Encabezado General	A. Nombre del Formato:				
UNIVERSIDAD TECNOLÓGICA DE TULANCINGO Organismo Descentralizado de la Administración Pública Estatal	**REPORTE DE ACTIVIDADES**				
F-22-01-R1;210817	B: Código/Revisión;Fech	F-19-06-R2;020718			
Datos de los Registros (evidencia):		C. Página	1	de	1
D. Fecha de elaboración:	07-nov-22	E. Periodo al que aplica:	2022		

NOMBRE:	Francisco Ramos Lozano
PUESTO:	Jefe del Departamento de Sistemas y Soporte Técnico
ÁREA DE ADSCRIPCIÓN:	Dirección de Planeación y Evaluación
LUGAR DE LA COMISIÓN:	Ciudad de México
PERIODO DE LA COMISIÓN:	03 de noviembre de 2022

ACTIVIDADES REALIZADAS

En el Congreso se tomaron diversas conferencias que nos presentaron y que el panorama de amenazas continúa evolucionando con ataques más sofisticados y técnicas evasivas. El ransomware es una de las formas más escalofriantes del cibercrimen que enfrentan las organizaciones en la actualidad y que no desaparecerá.
Nos informaron y presentaron que hubo un aumento de siete veces en la actividad de ransomware en diciembre del 2021 en comparación con julio de 2020.
Una encuesta global de ransomware también mostró que el 67 % de las organizaciones fueron el objetivo del ransomware y casi la mitad indicó que fue atacado más de una vez.

RESULTADOS OBTENIDOS:

Concientizar a toda la comunidad universitaria sobre ataques de ransomware, e implementar las estrategias, los procesos y la tecnología para evitar en la medida de lo posible el daño. La planificación y preparación antes de que ocurra un ataque es clave. Para ayudar a los equipos de seguridad a mitigar el daño de las amenazas y minimizar el tiempo que lleva responder, implementar soluciones que cubran todas las etapas de la reducción de la superficie de ataque, la prevención y la detección de amenazas, la contención y la respuesta.

CONTRIBUCIONES A LA INSTITUCIÓN:

La Institución tiene que desarrollar un programa de seguridad de sus copias de datos. Cuando se combina con el compromiso de la cadena de suministro digital y una fuerza laboral que trabaja a distancia en la red, se puede minimizar el riesgo y la perdida de información.

CONCLUSIONES:

La planificación y preparación de la seguridad antes de que ocurra un ataque es clave. Para ayudar a los equipos de seguridad a mitigar el daño de las amenazas y minimizar el tiempo que lleva responder, las organizaciones deben contemplar soluciones que cubran todas las etapas de la reducción de la superficie de ataque, la prevención y la detección de amenazas, la contención y la respuesta.