**Resumen tema delitos informáticos:**

**CONCEPTO DE DELITO INFORMÁTICO**

Delito informático son aquellas actividades ilícitas o antijurídicas que:

Se cometen mediante el uso de entornos digitales, redes, blockchain, computadoras, sistemas informáticos u otros dispositivos de las nuevas tecnologías de información y comunicación. Y a grandes rasgos, tienen por objeto causar daños (de cualquier tipo) provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos).

**PRINCIPALES CARÁCTERISTICAS DE LOS DELITOS**

**INFORMÁTICOS:**

Debe existir una acción u omisión por parte de un sujeto que esté prevista en el sistema jurídico penal, que sea antijurídica y que no se encuentre amparada por alguna causa con justificación. Asimismo, debe existir la culpabilidad del sujeto, es decir, que sea responsable del hecho generado. Y al mismo se le debe aplicar una sanción. Pero a esto hay que sumarle una particularidad que tiene este tipo de delitos: Tiene que ser cometido con la utilización de algún medio informático.

**SUJETOS INTERVINIENTES EN LOS DELITOS INFORMÁTICOS:**

Cada acción delictiva se caracteriza por ser realiza por un sujeto activo (responsable del acto) y ser ocasionada perjudicando a un sujeto pasivo (víctima del acto).

**SUJETO ACTIVO: QUIEN COMETE EL DELITO:**

Las personas que cometen los “Delitos informáticos” tienen habilidades para el manejo de los sistemas informáticos, y generalmente, su entorno ayuda a la realización de dichas actividades, es decir, tiene un lugar estratégico para cometer el acto.

**SUJETO PASIVO: VICTIMA DEL DELITO:**

El sujeto pasivo es la víctima del delito – El propietario legítimo de los bienes jurídicos afectados – Aquella persona sobre quien recae la acción u omisión que realiza el sujeto activo.

La mayoría de los casos los sujetos pasivos no adoptan ningún tipo de precaución ni aportan información para hacer posible una denuncia. Incluso algunos, ni siquiera son conscientes de haber sido víctimas de un delito informático.

En cuanto a la seguridad del sujeto pasivo, se recomienda utilizar contraseñas difíciles de adivinar, no utilizar las mismas claves para todo, configurar opciones de privacidad en redes sociales, no compartir datos personales o imágenes intimas por chat, realizar copias de seguridad de los archivos, no utilizar cámaras web con desconocidos, entre otras.

**SISTEMAS COMO MEDIO DE COMISIÓN DE DELITOS INFORMÁTICOS:**

Los sistemas más comunes y frecuentes, en los cuales la mala utilización genera el acto delictivo son el correo electrónico, celulares, mensajes de textos, redes sociales.

**MECANISMOS COMO MEDIO DE COMISIÓN DE DELITOS INFORMÁTICOS:**

Millones de usuarios quedan expuestos constantemente a ataques y fraudes, donde el ciberdelincuente realiza una recopilación de una gran cantidad de datos personales, cuentas, claves bancarias y tarjetas de crédito con el objeto de usarlos con fines ilícitos. Una vez que tiene esta información la utilizan para venderla o manipular al usuario como medio de extorsión.

Estos ciberdelincuentes tienen mecanismos para llegar a estos actos ilícitos. Entre las prácticas más comunes a las que nos podemos ver expuestos se encuentran el phishing, el botnet, el malware, el rasonware, robo cibernético, sabotaje de instalaciones.

**CLASIFICACION DE LOS DELITOS INFORMÁTICOS:**

Se los puede clasificar de dos formas:

**Como instrumento o medio**: En esta categoría se encuentran las conductas criminales que utilizan a las computadoras como método, medio o símbolo en la comisión del ilícito.

**Como fin u objetivo**: Se clasifican como de fin u objetivo cuando las conductas criminales van dirigidas directamente contra las computadoras, accesorios o programas como entidad física.

**LOS PRINCIPALES DELITOS INFORMÁTICOS:**

En esta categoría se encuentran la estafa, el fraude, el ciberterrorismo, calumnia e injurias, pedofilia, grooming

**LEGISLACION ARGENTINA:**

**LEY 11.723 DE PROPIEDAD INTELECTUAL:**

La propiedad intelectual es la protección que le da la ley al autor de una obra científica, literaria, artística o didáctica por su creación intelectual. Esta ley abarca los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales y establece penas en caso de piratería, entre otros.

Le permite exponerla o reproducirla por cualquier medio, traducirla, explotarla comercialmente o autorizar a otros a hacerlo. También le permite impedir que cualquier persona no autorizada ejerce estos derechos.

**LEY 25.326 DE PROTECCIÓN DE DATOS PERSONALES**:

Esta ley, promulgada en octubre de 2000 tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

**LEY 26.388 DE MODIFICACIÓN DE CÓDIGO PENAL:**

* DAÑO A BIENES INTANGIBLES Y VIRUS:

Se permite ahora el daño a bienes intangibles. Entre ellos se incluye, por ejemplo, el borrado de software o de datos contenidos en un ordenador. Sumado a lo dicho, se incluye como delito el distribuir programas destinados a causar daños, por ejemplo, los virus informáticos.

* SEGURIDAD DE LOS MEDIOS DE TRANSPORTE Y COMUNICACIÓN:

Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.