acceso desde el exterior a la infraestructura interna.	EVERIS	Todos	Global	2	CISA, CEH, CISSP, GPEN, GCIH	ISO 27001, ISO 9000, ISO 14000, CMMI v5	5
Auditoría Normativa Legal (LOPD, ENS, etc.)	Servicio destinado a la revisión del cumplimiento de una organización con respecto a una normativa legal vigente, conforme a lo establecido en las directrices que pudieran ser de aplicación según guías y/o instituciones reguladoras.	EVERIS	Todos	España, Colombia, Italia, Perú.	5	CISA, CISM, CRISC, CISSP, ITIL Expert	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>25
Auditoría en base a ISO22301:2012	Análisis del Sistema de Gestión de Continuidad de Negocio implantado y su cumplimiento con respecto a la norma de referencia ISO 22301:2012. Obtención de posibles No conformidades.	EVERIS	Todos	España, Europa y Latinoamérica	4	CRISC, ISO 22301:2012, Lead Auditor, AMBCI	ISO 27001, ISO 9000, ISO 14000, CMMI v5	2
CONNtrol - Auditoría Ciberseguridad	Auditoría orientada a la detección de vulnerabilidades, evaluación de riesgos y amenazas. Generación de un plan de medidas y recomendaciones.	GETRONICS	Todos	España, Europa y Latinoamérica	9	CISA, CISM, CISSP, NERC CIP, IEC 62443, IEC 61850, Lead Auditor 27001, 22301, 20000	ISO 27001, ISO 20000, CMMI	>30

ÍNDICE

AUDITORÍA (4/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditorias de cumplimiento PCI-DSS	Se requiere para todas las empresas, organismos y entidades que trabajen con datos de tarjetas bancarias, l Auditoría conforme a PCI-DSS.	GRUPO SIA	Todos	Europa	3	PCI DSS QSA, CISA, CISM, CISSP, CRISC, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, CHFI, Comptia Security+	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	18
Auditoria de cumplimiento de la normativa sobre protección de datos de carácter personal.	Auditoria de cumplimiento de la normativa sobre protección de datos de carácter personal.	GRUPO SIA	Todos	España	68	CDPP, CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	>40
Auditoria de cumplimiento ENS	Auditoría de cumplimiento de los requisitos y exigencias establecidos por el Real Decreto 3/2010, de 8 de enero, para velar que los servicios prestados a través de medios electrónicos reúnan las condiciones de seguridad adecuadas para su uso por los ciudadanos.	GRUPO SIA	Todos	España	68	CDPP, CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	5
Auditoria de cumplimiento ISO 27001/27002	Auditoria de cumplimiento para la implantación de un Sistema de Gestión de Seguridad de la Información (SGS) en base a la norma ISO 27001.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	19

ÍNDICE

AUDITORÍA (5/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoria de cumplimiento ISO 22301	Auditoria de cumplimiento ISO 22301 de Continuidad de Negocio.	GRUPO SIA	Todos	Global	56	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	10
Auditoría de Ciberseguridad	SANS.	GRUPO SIA	Todos	Global	30	CEH, CPHE, CHFI, CISSP, Comptia Security+ Akamai Kona McAfee NSP Sun Computing Técnica Sun Network Administrator Sun System Administrator	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	5
Auditoria de código fuente	Análisis del código del aplicativo de cara a identificar problemáticas generales de programación relativas a la seguridad.	GRUPO SIA	Todos	Global	5	CDPP, CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	30
Auditoría de Arquitectura tecnológica	Análisis de la arquitectura tecnológica de una Organización para la adecuada configuración, y más eficiente, de los dispositivos tecnológicos necesarios.	GRUPO SIA	Todos	Global	5	CDPP, CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	3

ÍNDICE

AUDITORÍA (6/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Vulnerabilidades SCADA	Estudio de vulnerabilidades en redes de control de procesos industriales.	INYCOM	Todos	Global	>5	CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU, Certificaciones de fabricantes de seguridad	AENOR ISO27001, AENOR ISO20000-1	
Physical Infrastructure - Security Audit	Servicio que aporta el estado situacional para una optimización con un diseño seguro en la infraestructura física. Auditoria de la arquitectura de la infraestructura física de comunicaciones.	INYCOM	Todos	Global	>2	CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU, Certificaciones de fabricantes de seguridad	AENOR ISO27001, AENOR ISO20000-1	
Plant Network - Security Audit	Servicio de aporta el estado situacional de los servicios actuales. Auditoria de la lógica de la red de comunicaciones.	INYCOM	Todos	Global	>2	CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU, Certificaciones de fabricantes de seguridad	AENOR ISO27001, AENOR ISO20000-1	
Endpoint Security Audit	Seguridad para equipos HMI. Auditoría de la protección de riesgos para equipos finales en planta.	INYCOM	Todos	España				

ÍNDICE

AUDITORÍA (7/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
KICS - CSA	Auditoría de vulnerabilidades KICS.	INYCOM	Todos	España	1	Technical training #KL 038.10	Kaspersky	
Análisis de vulnerabilidades	Análisis de vulnerabilidades de los Sistemas de Control haciendo uso de una metodología propietaria que garantiza la fiabilidad de las pruebas y limita el impacto sobre los sistemas. Objetivos: • Identificación y verificación de vulnerabilidades técnicas en los sistemas implicados. • Identificación y verificación de vulnerabilidades técnicas en la red de comunicaciones y en los dispositivos de la red de campo. • Investigación y desarrollo de exploits para las vulnerabilidades encontradas. • Verificación y testeo de debilidades en la configuración de sistemas y aplicativos. • Pruebas de esfuerzo y estrés de los sistemas y dispositivos existentes en el sistema de control industrial estudiado.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administación pública, TELCO	España	4			
Test de intrusión interno/externo	Destinado a comprobar si es posible lograr una intrusión no autorizada a un sistema de automatización y control. Partiendo desde una localización acordada con el cliente y bajo una serie de premisas negociadas con anterioridad. Incluye la identificación y exploiting de vulnerabilidades, así como la utilización de técnicas de ingeniería social. Realizado de forma que no se altere la operativa cotidiana de la organización y de sus procesos.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administación pública, TELCO	España	1			
Análisis de código fuente de software SCADA y equipamiento industrial	Análisis del código fuente de aplicaciones SCADA o del firmware de equipamiento embebido (RTUs, PLCs, etc.), teniendo en cuenta las principales guías de buenas prácticas para la programación segura de aplicaciones.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administación pública, TELCO	España	4			
Auditoria normativa legal	Auditoria y análisis GAP respecto a la ENS, LPIC, LOPD.	ITS SECURITY	Todos	España	3	CISA, GICSP	ISO 27001	

ÍNDICE

AUDITORÍA (8/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis forense	Servicio orientado a identificar la autoría y los métodos usados durante un ataque a los sistemas de información de la organización, así como la información o procesos que han sido alterados durante su ejecución. También proporciona los conocimientos para prevenir dichas intrusiones en el futuro. El análisis forense es la solución ideal para las organizaciones que tienen la necesidad de investigar el origen de incidentes de seguridad que se producen en sus equipos.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administación pública, TELCO	España	3	CISA, GICSP	ISO 27002	23
Análisis y auditoría de seguridad de redes industriales & SCADA	Análisis del estado actual de redes de comunicaciones del entorno OT. Inventariado de dispositivos, redes, análisis de tráfico, estudio de ciberseguridad desde diferentes puntos de vista (seguridad física, acceso remoto, vulnerabilidades, resiliencia, datos, etc.). Identificación del GAP entre la infraestructura analizada y las mejores prácticas de ciberseguridad definidas en los estándares internacionales (IEC62443, NIST, C2M2, etc.).	LOGITEK	Todos	Global	4	ISA99, CSSA, CEH		9
Nivel de madurez en ciberseguridad industrial	Servicios de evaluación del nivel de ciberseguridad industrial en entornos OT utilizando los framework internacionalmente reconocidos: NIST-800-53, 800-82r2 y C2M2.	LOGITEK	Todos	España, Portugal	2	ISA99/IEC, CEH, CSSA, CCNA	ISO 9001	2
Auditoría de seguridad de redes Smart Metering	Identificación de vulnerabilidades y vectores de ataque en arquitecturas de telemedida inteligente. Con un enfoque global a toda la arquitectura, tanto en lo relativo a la banda estrecha (comunicación contador-concentrador), como al resto de la arquitectura y sistemas de comunicaciones hasta el centro de telegestión. Elaboración de informes de recomendaciones de remediación.	MINSAIT	Todos	Global	12			2

ÍNDICE

AUDITORÍA (9/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría de código seguro SCADA	Realización de auditorías de código estático y dinámico en sistemas de control industrial ICS/SCADA, detección de vulnerabilidades y recomendaciones de acción.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12
Red Team ICS/SCADA	Equipo de evaluación continua de evaluación de vulnerabilidades en tráfico, protocolos y sistemas diseñados de forma específica para infraestructuras industriales.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12
Laboratorio ICS/SCADA	Laboratorio de pruebas de penetración y generación de defensas para sistemas de control ICS/SCADA.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12
Secuity Audit	Auditoría de las políticas de seguridad implantadas en distintas plataformas Firewall existentes.	NTT	Todos	Global	60	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	
Vulnerability Assessments	Auditoría de vulnerabilidades existentes y recomendaciones para mitigarlas.	NTT	Todos	Global	60	CISA, CISSP, Vendor certifications	ISO 27001 ISO 9000 ISO 14001	

ÍNDICE

AUDITORÍA (10/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
IEC 62443 Assesment	Identificación de vulnerabilidades en materia de ciberseguridad y medidas de mitigación de riesgos basados en normativa IEC 62443 - Disponible para Phoenix Contact y terceros - Informe con recomendaciones para mitigación de riesgos.	PHOENIX CONTACT	Todos	Global	3			
Evaluación de ciberseguridad en plantas industriales	El objetivo de la evaluación es determinar el nivel de ciberseguridad dentro de un contexto que permita identificar vulnerabilidades, puntos débiles y oportunidades de mejora en todos los ámbitos. De esta forma se analizan tanto aspectos técnicos como organizativos y procedimentales. Estos últimos están asociados, a diferencia de lo que ocurre en el ámbito TI, con actividades de ingeniería, mantenimiento y producción propias de otro colectivo profesional no familiarizado con la ciberseguridad. Dentro de este servicio se llevan a cabo, desde distintos puntos, test de intrusión a los sistemas de control para tratar de identificar vulnerabilidades que afecten a los dispositivos industriales.	S2 GRUPO	Todos	Global	10	ITIL, PMP, PRINCE2, CISA, CISM, CRISC, ISO 27001 Certified Lead Auditor, ISO 22301 Certified Lead Auditor, CISSP, GPEN, GICSP, APMG ISO 20000, APMG CMDB	FIRST, TF-CSIRT Trusted Introducer, ISO 9001, UNE 166002, ISO 27001, ISO 14001, ISO 20000-1	>10
Evaluación técnica de vulnerabilidades OT	Identificación de vulnerabilidades a nivel técnico para sus sistemas de automatización y control mediante metodologías que garantizan la nula afección a la continuidad de los procesos automatizados. Esta identificación se acompaña de una evaluación de las vulnerabilidades en términos de severidad y riesgo, así como de una propuesta de contramedidas factibles alineadas con la realidad de los sistemas industriales.	S21SEC	Cualquiera	España, Europa y Latinoamérica	8	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>20

AUDITORÍA (11/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Test de intrusión OT básico	Test de intrusión contra equipos empotrados (por ejemplo, RTU, PLC, etc.) y plataformas ICS para identificar vulnerabilidades conocidas, vulnerabilidades de día cero y carencias de funcionalidades de seguridad desde una perspectiva de software.	S21SEC	Cualquiera	España, Europa y Latinoamérica	10	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>30
Test de intrusión OT avanzado	Test de intrusión avanzado contra equipos empotrados que incluye el test de intrusión anterior, así como pruebas de hardware hacking (ej. Ataques de canal lateral, de inyección de faltas, de ingeniería inversa...), así como pruebas de conformidad de protocolos y servicios de comunicaciones.	S21SEC	Cualquiera	España, Europa y Latinoamérica	10	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>20
Red y Purple teams para OT	Simulación de ataques reales pero controlados contra infraestructuras OT para mejorar las capacidades de protección, detección, respuesta y recuperación del cliente. El equipo blanco incluye a personas de OT del cliente y establece las banderas rojas durante las pruebas.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	2

ÍNDICE

AUDITORÍA (12/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Inventario básico de activos OT	Confección de un inventario de activos de OT clave que sustentan los procesos industriales automatizados	S21SEC	Cualquiera	España, Europa y Latinoamérica	8	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>10
Inventario avanzado de activos OT	Confección de un inventario exhaustivo de todos los activos OT relevantes que sustentan los procesos industriales automatizados a través de herramientas de automatización punteras.	S21SEC	Cualquiera	España, Europa y Latinoamérica	8	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>5
FORENSICLab	FORENSICLab es uno de los más completos laboratorios de informática forense europeo, con presencia física en España y Francia, con la capacidad técnica y humana contrastada para la adquisición, conservación, documentación, análisis y presentación de evidencias digitales que, en caso de ser necesario, pudieran ser aceptadas legalmente en un proceso judicial.	SCASSI	Cualquier sector	Nacional / Internacional	5	CHFI, CEH	PASSI	
Test de vulnerabilidad y de intrusión	Test de vulnerabilidad y de intrusión.	SCASSI CIBERSEGURIDAD	Todos	Global	6			30
Auditoría técnica de infraestructuras y sistemas	Auditoría técnica de infraestructuras y sistemas.	SCASSI CIBERSEGURIDAD	Todos	Global	6			10

ÍNDICE

AUDITORÍA (13/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría de las herramientas de seguridad (sondas, anti-virus, SIEM…)	Auditoría de las herramientas de seguridad (sondas, anti-virus, SIEM…).	SCASSI CIBERSEGURIDAD	Todos	Global	6			5
Análisis de código	Análisis de código.	SCASSI CIBERSEGURIDAD	Todos	Global	5			10
Auditoría organizacional / de conformidad seguridad	Auditoría organizacional / de conformidad seguridad.	SCASSI CIBERSEGURIDAD	Todos	Global	6			20
Preparación "Be Ready" ISO 27001 Auditoría de certificación	Proponemos un acompañamiento acotado en el tiempo y orientado a los resultados: Análisis y plan de acción: entrevistas, análisis documental, visitas… Puesta en marcha del plan de acción: organización del SGSI, plan de tratamiento de los riesgos, indicadores y paneles de control... Auditoría de prueba: simulación de una Auditoría de certificación. Auditoría de certificación: preparación de la Auditoría, presencia física durante la Auditoría.	SCASSI CIBERSEGURIDAD	Todos	Global	5		ISO 27001	5
Cybersecurity SAM Engagement	Servicio de auditoría ligera avalado por MICROSOFT ESPAÑA. El servicio se basa en el análisis de los Critical Security Controls (CSC): la auditoría concentra toda la rigurosidad de ISO 27001 en el análisis de los 20 puntos más críticos para su ciberseguridad: * Análisis de inventario SW y HW * Estudio de vulnerabilidades * Test de la robustez de sus aplicaciones, sistemas y redes * Análisis de seguridad perimetral Y mucho más … SCASSI colabora con la DCU, la unidad de MICROSOFT especializada en el análisis mundial de ataques de malwares, para ayudarle a mejorar la seguridad de su organización.	SCASSI CIBERSEGURIDAD	Todos	Global	6	CEH, CISSP, ISO 27001, ISO 22301		1

ÍNDICE

AUDITORÍA (14/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría de seguridad de redes industriales	Secure&IT	Secure&IT	Industria	Global	>5	LEAD AUDITOR ISO 20000/ISO 27001/ ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. LDO. DERECHO, PERITO INFORMATICO JUDICIAL		
IEC 62443 Assessment	Identificación de fallos de seguridad y medidas de mitigación de riesgos basados en normativa IEC 62443 - Basado en estándares IEC 62443. - Disponible para Siemens y terceros. - Question-based. - Informe con recomendaciones para mitigación de riesgos. Recommendations for risk mitigation	SIEMENS	Todos	Global				
ISO 27001 Assessment	Identificación de fallos de seguridad y medidas de mitigación de riesgos basados en normativa IEC 27001 - Basado en estándares IEC 27001. - Disponible para Siemens y terceros. - Question-based. - Informe con recomendaciones para mitigación de riesgos.	SIEMENS	Todos	Global				
SIMATIC PCS 7 & WinCC Assessment	Identificación de fallos de seguridad y medidas de mitigación de riesgos basados en contexto PCS 7 & WinCC. - Basado en estándares y concepto seguridad de SIMATIC PCS 7 & WinCC - Solución personalizada para sistemas SIMATIC PCS 7 & WinCC. - Informe con recomendaciones para mitigación de riesgos.	SIEMENS	Todos	Global				

ÍNDICE

AUDITORÍA (15/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Risk & Vulnerability Assessment	Identificación de fallos de seguridad y medidas de mitigación de riesgos basados en programas de seguridad. - Análisis de riesgos, vulnerabilidades y fallos de seguridad de datos instalados. - Clasificación y categorización de riesgos considerando su criticidad. - Informe con recomendaciones para control y mitigación de riesgos. - Basado en programa de seguridad de análisis de riesgos.	SIEMENS	Todos	Global				
Auditoría de Protección de datos	Auditoría sobre cumplimiento LOPD y RD1720/2007 por el que se aprueba el Reglamento de desarrollo.	TELEFÓNICA - GOVERTIS	Todos	Global	25	Acreditación DPD según esquema AEPD, CDPSE		100
Auditoría de Conformidad ENS	Auditoría de implantación y cumplimiento Esquema Nacional de Seguridad.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		>50
Auditoría de Conformidad ENI	Auditoría de implantación y cumplimiento Esquema Nacional de Interoperabilidad.	TELEFÓNICA - GOVERTIS	Todos	Global	25	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		

ÍNDICE

AUDITORÍA (16/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Ingeniería inversa	Ingeniería inversa de aplicaciones, servicios, equipamiento y protocolos de comunicaciones destinada a la identificación, categorización y mitigación de fallas de seguridad.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Ingeniería social	Ejercicio de concienciación basado en la aplicación de técnicas de engaño y habilidades sociales sobre usuarios con el objetivo de acceder a localizaciones físicas privadas, sistemas de información y redes de comunicaciones obteniendo privilegios e información confidencial de una organización	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

AUDITORÍA (17/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis de vulnerabilidades	Análisis de vulnerabilidades de los diferentes elementos presentes en un ecosistema industrial (sistemas IT/OT, equipamiento embebido, redes de comunicaciones y electrónica de red, aplicaciones/servicios) destinado a indentificar debilidades en materia de seguridad mediante la aplicación de técnicas de análisis manuales (exploiting, fuzzing, testing, etc.) y automatizadas basadas en herramientas tanto de terceros como propietarias.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		
Test de intrusión interno/externo	Servicio que busca comprobar si un atacante podría llevar a cabo una intrusión en los diferentes activos presentes en la infraestructura de una organización, combinando técnicas de exploiting e ingeniería social.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

AUDITORÍA (18/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría Ciberseguridad industrial	Auditoría completa del estado de la ciberseguridad en entornos industriales (dispositivos de red y comunicaciones, automatización y control).	TSK	Energía, Plantas industriales, Medio ambiente	Global	3	CCNA	ISO 9001, 14001, 27001 OSHAS 18001, UNE 166002	
Auditoría Ciberseguridad Smart Home	Sistemas de Smart Home conforme de Security Qualification (SQ)®.	TÜViT	Electricidad	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	
Auditoría Ciberseguridad Procesos	Sistemas de Vigilancia de los Procesos conforme de Security Qualification (SQ)®.	TÜViT	Industria en general	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	
Auditoría Ciberseguridad SCADA	Sistemas de SCADA conforme de Security Qualification (SQ)®.	TÜViT	Industria	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	

AUDITORÍA (19/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Evaluación Smart Grid Common Criteria	Evaluación de los componentes de Smart Grid conforme Common Critiera (CC, ISO 15408).	TÜViT	Electricidad, Gas, Agua	Global	>40	Evaluador de CC	Federal Office for Information Security Germany	
Interoperabilidad Smart Grid	Evaluación de la interoperabilidad y conformidad de los sistemas de Smart Grid.	TÜViT	Electricidad, Gas, Agua	Global	>10	Experto de Conformidad	Federal Office for Information Security Germany	>5
Auditoría ISO 27001	Information Security Management Systems (ISMS).	TÜViT	Todos	Global	>10	ISO 27001 Lead Auditor	DAkkS y Certificadora TÜV NORD CERT	>100
Auditoría ISO 20000	IT Service Management Systems (ITSM).	TÜViT	Todos	Global	>5	ISO 20000 Lead Auditor	APMG y Certificadora TÜV NORD CERT	>30
Auditoría ISO 22301	Business Continuity Management Systems (BCM).	TÜViT	Todos	Global	>5	ISO 22301 Lead Auditor	DAkkS y Certificadora TÜV NORD CERT	>5
Evaluación Trusted Product ISO 27001 Tool	Evaluación de herramientas para implementación de ISO 27001 en un empresa.	TÜViT	Todos	Global	>4	ISO 27001 Lead Auditor	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>5
Seguridad de Productos para exportación a EE.UU. (hardware, firmware, software (o combinación)	Pruebas de módulos criptográficos conforme de FIPS 140-2/3.	TÜViT	Todos	Global	>4	Evaluador de FIPS	NIAP	>20

ÍNDICE

AUDITORÍA (20/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Auditoría Certificación de Ofrecedores de Servicios Confianzas	ETSI y nueva regulación eIDAS.	TÜViT	Ofrecedores de Servicios Confianzas	Global	>5	ETSI Auditor y ISO 27001 Lead Auditor	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>20
Evaluación de Seguridad de productos de TI (hardware y software)	Evaluación de los productos de TI conforme Common Critera (CC, ISO 15408).	TÜViT	Todos	Global	>40	Evaluador de CC	Federal Office for Information Security Germany	>150
Auditoría de Centro de Procesamiento de Datos (CPD)	Seguridad física en los CPDs conforme de Trusted Site Infrastructure (TSI) y Eficiencia Energética en los CPDs conforme de Trusted Site eEfficiency (TSe2).	TÜViT	Todos	Global	>8	TSI Professional	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>200
Auditoría Mobile Security	Evaluación de infraestructuras móviles.	TÜViT	Todos	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>50

ÍNDICE

AUDITORÍA (21/21)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Evaluación de Usabilidad de software	Conforme de DIN EN ISO 9241; ISO 9241-210; ISO 9241-110.	TÜViT	Todos	Global	>2	Experto de usabilidad	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>20
Auditoría Trusted Site Security	Cada sitio infraestructura conforme de Security Qualification (SQ)®.	TÜViT	Todos	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>50
Auditoría Trusted Product Security	Cada producto conforme de Security Qualification (SQ)®.	TÜViT	Todos	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>20

ÍNDICE

CERTIFICACIÓN (1/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Certificación Europrise Privacy Seal	Servicio de Certificación Europrise Privacy Seal.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		8
Certificación Sellos Europeos de Privacidad	Servicio de Certificación Sellos Europeos de Privacidad.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		6
Certificación ISO 27001	Servicio de Certificación ISO 27002.	ECIJA	Todos	Europa	10	CISA, CISM, ITIL, 27001, Lead Auditor, Europrice, Postgrado Ciberberseguridad, Hacking Ético		10
Servicio de monitorización de seguridad para redes de control industrial	Este servicio tiene como objeto detectar cualquier anomalía, cambio o amenaza que pueda suponer un riesgo para la infraestructura tan pronto ésta se haya producido, minimizando la posibilidad de que se materialice un impacto grave en la infraestructura supervisada. El sistema de monitorización se fundamenta en el despliegue de sondas o agentes que se integran en los sistemas supervisados. La intervención humana se produce una vez detectada una situación que lo requiere. La integración de los sistemas se realiza siempre con las máximas garantías para la continuidad de los procesos supervisados. El servicio se presta desde el iSOC de S2-CERT en formato 24x7.	S2 GRUPO	Todos	Global	>100	ITIL, PMP, PRINCE2, CISA, CISM, CRISC, ISO 27001 Certified Lead Auditor, ISO 22301 Certified Lead Auditor, CISSP, GPEN, GICSP, APMG ISO 20000, APMG CMDB	FIRST, TF-CSIRT Trusted Introducer, ISO 9001, UNE 166002, ISO 27001, ISO 14001, ISO 20000-1	>10

ÍNDICE

CERTIFICACIÓN (2/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis avanzado de dispositivos para potenciales certificaciones	Este servicio incluye pruebas de hardware hacking (ej. Ataques de canal lateral, de inyección de faltas, de ingeniería inversa…), así como pruebas de conformidad de protocolos y servicios de comunicaciones.	S21SEC	Cualquiera	España, Europa y Latinoamérica	10	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA		1
Seguimiento y soporte en resolución de vulnerabilidades en entornos industriales	Servicio orientado al acompañamiento que implica el descubrimiento de vulnerabilidades para la búsqueda de soluciones o medida de mitigación.	S21SEC	Cualquiera	España, Europa y Latinoamérica	10	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA		2
Certificación de producto	Certificación propia para producto/dispositivo en ciberseguridad. Inspecciones, ensayos y cumplimiento contra estándares (Prime, DLMS, ISA 62443).	TECNALIA	Industria, eléctrico	Global	8			>100
CSA STAR	Implantación y Certificación de servicios e infraestructuras Cloud	TELEFÓNICA - GOVERTIS	Todos	Global	5	CISA, CISM, ISO 27001 Lead Auditor, Certified ITIL, Certified ISO 20000, ISO 22301 Lead Auditor, CISSP		10
ITSEF	Poseemos un laboratorio de prestigio internacional para la realización de evaluaciones y certificaciones de seguridad de los elementos hardware y software de cualquier sistema, llegando a poder realizar hasta la certificación de mayor nivel de Common Criteria, EAL7.	THALES	Infraestructuras Críticas	Global	100			

ÍNDICE

CERTIFICACIÓN (3/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Certificación Smart Home	Sistemas de Smart Home conforme de Security Qualification (SQ)®.	TÜViT	Electricidad	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>5
Certificación de Procesos	Sistemas de Vigilancia de los Procesos conforme de Security Qualification (SQ)®.	TÜViT	Industria en general	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>5
Certificación SCADA	Sistemas de SCADA conforme de Security Qualification (SQ)®.	TÜViT	Industria	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>10
Certificación ISO 27001	Information Security Management Systems (ISMS).	TÜViT	Todos	Global	>10	ISO 27001 Lead Auditor	DAkkS y Certificadora TÜV NORD CERT	>100
Certificación ISO 20000	IT Service Management Systems (ITSM).	TÜViT	Todos	Global	>5	ISO 20000 Lead Auditor	APMG y Certificadora TÜV NORD CERT	>30

ÍNDICE

CERTIFICACIÓN (4/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Certificación ISO 22301	Business Continuity Management Systems (BCM).	TÜViT	Todos	Global	>5	ISO 22301 Lead Auditor	DAkkS y Certificadora TÜV NORD CERT	>5
Trusted Product ISO 27001 Tool	Evaluación de herramientas para implementación de ISO 27001 en un empresa.	TÜViT	Todos	Global	>4	ISO 27001 Lead Auditor	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009)	>1
Certificación de Ofrecedores de Servicios Confianzas	ETSI y nueva regulación eIDAS.	TÜViT	Ofrecedores de Servicios Confianzas	Global	>5	ETSI Auditor y ISO 27001 Lead Auditor	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>20
Centro de Procesamiento de Datos (CPD)	Seguridad física en los CPDs conforme de Trusted Site Infrastructure (TSI).	TÜViT	Todos	Global	>8	TSI Professional	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>200
Centro de Procesamiento de Datos (CPD)	Eficiencia Energética en los CPDs conforme de Trusted Site eEfficiency (TSe2).	TÜViT	Todos	Global	>8	TSI Professional	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>50

ÍNDICE

CERTIFICACIÓN (5/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Mobile Security	Certificación de aplicaciones móviles, de aplicaciones del sitios web, infraestructuras web.	TÜViT	Todos	Europa	>5	Experto de aplicaciones móviles	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>200
Usabilidad de software	Conforme de DIN EN ISO 9241; ISO 9241-210; ISO 9241-110.	TÜViT	Todos	Europa		Experto de usabilidad	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	
Trusted Site Security	Cada sitio infraestructura conforme de Security Qualification (SQ)®.	TÜViT	Todos	Europa	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>50
Trusted Product Security	Cada producto conforme de Security Qualification (SQ)®.	TÜViT	Todos	Global	>5	Ethical Hacker	Certificadora TÜViT (conforme con DIN EN ISO/IEC 17025:2005, DIN EN 45011:1998, DIN EN ISO/IEC 17065:2013-01 y ISO/IEC 17007:2009	>20

ÍNDICE

CERT (1/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión de alerta temprana y gestión de incidentes de seguridad	Gestión de las alertas tempranas y boletines, detección de incidentes de seguridad provenientes del SIEM. Gestión de incidentes de seguridad: registro, asignación, coordinación, revisión periódica.	ATOS	Todos	Global	20	CEH, Cisco CCNA, CCNP, Checkpoint CCSA, CCSE, CCNSP, ACSA / ACSE, ArcSight 5.0, HP Fortify security, IBM InfoSphere Guardium, MCP, MCSE, SCAE (Skybox), BlueCoat BCCPA, Juniper Networks JNCIA-FWV, JNCIS-FWV, JNSA FW, IDP JNSS FW IDP	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	20
INCIDENT RESPONSE	Apoyo y consejo ante un incidente de ciberseguridad a través del teléfono gratuito telephone 900 104 89 o vía email mediante: email incidencias@bcsc.eus / arazoak@bcsc.eus.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT.ES
VULNERABILITY RESPONSE COORDINATION	Facilitamos la comunicación entre quienes descubren vulnerabilidades y los fabricantes, promoviendo así una divulgación responsable a través de una comunicación fluida y honesta.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT.ES
ALERTS AND WARNINGS	Información práctica y relevante para mitigar y remediar vulnerabilidades de seguridad en sistemas tecnológicos.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT.ES
ANNOUNCEMENTS	Información sobre amenazas y riesgos de especial relevancia.	BCSC	Todos	Euskadil	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT.ES
SECURITY-RELATED INFORMATION DISSEMINATION	Elaboramos guías de buenas prácticas y estudios e informes situacionales en el ámbito de la ciberseguridad.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT.ES

ÍNDICE

CERT (2/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
AWARENESS BUILDING	Impartimos jornadas de concienciación de cara a elevar el nivel de madurez en ciberseguridad de la ciudadanía y de las empresas.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITI	FIRST, CSIRT. ES
BASQUE INTERNET SPACE MONITOR	Monitorizamos el espacio de Internet de Euskadi de cara a identificar riesgos potenciales y puntos de mejora para elevar el nivel de madurez de ciberseguridad de Euskadi.	BCSC	Todos	Euskadi	4	4	GMOB, CRISC, CISA, CISM, PMP, CCNA, ITIL	FIRST, CSIRT. ES
Respuesta ante incidentes de seguridad	Servicio Cyberincident Response ante incidentes de seguridad informáticos, con análisis de malware en remoto, soporte y desplazamiento *on site*, toma de medidas de contención desde el momento inicial hasta la remediación del caso completo, incluyendo forense digital completo de los equipos afectados.	DELOITTE	Todos	Global	15	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	10
Gestión de Crisis	Servicio global de respuesta ante crisis, escalada desde cualquier ámbito, ya sea tecnológico, humano, natural, etc., con coordinación entre diferentes áreas tantos técnicas como organizativas y con soporte técnico, legal, financiero, etc.	DELOITTE	Todos	Global	5	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH, GCFA	ISO 27001, ISO 22301	5
Gestión de Vulnerabilidades	Control Vulnerabilidades en sistemas y redes. Control Vulnerabilidades en Software Cliente. Control de Vulnerabilidades en SSOO y parches.	EVERIS	Todos	Global	5		TF-CSIRT FIRST	5
Análisis Forense	Análisis forense Remoto. Análisis forense *in situ*. Análisis forense de discos. Análisis forense de redes.	EVERIS	Todos	Global	5	CEH, CHFI, GCIH	TF-CSIRT FIRST	5
Análisis Antimalware	Análisis de malware. Informes y procedimiento de resolución.	EVERIS	Todos	Global	5	CEH, CHFI, GCIH	TF-CSIRT FIRST	5
Soporte a Incidentes de Seguridad	Atención a incidentes de seguridad. Ayuda remota a incidentes. Informes de control del sistema.	EVERIS	Todos	Global	5	CEH, CHFI, GCIH	TF-CSIRT FIRST ISO 27001 ISO/IEC 27035:2011	5
Implementación de HoneyNets	Servicio cuyo objeto es la implantación de una infraestructura tecnológica con vulnerabilidades (dispuestas de forma intencionada), que invite a ataques de terceros, y permita así estudiar técnicas y patrones de comportamiento.	EVERIS	Todos	Global	5	CEH, CHFI, CISSP, CISA		5

ÍNDICE

CERT (3/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Gestión de crisis de incidentes de seguridad	Servicio de respuesta ante una crisis provocada por un incidente de seguridad. Actuación de expertos que intervienen de manera rápida para detectar, analizar, contener y coordinar las acciones necesarias.	GRUPO SIA	Todos	Global	16	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	4
Gestión de Vulnerabilidades	Servicio de gestión de vulnerabilidades en los sistemas informáticos.	GRUPO SIA	Todos	Global	20	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	2
Análisis forense	Análisis Forense pericial, *insitu* y remoto.	GRUPO SIA	Todos	Global	8	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	3

ÍNDICE

CERT (4/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Análisis de malware	Análisis de malware.	GRUPO SIA	Todos	Global	8	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	3
Alerta temprana	Notificación de las vulnerabilidades y amenazas más importantes que puedan afectar a los activos del cliente.	GRUPO SIA	Todos	Global	12	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	2

CERT (5/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Cert de Seguridad e Industria (CERTSI)	Este servicio CERT incluye: - Servicios de detección proactiva en remoto, detector de incidentes, elaboración de informes. - Servicios reactivos: Respuesta a incidentes de ciberseguridad (24x7x365). - Servicios preventivos: publicación de avisos y alertas de ciberseguridad, publicación de vulnerabilidades conocidas, remisión de vulnerabilidades 0day a operadores de IICC, difusión de la alerta temprana mediante el envío de boletines a suscriptores interesados, publicación de guías, estudios e informes. - Soporte a la implementación de los Planes Estratégicos Sectoriales (PES), Plan de Seguridad del Operador (PSO), Plan de Protección Específico (PPE). - Organización de Ciberejercicios orientados a la mejora de la concienciación, formación, adiestramiento, colaboración e intercambio de información y análisis del nivel de seguridad. - Compartición de información de ciberamenazas con operadores de IICC a través de una plataforma para identificar indicadores de compromiso (IOC). - Elaboración de informes de exposición de operadores de IICC. - Servicios de soporte a FCSE. - Desarrollo de herramientas y aplicaciones específicas para FCSE. - Concienciación en CS a los grupos de interés del CERT.	INCIBE	Todos	Global	7	CISA, CISM, CRISC, AUDITOR SGSI, IMPLANTADOR SGSI CISSP, GIAC-GCFA, GIAC-GPEN, ITIL, PMP, EC Council Certified Ethical Hacker CEH, EC Council Certified Secure Programmer (ECSP), EC Council Computer Hacking Forensic Investigator (CHFI), CCS-T, EFQM, SCJP, MCSE, MCT, MCSA, eCPPT	FIRST, TRUSTED INTRODUCER, ISO 27001, ISO 9001	N/A
Alerta Temprana	El servicio de Alerta Temprana realiza la gestión de las publicaciones de amenazas que pudieran afectar a nuestros clientes incluyendo un plan de mitigación y seguimiento de las vulnerabilidades sobre los sistemas y una herramienta para facilitar la gestión del servicio. El servicio se ofrece desde el Cibersecurity Operation Center de Indra (i-CSOC). El servicio de Alerta Temprana realiza la identificación, análisis, comunicación y seguimiento de vulnerabilidades.	MINSAIT	Todos	Global				2

CERT (6/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicio de Respuesta a Incidentes de Ciberseguridad	El servicio de Capacidad de Respuesta a Incidentes se encarga de aplicar medidas preventivas y reactivas ante incidentes de seguridad. El servicio se ofrece en modo remoto desde el Cibersecurity Operation Center de Indra (i-CSOC). El servicio puede requerir puntualmente intervenciones *insitu* para "hacking ético para test de intrusión y análisis de vulnerabilidades", intervenciones *in situ* puntuales para asistencia ante incidentes graves y análisis forense para búsqueda de evidencias en servidores y equipos de usuario. La atención del servicio por parte del i-CSOC es de 24x7 atendido por operadores de 1er nivel y guardias de asistencia telefónica por técnicos especializados de niveles 2 y 3.	MINSAIT	Todos	Global				2
Alerta Temprana	El servicio de Alerta Temprana realiza la gestión de las publicaciones de amenazas que pudieran afectar a nuestros clientes incluyendo un plan de mitigación y seguimiento de las vulnerabilidades sobre los sistemas y una herramienta para facilitar la gestión del servicio. El servicio se ofrece desde el Cibersecurity Operation Center de Indra (i-CSOC). El servicio de Alerta Temprana realiza la identificación, análisis, comunicación y seguimiento de vulnerabilidades.	MINSAIT	Todos	Global				2
Industrial ICS CERT	Servicios de respuesta a incidentes, laboratorios de análisis forense digital, scada, dispositivos electrónicos, tests de penetración, Seguridad en el diseño de aplicaciones y comprobación.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12

ÍNDICE

CERT (7/7)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicio de respuesta a incidentes de seguridad	Servicio de gestión y respuesta ante incidentes de seguridad, incluyendo la identificación del origen, diagnóstico e informe del mismo, incluyendo capacidades de remediación, análisis forense, reversing de malware.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Mas de 20	CISSP, CEH, CIH, GCIH, GPEN, OSCE, GXPN, CCNA, CPTE	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 10
CERT	Para anticiparnos a la detección de las amenazas cibernéticas, proporcionamos inteligencia a medida sobre vulnerabilidades, amenazas y ataques de los componentes hardware y software más comunes en las infraestructuras de los sistemas de información, comunicaciones y operacionales. Servicio ofrecido desde 1997 y con una disponibilidad 24x7 Los datos de vulnerabilidades se califican mediante la comprobación cruzada y el análisis de diferentes fuentes, se clasifican utilizando una puntuación de riesgo basada en las métricas estándar CVSS y EISPP y se enriquecen con las soluciones recomendadas, incluyendo las revisiones o soluciones conocidas.	THALES	Infraestructuras Críticas	Global		CEH, CISA, CISM, ITIL Expert	ISO 27001	

SOC (1/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Manage Security Operations (MSO)	Operación de procesos y tecnologías de seguridad desde centros de excelencia.	ACCENTURE	Todos	Global	500	CISA, CISM, CISSP, ITIL, Certificaciones de fabricantes de ciberseguridad	ISO 9001, ISO 27001, ISO 20000, ISO 14001, CMMI L5	30
Servicio de gestión y monitorización de la seguridad	Servicios de gestión, administración y mantenimiento de plataformas tecnológicas de seguridad, incluyendo entre otros, SIEM, IPS, cortafuegos, antimalware, antispam, etc. Servicio de monitorización de eventos de seguridad mediante SIEM (24x7).	ATOS	Todos	Global	20	CEH, CCNA, CCNP, CCSA, CCSE, CCNSP, ACSA / ACSE, ArcSight 5.0, HP Fortify security, IBM InfoSphere Guardium, MCP, MCSE, SCAE (Skybox)	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	25
Servicios gestionados de seguridad	Servicios de gestión, administración y mantenimiento de plataformas tecnológicas de seguridad, incluyendo entre otros, SIEM, IPS, cortafuegos, antimalware, antispam, etc.	DELOITTE	Todos	Global	40	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH, Certificaciones de fabricantes	ISO 27001, ISO 22301	>20
Servicios de protección contra DoS	Servicios gestionados de protección frente a ataques de denegación de servicio (DoS) en la nube.	DELOITTE	Todos	Global	10	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH, Certificaciones de fabricantes	ISO 27001, ISO 22301	10
Análisis Forense	Análisis detallado de un incidente de seguridad con objeto de determinar el impacto del mismo, la causa raíz que propicio su ocurrencia así como la identificación de acciones correctivas / recomendaciones a contemplar para evitar incidentes similares.	EVERIS	Todos	España	2	CHFI, CEH	ISO27001	5
Implantación de Soluciones de Gestión y Monitorización de Eventos de Seguridad	Servicio orientado a la definición e implantación de un modelo de centralización y monitorización de eventos de seguridad, pudiendo optarse por herramientas comerciales u enfoques open-source.	EVERIS	Todos	España, Europa y Latinoamérica	3	CHFI, CEH	ISO27001	5

ÍNDICE

SOC (2/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Monitorización de la Seguridad	- Detección de Intrusos de red. - Detección de Intrusos de host. - Detección de Intrusos por Honeypot. - Correlación de Eventos.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
Monitorización de la Disponibilidad	Control de sistemas funcionando. Control de servicios funcionando. Control de puertos de red funcionando.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
Monitorización del Rendimiento	Control de Almacenamiento. Control de uso de CPU. Control de uso de Memoria.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
Monitorización de Redes	Control de ancho de banda.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
Monitorización Cumplimiento	Control de Usuarios. Control de Accesos a Documentos. Control de Flujos de red. Control de Sesiones. Control de Configuración. Control de Virus. Control de Accesos WEB. Control de Cuentas email.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
Monitorización de Fuga de Archivos	Control de USB. Control de impresión.	EVERIS	Todos	Global	5	CISA, CISSP, CISM, CEH, GPEN, GCIH	ISO27001	5
CONNtrol - SOC ciberseguridad de sistemas	Supervisión, gestión y monitorización de la seguridad de sistemas de control. 7x24.	GETRONICS	Todos	España, Europa y Latinoamérica	5			

SOC (3/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Monitorización y Gestión de incidentes de seguridad	Servicio monitorización de alertas de seguridad de los servicios monitorizados, atención y respuesta desde el Centro Experto de Ciberseguridad que opera en 24x7.	GRUPO SIA	Todos	Global	16	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	4
Inycom - Industrial SOC	Gestión de alerta, control y soporte de incidentes en redes de control industrial.	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	AENOR ISO27001, AENOR ISO20000-1	
Monitorización de seguridad	Servicio de seguridad ofrecido en remoto desde el SOC de ITS en modalidad 24x7x365. Destinado a supervisar, identificar y reportar los eventos de seguridad que se producen en la infraestructura industrial a partir de *logs* generados por diversas fuentes (dispositivos IT y OT, infraestructura de comunicaciones, dispositivos de seguridad (Firewalls, IPS, diodos de datos, etc.), registros de auditoría de sistemas operativos, etc.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	12	CISA, GICSP	ISO 27001	
Gestión de dispositivos e incidentes de seguridad	Servicio remoto llevado a cabo desde el centro de operaciones de seguridad de ITS, destinado al mantenimiento y configuración de los sistemas de seguridad y electrónica de red que integran la infraestructura industrial de las organizaciones, así como actuar de forma reactiva ante los incidentes de seguridad producidos en cualquier momento.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	12	CISA, GICSP	ISO 27002	

ÍNDICE

SOC (4/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Mitigaciones DDoS	Servicio destinado a paliar las consecuencias de ataques de Denegación de Servicio sufridos por las infraestructuras OT e IT de las organizaciones, mediante la re-configuración o tuneo temporal de los dispositivos de seguridad que ejercen el rol de frontera.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	6	CISA, GICSP	ISO 27003	
Soporte técnico de seguridad	Apoyo técnico en materia de seguridad en formato 24x7x365, ofreciendo soporte ante incidencias ocurridas en los sistemas y aplicativos de seguridad desplegados en la organización.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	12	CISA, GICSP	ISO 27004	
Análisis forense	Servicio orientado a identificar la autoría y los métodos usados durante un ataque a los sistemas de información de la organización, así como la información o procesos que han sido alterados durante su ejecución. También proporciona los conocimientos para prevenir dichas intrusiones en el futuro. El análisis forense es la solución ideal para las organizaciones que tienen la necesidad de investigar el origen de incidentes de seguridad que se producen en sus equipos.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España	3	CISA, GICSP	ISO 27005	
Servicio de monitorización de seguridad	Prestación del servicio de monitorización de eventos de seguridad mediante SIEM instalado en una red de control, en modalidad 24x7. El servicio se ofrece desde el Cibersecurity Operation Center de Indra (i-CSOC) en modalidad 24x7 los 365 días del año.	MINSAIT	Todos	Global				
Industrial Cyber SOC	Servicios de innovación y generación de capacidades adaptativas y evolutivas en defensas de infraestructuras multinivel y multicapa sobre sistemas ICS/SCADA.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12

SOC (5/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Managed Security Services (MSS)	Servicios de Seguridad Gestionada, consistente de forma global con centros de soporte propios y equipos de consultores de seguridad específicos para soportar estos servicios: Managed Firewall, Managed IPS, Managed Web Gateway, Managed WAF, Managed eMail, Managed SIEM.	NTT	Todos	Global	SOC's a nivel Internacional		ISO 27001 ISO 9000 ISO 14001	
Cloud Security Services (CSS)	Servicios de Seguridad en Cloud consistentes de forma global con cloud propio de NTT que permite ofrecer servicios como: Email Security-as-a-Service, Web Security-as-a-service, Security Appliance-as-a-Service, Real-time Threat Management-as-a-Service, Vulnerability Management-as-a-Service, Global Threat Intelligence Platform.	NTT	Todos	Global	Cloud a nivel Internacional		ISO 27001 ISO 9000 ISO 14001	
Managed Services for Enterprise Services (MSEN)	Servicios de soporte gestionados para redes empresariales, consistentes de forma global con centros de soporte propios y equipos multidisciplinares. Se comercializa con 3 niveles que permiten gran flexibilidad a la hora de abordar cualquier servicio: Insite Essentials, Advanced y Premier.	NTT	Todos	Global	NOC's y SOC's a nivel Internacional		ISO 27001 ISO 9000 ISO 14001	
SOC OT	Servicio de SOC basado en la monitorización de eventos de seguridad y eventos de salud relacionados con los sistemas de automatización y control industrial para brindar asesoramiento sobre cómo resolver posibles incidentes.	S21SEC	Cualquiera	España, Europa y Latinoamérica	>50	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC, CCNA, Certificaciones de fabricantes relacionados con el servicio (Fortinet, PaloAlto, Checkpoint, Stormshield, Cisco, F5)	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet, FIRST, CERT AUTORIZED, TF-CSIRT	>6

ÍNDICE

SOC (6/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
SOC - Redes IIoT	Vigilancia continua con reportes periódicos; Estado de la seguridad de una red industrial con dispositivos IoT.	SARENET	Todos	España	>20			
Apoyo al SOC (N2 – N3)	Apoyo al SOC (N2 – N3).	SCASSI CIBERSEGURIDAD	Todos	Global	6			10
WINSOC	WINSOC es un servicio llave en mano para la creación de un SOC orientado a su actividad. Este servicio abarca desde el diseño de la infraestructura, la planificación de recursos o el despliegue tecnológico, hasta la puesta en marcha de las acciones de prevención, supervisión y control de la seguridad de los sistemas y redes de la organización.	SCASSI CIBERSEGURIDAD	Todos	Global	6	CEH, CISSP		10
Secure&Guard	Gestión de vulnerabilidades, es un proceso de monitorización continua que proporciona una unidad de gestión en tiempo real de todos los procesos que ocurren en las redes y sistemas internos y externos de la organización.	SECURE&IT	Todos	Global	>5	Lead Auditor ISO 20000/ISO 27001/ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. Ldo. Derecho, Perito Informatico Judicial		
Secure&Guard	Cibervigilancia digital y prevención de amenazas, proporciona una unidad de respuesta, responsable de la monitorización, detección y aislamiento de incidentes. La unidad de respuesta es el punto central de monitorización y correlación de todos los eventos registrados dentro de la organización y el encargado de decidir como se manejarán. El servicio comprende: brotes de malware, ataques de phising, fugas de información, detección de fraude y reputación online.	SECURE&IT	Todos	Global	>5	Lead Auditor ISO 20000/ISO 27001/ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. Ldo. Derecho, Perito Informatico Judicial		

ÍNDICE

SOC (7/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
AntiDDoS	Servicio prestado desde la propia Red de Telefónica que proporciona una protección frente a ataques de denegación de servicio, distribuidos o no, incluyendo la detección automática y mitigación de éstos evitando que se paralice la actividad de un negocio.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 60	n/a	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 30
RED TEAM	Designed to continuously test and improve the effectiveness and respond capabilities of corporate information security defenses (Blue Team) mimicking real-world scenarios by replicating the Techniques, Tactics and Procedures (TTPs) of real-world adversaries.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 50	OSCP, OSCE, OSWP, EC-Council CEH, CREST CPSA, CREST CRT, GIAC GREM, ISC2 CISSP, ISACA CRISC, CompTIA Security +, SPSE Python Scripting Expert	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 20
PENTESTING & SECURITY ASSESSMENT	Pentesting & Security Assessment covering infrastructure, software and employees testing to make appropriate decisions to secure an organization.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 50	OSCP, OSCE, OSWP, EC-Council CEH, CREST CPSA, CREST CRT, GIAC GREM, ISC2 CISSP, ISACA CRISC, CompTIA Security +, SPSE Python Scripting Expert	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 200
IT VULNERABILITY SCANNING	Vulnerability Analysis for internal and external scanning to detect vulnerabilities across IT network infrastructure.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 20	CompTIA Security + EC-Council CEH Certificaciones de fabricantes	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 200
WEB APPLICATION SCANNING	Web Application Scanning for internet facing web applications that incorporates and automates the latest techniques and tools used by real attackers in a persistent process over time.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 20	CompTIA Security + EC-Council CEH Certificaciones de fabricantes	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 200

ÍNDICE

SOC (8/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
IT SECURITY MONITORING	Monitoring, correlation and automated remediation, integrating the security events of the IT infrastructure into our advanced iMSSP platform, in order to minimize the impact on a client of a possible materialization of a threat.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 50	CISA, CISM, CISSP, CCSA, CSA STAR, GICSP, OSCP, CEH, PMP, ITIL, Certificaciones de fabricantes	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 150
IT SECURITY DEVICE MANAGEMENT	Administration, maintenance, support and health monitoring services for security technology platforms, including, among others, SIEM, IPS, IDS, antivirus, firewall, anti-malware, anti-spam, etc	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 200	CISA, CISM, CISSP, CCSA, CSA STAR, GICSP, OSCP, CEH, PMP, ITIL, Certificaciones de fabricantes	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	Más de 2000
CSOC (Cyber Security Operation Center)	Thales ha desarrollado una completa cartera de servicios SOC para responder a las necesidades clave de seguridad cibernética de los clientes: 1. Anticipando las amenazas y los riesgos de la seguridad cibernética. 2. Detectando los ataques cibernéticos y comportamientos anómalos, y respondiendo en tiempo a los incidentes para mantener la continuidad del negocio. 3. Cumpliendo con las regulaciones. Tenemos la capacidad de proporcionar una gama completa de modelos de implementación y explotación SOC capaces de adaptarse a las necesidades y expectativas específicas de cada cliente: - Solución interna: solución completa propietaria, para los clientes que desean tener un control de extremo a extremo de su solución. - Solución híbrida: para los clientes que necesitan mantener el procesamiento de datos en sus instalaciones. - Totalmente subcontratado: servicio totalmente proporcionado por Thales desde uno de sus SOCs.	THALES	Todos	Global	300	CEH CISA CISM ITIL Expert	ISO 27001	

ÍNDICE

SOC (9/9)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Respuesta a incidentes de ciberseguridad OT	Servicio destinado a ofrecer una respuesta temprana ante posibles incidentes de seguridad que afecten a las organizaciones, identificando la raíz del problema y aplicando medidas compensatorias de forma reactiva para paliar sus efectos.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

INTELIGENCIA (1/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Servicio de inteligencia global	Servicio de inteligencia global para proporcionar información sobre vulnerabilidades, avisos y amenazas Análisis en profundidad de las amenazas emergentes, incluyendo análisis de malware, fugas de información, ataques DDoS, activismo y hacktivismo, vulneración de mecanismos de seguridad, conductas peligrosas, suplantaciones de identidad, robo de credenciales, espionaje, usurpación de dominios, contenidos ofensivos, etc.	ATOS	Todos	Global	15	CEH, Cisco CCNA, CCNP, Checkpoint CCSA, CCSE, CCNSP, ACSA / ACSE, ArcSight 5.0, HP Fortify security, IBM InfoSphere Guardium, MCP, MCSE, SCAE (Skybox), BlueCoat BCCPA, Juniper Networks JNCIA-FWV, JNCIS-FWV, JNSA FW, IDP JNSS FW IDP	ISO 9001, ISO 20000, ISO 27001, CMMI DEV 3, CMMI SVC 3, UNE-EN 9100, ISO 14001, OHSAS 18001, PECAL, PCI-DSS QSA	10
Intelligence and Analytics	Ayesa ofrece un servicio de gestión de inteligencia a través de múltiples puntos de vista: Alertas de seguridad, prevención de incidentes, resumen de sensibilidades, volumen de menciones, tendencias, usuarios influyentes, opiniones, posibles daños reputacionales, información sobre sus altos directivos, campañas de phishing e información en la Deep Web.	AYESA	Todos	Global				
Cyberwatch	Servicios de vigilancia, eCrime e inteligencia digitales, incluyendo protección de marca, vigilancia de campañas online, antiphishing, anti-botnet, anti-malware, etc.	DELOITTE	Todos	Global	10	CISA, CISM, CISSP, CCSA, GICSP, OSCP, CEH	ISO 27001, ISO 22301	>15
Intelligence (Puesta en operación)	Parametrización, formación a cliente y puesta en operación de herramientas de cibervigilancia (proveedores de dos soluciones probadas).	EVERIS	Todos	Global	21	CISA, CISSP, CISM, CRISC, GPEN, GCIH, OSCP, OSCWP, ITIL Service Manager.	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>10
Intelligence (Vigilancia)	Servicios de vigilancia a clientes para ayudarles: - Detectar Fraude. - Detectar Malware en sus páginas o páginas referenciadas. - Análisis de Marca.	EVERIS	Todos	Global	21	CISA, CISSP, CISM, CRISC, GPEN, GCIH, OSCP, OSCWP, ITIL Service Manager	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>10

ÍNDICE

INTELIGENCIA (2/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Intelligence (Análisis)	Realización de análisis bajo demanda de diversas tipologías (investigación riesgo - país, investigación sobre compañías).	EVERIS	Todos	Global	21	CISA, CISSP, CISM, CRISC, GPEN, GCIH, OSCP, OSCWP, ITIL Service Manager	ISO 27001, ISO 9000, ISO 14000, CMMI v5	>10
Servicio de ciberinteligencia	El servicio de ciberinteligencia de SIA está especializado en Open Source Intelligence (OSINT), orientado al análisis y detección de: - Movimientos sociales y Hacktivismo. - Ciberterrorismo. - Reputación on-line (marca, personas relevantes). - Alerta temprana de ciberamenazas. - Inteligencia competitiva. - Inteligencia estratégica.	GRUPO SIA	Todos	Global	7	CISA, CISM, CISSP, CRISC, CGEIT, ITIL, CICISO, PCI DSS QSA ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 20000 Lead Auditor, CEH, CPHE, Compita Security+, CHFI, Director de Seguridad, Postgrado en Inteligencia	ISO 9001 ISO 14001 ISO 27001 ISO 20000 PCI-QSA ISO 22301 ISO 15504 L3	5
Vigilante de Logs - Plataforma de Reportes (Análisis Tech BigData opcional)	Centralizado de cuadros de mando (dashboard) con logs de todos los eventos de los sistemas en la red; logs de servicio de las aplicaciones a monitorizar, syslog de los sistemas operativos y logs de los servidores de aplicaciones industriales.	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	AENOR ISO27001, AENOR ISO20000-1	
Observatorio de inteligencia en seguridad	Servicio destinado a la monitorización de la web 2.0 con el objetivo principal de realizar un seguimiento constante de la actividad en páginas web y redes sociales, y crear alertas cuando se detecte alguna incidencia en lo que se refiere a la reputación corporativa, movimientos de competidores, nuevas oportunidades de mercado, o amenazas y vulnerabilidades de seguridad que puedan afectar a los sistemas informáticos de las organización.	ITS SECURITY	Industrial, Energía, Transporte, Banca, Administración pública, TELCO	España				

ÍNDICE

INTELIGENCIA (3/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Threat Intelligence	Servicio de sensores inteligentes de seguridad SCADA, modelado de amenazas, gestión de vulnerabilidades y gestión de riesgos.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	9	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	12
Ciberinteligencia	Servicios de ciberinteligencia para la detección, prevención y mitigación de amenazas y acciones fraudulentas sobre infraestructuras, activos, personas, branding, etc.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	10	DSICE, CISA, CISM, ITIL, CEH, CHFI, ECSA, CISSP, GIAC-GPEN, ISO27001LA, ECPPT, ICS-CERT OPSEC, CSSA, CREA, GCHI, ENCE, ACE, PMP	ISO27001, ISO9000, ISO14000	13
Vigilancia digital orientada a entornos industriales	Detección de campañas maliciosas activas en entornos industriales y generación de inteligencia para su posterior consumo en los SOC o CERT.	S21SEC	Cualquiera	España, Europa y Latinoamérica	6	GRID (GIAC Response and Industrial Defense), GICSP (Global Industrial Cyber Security Professional), ISA/IEC 62443 (Fundamentals specialist), ISO 27001 Lead Auditor, OSCP, CEH, CISA, CISM, CISSP, CRISC	ISO 27001, ISO 9001, ISO 20000-1, RD3/2010 (ENS), RD 3/2010 (ENS), IQNet	>8

ÍNDICE

INTELIGENCIA (4/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Secure&Guard	Servicio de Ciberinteligencia de Amenazas es un servicio especializado y customizable (brotes de malware, ataques de phising, fugas de información, detección de fraude, amenazas dirigidas y reputación online) que reduce el tiempo de respuesta de los incidentes y, por lo tanto, la ventana de oportunidad para los ciberatacantes.	Secure&IT	Todos	Global	>5	Lead Auditor ISO 20000/ISO 27001/ISO23301, CISA, CISM, CISSP, CEH, CCNA, CCNP R&S, CBCP, OSCP, ITIL V3, SIEMENS CPIN SECURITY, R&S, NOZOMI NETWORK CERTIFIED for SCADAguardian. Ldo. Derecho, Perito Informatico Judicial		
Digital Risk Protection	Servicio de detección de amenazas que, a partir de fuentes públicas, comerciales, listas de correo, redes sociales, canales de alerta temprana de vulnerabilidades, etc. Aporta inteligencia aplicable al entorno del cliente.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 30	OPST, ACSA, Chief Auditor ISMS, FireEye Systems Engineer, FireEye Product Specialist, CISA, GCIH, GPEN, CEH, CISSP, OSCE, GXPN, CCNA, CPTE, ITIL Foundation v3, CCS-T, CCS-SP, Director de Seguridad, Investigador Privado, Information Security for Technical Staff, Fundamentals of Incident Handling Advanced Incident Handling for Technical Staff	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	

ÍNDICE

INTELIGENCIA (5/5)

Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones profesionales	Certificaciones de empresa	Número de referencias
Bespoke CTI Projects	Servicio de inteligencia (OSINT) personalizado destinado a apoyar la toma de decisión en distintos ámbitos de riesgo empresarial. Basada en nuestra experiencia de trabajando en el ámbito de la inteligencia de fuente abierta y un profundo conocimiento del estado de arte de las tecnologías, se pone nuestra experiencia y nuestros conocimientos tecnológicos a disposición del cliente. El servicio se opera por una unidad de inteligencia diseñada a medida, con los perfiles y la tecnología mas apropiada, para el entorno del cliente.	TELEFÓNICA - ELEVENPATHS	Todos	Nacional / Internacional	Más de 30	OPST, ACSA, Chief Auditor ISMS, FireEye Systems Engineer, FireEye Product Specialist, CISA, GCIH, GPEN, CEH, CISSP, OSCE, GXPN, CCNA, CPTE, ITIL Foundation v3, CCS-T, CCS-SP, Director de Seguridad, Investigador Privado, Information Security for Technical Staff, Fundamentals of Incident Handling Advanced Incident Handling for Technical Staff	ISO 27001, ISO 9000, ISO 20000, CUMPLIMIENTO ENS Acreditado, CUMPLIMIENTO LOPD Acreditado	
Ti Sight	Servicios de vigilancia digital de organizaciones industriales: Informe huella digital, Usuarios corporativos, Spam y malware, Propiedad intelectual, Reputación online, Cambios en el perímetro, Dominios fraudulentos, Vulnerabilidades y Exploits, Compromiso de la web.	TITANIUM INDUSTRIAL SECURITY	Todos	Global	15	GICSP, CSSA, CISSP, ITIL, PMP, OSCP, OSWE, IC32, IC33, IC34, IC37, CCNA, CCNP, Lead auditor ISO 27001, Fortinet NS7, Forescout Silent Defense Administrator, Nozomi NA for SCADaguardian, ICS-CERT 210W, FireEye SystemsEngineer, FireEyeProduct Specialist, Administtración SMARTFENSE, Implementación SMARTFENSE		

ÍNDICE

SOLUCIONES

ÍNDICE

CONTROL DE ACCESO (1/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Firma biométrica (manuscrita digitalizada, voz,…)	AtoSFirma2e	Integración de procesos de firma biométrica en trámites telemáticos.	ATOS	Todos	España	3		10
Firma electrónica basada en certificados (avanzada/ reconocida)	AtoSFirma	Integración de funcionalidades de firma electrónica basada en certificados y criptografía en aplicaciones de escritorio (Windows, macOS, Linux) y móviles (iOS, Android). Solución web de Portafirmas.	ATOS	Todos	España	3		100
Gestión de identidades	Evidian Enterprise Single Sign On	Solución corporativa de Single Sign On.	ATOS	Todos	Global	50		600
Control de Acceso web	Evidian Web Access Manager	Federación de identidades, autorización basada en políticas, autenticación web y SSO.	ATOS	Todos	Global	50		400
Gestión de Identidades	Evidian Identity Governance & Administration	Gobierno, gestión y control las identidades de los usuarios, las políticas, los procesos y los derechos de acceso.	ATOS	Todos	Global	50		200
Plataforma PKI & Firma electrónica	IDnomic ID PKI (ID CA, ID RA, CMS), Vericert (VA), Metatime (TSA), Metasign (Digital Signature).	Solución integral para generar certificados electrónicos y gestionar su ciclo de vida.	ATOS	Todos	Global	>50		>100
Gestión de identidades	Evidian Analytics & Intelligence	Cumplimiento sostenible, análisis de riesgos y análisis.	ATOS	Todos	Global	50		200
Autenticación	Evidian Authentication Manager	Autenticación multifactor de Windows y restablecimiento de contraseña de autoservicio.	ATOS	Todos	Global	50		600

ÍNDICE

CONTROL DE ACCESO (2/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Acceso seguro a unidades USB de almacenamiento	SafeDoor	Solución HW/SW que proporciona protección integral ante vectores de ataque a través de dispositivos de almacenamiento USB: - Ataques de sobretensión eléctrica - badUSB - Malware (Antivirus integrado) Incluye gestión y trazabilidad centralizada de la información transferida con enlace a sistemas SIEM.	authUSB	Todos	Global	Nacional / Internacional	Certificación LINCE ENS Nivel Alto	
Jump Server OT	W6 Secure Access Server (W6 SAS)	Servidor bastión para el acceso seguro de los equipos de soporte y mantenimiento de sistemas ICS. W6 SAS proporciona autenticación fuerte, autorización basada en LDAP para la ejecución exclusiva de las aplicaciones permitidas, y trazabilidad de todas las acciones realizadas desde este jump server (incluyendo videograbación de la sesión). Cuenta con una funcionalidad de intercambio seguro de archivos mediante el análisis de amenazas conocidas y desconocidas.	CIC Consulting Informatico	Nuclear, Aguas, Utilities, Industrial	España	3		2
Analizador de Vulnerabilidades Autenticado	Vulnerability Analyzer	Vulnerability Analyzer descubre las vulnerabilidades de los productos (incluido el sistema operativo) instalados. No requiere autenticación ni instalación en el equipo auditado ya que es portable. Al ejecutarse en el equipo, se realiza un análisis de caja blanca, evitando falsos positivos y descubriendo vulnerabilidades de todos los productos instalados, aunque no tengan puertos abiertos. El informe generado sigue los estándares CVE para la identificación y CVSS para la puntuación de vulnerabilidades.	DIGITAL CUBES	Todos	Global			3
Protección de estaciones de trabajo	FortiClient	Análisis de vulnerabilidades, protección antimalware, protección antiexploit, firewall de aplicaciones, control de aplicaciones y control de la navegación. También se integra con FortiSandbox para protección de amenazas zero day.	FORTINET	Todos	Global			
NGFW	FortiGate	Firewall de nueva generación. Permite el control de aplicaciones industriales, ataques a sistemas de control (IPS). Y antimalware. Disponibles distintos modelos ruggerizados. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			
VPN	FortiGate	Concentrador VPN Sede a Sede y de acceso remoto. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			

ÍNDICE

CONTROL DE ACCESO (3/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Acceso 3G/4G	FortiExtender	Dispone de modem 3G/4G para control de acceso remoto en ubicaciones donde se requiere este tipo de acceso. La gestión se realiza a través del FortiGate.	FORTINET	Todos	Global			
Acceso seguro a red cableada	FortiSwitch	El control de acceso a la red a través de los puertos de los FortiSwitches se realiza a través del FortiGate, dotando de capacidades de firewall de nueva generación a todos los puertos de un switch. Disponibles también modelos ruggerizados del producto.	FORTINET	Todos	Global			
Acceso seguro a red inalámbrica	FortiAP	El control de acceso a la red inalámbrica se realiza a través del FortiGate, dotando de capacidades de firewall de nueva generación a todos los SSID radiados por un AP. Disponibles también modelos ruggerizados del producto.	FORTINET	Todos	Global			
Autenticación fuerte y servidor radius	Fortiauthenticator	Sistema de autenticación de doble factor. Control de admisión a la red. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			
KICS	Kaspersky Industrial Cybersecurity	Control de acceso que soporta un enfoque a modo White list y Black list, de forma granular con políticas por usuario, equipo, grupos de usuarios o grupo de equipos.	INYCOM	Todos	España	5	Technical training #KL 038.10	
INYCOM	INYCOM - Vigilancia de Accesos OT/IT	Solución de control de accesos a servicios en la red del entorno industrial.	INYCOM	Todos	Global	>20		
Block Chain	XAGE Remote Access	Solución para el control de acceso remoto dinámico.	LOGITEK	Todos	España	1		0
Medida de control de acceso de dispositivos removibles a áreas de sistemas de control industrial	FEE(P) USB Frontier	KIOSKO de sanitización de dispositivos móviles, portátiles y en general soportes de almacenamiento (USB, CD, DVD...). Dispone de workflow personalizable para implementar el control de "acceso a dispositivos móviles y portátiles" en sistemas digitales de proceso y adecuarse a los procesos internos de la organización. Permite el cumplimiento de normativas de referencia y guías de buenas prácticas como la NRC RG5.71 B.1.19, NEI08-09 (Rev 6), NIST AC-19, etc.	MINSAIT	Nuclear, Energía y Defensa	Global	10		3

CONTROL DE ACCESO (4/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
PKI y Firma Electrónica	Plataforma PKI & Firma electrónica	Amplia gama de productos y soluciones de PKI y firma electrónica que aportan flexibilidad para adaptarse a las necesidades de cada cliente, acompañándolo en todas las fases de integración incluyendo asesoría jurídica, la consultoría para la adecuación de procesos a la firma, los desarrollos de integración hasta finalmente el suministro de certificados y servicios de confianza. Contamos con más de 15 años de experiencia liderando proyectos de firma electrónica, tanto en el sector público como en el privado. La Suite propia incluye: - Motores de firma electrónica con certificado y de firma biométrica (firma manuscrita digitalizada) y solución BPM/Workflow (Portafirmas). - Solución BPM/Workflow de firmas (Portafirmas) con diseño responsive Web, compatibilidad con los navegadores Web más comunes y multidispositivo (desktop, movilidad). - Aplicaciones desktop standalone con interfaz gráfica para la generación y validación de firmas así como aplicaciones móviles nativas para iOS y Android que habilitan los procesos de firma con certificados o smartcard (p.ej. DNIe). - Asignación de niveles de confianza (LoA) a las sesiones establecidas, facilidad de uso del proceso de login, especialmente en movilidad, así como correlación de eventos entre autenticación y uso de las claves. - Servicios de confianza (sellado de tiempo, emisión de certificados o custodia centralizada de claves) desde nuestra plataforma de validación de certificados multi-PSC y de firmas. - Consultoría especializada, técnica y jurídica, en implantaciones de plataformas PKI y de firma electrónica.	MINSAIT	SSFF, Sanidad, Industria, Energía, AAPP	Todos	9		18
Identificación fehaciente de Identidad	Digital OnBoarding	La digitalización del cliente origina nuevos retos en la identificación siendo necesaria la gestión de la identidad durante todo el customer journey. Digital OnBoarding, proporciona una suite de identificación fehaciente del cliente que redefine una nueva experiencia de alta sencilla, segura y contextual, mediante una monitorización de seguridad del dispositivo y trazabilidad, ofreciendo seguridad y confianza, cumplimiento, experiencia de usuario y evolución natural hacia nuevos modelos de negocio.	MINSAIT	SSFF, TELCO, Industria y Energia	Todos	16	Cumplimiento regulatorio - Sepblac (España) - BCRA (Argentina) - CNBV (México)	5

ÍNDICE

CONTROL DE ACCESO (5/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Verificación de seguridad de dispositivos movile	Mobile Security	Los dispositivos móviles se están convirtiendo en los habilitadores clave del negocio en la era digital generando oportunidades en distintas industrias. Mobile Security es la solución de monitorización y control más completa del mercado. - Capacidades de actuación en el dispositivo local alineadas con riesgo de negocio. - Con la mayor adaptación a la inteligencia de negocio y sectorial - Integrada en la experiencia de usuario y aplicación (menor intrusión al usuario final).	MINSAIT	SSFF, TELCO, Industria y Energia	Todos	5	No aplica	1
	InXait	Base para extraer información, habitos, para extraer dataset y sanear un modulo de identificación adaptativa. Recoge patrones del comportamiento de usuario de cara a perfilar o a conocer al usuario en dispositivos móviles.	MINSAIT	Todos	Todos	9	No aplica	

ÍNDICE

CONTROL DE ACCESO (6/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Gestión completa de la identidad del usuario	IDEaaS	Es una suite que da la funcionalidad total de Identity Access Manager. Esta formado por los siguientes componentes que se pueden instalar de forma individual: - IDEaaS API Manager. Solución que analiza, gobierna, contea y protrege las APIs de exposición. - IDEaaS Access Manager (AM): gestor de SSO multi-tennat que puede ser instalada onPremise o ser consumida vía SaaS. Aporta soluciones de (IDP, SP, Proxy IDP, AS, ProxyOauth), dando solvencia a la seguridad interna de identidades y aplicaciones, pero aportando la flexibilidad de integración con Redes Sociales. Su versatilidad en MFA (Multi factor autent) y la disposición de utilizar de forma simultánea varios almacenes de datos simplica la integración. Cumple con los estándares requeridos por los mercados (xACML, JWT,...) y ampliando con nuevos cyphers para Tokens las características de JWS y JWE, siendo una solución óptima para securizaciones de apps móviles. - IDEaaS Identity Manager (IDM): gestor de automatización del ciclo de vida de las identidades y através de workflows y role maining. Amplía la seguridad del ciclo de vida de las identidades, eliminando vulnerabilidades de exceso de privilegios y de cuentas huérfanas. Compatible con varios estándares de conectores del mercado, tanto aplicaciones empresariales nativas como aplicaciones SCID. - IDEaaS IPT Broker: gestor de seguridad para protección de los protocolos de IOT (COaP, XMPP, MQTT). Protege y audita las conexiones mediante la integración con la solución de seguridad IDEaaS AM.	MINSAIT	Todos	Todos	9	No aplica	
Biometría	eGates	Solución para el control automatizado del paso de fronteras, que integra validación del documento de viaje, verificación biométrica facial y dactilar y consulta policial. Permite distintas topología o formatos de despliegue: quiosco (two-step segregated), puerta simple (one-step integrated) y esclusa (mantrap). Además, la solución incorpora los puestos de supervisión de la instalación de eGates, tanto en puesto fijo como en movilidad, y los puestos de verificación manuales.	MINSAIT	Todos	Todos	20		

ÍNDICE

CONTROL DE ACCESO (7/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Biometría	idVerification	idVerification es la solución de Minsait para la validación de documentos identificativos. Esta solución soporta distintos niveles de validación en función de las capacidades del terminal desde el que se realice, siendo las más básicas las realizadas con una simple cámara (por ejemplo un dispositivo móvil) y las más exhaustivas con un equipo que incluya un lector de documentos de 3 luces (visible, infrarrojo y ultravioleta). La solución puede adoptar el formato de un quiosco de visitas, la cual permite automatizar ese proceso y, además, comprobar mediante algoritmos biométricos que la persona que presenta el documento es efectivamente su propietario.	MINSAIT	Todos	Todos	20		
Biometría	iHawk	Solución para el control de acceso mediante reconocimiento facial en campo abierto, es decir, a distancia y con el individuo en movimiento. La solución permite definir distintas zonas del recinto, permisos, reglas, alarmas, etc.	MINSAIT	Todos	Todos	20		
Biometría	Sibed	Solución que permite gestionar el flujo completo de la emisión de documentos como DNIs, pasaportes, carnets de conducir, tarjetas de empleado, tarjetas de votante, etc. Dentro de la funcionalidad de Sibed se incluyen desde la propia personalización y emisión de los documentos hasta la gestión de stocks de los consumibles, que puede ser centralizada o distribuida, así como el pago de posibles tasas. Mediante la solución Sibed se garantiza el cumplimiento de los estándares necesarios para habilitar al ciudadano en el uso de sistemas automatizados de control de fronteras.	MINSAIT	Todos	Todos	20		
Autoridad de Registro	Castor	Gestiona el ciclo de vida de los certificados digitales, tanto en el momento de emisión como en el de revocación y permite el almacenamiento del certificado en un dispositivo criptográfico. Es sencillo incorporar nuevos recursos para que adquieran el conocimiento de la solución de forma ágil.	MINSAIT	Todos	Todos	4		

ÍNDICE

CONTROL DE ACCESO (8/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
NGFW VPN	NGFW con Global Protect	Mediante la solución Sibed se garantiza el cumplimiento de los estándares necesarios para habilitar al ciudadano en el uso de sistemas automatizados de control de fronteras.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
NGFW VPN	NGFW con Global Protect	Concentrador VPN sede a sede y para accesos remotos.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
NGFW IPS	NGFW Threat Prevention	Sistema de seguridad en redes scada, soportando protocolos industriales (dnP3, ICCP, Modbus/ tCP,...) y cumplimiento de regulaciones NERC CIP, ISA 62443. Capacidad de caracterizar tráfico y aplicaciones industriales propietarias. Tecnologías IPS, antispyware y antvirus en red.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
Seguridad SaaS	Aperture	Es un producto de seguridad SaaS (Software as a Service). Protege las aplicaciones basadas en cloud escaneando ficheros y permisos para la exposición externa e información sensible. Focalizado en DLP (Data Loss Prevention) para PII (Personally Identifying Information) y PCI (Payment Card Industry) entre otros. Protege estas aplicaciones SaaS: Box, Salesforce, Dropbox, Google Drive, Office 365, etc.	PALO ALTO NETWORKS	Todos	Global	>100	SOC2 Type II	

ÍNDICE

CONTROL DE ACCESO (9/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Servicio Cloud Publica NGFW y VPN	GlobalProtect Cloud Service	GlobalProtect Cloud Service operacionaliza el despliegue aprovechándose de una infraestructura basada en cloud operada por Palo Alto Networks. Basada en nuestra plataforma de seguridad de nueva generación, GlobalProtect Cloud Service se gestiona con Panorama, permitiendo crear y desplegar políticas de seguridad consecuentes a través de toda la organización. GlobalProtect Cloud Service sigue un modelo de propiedad compartida que permite mover los gastos de seguridad de tu sede remota y usuarios móviles a un modelo más eficiente y predictible badaso en OPEX.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK, SOC2 Type II	
Next-Generation Security para Clouds Públicas y Privadas	VM-Series	Las VM-Series son un formato virtualizado de nuestro next-generation firewall que puede ser desplegado en un amplio rango de entornos tanto de nube pública como privada. Tanto en entornos de nube pública como privada, las VM-Series se pueden desplegar como firewall perimetral, terminador de VPN IPsec y firewall de segmentación, protegiendo tu negocio con políticas de reconocimiento de aplicaciones y prevención de amenazas.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
VPN	mGuard Secure VPN Client	Cliente de software VPN para la conexión de PC con Windows a una red privada virtual (VPN). Para ordenadores, portátiles o tablets con Windows 10, Windows 8.x o Windows 7 Compatible con todo el sistema mGuard Compatible con los routers de radiotelefonía móvil de Phoenix Contact Máxima seguridad con el protocolo IPsec en la capa 3 De acuerdo con certificados actuales como x509.v3 Transmisión segura de datos con encriptación AES 128/192/256 bits Autenticación ampliada frente a switches y puntos de acceso según IEEE 802.1x.	PHOENIX CONTACT	Todos	Global	12		
VPN	mGuard Remote Serive	Comunicación VPN IPsec muy segura Autenticación de 2 factores Gestión de usuarios y derechos para el acceso seguro a distintos clientes e instalaciones Alta disponibilidad industrial en todo el mundo Tecnología de seguridad mGuard probada en la industria.	PHOENIX CONTACT	Todos	Global	12		

ÍNDICE

CONTROL DE ACCESO (10/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
VPN	mGuard Secure Cloud	Infraestructura VPN escalable y sencilla de altas prestaciones, la cual, permite conectar técnicos de soporte o personal de servicio con máquinas y sistemas a través de Internet.	PHOENIX CONTACT	Todos	Global	12		
VPN	mGuard Centerport	Concentrador VPN Sede a Sede y de acceso remoto. En formato rack de 19" con capacidad de hasta 3000 túneles VPN más de 600 MBit/s de tasa de transferencia de datos VPN, NAT, cortafuegos, ampliación de funciones con licencias.	PHOENIX CONTACT	Todos	Global	12		
VPN	mGuard RS4000-P	Concentrador VPN Sede a Sede y de acceso remoto, en formato carril DIN con capacidad de hasta 250 túneles VPN. Incluidas funciones de router NAT con firewall avanzado, posibilidad de redundancia de routing y VPNs, Deep Packet Inspection de protocolos como Modbus TCP y OPC DA, CIFS Integrity Monitoring, y más funciones especiales de ciberseguridad en industria.	PHOENIX CONTACT	Todos	Global	12		
VPN	TC CLOUD CLIENT	Router y pasarelas industriales VPN con tecnología Ipsec para conexión directa, sencilla y segura con la plataforma mGuard Secure Cloud.	PHOENIX CONTACT	Todos	Global	12		
VPN	PLCnext	Conectividad VPN como cliente OpenVPN o Ipsec en los sistemas PLCnext Control diseñados conforme a norma IEC62443 con firewall incorporado, servidor OPC UA y capacidad de implementación directa y determinista de programación en lenguajes de alto nivel C#, C++ o Matlab Simulink.También posible con JAVA o Python.	PHOENIX CONTACT	Todos	Global	12		
Control de acceso a la red	Sistemas de control de acceso a la red	Permite al administrador configurar políticas de acceso contextuales en el NAC para controlar el acceso a la nube y al centro de datos en función de dispositivos, localizaciones, recursos, usuarios y grupos, o incluso perfilado de endpoint.	SARENET	Todos	España	>10		
Control de acceso a aplicaciones	SIMATIC LOGON	Control de acceso para estaciones de operador e ingeniería.	SIEMENS	Todos	Global	5		20
Autenticación, control de acceso y protección de sistemas	CROSSBOW	Solución de autenticación, control de acceso y protección de sistemas.	SIEMENS	Energía	Global	20		5

ÍNDICE

CONTROL DE ACCESO (11/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
NAC	ROS (RS 900 RSG2488...)	Solución para control de acceso en la red.	SIEMENS	Infraestructuras y energía		>100		>100
NGFW & 0-Day IPS	STORMSHIELD Network Security	SNS es una solución completa para proteger las redes TI y OT. Analiza los protocolos industriales (DNP3, Modbus, S7) así como los de TI. Gracias a nuestra herramienta de supervisión, dispondrá de una lista completa de los dispositivos activos en la red en tiempo real. Esta visibilidad global de la red proporciona una valiosa ayuda para la gestión del inventario de dispositivos que generan tráfico en la red. Con los equipos Stormshield Network Security, se puede gestionar desde una misma consola de administración un único software con independencia de que el equipo se encuentre en una red OT o TI. Este software se despliega en distintos appliances Hardware con características aptas para entornos TI o bien OT reforzando la protección de los PLCs.	STORMSHIELD	Todos	Global	>250	Common Criteria EAL4+ v3, EU Restricted, NATO Restricted	>1000
Control de dispositivos, control Wifi/3G	STORMSHIELD Endpoint Security Full Control	La solución de seguridad que permite un control granular sobre cualquier acción autorizada o bloqueada en estaciones de trabajo y servidores. Permite monitorizar los diferentes comportamientos de un puesto de trabajo y definir aquellos que se consideran legítimos o que deban ser bloqueados. Es una solución esencial para ayudar a combatir fugas o pérdidas de datos sensibles, bloqueando el uso malicioso de las aplicaciones corporativas autorizadas por la empresa. La supervisión del puesto de trabajo incluye las comunicaciones con el exterior (Wi-Fi, Bluetooth, Modems 3G, etc.), periféricos externos (USB media, USB imaging, escritura en CD/DVD/BluRay, etc.) y el cumplimiento de las políticas corporativas (últimos parches del sistema operativo, procesos y servicios en ejecución, etc.).	STORMSHIELD	Todos	Global	>250	Common Criteria EAL en progreso	>100

ÍNDICE

CONTROL DE ACCESO (12/12)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
FIREWALL	TXONE EDGE FIRE	Firewall para entornos industriales.	TREND MICRO	Industrial	Global		CE UL UL 60950-1 RoHS RoHS2 CRoHS WEEE EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A	
IPS	TXONE EDGE IPS	IPS para entornos industriales, gestionando tráfico Este/Oeste.	TREND MICRO	Industrial	Global		CE UL UL 60950-1 RoHS RoHS2 CRoHS WEEE EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A	
IPS	TippingPoint TPS	Prevención de intrusos a nivel de red incorporando tecnología de parcheado virtual. Gestionando tráfico norte/sur	TREND MICRO	Industrial/IT	Global		UL 60950-1 IEC 60950-1EN 60950-1 CSA 22.2 60950-1RoHS Clase A, FCC, VCCI, KC EN55022 CISPR 22 EN55024 CISPR 24 EN61000-3-2 EN61000-3-3 marcado CE	

ÍNDICE

CUMPLIMIENTO (1/3)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Control de Dispositivos USB	SafeDoor	Acceso Seguro al Contenido de los Dispositivos de almacenamiento USB: - Evita los tres niveles de ataque que por este medio se pueden producir. (HW., Eléctrico y Malware.) - Monitorización y Gestión Dispositivos USB a través Consola Central. - Evita fugas de información a través dispositivos USB. - Auditoria y trazabilidad de Dispositivos, Contenido y Usuarios. - Soporta unidades USB con cifrado Hardware y Software Adecuación y Cumplimiento ENS. Adecuacion y Cumplimiento con LOPD.	authUSB	Infraestructuras críticas Defensa Industria	Global	Nacional / Internacional	Certificación LINCE ENS Nivel Alto	
Clasificación de Información	Boldon James	Gestión y Aplicación de las políticas de Seguridad de la Información en la empresa.	CALS	Todos	Global	25	N/A	80
Gestión Integral de Riesgos	STREAM	Gestión de Riesgos en materia de Ciberseguridad en tiempo real orientada al negocio.	CALS	Todos	Global	20	N/A	25
Gestión de Auditoría Basada en Riesgos	Visión	Gestión de Riesgos para departamentos de auditoría, Gestión de Riesgos y Cumplimiento Normativo.	CALS	Todos	Global	35	N/A	35
Compliance	Blade Compliance	Permite asegurar el cumplimiento de normativas gubernamentales y especificas del sector.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	70
Operaciones de seguridad	W6 Security Management	Solución que permite la gestión de las actividades de cumplimiento de la seguridad realizadas en la red OT. Permite la gestión del ciclo de vida de incidentes de seguridad y vulnerabilidades, la gestión de activos de información de los sistemas digitales y sus controles. Cuenta con una potente funcionalidad de BI con indicadores de cumplimiento frente a una norma, indicadores de incidentes y trabajos relacionados con la gestión de vulnerabilidades. Dispone de integración con sistemas SIEM.	CIC Consulting Informatico	Nuclear, Utilities, Aguas	España	3		2
Cuadro de Mando	W6 Integrated Security Dashboard (W6 ISD)	Solución de gobierno de la seguridad que permite integrar en una sola herramienta la información de alertas e incidencias provenientes de los diferentes sistemas de seguridad de la organización: SIEM, gestión de tickets, endpoints, seguridad perimetral.	CIC Consulting Informatico	Nuclear	España	3		2

ÍNDICE

CUMPLIMIENTO (2/3)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Medida de control de acceso de dispositivos removibles a áreas de sistemas de control industrial	FEE(P) USB Frontier	KloSKo de sanitización de dispositivos móviles, portátiles y en general soportes de almacena- miento (USb, Cd, dvd...). Dispone de workflow personalizable para implementar el control de "acceso a dispositivos móviles y portátiles" en sistemas digitales de proceso y adecuarse a los procesos internos de la organización. Permite el cumplimiento de normativas de referencia y guías de buenas prácticas como la nRC Rg5.71 b.1.19, nEI08-09 (Rev 6), nISt AC-19,...etc.	MINSAIT	Nuclear, Energía y Defensa	Global	10		3
Seguridad SaaS	Aperture	Es un producto de seguridad SaaS (Software as a Service). Protege las aplicaciones basadas en cloud escaneando ficheros y permisos para la exposición externa e información sensible. Focalizado en DLP (Data Loss Prevention) para PII (Personally Identifying Information) y PCI (Payment Card Industry) entre otros. Protege estas aplicaciones SaaS: Box, Salesforce, Dropbox, Google Drive, Office 365, etc.	PALO ALTO NETWORKS	Todos	Global	>100	SOC2 Type II	>100
Servicio Cloud Para Almacenamiento de logs	Logging Service	Palo Alto Networks Logging® Service es una oferta basada en cloud para logs de red de contenido rico mejorado por nuestra oferta de seguridad, incluyendo aquellos de nuestros Next-Generation Firewalls y GlobalProtect™ Cloud Service. La naturaleza de Logging Service basada en cloud permite a los clientes recoger tasas de logs siempre crecientes, sin necesidad de un plan de almacenamiento y capacidad de cómputo local.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	
Auditorías de seguridad	Sistemas de auditoría continuos basados en tecnología Nozomi	Seguimiento de normativas y compliances de fabricantes. (RGPD, PCI...). Supervisión continua de todos los elementos activos relacionados con la Ciberseguridad mediante sondas y agentes interrogando a los activos (equipos, routers, impresoras, etc.). La información se recolecta para después ser visualizada en una herramienta web.	SARENET	Todos	España	>10		

ÍNDICE

CUMPLIMIENTO (3/3)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Gestión Integral del Riesgo, Gobierno y Cumplimiento	Sandas GRC	Herramienta de Gestión Integrada del Riesgo, Gobierno y Cumplimiento para entornos tanto de Tecnologías de Información (IT) como de Tecnologías de Operación (OT) y el Internet de las Cosas (IoT). Integra la capa de cumplimiento multinorma en estos entornos junto con la capa operativa de seguridad proporcionando inteligencia directa y accionable. Gestiona de forma unificada y eficiente los requisitos legales, de seguridad y riesgos de su organización: Infraestructuras críticas o estándares internacionales como ISO 27001, ISO 27002, ISO 22301, RGPD, NIST SP 800-30, ISA/IEC 62443, Guías de Seguridad de la GSMA, entre otras. Permite la creación de cuadros de mando personalizados incluyendo información de la capa operativa de seguridad.	TELEFÓNICA - GOVERTIS	Todos	Global	>100		>100

MONITORIZACIÓN DE RED (1/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Monitorización en tiempo real	Smart view monitor	Supervisión centralizada que permite a los administradores identificar inmediatamente cualquier cambio en la red, en los patrones de tráfico, en las pasarelas, túneles, usuarios remotos y descubrir actividad maliciosa. Monitorización en linea o fuera línea.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	100
Monitoriza log	Smart view log	Solución de monitorización de Log.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	150
SIEM	Smart view event	Solución SIEM.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	110
Análisis de protocolo y detección en tiempo real	W6 ViewSCADA	Solución para la monitorización y detección y alerta de anomalías de protocolo industrial (IEC-101, IEC-104). Permite además la recolección a largo plazo, análisis y visualización del tráfico entre el SCADA y sus RTU.	CIC Consulting Informatico	Utilities	España	2		1
NOC y SOC	FortiSIEM	Capacidades NOC + SOC. Gracias a su CMDB permite realizar la gestión del inventario activos, detectar cambios de configuraciones de cualquier elemento de red, monitorización de sistemas, así como monitorizar el rendimiento y disponibilidad de los mismos. Correlación de eventos de seguridad de todos los elementos conectados a la red. Monitorización de procesos críticos de negocio. También se integra con FortiGuard Labs para compartir Indicadores de compromiso (IOC) y detectar cualquier actividad sospechosa en la red.	FORTINET	Todos	Global			
Plataforma Virtual (Appliance o cloud)	Vigilant ICS Cybersecurity	Monitor único de todos los riesgos de la planta. Monitoriza y controla riesgos como: Actualizaciones de sistemas operativos de los sistemas SCADA, Actualización de protección malware, copias de seguridad de los sistemas SCADA, gestión de eventos en la electrónica de comunicaciones en la red SCADA.	INYCOM	Todos	España			

MONITORIZACIÓN DE RED (2/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Plataforma Virtual (Appliance o cloud)	Vigilant SCADA Cybersecurity	Monitor único de todos los riesgos de la planta. Monitoriza y controla riesgos como: Actualizaciones de sistemas operativos de los sistemas SCADA, actualización de protección malware, copias de seguridad de los sistemas SCADA, gestión de eventos en la electrónica de comunicaciones en la red SCADA.	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	
Plataforma Virtual (Appliance o cloud)	IIoT Risk Manager - Vigilancia Completa	Proyectos Industrial Internet of Things, Monitor único de riesgos entre las comunicaciones de la sensorística y la plataforma de analítica de datos. Monitor único de servicios de copias de seguridad, redes y equipos finales.	INYCOM	Todos	Global	>10	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	

ÍNDICE

MONITORIZACIÓN DE RED (3/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Monitorización de red	Kaspersky Industrial CyberSecurity for Network	Sistema IDS no intrusivo con DPI de protocolos de comunicación industrial (modbus, conjunto IEC, ISO, S7Comm, GOOSE, MMS, etc…). Dispone de una arquitectura modular donde los sensores pueden implementarse de manera independiente a partir de una unidad de control central. Posee aprendizaje mecánico, detecta anomalías dentro de los procesos industriales. Permite la identificación de todos los activos de red conectados vía Ethernet (SCADA, HMI, estaciones de Ingeniería, PLC y RTU) creando un inventario. Herramientas forenses para el análisis de datos y también impide la realización de cambios en los registros de ICS.	KASPERSKY	Industria, Infraestructuras críticas	Global			
SNMP Monitor	Industrial HiVision	Solución para la gestión y monitorización del estado de dispositivos de electrónica de red y otros dispositivos SNMP (PLC, PC, Servers, etc.).	LOGITEK	Todos	Global	2	Certified partner for Industrial HiVision	15
Traffic Monitor	Detector anomalías de red	Solución de inventariado y análisis del tráfico en movimiento de la red para la detección de anomalías, intrusiones, malware y comportamiento anómalo de los dispositivos.	LOGITEK	Cualquiera	España	2		8
Gestión integral (Monitorización, control local y remoto)	Managed Services for Enterprise Networks	MSEN es un servicio proactivo de gestión operacional de infraestructuras TI flexible, cost-effective y en tiempo real, alineado con ITIL y siguiendo procesos consistentes a nivel global. Servicios con soluciones de portal dedicado, monitorización proactiva, gestión de configuraciones, eventos, disponibilidad, capacidad, etc. con el objetivo de ofrecer una respuesta más rápida y de resolución de incidentes.	NTT	Todos	Global			
Claroty	Oylo Senses	Monitorización de detección de anomalías, gestión de vulnerabilidades en sistemas de control industrial aplicando DPI.	OYLO	Industrial	España y Chile	14	8	
Gestión centralizada de NGFW	Panorama	Sistema de gestión centralizada, que permite monitorizar y administrar todos los NGFW de la red de un cliente, y desplegar políticas en los mismos.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100

ÍNDICE

MONITORIZACIÓN DE RED (4/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Big Data	Autofocus	Big Data que recopila y correla toda la información de amenazas e indicadores de compromiso (IoC) recogidos por todos los clientes de Wildfire de Palo Alto Networks, feeds de terceros (Cyberthreatalliance.org) e investigaciones propias (Unit42), con el fin de dotar a los administradores de seguridad de una potente herramienta de investigación ante amenazas.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
Análisis de comportamiento con capacidad de respuesta activa en red	LigthCyber Behavioral Analytics	LightCyber™ Behavioral Analytics permite a las empresas detener atacantes activos y malware que opera en la red. LightCyber aprende el comportamiento esperado de los usuarios y dispositivos y detecta la actividad anómala de un ataque. Su modelo centrado en la red detecta ataques durante cada fase del ciclo de vida del ataque, asegurando la detección y eliminación de cada fase.	PALO ALTO NETWORKS	Todos	Global	>100		>100
Servicio Cloud para almacenamiento de logs	Logging Service	Palo Alto Networks Logging® Service es una oferta basada en cloud para logs de red de contenido rico mejorado por nuestra oferta de seguridad, incluyendo aquellos de nuestros Next-Generation Firewalls y GlobalProtect™ Cloud Service. La naturaleza de Logging Service basada en cloud permite a los clientes recoger tasas de logs siempre crecientes, sin necesidad de un plan de almacenamiento y capacidad de cómputo local.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	
Software para gestión de redes industriales	FL NETWORK MANAGER	Software para actualizción del firmware de varios equipos de manera sencilla y rápida. Planificación de direcciones IP para un cómodo desarrollo de las direcciones IP a través de DCP, BOOTP, DHCP. Vista de conjunto de todos los componentes de red gracias al escaneo de red, incluso con direcciones IP desconocidas. Servidor TFTP, DHCP/BOOTP integrado. Configuración sencilla de muchos componentes de infraestructura con la configuración multidispositivo. Comunicación segura con los componentes de red a través de SNMPv3. Configuración de los equipos con capacidad SNMP deseados gracias al SNMP Scripting.	PHOENIX CONTACT	Todos	Global	12		

ÍNDICE

MONITORIZACIÓN DE RED (5/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Software para gestión de redes industriales	FL SNMP OPC server	Los servidores FL SNMP OPC recopilan información de dispositivos y de la red que pueden leerse mediante SNMP. De este modo, podrá integrar sus dispositivos basados en SNMP en sistemas de control de procesos basados en OPC (SCADA) o en sistemas de interfaz hombre-máquina (HMI).	PHOENIX CONTACT	Todos	Global	8		
Análisis de red y detección en tiempo real	Darktrace Industrial Immune System for ICS.	El sistema inmune de Darktrace visualiza y analiza los datos de una red en tiempo real y establece una base evolutiva de lo que "es normal". Matemática Bayesiana avanzada y el aprendizaje máquina de última generación detectan anomalías y alertan para su posterior investigación, siendo capaz de descubrir los ataques que surjan aunque previamente sean desconocidos. La prevención total de todas las amenazas "ciber" no es realista, pero si es la alerta temprana de las amenazas para que estas puedan ser mitigadas antes que se conviertan en una auténtica crisis. Darktrace utiliza algoritmos avanzados de aprendizaje. Nos nutrimos de más de 300 fuentes de información, y realizamos modelización de cada dispositivo, usuario y de la red en general. La interface de usuario ofrece una herramienta sencilla e intuitiva para investigar que no requiere un experto en ciberseguridad, ni formación, solo un conocimiento de su red y el apoyo de nuestros expertos analistas.	ROOM33 COM S.A.	Todos	Global	N/A	GovCERT	>250
Ventana de cliente	Ventana de cliente	Supervisión de la red monitorizando protocolos, aplicaciones y usuarios que generan el tráfico en la WAN	SARENET	Todos	España	>20	N/A	1.000
Monitorización de vulnerabilidades en red IT/IoT	Auditorías evolutivas de seguridad	Monitorizacion del tráfico de red Cloud/IT/OT/IIoT para detectar amenazas o comportamientos anómalos. Supervisión continua de todos los elementos activos IP relacionados con la Ciberseguridad mediante sondas y agentes, interrogando a los activos (routers, switches, PLCs, HMIs, SCADA, impresoras, lectores código de barra, IoT, etc.). La información se recolecta para después ser visualizada en una plataforma centralizada (web).	SARENET	Todos	España	>10	N/A	
Centro de operaciones de red (NOC)	Centro de operaciones de red (NOC)	Servicio de atención de las alertas y actuaciones sobre esos servicios de red. Con este Servicio Integral de Seguridad Gestionada una PYME puede externalizar todo lo relativo a servicios de red de área extensa sin tener que contar con técnicos especializados en su plantilla.	SARENET	Todos	España	>10	N/A	

ÍNDICE

MONITORIZACIÓN DE RED (6/6)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Monitorización en tiempo real	SINEMA SERVER	Monitorización del estado de las redes en tiempo real.	SIEMENS	Todos	Global	30		20
Monitorización en tiempo real	SIMATIC NET	Monitorización OPC.	SIEMENS	Todos	Global	50		>100
Monitorización y ayuda puesta en marcha	PRONETA	Software de monitorización, puesta en marcha y comprobación de cableado.	SIEMENS	Todos	Global	50		50
NGFW & 0-Day IPS	STORMSHIELD Network Security	SNS es una solución completa para proteger las redes TI y OT. Analiza los protocolos industriales (DNP3, Modbus, S7) así como los de TI. Gracias a nuestra herramienta de supervisión, dispondrá de una lista completa de los dispositivos activos en la red en tiempo real. Esta visibilidad global de la red proporciona una valiosa ayuda para la gestión del inventario de dispositivos que generan tráfico en la red. Con los equipos Stormshield Network Security, se puede gestionar desde una misma consola de administración un único software con independencia de que el equipo se encuentre en una red OT o TI. Este software se despliega en distintos appliances Hardware con características aptas para entornos TI o bien OT reforzando la protección de los PLCs.	STORMSHIELD	Todos	Global	>250	Common Criteria EAL4+ v3, EU Restricted, NATO Restricted	>1000
Sonda	Cybels Sensor	Sonda de confianza para la detección de ciberataques y la protección de infraestructuras críticas y redes de información sensible.	THALES	Infraestructuras Críticas y redes sensibles	Global			
Monitorización y protección avanzada de red	Deep Discovery	Solución formada por dos componentes. Deep Discovery Inspector que proporciona inspección del tráfico de red, detección avanzada de amenazas y análisis en tiempo real con presentación de informes. Deep Discovery Advisor opcional que proporciona análisis Sandbox abierto, escalable, y personalizable para la detección de ataques dirigidos y APTs.	TREND MICRO	Todos	Global		Common Criteria	7
Sonda de Red	Deep Discovery Inspector	Sonda de red para análisis de copia de tráfico siendo capaz de analizar más de 100 protocolos incluyendo MODBUS.	TREND MICRO	Industrial IT	Global			

ÍNDICE

MONITORIZACIÓN DE SISTEMAS (1/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Seguridad de aplicaciones web	FortiWeb	Firewall de aplicaciones web. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			
Seguridad para el correo electrónico	FortiMail	El correo electrónico es el principal vector de ataque. También en entornos industriales se han dado casos de utilización de este vector de ataque, por lo que sigue siendo muy importante implementar dispositivos específicos como FortiMail para proteger eficazmente los sistemas de control de una organización. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			
NOC y SOC	FortiSIEM	Capacidades NOC + SOC. Gracias a su CMDB permite realizar la gestión del inventario activos, detectar cambios de configuraciones de cualquier elemento de red, monitorización de sistemas, así como monitorizar el rendimiento y disponibilidad de los mismos. Correlación de eventos de seguridad de todos los elementos conectados a la red. Monitorización de procesos críticos de negocio. También se integra con FortiGuard Labs para compartir Indicadores de compromiso (IOC) y detectar cualquier actividad sospechosa en la red.	FORTINET	Todos	Global			
Plataforma Virtual (Appliance)	Vigilant ICS Cybersecurity	Monitor único de todos los riesgos de la planta. Monitoriza y controla riesgos como: Actualizaciones de sistemas operativos de los sistemas SCADA, actualización de protección malware, copias de seguridad de los sistemas SCADA, gestión de eventos en la electrónica de comunicaciones en la red SCADA.	INYCOM	Todos	Global	> 20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	

MONITORIZACIÓN DE SISTEMAS (2/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Plataforma Virtual (Appliance o cloud)	IIoT Risk Manager - Vigilancia Completa	Monitor único de riesgos entre las comunicaciones de la sensorística y la plataforma de analítica de datos. Monitor único de servicios de copias de seguridad, redes y equipos finales.	INYCOM	Todos	Global	>10	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	
Monitorización de Endpoint en tiempo real	FEE(P) Digital Defense	Solución que combina capacidades antimalware con ciberinteligencia. El objetivo es dotar de seguridad sin causar un impacto a la operación del negocio. Transparencia para el usuario y simplicidad para el administrador son las características más relevantes. Como factor diferencial, FEE(P) Digital Defense permite mediante un motor de inteligencia identificar equipos comprometidos y equipos desde los que se realizan operaciones sospechosas.	MINSAIT	Todos	Global	10		15
Integrity checking	VITAL Integrity	Identificación/restauración de intentos de cambios no autorizados en sistemas de ficheros y procesos.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	12	CCSA, CCSE, CCNP, FCNSA, FCNSE, MCD, MCA, CEH, CREA, GCHI, ENCE, ACE	13

ÍNDICE

MONITORIZACIÓN DE SISTEMAS (3/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Monitorización y parcheo en tiempo real de sistemas de seguridad	MGUARD DEVICE MANAGER UNLIMITED	Software de gestión de equipos central para FL MGUARD para tantos equipos como se deseen en el campo. Para instalar en un PC. No son necesarias más licencias.	PHOENIX CONTACT	Todos	Global	4		
Monitorización de vulnerabilidades en la red IT/IoT	Auditorías evolutivas de seguridad	Monitorizacion del tráfico de red Cloud/IT/OT/IIoT para detectar amenazas o comportamientos anómalos. Supervisión continua de todos los elementos activos IP relacionados con la Ciberseguridad mediante sondas y agentes, interrogando a los activos (routers, switches, PLCs, HMIs, SCADA, impresoras, lectores código de barra, IoT, etc.). La información se recolecta para después ser visualizada en una plataforma centralizada (web).	SARENET	Todos	España	>10	N/A	
Centro de operaciones de red (NOC)	Centro de operaciones de red (NOC)	Servicio de atención de las alertas y actuaciones sobre esos servicios de red. Con este Servicio Integral de Seguridad Gestionada una PYME puede externalizar todo lo relativo a servicios de red de área extensa sin tener que contar con técnicos especializados en su plantilla.	SARENET	Todos	España	>10	N/A	
Monitorización en tiempo real de red y seguridad en tiempo real	SINEMA SERVER	Monitorización del estado de las redes en tiempo real.	SIEMENS	Todos	Global	30		20
Monitorización en tiempo real de red	SIMATIC NET	Monitorización OPC.	SIEMENS	Todos	Global	50		>100
Monitorización y ayuda puesta en marcha	PRONETA	Software de monitorización, puesta en marcha y comprobación de cableado.	SIEMENS	Todos	Global	50		50
Protección y monitorización de sistemas	RUGGED APE	Solución de Protección y monitorización de sistemas.	SIEMENS	Todos	Global	>50		5

ÍNDICE

MONITORIZACIÓN DE SISTEMAS (4/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
AntiAPT, AntiMalware	STORMSHIELD Endpoint Security Full Protect	La solución de seguridad que bloquea ataques avanzado y no conocidos que pasan desapercibidos para los sistemas convencionales de seguridad. Stormshield Endpoint Security Full Protect es la culminación de años de Investigación y Desarrollo que permite reconocer e identificar ataques avanzados desconocidos sin necesidad de actualización de firmas de detección o del propio producto. Por este motivo se trata de una solución especialmente eficiente para entornos offline y redes sin conectividad internet. Esta tecnología se utiliza mundialmente en un gran número de clientes que requieren este tipo de detección avanzada: seguridad industrial, Defensa y entornos críticos y en general cualquier empresa pequeña o grande que necesite protegerse eficazmente contra estas amenazas.	STORMSHIELD	Todos	Global	>250	Common Criteria EAL en progreso	>100

MONITORIZACIÓN DE SISTEMAS (5/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Log Inspection (Correlador de logs S.O) **Monitorización de integridad de ficheros críticos de S.O**	Deep Security	El modulo de Log Inspection, realiza el envío de logs de S.O a consola central de Deep Security.	TREND MICRO	Industrial IT	Global		Partner tecnológico avanzado de Amazon Certificación Red Hat Ready Validación para Cisco UCS Common Criteria EAL 2+ Validación para EMC VSPEX Partner empresarial de HP Programa de protección de aplicaciones de Microsoft Partner certificado de Microsoft Validación para NetApp FlexPod Partner de Oracle PCI Suitability Testing para HIPS (NSS Labs) Certificación SAP (NW-VSI 2.0 y HANA) Validación para VCE Vblock Virtualización por VMware Validación para FIPS 140-2 VMware Cloud en AWS	

ÍNDICE

PROTECCIÓN DE RED (1/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Cifrado de red	Trustway IP Protect	Implementación de la suite de protocolos IPSec Hasta 10 Gbits / s (clúster) Hardware criptográfico Infraestructura de gestión para productos criptográficos nivel Confidencial sector Defensa.	ATOS	Todos	Global	>50	Common Criteria EAL4+, Reinforced Qualification (ANSSI QR), NATO SECRET and EU RESTRICTED	>100
Firewall L2 y L3	Blade Fw, IPS.	Control básico de acceso.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	300
Control de identidad	Industrial/Ruggedized Gateways.	Control del acceso a las aplicaciones en base a la terna usuario/equipo/ip.	CHECK POINT	Todos	Global	10	NSS labs en IPS, NGFW, Miercom, Common Criteria	90
Protección en tiempo real de amenazas a sistemas industriales	FortiGate	Firewall de nueva generación con Antimalware, AntiAPT, Sistema de Prevención de ataques (incluidos ataques a aplicaciones industriales), inspección y protección de aplicaciones (incluidas aplicaciones industriales). Se puede utilizar como sistema de virtual patching para protección de sistemas. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global		NSS Labs, Common Criteria, VB100, ICSA Labs, Department of Defense UC APL, Pv6 Ready Phase 2, CVE-Compatible, FIPS 140-2	
Firewall L3 y L4	FortiGate	Firewall en nivel de control y supervisión. Disponible en formato appliance físico o máquina virtual para distintos hipervisores,	FORTINET	Todos	Global		NSS Labs, Common Criteria, VB100, ICSA Labs, Department of Defense UC APL, Pv6 Ready Phase 2, CVE-Compatible, FIPS 140-2	

ÍNDICE

PROTECCIÓN DE RED (2/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Plataforma Virtual o Servidor Físico (Appliance)	Vigilant ICS Cybersecurity	Vigilante único que protege los riesgos de la red de planta. Monitoriza y controla riesgos que incluyen: Actualizaciones de sistemas operativos de los sistemas SCADA, Actualización de protección malware, copias de seguridad de los sistemas SCADA, gestión de eventos y administración remota para la electrónica de comunicaciones en la red SCADA.	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT, CCNA, CCNP, CSSS Cisco VPN/Security Sales Expert, Smart Business Communication System for Account Managers 650_173 - ENU	
KICS	PROTECCIÓN INDUSTRIAL	Servicios expertos para la protección completa en todas las fases de comunicaciones OT.	INYCOM	Todos	España	>2		
Firewall DPI	Tofino Xenon (Hirschmann)	Dispositivos firewall industrial DPI (Deep Packet Inspection) sobre protocolos industriales (Modbus, Ethernet/IP, OPC).	LOGITEK	Todos	Global	4	Certified Partner for Tofino Xenon	9
Firewall DPI	EdgeIPS	Dispositivos firewall con dpi para varios protocolos industriales con análisis, detección y prevención de explotación de vulnerabilidades.	LOGITEK	Todos	España	2		
Diodo de Datos	Data Diode (FOX IT)	El diodo de datos es un dispositivo puramente hardware (no existe firmware como el caso de los firewalls) que separa/protege dos redes asegurando la unidireccionalidad en el flujo de información. Es decir, asegura que la información de una red llegue a la otra red (pero no viceversa).	LOGITEK	Todos	Global	2	Certified Partner for FOX IT Data Diode	2

ÍNDICE

PROTECCIÓN DE RED (3/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Limitaciones de contenido	VITAL Inspect	Inspección/Notificación anomalías contenido de tráfico en sistemas de control industrial.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	12	CCSA, CCSE, CCNP, FCNSA, FCNSE, MCD, MCA, CEH, CREA, GCHI, ENCE, ACE	8
Firmado de Tráfico	VITAL Traffic	Sistema de firmado continuo de tráfico para análisis y validación forense.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	12	CCSA, CCSE, CCNP, FCNSA, FCNSE, MCD, MCA, CEH, CREA, GCHI, ENCE, ACE	13
Big Data	Autofocus	Big Data que recopila y correla toda la información de amenazas e indicadores de compromiso (IoC) recogidos por todos los clientes de Wildfire de Palo Alto Networks, feeds de terceros (Cyberthreatalliance.org) e investigaciones propias (Unit42), con el fin de dotar a los administradores de seguridad de una potente herramienta de investigación ante amenazas.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
NGFW IPS	NGFW Threat Prevention	Sistema de seguridad en redes scada, soportando protocolos industriales (dnP3, ICCP, Modbus/ tCP,...) y cumplimiento de regulaciones NERC CIP, ISA 62443. Capacidad de caracterizar tráfico y aplicaciones industriales propietarias. Tecnologías IPS, anti-spyware y antivirus en red.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100

ÍNDICE

PROTECCIÓN DE RED (4/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Monitorización y prevención en tiempo real frente a amenazas industriales	Next-Generation Firewal	Sistema de seguridad en redes scada, soportando protocolos industriales (dnP3, ICCP, Modbus/ tCP,...) y cumplimiento de regulaciones NERC CIP, ISA 62443. Capacidad de caracterizar tráfico y aplicaciones industriales propietarias. Establecimiento de reglas de sanidad y capacidad de reconocimiento de amenazas conocidas y desconocidas (vulnerabilidades de día 0 y APts).	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
Servicio Cloud Publica NGFW y VPN	GlobalProtect Cloud Service	GlobalProtect Cloud Service operacionaliza el despliegue aprovechándose de una infraestructura basada en cloud operada por Palo Alto Networks. Basada en nuestra plataforma de seguridad de nueva generación, GlobalProtect Cloud Service se gestiona con Panorama, permitiendo crear y desplegar políticas de seguridad consecuentes a través de toda la organización. GlobalProtect Cloud Service sigue un modelo de propiedad compartida que permite mover los gastos de seguridad de tu sede remota y usuarios móviles a un modelo más eficiente y predictible badaso en OPEX.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK, SOC2 Type II	
Next-Generation Security para Clouds Públicas y Privadas	VM-Series	Las VM-Series son un formato virtualizado de nuestro next-generation firewall que puede ser desplegado en un amplio rango de entornos tanto de nube pública como privada. Tanto en entornos de nube pública como privada, las VM-Series se pueden desplegar como firewall perimetral, terminador de VPN IPsec y firewall de segmentación, protegiendo tu negocio con políticas de reconocimiento de aplicaciones y prevención de amenazas.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
Análisis de comportamiento con capacidad de respuesta activa en red	Palo Alto Networks LigthCyber Behavioral Analytics	LightCyber™ Behavioral Analytics permite a las empresas detener atacantes activos y malware que opera en la red. LightCyber aprende el comportamiento esperado de los usuarios y dispositivos y detecta la actividad anómala de un ataque. Su modelo centrado en la red detecta ataques durante cada fase del ciclo de vida del ataque, asegurando la detección y eliminación de cada fase.	PALO ALTO NETWORKS	Todos	Global	>100		>100
Firewall L2 y L3	MGUARD	Firewalls industriales en diferentes formatos para protección de red.	PHOENIX CONTACT	Todos	Global	12		

ÍNDICE

PROTECCIÓN DE RED (5/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Firewall avanzado	FL MGUARD RS 4000	Firewalls industriales en carril DIN con inspección profunda de paquetes para protocolos industriales específicos Y con chequeo periódico de integridad de sistemas de ficheros en PCs industriales.	PHOENIX CONTACT	Todos	Global	12		
VPN-MPLS	RED PRIVADA VIRTUAL SARENET	Diseño e implementación de redes de área extensa privada Intersede. Con líneas de respaldo en HA.	SARENET	Todos	España	>10	N/A	
VPN-MPLS	CONTROLES PERIMETRALES DE SEGURIDAD EN LA FRONTERA	Utilización de cortafuegos de última generación para fiscalizar todo el tráfico de redes corporativas hacia Internet con cortafuegos de Fortinet.	SARENET	Todos	España	>10	N/A	
Protección ante DDoS	Servicio de defensa perimetral	Se trata de una frontera para frenar ataques volumétricos o de sesiones contra clientes de conectividad. El servicio de defensa perimetral es una herramienta web, desarrollada y gestionada por Sarenet, orientada a frenar ataques de DDoS lanzados contra IPs de Internet asociadas a las conexiones del cliente en el perímetro de Sarenet.	SARENET	Todos	España	>10	N/A	
PROYECTOS DE SEGMENTACION DE RED	SEGMENTACION DE REDES Cloud/IT/OT	Segmentación de redes IT/OT/Cloud y fiscalización de tráfico con tecnologia Fortinet utilizando Switches inteligentes de última generación.	SARENET	Todos	España	>10	N/A	
Firewall y VPN	SIMATIC S7CP SECURITY	Acceso a controladores diseñados específicamente con requisitos de ciberseguridad.	SIEMENS	Todos	Global	>100	Achilles	>100
Firewall y VPN	SCALANCE S	Stateful Inspection Firewall para proteger los segmentos de red de accesos no autorizados.	SIEMENS	Todos	Global	>100	Achilles	>100
Protección wireless y NAC	SCALANCE W	Solución de comunicación inalámbrica fiable y segura en los entornos industriales más adversos.	SIEMENS	Todos	Global	>100	Achilles	>100
Protección NAC	SCALANCE X	Solución para control de acceso en la red.	SIEMENS	Todos	Global	>100	Achilles	>100
Firewall WAN	SCALANCE M	Stateful Inspection Firewall WAN para protegerla comunicación WAN de accesos no autorizados.	SIEMENS	Todos	Global	>100	Achilles	>100
Protección NAC	ROS (RS 900 RSG2488...)	Solución para control de acceso en la red.	SIEMENS	Infraestructuras y energía	Global	>100		

ÍNDICE

PROTECCIÓN DE RED (6/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Protección NAC, filtrado de red y VPN	ROX (RX 1400, RX 1500…)	Solución para control de acceso en la red.	SIEMENS	Infraestructuras y energía	Global	>100		
CIFRADOR	DATACRYPTOR. SERIE 5000	La serie 5000 de Datacryptor es una familia segura de cifradores de alto rendimiento que permite el intercambio de datos a alta velocidad y con una latencia cercana a cero. Beneficios clave: • Permite la interconexión de cientos de cifradores en arquitecturas de malla. • La optimización del rendimiento, hasta un 95% de eficiencia de red. • El control de flujo y la fragmentación garantizan la entrega de paquetes a través de diversas redes.	THALES	Todos	Global		CC EAL3	
Diodo de datos	ELIP-SD	Posibilita una comunicación unidireccional para transferir información entre redes con distinto nivel de clasificación, satisfaciendo los requisitos de interconexión de sistemas con diferente sensibilidad.	THALES	Todos	Global	100	CC EAL7	
VPN	MISTRAL	Mistral es una familia completa de equipos de cifrado para redes sensibles, permite la configuración, establecimiento y supervisión de redes VPN IPsec: • Emplea algoritmos de cifrado de bloques AES con claves de 128 0 256 bits. • Permite la gestión del ciclo de vida de las claves. • Interface SNMPV3.	THALES	Todos	Global	100	CC EAL3+	

ÍNDICE

PROTECCIÓN DE RED (7/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
HSM	HSM nShield	Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográficos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa. Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográficos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa.	THALES	Todos	Global			
Monitorización y Protección Avanzada de Red	Deep Discovery	Solución formada por dos componentes. Deep Discovery Inspector que proporciona inspección del tráfico de red, detección avanzada de amenazas y análisis en tiempo real con presentación de informes. Deep Discovery Advisor opcional que proporciona análisis Sandbox abierto, escalable, y personalizable para la detección de ataques dirigidos y APTs.	TREND MICRO	Todos	Global		Common Criteria	7
Control de acceso en la red	Network VirusWall Enforcer	Solución de control de acceso en la red sin agente (NAC), protegiendo tanto dispositivos gestionados como no gestionados, locales o remotos permitiendo cumplir con las políticas de seguridad de la organización antes de que puedan acceder a la red.	TREND MICRO	Todos	Global			10

ÍNDICE

PROTECCIÓN DE RED (8/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
IPS	TippingPoint TPS	Prevención de intrusos a nivel de red incorporando tecnología de parcheado virtual	TREND MICRO	Industrial IT	Global		CE UL UL 60950-1 RoHS RoHS2 CRoHS WEEE EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A	
IPS	TXONE EdgeIPS	Prevención de intrusos a nivel de red específico para entornos industriales	TREND MICRO	Industrial	Global		CE UL UL 60950-1 RoHS RoHS2 CRoHS WEEE EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A	

PROTECCIÓN DE RED (9/9)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
HIPS	Deep Security	HostIPS para proteger sistemas, realizando escaneo de vulnerabilidades sobre los servidores, ofreciendo protección IDS/IPS a nivel de red.	TREND MICRO	Industrial IT	Global		Partner tecnológico avanzado de Amazon Certificación Red Hat Ready Validación para Cisco UCS Common Criteria EAL 2+ Validación para EMC VSPEX Partner empresarial de HP Programa de protección de aplicaciones de Microsoft Partner certificado de Microsoft Validación para NetApp FlexPod Partner de Oracle PCI Suitability Testing para HIPS (NSS Labs) Certificación SAP (NW-VSI 2.0 y HANA) Validación para VCE Vblock Virtualización por VMware Validación para FIPS 140-2 VMware Cloud en AWS	

ÍNDICE

PROTECCIÓN DE SISTEMAS (1/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Proteccion Frente ataques a través de Dispositivos USB	SafeDoor	Solución HW/SW que proporciona acceso seguro al contenido de dispositivos de almacenamiento externo ofreciendo protección integral ante los 3 vectores de ataque USB: - Nivel Eléctrico: Ataques de sobretensión tipo UsbKiller - Nivel Hardware: Tipología badUSB - Nivel Software: Malware (Antivirus integrado) Equipo ligero, compacto y portable, no requiere instalación de drives o software. Soporta modo de operación interactiva (multiplataforma con interfaz web) o totalmente automatizada (modo frontera, transferencia a destinos de red o volcado de la información a memorias internas de servicio, con soporte a unidades con cifrado Harware y Software) Dispone de sistema de actualizaciones offline -firmware y firmas AV- para su instalación en redes OT o restringidas. Incluye software de gestión centralizada para múltiples equipos safeDoors que gestiona, audita y ofrece trazabilidad completa de los dispositivos USB y archivos transferidos, con enlace a sistemas SIEM para gestión de incidencias.	authUSB	Todos	Global	Nacional / Internacional	Certificación LINCE ENS Nivel Alto	
Clasificación de Información	Boldon James	Gestión y Aplicación de las políticas de Seguridad de la Información en la empresa.	CALS	Todos	Global	25	N/A	80
Protección de Sistemas	ABATIS	Antimalware para Windows y Linux basado en tecnología Host Integrity. No está basado en firmas ni listas. Bloquea todo tipo de ejecución de exe o Dll. Ocupa 100Kb aprox y por ello puede instalarse en dispositivos SCADA, Smart Grids, sistema de videovigilancia IP, POS, ATMs y todos los sistemas que utilicen versiones de Windows anteriores a Windows 8.	CALS	Todos	Global	10	N/A	
Control ejecución de comandos en aplicaciones SCADA	Aplication Control	Capacidad para controlar, a nivel de aplicación, la ejecución de mas de 400 comandos en la mayoría de los protocolos SCADA.	CHECK POINT	Todos	Global	15	NSS labs en IPS, NGFW, Miercom, Common Criteria	120

ÍNDICE

PROTECCIÓN DE SISTEMAS (2/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Seguridad de puesto	End Point Securirty	Agente de seguridad del endpoint que incluye todas las características y funciones necesarias para una real e eficiente seguridad combinando el mejor firewall, control de acceso da red (NAC), control de programas, anti-virus, anti-spyware, encriptación total del disco duro, encriptación de medias, con protección de los puertos y acceso remoto.	CHECK POINT	Todos	Global	10	NSS labs en IPS, NGFW, Miercom, Common Criteria	60
Protocolos y sistemas SCADA	Industrial/Ruggedized Gateways	Protecciones para amenazas específicas en los dispositivos de ICS/SCADA.	CHECK POINT	Todos	Global	15	IEC 61850-3 and IEEE 1613	6
Protección web	FortiWeb	Firewall de aplicaciones Web. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global		ICSA, VB100	
Protección de Estaciones de trabajo	FortiClient	Análisis de vulnerabilidades, protección antimalware, protección antiexploit, firewall de aplicaciones, control de aplicaciones y control de la navegación. También se integra con FortiSandbox para protección de amenazas zero day.	FORTINET	Todos	Global		VB100, NSS Labs	
Protección en tiempo real de amenazas a sistemas industriales	FortiGate	Firewall de nueva generación con Antimalware, AntiAPT, Sistema de Prevención de ataques (incluidos ataques a aplicaciones industriales), inspección y protección de aplicaciones (incluidas aplicaciones industriales). Se puede utilizar como sistema de virtual patching para protección de sistemas. También se integra con FortiSandbox para protección de amenazas zero day. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global		NSS Labs, Common Criteria, VB100, ICSA Labs, Department of Defense UC APL, Pv6 Ready Phase 2, CVE-Compatible, FIPS 140-2	
Sandbox	FortiSandbox	Protección de amenazas zero day. Permite la integración con otros dispositivos de seguridad de Fortinet (FortiGate, FortiWeb, FortiMail, FortiClient…) o de terceros (Carbon Black, STIX..). También monitoriza carpetas compartidas de servidores de ficheros y permite el análisis bajo demanda de cualquier fichero sospechoso. Posibilidad de integración mediante API con herramientas de terceros o desarrollos propietarios. Disponible en formato appliance físico o máquina virtual para distintos hipervisores.	FORTINET	Todos	Global			

ÍNDICE

PROTECCIÓN DE SISTEMAS (3/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Whitelisting, Fortificación	Checker	Producto de seguridad para sistemas de autoservicio líder del mercado, protegiendo desde hace ya más de 7 años cerca de 80.000 cajeros automáticos en más de 20 entidades de todo el mundo. La clave del éxito de checker es simple: "Proteger sin interferir", checker es capaz de ejercer un férreo control sobre el sistema con un único producto, sin apenas consumir recursos, sin afectar a su disponibilidad y siendo completamente independiente del fabricante del equipo en el que se instale.	GMV	Todos	Global	8		12
Tecnología Virtual	Virtualización Industrial Scada	Seguridad para la industria obsoleta. Virtualización experta para equipos en redes de control de proceso (Process Control Network, HOST PCN). Es la Virtualización de los sistemas SCADA que consiste en un HOST centralizado en planta con todos los equipos HMI virtualizados y controlados de manera segura.	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	
Tecnología Virtual	Virtualización Pin (Plant Information Network)	Seguridad en la gestión de sistemas en la industria. Integración de servicios en un HOST - PIN (Plant Information Network) de servidores virtuales que controlan el acceso e implementan políticas o directivas sobre la gestión y uso de los equipos o sistemas operativos de equipos HMI. Controladores de dominio en planta, servidores de copias de seguridad de los equipos en planta, monitorización de la red en planta, sincronización horaria de los equipos en planta, servicios de accesos remotos a sistemas SCADA, ...	INYCOM	Todos	Global	>20	Certificaciones AENOR ISO27001 Especialista implantador de SGSI, ISO20000 Especialista implantador de SGSTIC, ITIL, Lean IT	
KICS	PROTECCIÓN INDUSTRIAL	Protección del equipo final y comunicaciones entre sistemas finales SCADA.	INYCOM	Todos	España	>2		
Sistemas de Gestión de Cambios	AutoSave (MDT Software)	Los Sistemas de Gestión de Cambios permiten la traza de usuarios que desarrollan y/o modifican la aplicación, la gestión de versiones de los ficheros de configuración de los PLCs y sistemas SCADA, la automatización de las políticas de backup de dichos ficheros, la gestión documental y la creación de imágenes de servidores y PC´s de forma automática.	LOGITEK	Todos	Global	3	Certified Partner for AutoSave (MDT)	12

ÍNDICE

PROTECCIÓN DE SISTEMAS (4/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
RTU con firewall integrado	LKREMOTE	Dispositivos RTU con funcionalidades de seguridad embebidas (VPN Server, Firewall, acceso HTTPS…).	LOGITEK	Todos	Global	4	Certified Partner for RTU Logitek	50
OPC UA	Kepware	Servidores OPC UA (permiten autenticación, autorización, encriptación, auditabilidad).	LOGITEK	Todos	Global	4	Certified Partner for Kepware	20
Whitelisting applicaciones	SafeLock	Solución para controlar los procesos que pueden ejecutarse en una plataforma Windows o Linux. Evita ejecución de malware o modificación no autorizada del sistema.	LOGITEK	Cualquiera	España	2		
Fault Tolerant	Stratus FTServer	Servidores con redundancia hardware que garantizan el 99.999+% de disponibilidad (fault tolerant).	LOGITEK	Cualquiera	España	2	Stratus Certified	5
Fault Tolerant	Stratus ZTC Edge	Servidores industriales con virtualización incorporada que garantizan el 99.999% de disponibilidad (fault tolerant).	LOGITEK	Cualquiera	España	2	Stratus Certified	
Estación Remota cibersegura	S4W	Estación remota para telegestión inteligente de las instalaciones de agua. Implementa el más alto nivel de seguridad mediante la autentificación mutua de usuarios y de todos los sistemas conectados mediante certificados electrónicos, cifrado de las comunicaciones, y trazabilidad mediante la conexión a servidores syslog. Forma parte del ecosistema S4 compuesto además por SG4000 (servidor vpn de comunicaciones públicas 2G/3G y ADSL), S4-Manager (gestión de usuarios y sincronización automática de configuraciones, S4-Keys (PKI para la firma de certificados).	LACROIX SOFREL	Agua	Global	>100		>100
Estación Remota cibersegura	S4TH	Estación remota para telegestión inteligente de salas de calderas y redes de calor. Implementa el más alto nivel de seguridad mediante la autentificación mutua de usuarios y de todos los sistemas conectados mediante certificados electrónicos, cifrado de las comunicaciones, y trazabilidad mediante la conexión a servidores syslog. Forma parte del ecosistema S4 compuesto además por SG4000 (servidor vpn de comunicaciones públicas 2G/3G y ADSL), S4-Manager (gestión de usuarios y sincronización automática de configuraciones, S4-Keys (PKI para la firma de certificados).	LACROIX SOFREL	Energía	Global	>100		>100

PROTECCIÓN DE SISTEMAS (5/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Protección frente a vectores de ataque por dispositivos USB	Frontera USB	Solución que combina el uso de dispositivos USB seguros con software de control y bloqueo en los ordenadores que evite utilización de USBs no inventariados: - Uso de USBs con firmware que no sea público y firmado con certificado hardware. - Uso únicamente USB con garantía de origen en fábrica, debidamente inventariados y con alguna de las protecciones anteriores. - Uso de software de control y bloqueo en los ordenadores que evite utilización de USBs no inventariados con comprobación de Hardware ID del dispositivo (tanto memorias como teclados, ratones, etc..).	MINSAIT	Todos	Global	12		2
Monitorización de Endpoint en tiempo real	FEE(P) Digital Defense	Solución que combina capacidades antimalware con ciberinteligencia. El objetivo es dotar de seguridad sin causar un impacto a la operación del negocio. Transparencia para el usuario y simplicidad para el administrador son las características más relevantes. Como factor diferencial, FEE(P) Digital Defense permite mediante un motor de inteligencia identificar equipos comprometidos y equipos desde los que se realizan operaciones sospechosas.	MINSAIT	Todos	Global	10		15
Sistema de actualización asíncrono	VITAL Lock	Sistema “exclusa” de actualización a través de pasarela de comunicación. Permite actualización de sistemas y entornos sobre infraestructuras OT offline.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	12	CCSA, CCSE, CCNP, FCNSA, FCNSE, MCD, MCA, CEH, CREA, GCHI, ENCE, ACE	8

PROTECCIÓN DE SISTEMAS (6/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Firmado de binarios	VITAL Sign	Sistema de control de integridad y autorización a través de firmado de binarios.	MNEMO	Oil & Gas, AAPP, Energía, Utilities, Financiero, Salud, Telco, Transporte, Marítimo, Areonáutico	Global	12	CCSA, CCSE, CCNP, FCNSA, FCNSE, MCD, MCA, CEH, CREA, GCHI, ENCE, ACE	7
Protección de Sistemas (Endpoints y Servidores)	TRAPS	Seguridad de APts para endpoints (Permite securizar sistemas operativos incluyendo parcheo virtual). Tecnologías anti-Exploit y anti-Malware. Capacidad de análisis de ficheros desconocidos mediante sandbox en la nube (Wildfire).	PALO ALTO NETWORKS	Todos	Global	>100	NERC CIP (CIP-007-5, CIP-010-1, CIP-014-1)	>100
Monitorización y prevención en tiempo real frente a amenazas industriales	Next-Generation Firewal	Sistema de seguridad en redes scada, soportando protocolos industriales (dnP3, ICCP, Modbus/ tCP,...) y cumplimiento de regulaciones NERC CIP, ISA 62443. Capacidad de caracterizar tráfico y aplicaciones industriales propietarias. Establecimiento de reglas de sanidad y capacidad de reconocimiento de amenazas conocidas y desconocidas (vulnerabilidades de día 0 y APts).	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK	>100
Monitorización y prevención frente a APTs	Wildfire	Solución de Sandboxing en nube pública o privada que permite analizar ficheros para hacer frente a amenazas desconocidas y APTs, generando firmas de respuesta ante las mismas, las cuales se envían a los Next Generation Firewalls de Palo Alto Networks en menos de 15 minutos para proteger la red frente a las mismas.	PALO ALTO NETWORKS	Todos	Global	>100	SOC2 Type II	>100
ENDPOINT	SEGURIDAD DE EQUIPO FINAL (ENDPOINT)	Protección de los puntos finales utilizando uno de los endpoints más destacados del mercado, que detiene la más amplia variedad de amenazas, capaz de interpretar las ejecuciones de programas, para decidir si suspende las mismas si sospecha que se trata de un virus.	SARENET	Todos	España	>10	N/A	
EndPoint	Seguridad de equipo final (EndPoint)	Protección de los puntos finales utilizando uno de los endpoints más destacados del mercado, que detiene la más amplia variedad de amenazas, capaz de interpretar las ejecuciones de programas, para decidir si suspende las mismas si sospecha que se trata de un virus.	SAt	Todos	España	>10	N/A	

ÍNDICE

PROTECCIÓN DE SISTEMAS (7/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Protección de acceso y cifrado	SIMATIC S7-1200/1500	Controladores diseñados específicamente con requisitos de ciberseguridad.	SIEMENS	Todos	Global	>100	Achilles	>100
Autenticación, control de acceso y protección de sistemas	CROSSBOW	Solución de autenticación, control de acceso y protección de sistemas.	SIEMENS	Energía	Global	20		5
Protección y monitorización de sistemas	RUGGED APE	Solución de Protección y monitorización de sistemas.	SIEMENS	Todos	Global	>50		5
AntiAPT, AntiMalware	STORMSHIELD Endpoint Security Full Protect	La solución de seguridad que bloquea ataques avanzado y no conocidos que pasan desapercibidos para los sistemas convencionales de seguridad. Stormshield Endpoint Security Full Protect es la culminación de años de Investigación y Desarrollo que permite reconocer e identificar ataques avanzados desconocidos sin necesidad de actualización de firmas de detección o del propio producto. Por este motivo se trata de una solución especialmente eficiente para entornos *offline* y redes sin conectividad internet. Esta tecnología se utiliza mundialmente en un gran número de clientes que requieren este tipo de detección avanzada: seguridad industrial, Defensa y entornos críticos y en general cualquier empresa pequeña o grande que necesite protegerse eficazmente contra estas amenazas.	STORMSHIELD	Todos	Global	>250	Common Criteria EAL en progreso	>100

ÍNDICE

PROTECCIÓN DE SISTEMAS (8/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
HSM	HSM nShield	Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográfcos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa. Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográfcos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa.	THALES	Todos	Global			
Defensa en profundidad	Deep Security	Plataforma avanzada de seguridad con gestión centralizada para proteger servidores físicos y virtuales, sus aplicaciones y datos sin tener que aplicar parches de urgencia. Solución basada en agentes y aplicación automatizada de políticas de seguridad.	TREND MICRO	Todos	Global		HIPAA, NIST, SAS 70	15
Bastionado de sistemas	Trend Micro Safe Lock	Solución que permite evitar la intrusión y ejecución de malware. Con un impacto limitado en el rendimiento del sistema y no hay necesidad de actualizar los archivos de patrones. Protege los sistemas industriales de control y los dispositivos integrados para los cuales se requiere una alta disponibilidad, y los dispositivos de funciones fijas en ambientes cerrados.	TREND MICRO	Todos	Global			10
Protección de sistemas embebidos	Trend Micro Portable Security 2 Malware Scanning & Cleanup too	Solución que escanea y elimina el malware con una herramienta de análisis en una unidad flash USB. En gran variedad de sistemas con interfaces USB instalados, se puede detectar y eliminar el malware fácilmente.	TREND MICRO	Todos	Global			3
Protección de dispositivos externos	Trend Micro USB Security	Protección de malware en dispositivos USB de intercambio de datos.	TREND MICRO	Todos	Global			4

ÍNDICE

PROTECCIÓN DE SISTEMAS (9/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Antimalware avanzado Web Reputation Control de aplicaciones Log Inpection Monitorizacion de Integridad de ficheros Firewall IPS - Virtual Patching.	Deep Security	Protección integral para datacenters/Servidores/Endpoint: Antimalware avanzado Web Reputation Control de aplicaciones Log Inpection Monitorizacion de Integridad de ficheros Firewall IPS - Virtual Patching.	TREND MICRO	Industrial IT	Global		Partner tecnológico avanzado de Amazon Certificación Red Hat Ready Validación para Cisco UCS Common Criteria EAL 2+ Validación para EMC VSPEX Partner empresarial de HP Programa de protección de aplicaciones de Microsoft Partner certificado de Microsoft Validación para NetApp FlexPod Partner de Oracle PCI Suitability Testing para HIPS (NSS Labs) Certificación SAP (NW-VSI 2.0 y HANA) Validación para VCE Vblock Virtualización por VMware Validación para FIPS 140-2 VMware Cloud en AWS	

PROTECCIÓN DE SISTEMAS (10/10)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Control de Applicaciones y antimalware	SafeLock	Solución Whitelisting específica para proteger entornos industriales sin impacto en rendimiento.	TREND MICRO	Industrial	Global			
Antimalware	Portable Security	Solución antimalware para entornos que no permitan instalación de software. Toda la solución se encuentra ubicada en un USB el cual deberemos conectar en el dispositivo a analizar.	TREND MICRO	Industrial	Global			

ÍNDICE

CIBER RESILIENCIA (1/2)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Servicios profesionales expertos 24x7	Incident Response	Mitigar la amenaza, minimizar las perdidas y recuperar el BAU (Business As Usual) de la organización.	CHECK POINT	Todos	Global	30	NSS labs en IPS, NGFW, Miercom, Common Criteria	2
Predicción de resiliencia	SimulIT	SimulIT es la combinación de una metodología y una herramienta que permite el cálculo de la fiabilidad, disponibilidad y facilidad de mantenimiento para todos los activos de una infraestructura TIC, incluyendo hardware, software, procesos y operaciones, los eventos de seguridad informática y los desastres naturales.	GMV	Todos	Global	4		5
Veaam Cloud	Planes de contingencia	Implementamos la tecnología Veeam en nuestros centros de datos (Veeam Cloud Service Provider), para ofrecer a los usuarios de este sistema de réplicas continuas en entornos virtualizados.	SARENET	Todos	España	>10	N/A	

ÍNDICE

CIBER RESILIENCIA (2/2)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Antimalware avanzado **Web Reputation** **Control de aplicaciones** **Log Inpection** **Monitorizacion de Integridad de ficheros** **Firewall** **IPS - Virtual Patching.** **Análisis forense** **XDR**	Deep Security	Protección integral para datacenters. Antimalware avanzado Web Reputation Control de aplicaciones Log Inpection Monitorización de Integridad de ficheros Firewall IPS - Virtual Patching	TREND MICRO	Industrial IT	Global		Partner tecnológico avanzado de Amazon Certificación Red Hat Ready Validación para Cisco UCS Common Criteria EAL 2+ Validación para EMC VSPEX Partner empresarial de HP Programa de protección de aplicaciones de Microsoft Partner certificado de Microsoft Validación para NetApp FlexPod Partner de Oracle PCI Suitability Testing para HIPS (NSS Labs) Certificación SAP (NW-VSI 2.0 y HANA) Validación para VCE Vblock Virtualización por VMware Validación para FIPS 140-2 VMware Cloud en AWS	

ÍNDICE

PROTECCIÓN INTEGRAL (1/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
HSM	HSM Trustway Proteccio, HSM Trustway Crypt2Pay	Dispositivo hardware de seguridad criptográfica que permite la generación y custodia de claves criptográficas.	ATOS	Todos	Global	>50		>100
Plataforma de Cifrado	Trustway DataProtect	Solución que proporciona la capacidad de cifrar todos los formatos de datos: máquinas virtuales, base de datos, sistema de archivos, aplicación y tokenización.	ATOS	Todos	Global	>50	Common Criteria EAL4+, Reinforced Qualification (ANSSI QR), NATO SECRET and EU RESTRICTED	>100
Plataforma IoT	Horus IoT Solutions	Suite de Seguridad IoT que garantiza la seguridad de IoT en todos los niveles: Horus Secure Elements for IoT, Horus Security Server, Horus PKI for IoT, Trusted blockchain, Atos Codex IoT, Horus Trust Infrastructure Appliances	ATOS	Todos	Global	>50	Common Criteria EAL 3+	>100
Protección de toda la superficie de ataque	Security Fabric	La visión de Fortinet consiste en proteger cualquiera de los vectores de ataque y compartir la inteligencia de amenazas de múltiples fuentes, para proporcionar una protección en tiempo real. Esto no es un mensaje de márketing, es una tecnología que integra las diferentes soluciones de Fortinet (FortiGate, FortiWeb, FortiMail, FortiClient...) para compartir indicadores de compromiso a nivel local (gracias a FortiSandbox) y a nivel Global a través de los laboratorios de investigación de amenazas de Fortinet).	FORTINET	Todos	Global			
KICS	PROTECCIÓN INDUSTRIAL	Protección para todas las fases de la red de control de proceso industrial.	INYCOM	Todos	España	>2		
Gestión integral (Monitorización, control local y remoto)	Managed Services for Enterprise Networks	MSEN es un servicio proactivo de gestión operacional de infraestructuras TI flexible, cost-effective y en tiempo real, alineado con ITIL y siguiendo procesos consistentes a nivel global. Servicios con soluciones de portal dedicado, monitorización proactiva, gestión de configuraciones, eventos, disponibilidad, capacidad, etc. con el objetivo de ofrecer una respuesta más rápida y de resolución de incidentes.	NTT	Todos	Global			

ÍNDICE

PROTECCIÓN INTEGRAL (2/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Plataforma Integrada de Seguridad	Next-Generation Security Platform	Solución global que aborda la seguridad desde un punto de vista integral, desplegándose en los puntos clave; Red con el NGFW y sus servicios de seguridad (Threat Prevention, URL Filtering, Global Protect), Nube de Inteligencia ante amenazas con Wildifre, y Protección Avanzada del Endpoint con TRAPS.	PALO ALTO NETWORKS	Todos	Global	>100	FIPS 140-2, CC EAL4+, CC NIAP NDPP, NDPP FW, UCAPL, French ANSSI CSPN, NEBS, CSfC, CESG, ICSA, NSS, USGv6, Section 508 Compliance, FSTEK, SOC2 Type II	>100
Seguridad Gestionada Sarenet	Servicio de defensa perimetral	Se trata de una frontera para frenar ataques volumétricos o de sesiones contra clientes de conectividad. El servicio de defensa perimetral es una herramienta web, desarrollada y gestionada por Sarenet, orientada a frenar ataques de DDoS lanzados contra IPs de Internet asociadas a las conexiones del cliente en el perímetro de Sarenet.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Cortafuegos frontera	Superficie de ataque que se encuentra entre la VPN de la empresa e Internet. Sarenet ofrece cortafuegos perimetrales de Fortinet y es un proveedor de servicios de seguridad gestionada (MSSP) partner de este fabricante. Con cortafuegos de última generación con control de aplicaciones, IPS, IDS, Antivirus y Web filtering.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Cortafuegos aplicaciones	Dispositivos especiíficos para proteger las aplicaciones web.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Control de flujos MPLS	Cortafuegos distribuido, que permite crear reglas por IPs, redes y VLANs para decir quién se ve con quién dentro de tu red.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Routers de sedes	Gestión completa de los routers de las sedes para que sean equipos eficientes sin fallos de seguridad.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Segmentación IT/OT/IIoT	Servicio de auditoría, monitorización y segmentación de la LAN central y de los centros más relevantes en entornos IT y OT/IIoT.	SARENET	Todos	España	>10	N/A	

ÍNDICE

PROTECCIÓN INTEGRAL (3/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Seguridad Gestionada Sarenet	Control de acceso a la red (NAC)	Mediante la utilización de herramientas de control de accesos podemos conectar a los trabajadores con los recursos de la empresa protegiendo sus dispositivos independientemente de la localización, ya sea en el centro de datos, la nube o en aplicaciones móviles.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Seguridad de punto final EndPoint	Protección de los equipos finales utilizando uno de los endpoints más destacados del mercado, que detiene la más amplia variedad de amenazas, capaz de interpretar las ejecuciones de programas, para decidir si suspende las mismas si sospecha que se trata de un virus.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Cibersoc. Auditorías evolutivas de seguridad	Supervisión continua de todos los elementos activos relacionados con la Ciberseguridad mediante sondas y agentes interrogando a los activos (equipos, routers, impresoras, etc.). La información se recolecta para después ser visualizada en una herramienta web.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Planes de contingencia	Implementamos la tecnología Veeam en nuestros centros de datos (Veeam Cloud Service Provider), para ofrecer a los usuarios de este sistema de réplicas continuas en entornos virtualizados una solución sencilla, rentable y con un alto grado de integración.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Centro de operaciones de seguridad SOC	Servicio de atención de alertas.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Soporte preventivo	Vigilancia de posibles amenazas, supervisión de la red y monitorización de los sistemas instalados, gestión de informes periódicos y bajo demanda, reuniones de seguimiento, asesoramiento continuo y recomendaciones puntuales.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Soporte evolutivo	Actualizaciones, nuevas configuraciones en los dispositivos instalados, incorporación de nuevas tecnologías, redimensionamientos.	SARENET	Todos	España	>10	N/A	
Seguridad Gestionada Sarenet	Soporte reactivo	Atención urgente a los problemas de seguridad detectados, resolución de incidencias y recuperación de datos.	SARENET	Todos	España	>10	N/A	

ÍNDICE

PROTECCIÓN INTEGRAL (4/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
PLATAFORMA CIFRADO	VORMETRIC	La plataforma de seguridad de datos de Vormetric permite administrar datos almacenados de manera eficiente en toda su empresa. Construida en una infraestructura modular, extensible, incluye varios productos de cifrado y seguridad de datos que pueden instalarse de manera individual, a la vez que ofrece una administración de claves centralizada y eficiente. Estos productos de cifrado y seguridad de datos tienen capacidades para el cifrado transparente a nivel de archivos, cifrado de capa de aplicación, tokenización, puerta de enlace de cifrado de nube, administración de claves integrada y registros de inteligencia de seguridad.	THALES	Todos	Global			
HSM	HSM nShield	Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográfcos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa. Los módulos de seguridad hardware (HSMs) proveen un entorno seguro, reforzado y resistente a la manipulación, para: • el almacenamiento y uso de claves • ejecución de procesos criptográfcos Con estos dispositivos se pueden implementar soluciones de seguridad, con la garantía de que satisfagan estándares establecidos y emergentes de sistemas criptográficos al mismo tiempo que mantienen altos niveles de eficiencia operativa.	THALES	Todos	Global			

ÍNDICE

PROTECCIÓN INTEGRAL (5/5)

Tipo de tecnología	Nombre	Descripción	Proveedor y contacto	Sector de aplicación	Alcance geográfico	Profesionales capacitados	Certificaciones de la tecnología	Número de referencias
Antimalware avanzado **Web Reputation** **Control de aplicaciones** **Log Inpection** **Monitorizacion de Integridad de ficheros** **Firewall** **IPS - Virtual Patching.** **Análisis forense** **XDR**	Deep Security	Protección integral para datacenters. Antimalware avanzado Web Reputation Control de aplicaciones Log Inpection Monitorizacion de Integridad de ficheros Firewall IPS - Virtual Patching	TREND MICRO	Industrial IT	Global		Partner tecnológico avanzado de Amazon Certificación Red Hat Ready Validación para Cisco UCS Common Criteria EAL 2+ Validación para EMC VSPEX Partner empresarial de HP Programa de protección de aplicaciones de Microsoft Partner certificado de Microsoft Validación para NetApp FlexPod Partner de Oracle PCI Suitability Testing para HIPS (NSS Labs) Certificación SAP (NW-VSI 2.0 y HANA) Validación para VCE Vblock Virtualización por VMware Validación para FIPS 140-2 VMware Cloud en AWS	

ÍNDICE

Pº de las Delicias, 30, planta 2 · 28045 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org
Blog: blog.cci-es.org
Twitter: @info_cci