UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

ASIGNATURA: Introducción a la Informática.

TEMA:
EL AUMENTO DE LOS DELITOS CIBERNÉTICOS EN EL SALVADOR EN LOS AÑOS 2014 - 2024 Y SUS CONSECUENCIAS JURÍDICAS.

INTEGRANTES:

•Carlos Ivan Cortez Cisneros - CC2428
•Carlos Ulises Vaquerano Merino – VM24282
•Daniela Guadalupe Reyes Mendoza - RM2421
• Samael Jeshua Mendoza Morales – MM24221

LICENCIADO: Pedro Antonio Trejo Noble.

CICLO: 2-2024

Que es un Delito Informático(dicc. Panhispánico)

Infracción penal cometida utilizando un medio o un instrumento informático

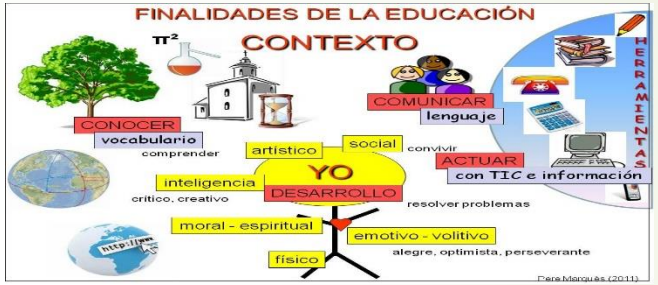
Se refiere a la manipulación en el ingreso, procesamiento o resultados de datos de un sistema que ocupe las Tecnologías de Información. Se hace uso de una operación informática que tenga como resultado información falsa, incompleta o fraudulenta.11 jul 2024

Tres ejemplos de delitos cibernéticos son el phishing y las estafas, el robo de identidad y los ataques de ransomware . Tenga cuidado con ellos cuando utilice Internet.

En la última década, El Salvador ha experimentado un notable incremento en la incidencia de delitos cibernéticos. Este fenómeno ha sido impulsado por la creciente digitalización de la sociedad y la economía, así como la adopción masiva de tecnologías de la información y la comunicación (TIC). Desde el 2014, el país ha visto un aumento significativo en la cantidad y sofisticación de los ataques cibernéticos, afectando tanto a individuos como a organizaciones.

El año del 2016, El salvador promulgo la Ley Especial contra los Delitos Informáticos y Conexos, con el objetivo de establecer un marco legal para la prevención, detección y sanción de estos delitos. A pesar de estos esfuerzos legislativos, los ciberdelincuentes han continuado adaptándose y evolucionando sus métodos, lo que ha llevado un incremento del 26% en los intentos de ciberataques en los últimos años. Las reformas recientes a la legislación penal buscan abordar estas nuevas amenazas, incluyendo la criminalización de actividades como el secuestro de datos y el fraude informático relacionado con criptomonedas,

Importancia del tema en el contexto salvadoreño



Comprender las dinámicas y tendencias de los delitos cibernéticos es esencial para los futuros profesionales del derecho, quienes deberán de enfrentar y resolver casos relacionados con esta problemática emergente.

Objetivo del proyecto

- Analizar cómo han crecido los delitos cibernéticos en El Salvador entre 2014 y 2024, revisando las leyes y las soluciones tecnológicas que se han usado, para proponer mejoras que ayuden a combatir mejor estos crímenes y proteger la seguridad digital.

Tipos de Delitos Cibernéticos

- **Malware:**
- Estos virus con forma de documentos, programas, código y mensajes son software malicioso que infectan sistemas informáticos, destruyen archivos, alteran el funcionamiento general y se "reproducen" a otros dispositivos y sistemas.
- **Ransomware**:Este tipo de malware se propaga por email (el cual lleva insertado un virus malicioso) y secuestra toda la información, cifrando los archivos, para pedir un rescate económico a cambio de los datos
- **Robo de identidad:** Si bien la identidad se puede robar por varios métodos, se da actualmente con más frecuencia con el uso de medios tecnológicos. Y es que apropiarse de la identidad es el primer paso realizar un fraude
- **Phishing:**Esta técnica de engaño se basa en simular, a través de correos electrónicos, la identidad de una persona, empresa o entidad bancaria de confianza para el usuario, para robarle información con un mensaje atractivo, como: "has ganado, debes pinchar en el enlace para reclamar tu premio", y es ahí cuando se hacen con información.

Estadísticas y datos relevantes

MES	2016	2017	2018	2019	2020	2021	2022
Enero	S/D	33	29	56	85	156	374
Febrero	S/D	23	39	40	71	129	265
Marzo	S/D	30	40	78	80	151	S/D
Abril	S/D	19	42	52	63	139	S/D
Mayo	S/D	28	57	56	54	173	S/D
Junio	S/D	32	57	73	56	191	S/D
Julio	16	30	64	97	65	513	S/D
Agosto	14	37	58	80	55	1386	S/D
Septiembre	16	42	40	71	89	724	S/D
Octubre	26	33	62	82	84	1893	S/D
Noviembre	18	42	61	66	93	589	S/D
Diciembre	24	37	42	75	66	329	S/D
Total	**114**	**386**	**591**	**826**	**861**	**6373**	**S/D**

Legislación(Leyes implementadas para combatir el ciberdelito)

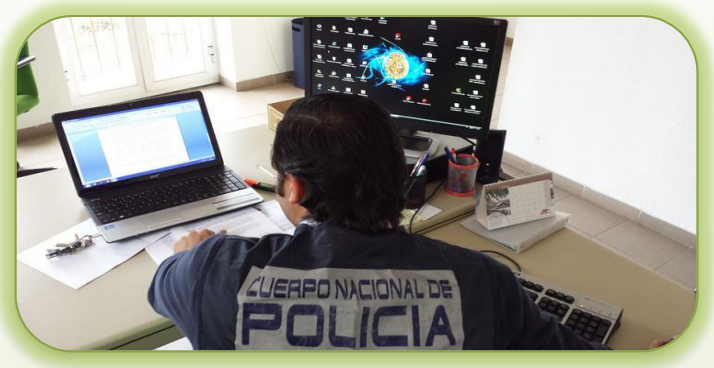
- La Policía Nacional Civil estableció el Grupo de Investigación de Delitos Informáticos (GIDI). Este grupo se encarga de investigar y manejar casos relacionados con delitos en línea. El GIDI se encarga de recopilar evidencia digital, analizar datos y colaborar con otras instituciones para combatir la delincuencia cibernética. Su creación responde a la necesidad de abordar el aumento de delitos informáticos en el país, especialmente con el crecimiento del acceso a internet.
- Debido a esta falta de regulación adecuada, se hizo evidente la necesidad de una ley más específica. Así, el 26 de febrero de 2016, se aprobó el Decreto Legislativo No. 260, que introdujo la Ley Especial contra Delitos Informáticos y Conexos (LEDIC). Esta ley entró en vigencia ocho días después de su publicación en el Diario Oficial, es decir, el 6 de marzo de 2016. La LEDIC busca fortalecer la protección contra delitos que amenazan la seguridad de los sistemas informáticos

Q ue debes hacer para protegerte de delitos informáticos

- Usa contraseñas seguras(Que incluyan combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Evita usar información personal
- Actualiza tu software regularmente para protegerte de vulnerabilidades
- Utiliza antivirus y un firewall o(sistema de seguridad de red)
- Conéctate a redes seguras.
- Ten cuidado de correos electrónicos y enlaces sospechosos

Que se debe hacer en casos de haber sido victima de delitos Cibernéticos.

- 1. Se puede acudir a la fiscalía General de la República y puedes hacer una denuncia de forma oral o escrita.
- Si no tienes la información del victimario o pruebas en el dispositivo electrónicos, la Fiscalía se encargará de hacer vaciados informáticos y de la investigación.
- Puedes acudir a la dependencia policial más cercana y ellos se encargarán de enviar el caso a la unidad especial GIDI.



Conclusiones

- **Entre 2014 y 2024, El Salvador ha experimentado un aumento significativo en los delitos cibernéticos, reflejando una tendencia global hacia la digitalización y el uso masivo de internet. Estos delitos incluyen fraudes electrónicos, hackeos, extorsión en línea y el robo de datos personales y financieros. A pesar de los esfuerzos gubernamentales por fortalecer la ciberseguridad, como la creación de leyes y la implementación de políticas para combatirlos, las amenazas cibernéticas continúan evolucionando, poniendo en riesgo tanto a individuos como a empresas. La falta de recursos y la limitada educación en ciberseguridad son desafíos persistentes que dificultan una respuesta eficaz ante este tipo de delitos. En resumen, aunque ha habido avances, la lucha contra los delitos cibernéticos en El Salvador sigue siendo un reto importante en la última década.**

Gracias por su atención