Seguridad de la Información	
Objetivos:	• Formar al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a: 1. Configuración de sistemas 2. Detección y reacción ante incidentes 3. Gestión de la Información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, distribución, transferencia, copias, distribución y destrucción
Destinatarios:	Curso dirigido a todo el PTGAS Máximo: 25 alumnos.
Duración:	15 horas.
Modalidad impartición:	Online Asíncrono, a través de la plataforma Moodle.
Profesorado:	Monitores internos de la UZ: Víctor Pérez Roche, David Giménez Muñoz, José Antonio Valero Sánchez.
Certificado:	Se otorgará a los participantes Certificado de Aprovechamiento, siendo requisito necesario la superación de las prácticas, ejercicios o test de conocimientos del curso.
Contenidos:	1. Fundamentos de la información: Activos. Dimensiones de la seguridad de la información. Amenazas y riesgos. ENS, GRPD. Política, Normativa y Procedimientos técnicos de la Universidad de Zaragoza 2. Cifrado de la información: Cifrado en tránsito y reposo. Cifrado de ficheros, volúmenes y cifrado en el Cloud. Cifrado de sistemas completos. Mecanismos de cifrado en UNIZAR 3. Certificados digitales: Certificado Digital del Empleado Público. Firma digital de documentos, validación de firmas. Gestión segura de certificados digitales: Exportación, importación y salvaguarda. Certificados digitales en UNIZAR con el proveedor HARICA 4. Metadatos: Visualización de metadatos y limpieza de documentos. Metadatos en plataformas de UNIZAR 5. Copias de seguridad: Copias de seguridad en la Universidad de Zaragoza. Sistemas de Información centrales y equipos de usuario. Copias de seguridad de Sistemas Centrales y de Escritorio en UNIZAR 6. Borrado seguro y destrucción de soportes: Borrado seguro de ficheros y sistemas. 7. Correo electrónico seguro: Introducción a los problemas de seguridad del correo electrónico. Spam, phising, suplantación… Revisión de cabeceras, OpenPGP, S/MIME. Arquitectura de correo electrónico en UNIZAR 8. Navegación web segura: Amenazas: Detectar sitios web maliciosos, phising, pharming, malware. Uso de Cookies 9. Gestión de credenciales:Buenas prácticas en contraseñas. Gestores de contraseñas. Uso de doble factor de autenticación en Unizar. TOTP, push…Gestión de credenciales y uso de 2FA en UNIZAR 10. Protección del Endpoint: Antivirus en Unizar. EDR en Unizar. Uso de recursos externos, Virustotal, Anyrun. Técnicas de infección. Sistemas de protección del Endpoint en UNIZAR. ESET, microCLAUDIA y EDR