Descripción General del Ejercicio

Exercise Name	Caso de Estudio Ransomware	
Fecha, Horario y Lugar del Ejercicio	4 de julio 10:00 a 12:00 Auditorio Picarte	
Actividades del Ejercicio	**Tiempo**	**Actividad**
	20 Minutes	Instrucciones
	40 Minutes	Módulo 1
	40 Minutes	Módulo 2
	20 Minutes	Discusión grupal
Propósito	Examinar la resiliencia a ataques cibernéticos de su organización en respuesta a un incidente de ciberseguridad de efecto significativo.	
National Institute of Standards and Technology Cybersecurity Framework	Desarrollar Gobernanza, Identificar, Proteger, Detectar, Responder, Recuperar	
Objetivos	1. Examinar las capacidades de respuesta a incidentes de la organización durante un incidente de ciberseguridad de efecto significativo 2. Evaluar las capacidades de la organización para coordinar el intercambio de información durante un incidente de ciberseguridad de efecto significativo 3. Identificar áreas de mejora en planes de respuesta a incidentes de ciberseguridad y resiliencia organizacional durante y después de un incidente de ciberseguridad de efecto significativo. 4. Explorar los planes de la organización para recuperar y restaurar servicios, recursos críticos o sistemas.	
Amenaza o Peligro	Ransomware	
Escenario	Un actor de amenazas ataca al administrador del sistema de <Organización> a través de un correo electrónico de phishing como punto de entrada a las redes/sistemas. Los atacantes comprometen la información de identificación personal (PII) e instalan ransomware en los ordenadores de la <Organización>.	