CIBERSEGURIDAD	Programa, título	Contenido	Duración	Máximo de personas en el curso	Objetivo del curso	Público objetivo	Modalidad
CURSO 1	**Ciberataques: Ingeniería Social**	Descripción del panorama de amenazas de ciberseguridad actual centrado en los tipos de Malware existentes (Troyanos, Ransomware, etc.). Se muestran ejemplos reales, se explica su funcionamiento y buenas prácticas para protegernos ante ellos.	1:30	30	Concienciar sobre los peligros de este tipo de ataques, aprender a reconocerlos y evitar infecciones.	Cualquier persona	Cualquier modalidad
CURSO 2	**Ciberataques: Malware**	Descripción del panorama de amenazas de ciberseguridad, centrado en las técnicas que utilizan los atacantes para engañar a los usuarios (phishing, Estafas, fraude del CEO, etc.) y obtener acceso a nuestros sistemas y datos. Se muestran casos reales y buenas prácticas para protegernos.	1:30	30	Aprender a identificar estos ataques sobre las personas para evitar caer en estafas y engaños a través de Internet.	Cualquier persona	Cualquier modalidad
CURSO 3	**ISO 27001**	Descripción de los principios esenciales de la normativa de Seguridad de la Información ISO 27001. Se explica en que consiste, cuales son sus elementos principales y como podemos implantar la normativa en las empresas.	2h	20	Conocer la norma de referencia en seguridad de la información, para tener una visión de alto nivel de sus elementos principales y como implantarla.	Departamento IT o seguridad. Directivos	Cualquier modalidad
CURSO 4	**GDPR**	Descripción de los principios esenciales de la normativa de protección de datos personales GDPR y su aplicación en la empresa. Se explica en que consiste, cuales son sus elementos principales y como podemos implantar la normativa en las empresas.	2h	20	Conocer la norma de referencia en seguridad de la información, para tener una visión de alto nivel de sus elementos principales y como implantarla.	Departamento IT o compliance. Directivos	Cualquier modalidad

CIBERSEGURIDAD	Programa, título	Contenido	Duración	Máximo de personas en el curso	Objetivo del curso	Público objetivo	Modalidad
CURSO 5	**ISO 27002 AVANZADO**	Descripción detallada de los contenidos de los controles de la ISO27002, que es el Anexo A de la ISO27001. Se facilita la comprensión de las exigencias del estándar, y las implicaciones de cumplimiento que conlleva.	8h* (podría extenderse más a petición del contratante)	Presencial (la capacidad de la sala donde se imparta) Online (lo que permita la herramienta online de impartición (¿Teams?))	Conocimiento profundo y entendimiento de las recomendaciones de seguridad establecidas por la ISO 27002 (el estándar de seguridad de mayor reconocimiento internacional). Gran apoyo al cumplimiento de la ISO27001, especialmente de cara a una certificación de un SGSI. Conocimientos generales de seguridad con una visión global necesarios para delinear un Plan Director de Seguridad.	CISO, Departamento de IT, Networking (Comunicaciones) y Seguridad IT.	Cualquier modalidad
CURSO 6	**PCI DSS BÁSICO**	Descripción general de los contenidos de los controles de PCI DSS, que es el estándar de seguridad de protección de datos de pagos realizados con tarjetas de pago (VISA, Mastercard, etc.) Se facilita la comprensión a alto nivel de las exigencias del estándar, y las implicaciones de cumplimiento que conlleva.	8h	Presencial (la capacidad de la sala donde se imparta) Online (lo que permita la herramienta online de impartición (¿Teams?))	Conocimiento general y entendimiento de los requisitos de seguridad establecidas por PCI DSS (conocido por muchos por ser el estándar de seguridad más exigente). Apoyo de cara a una certificación y para demostrar cumplimiento de PCI DSS.	CISO, Departamento de IT, Networking (Comunicaciones) y Seguridad IT.	Cualquier modalidad
CURSO 7	**PCI DSS AVANZADO**	Descripción detallada de los contenidos de los controles de PCI DSS, que es el estándar de seguridad de protección de datos de pagos realizados con tarjetas de pago (VISA, Mastercard, etc.) Se facilita la comprensión profunda de las exigencias del estándar, y las implicaciones de cumplimiento que conlleva. Cómo dejar registros de auditoría y pasar con éxito una auditoría de certificación. Claves para un mantenimiento contínuo del cumplimiento.	16h* (podría extenderse más a petición del contratante)	Presencial (la capacidad de la sala donde se imparta) Online (lo que permita la herramienta online de impartición (¿Teams?))	Conocimiento profundo y entendimiento de los requisitos de seguridad establecidas por PCI DSS (conocido por muchos por ser el estándar de seguridad más exigente). Gran apoyo de cara a una certificación y para demostrar cumplimiento de PCI DSS. Conocimientos generales para delimitar, y reducir en lo posible, el alcance del estándard en la compañía y así minimizar los esfuerzos de cumplimiento. Conocimiento de la preparación para superar con éxito una auditoría. Claves para un mantenimiento contínuo del cumplimiento.	CISO, Departamento de IT, Networking (Comunicaciones) y Seguridad IT.	Cualquier modalidad
CURSO 8	**DESARROLLO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD IT**	(Curso teórico-práctico.) Describe la necesidad de una política de seguridad corporativa y un cuerpo normativo. Define la estructura mínima de una política y una norma/procedimiento. Claves para que un documento sea eficaz. Relación de documentos más habituales. Ciclo de vida del desarrollo de un documento desde la identificación de la necesidad hasta la publicación a las partes interesadas y su posterior mantenimiento. Presentación y defensa ante el comité de seguridad.	16h* (podría extenderse más a petición del contratante)	Presencial (la capacidad de la sala donde se imparta) Online (lo que permita la herramienta online de impartición (¿Teams?))	Aprendizaje sobre cómo elaborar los documentos del cuerpo normativo de seguridad con vistas a su eficacia y la superación de posibles auditorías. Conocimiento del ciclo de vida de un documento del cuerpo normativo. Aprendizaje de defensa de los documentos ante un comité de seguridad o de dirección. Manteniemiento ante posibles auditorías y para asegurar su eficacia continua.	CISO, Departamento de IT, Networking (Comunicaciones) y Seguridad IT.	Cualquier modalidad