ACCIÓN F. TENDENCIAS FUTURAS: ANÁLISIS Y PROPUESTAS DE MEJORA PARA LA ADAPTACIÓN DE LA UNIDAD ANTE LOS RETOS TECNOLÓGICOS, SOCIALES, AMBIENTALES, ECONÓMICOS QUE SE AVECINAN

CASO 1

1. Inteligencia Artificial:

   - Edificios inteligentes
   - Chatbots

   Podemos utilizar la IA:

   - Tareas repetitivas.
   - Gestión académica mejorada.

   Desafíos:

   - Habilitación de los trabajadores. El personal de secretaría deberá estar adecuadamente formado para el uso de la IA en su trabajo habitual. Un personal no preparado podría ralentizar el buen funcionamiento.
   - Adecuación tecnológica al trabajo. Es necesaria una inversión económica, tanto en material informático, software como hardware, que actualice los sistemas para el uso de dicha tecnología.
   - Aislamiento de la Administración. La Universidad mediante convenios de colaboración con otras instituciones mantendrá los datos actualizados primando especialmente a las organizaciones de carácter público por regirse por una legislación más garantista en cuestión de protección de datos.

2. Ciberseguridad:

   La importancia de la ciberseguridad. Proteger los datos y sistemas de una organización no solo previene pérdidas financieras, sino que también protege la reputación y la confianza de los clientes.

   - Protección de Información Sensible: Asegura la privacidad y seguridad de los datos personales de los ciudadanos.
   - Seguridad de Servicios Públicos: Garantiza la continuidad y protección de servicios esenciales.
   - Integridad y Transparencia: Protege los sistemas de votación y otros procesos democráticos contra interferencias.

   Sistemas de EDR. Beneficios de la Monitorización con EDR:

   - Detección Temprana: Identifica amenazas en las primeras etapas del ataque, lo que permite una respuesta rápida y efectiva.
   - Respuesta Rápida: Minimiza el tiempo de respuesta ante incidentes, reduciendo el impacto potencial de las amenazas.
   - Análisis Profundo: Proporciona una visibilidad detallada de los eventos y comportamientos en los endpoints, facilitando el análisis forense.
   - Automatización: Mejora la eficiencia operativa al automatizar tareas de detección y respuesta, liberando a los equipos de seguridad para que se enfoquen en amenazas más complejas.

Amenazas Comunes

- Ransomware**:** El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo “secuestra” de varias maneras, cifrando la información, bloqueando la pantalla, etc. El usuario es víctima de una extorsión, se le pide un rescate económico a cambio de recuperar el normal funcionamiento del dispositivo o sistema. Los ransomware se utilizan para obtener un beneficio económico mediante la extorsión de sus víctimas.