CIBERCRIMEN

PRESENTADO POR JESÚS DEL CID

CONCEPTOS

EL CIBERCRIMEN ES UNA ACTIVIDAD DELICTIVA QUE SE DIRIGE A UNA COMPUTADORA, UNA RED INFORMÁTICA O UN DISPOSITIVO EN RED, O BIEN QUE UTILIZA UNO DE ESTOS ELEMENTOS.

CONDUCTA ILÍCITA TIPIFICADA POR LA LEY QUE AFECTA AL SOPORTE LÓGICO DE UN SISTEMA INFORMÁTICO, COMO SOFTWARE, DATOS O HARDWARE. UTILIZA EQUIPOS INFORMÁTICOS COMO MEDIO O FIN PARA LA COMISIÓN DEL DELITO.

SUBCATEGORÍA DE DELITOS INFORMÁTICOS QUE IMPLICA EL USO DE LA INTERNET O REDES DE COMPUTADORAS. PUEDE IMPLICAR QUE LA COMPUTADORA O RED SEA EL ARMA DEL CRIMEN, EL OBJETIVO, O SE UTILICE PARA ACTIVIDADES RELACIONADAS CON EL CRIMEN.

TIPOS DE CIBERCRIMEN

- FRAUDE POR CORREO ELECTRÓNICO E INTERNET.
- FRAUDE DE IDENTIDAD (EN CASO DE ROBO Y USO DE INFORMACIÓN PERSONAL).
- ROBO DE DATOS FINANCIEROS O DE PAGOS CON TARJETAS.
- ROBO Y VENTA DE DATOS CORPORATIVOS.
- CIBEREXTORSIÓN (EXIGIR DINERO PARA EVITAR UN ATAQUE BAJO AMENAZA).
- ATAQUES DE RANSOMWARE (UN TIPO DE CIBEREXTORSIÓN).
- CRYPTOJACKING (POR MEDIO DEL CUAL LOS HACKERS REALIZAN LA MINERÍA DE CRIPTOMONEDAS USANDO RECURSOS QUE NO SON PROPIOS).
- CIBERESPIONAJE (EN EL QUE LOS HACKERS ACCEDEN A LOS DATOS GUBERNAMENTALES O EMPRESARIALES).
- INTERFERENCIA CON SISTEMAS DE MANERA QUE SE COMPROMETE UNA RED.
- INFRACCIÓN DE DERECHOS DE AUTOR.
- APUESTAS ILEGALES.
- VENTA DE ARTÍCULOS ILEGALES EN LÍNEA.
- SOLICITUD, PRODUCCIÓN O POSESIÓN DE PORNOGRAFÍA INFANTIL.

CONCECUENCIAS

- **VULNERACIÓN DE LA SEGURIDAD:** COMPROMETE LA SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LOS SISTEMAS INFORMÁTICOS Y LA INFORMACIÓN PROCESADA.

- **IMPACTO ECONÓMICO:** GENERA PÉRDIDAS FINANCIERAS DEBIDO A FRAUDES, ROBOS Y DAÑOS A LA INFRAESTRUCTURA TECNOLÓGICA.

- **PROBLEMAS LEGALES:** AUMENTA LOS COSTOS ASOCIADOS CON LA RECUPERACIÓN Y LA GESTIÓN DE INCIDENTES DE CIBERCRIMEN, ADEMÁS DE SANCIONES PARA LOS DELINCUENTES.

AMENAZAS

- **CIBERTERRORISMO:** USO DE REDES DE COMPUTADORAS PARA CAUSAR DAÑO FÍSICO O DISRUPTIVO.
- **CIBERESPIONAJE:** OBTENCIÓN ILEGAL DE INFORMACIÓN CONFIDENCIAL MEDIANTE TÉCNICAS INFORMÁTICAS.
- **PORNOGRAFÍA INFANTIL:** CREACIÓN Y DISTRIBUCIÓN DE MATERIAL ILEGAL QUE EXPLOTA A MENORES.
- **ACCESO NO AUTORIZADO Y DAÑOS A DATOS:** INCLUYE ACTIVIDADES COMO EL ACCESO NO AUTORIZADO, SABOTAJE COMPUTACIONAL, Y LA INTERCEPCIÓN DE COMUNICACIONES SIN PERMISO.

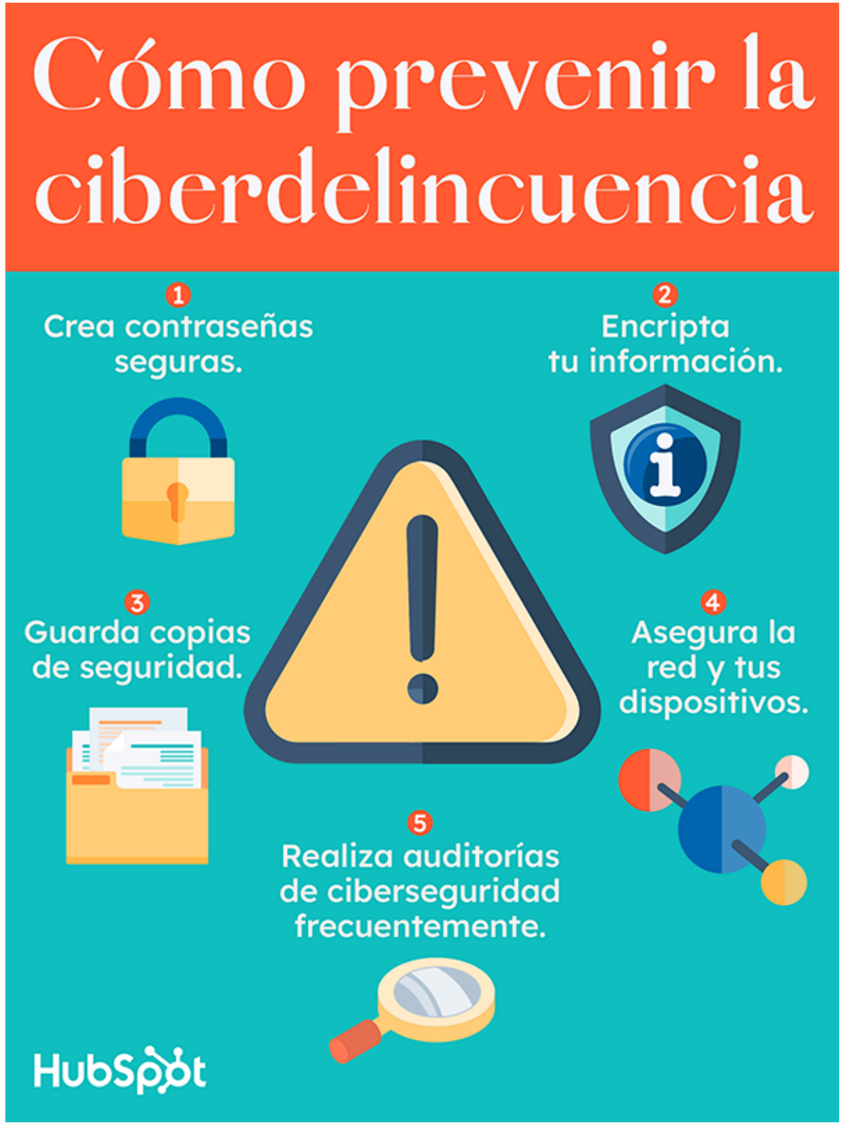
PREVENCIÓN

- **MEDIDAS DE SEGURIDAD:** IMPLEMENTACIÓN DE TECNOLOGÍAS DE PROTECCIÓN COMO FIREWALLS, ANTIVIRUS Y SISTEMAS DE DETECCIÓN DE INTRUSIONES.

- **CONCIENTIZACIÓN Y EDUCACIÓN:** CAPACITACIÓN DE USUARIOS SOBRE RIESGOS Y PRÁCTICAS SEGURAS PARA PREVENIR DELITOS INFORMÁTICOS.

- **ACTUALIZACIÓN DE SISTEMAS:** MANTENER EL SOFTWARE Y LAS APLICACIONES ACTUALIZADOS PARA PROTEGER CONTRA VULNERABILIDADES CONOCIDAS.

- **POLÍTICAS DE SEGURIDAD:** ESTABLECIMIENTO DE POLÍTICAS Y PROCEDIMIENTOS PARA LA GESTIÓN Y RESPUESTA A INCIDENTES DE CIBERCRIMEN.



VENTAJAS Y DESVENTAJAS

VENTAJAS:

- CREACIÓN DE NUEVAS LEGISLACIONES QUE REGULE LOS DELITOS INFORMÁTICOS.
- SE DEFINE UN GLOSARIO DE TÉRMINOS RELACIONADOS CON LAS T.I, LO QUE AYUDA A EVITAR CONFUSIONES.
- SE CONDENAN FUERTEMENTE DELITOS COMO EL ROBO DE LA INFORMACIÓN PERSONAL, LA PORNOGRAFÍA INFANTIL Y LA APROPIACIÓN DE LA PROPIEDAD INTELECTUAL.

DESVENTAJAS:

- RIESGOS DE SEGURIDAD: INCREMENTA LA EXPOSICIÓN A ATAQUES Y VIOLACIONES DE DATOS.
- COSTOS DE PROTECCIÓN: REQUIERE INVERSIONES SIGNIFICATIVAS EN SEGURIDAD Y GESTIÓN
- DE INCIDENTES.
- DESAFÍOS LEGALES Y NORMATIVOS: DIFICULTADES PARA LEGISLAR Y APLICAR NORMAS QUE SE AJUSTEN A LA RÁPIDA EVOLUCIÓN DEL CIBERCRIMEN.

VIDEO INSTRUCCIONAL

CONCLUSIÓN

ACTUALMENTE EXISTE LA NECESIDAD DE NO CONTAR CON UNA DEFINICIÓN ESTANDARIZA DEL CIBERCRIMEN, LA CAPACITACIÓN Y EDUCACIÓN COMO PRINCIPALES MEDIDAS PREVENTIVAS SON ESENCIALES PARA MITIGAR LOS EFECTOS DEL CIBERCRIMEN Y PROTEGER LOS SISTEMAS INFORMÁTICOS.

RECOMENDACIONES

- PROMOVER LA CREACIÓN Y ACTUALIZACIÓN DE LEYES ESPECÍFICAS PARA ABORDAR EL CIBERCRIMEN.
- FOMENTAR LA COLABORACIÓN ENTRE PAÍSES PARA ENFRENTAR LAS AMENAZAS CIBERNÉTICAS DE MANERA EFECTIVA.
- ASEGURAR INVERSIONES EN TECNOLOGÍAS Y RECURSOS PARA PROTEGERSE CONTRA EL CIBERCRIMEN.
- PROVEER CAPACITACIÓN CONTINUA A PROFESIONALES Y USUARIOS PARA MEJORAR LA SEGURIDAD Y MANEJAR LAS NUEVAS AMENAZAS.