Boletín 1-2005, artículo 2 º

CONCEPTOS BÁSICOS SOBRE EL FRAUDE INFORMÁTICO

Ing. Gustavo Rojas García

En la actualidad contamos con abundante evidencia, producto de la experiencia acumulada por varias organizaciones de diversa índole, que nos alerta sobre la necesidad de incrementar esfuerzos en procura de obtener mayores conocimientos relacionados con la protección de la infraestructura tecnológica, la que incluye gran variedad de equipos, accesorios y materiales informáticos, así como de variada y valiosa información, la que es utilizada para la prestación de diversos servicios en beneficio de sus clientes o usuarios.

En virtud de lo manifestado anteriormente, se aprovecha la oportunidad para fomentar una discusión acerca de la adecuada utilización de las herramientas (legales y tecnológicas) con que se cuenta, así como de la necesidad en la implementación de otras, que desde ya se hace imperativo conceptualizar, de tal forma que podamos estar preparados ante futuras eventualidades.

El presente artículo pretende ofrecer el marco legal base que aborda el tema del fraude informático, además de un caso a cargo del Ministerio Público, así como las recomendaciones y las conclusiones que consideramos en este problemático campo.

I Parte.Marco Jurídico

El **Artículo 217** del Código Penal costarricense, señala que comete "***Fraude Informático***" aquella persona que:

> *"…con la intención de procurar u obtener un beneficio patrimonial para si o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."*

Por otra parte, la Ley de Administración Financiera de la República y Presupuestos Públicos, en su **Artículo 111**, señala que:

> "*Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:*
>
> - *Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.*

- *Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.*
- *Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.*
- *Utilizar las facilidades del sistema para beneficio propio o de tercero.*"

Además de los anteriores, también merece citarse el **Artículo 229** del Código Penal relacionado con la "**Alteración de Datos y Sabotaje Informático**".En este artículo se tipifica la conducta dolosa de una persona que:

> "*…por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión.****Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público se impondrá pena de prisión de hasta ocho años***."(El destacado es nuestro)

Adicionalmente, encontramos que el **Artículo 196** del Código Penal aborda el tema relacionado con la "***Violación de Comunicaciones Electrónicas***".Dicho artículo señala que comete ilícito la persona que:

> "*…para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos, e imágenes contenidas en soportes electrónicos, informáticos, magnéticos y telemáticos […]*"

II Parte.Caso real: Fraude informático en contra del Instituto Nacional de Seguros (INS)

En el año 2004, la Fiscalía del Ministerio Público estableció cargos en contra un funcionario del Instituto Nacional de Seguros (INS), por el supuesto delito de peculado en contra de dicha entidad aseguradora.Se calcula que el funcionario habría sustraído una cifra cercana a los **¢283 millones** alterando pólizas del Seguro de Vida.

El "modus operandi"

Para lograr su cometido, el funcionario aprovechaba las debilidades en el sistema de cómputo, cambiando el nombre del propietario original de una póliza de vida cancelada (no vigente), y en su lugar escribía el de un cómplice ajeno a la institución.Luego lograba que el sistema informático le aprobara un préstamo, para posteriormente retirar el dinero desde las cajas del edificio central del INS.

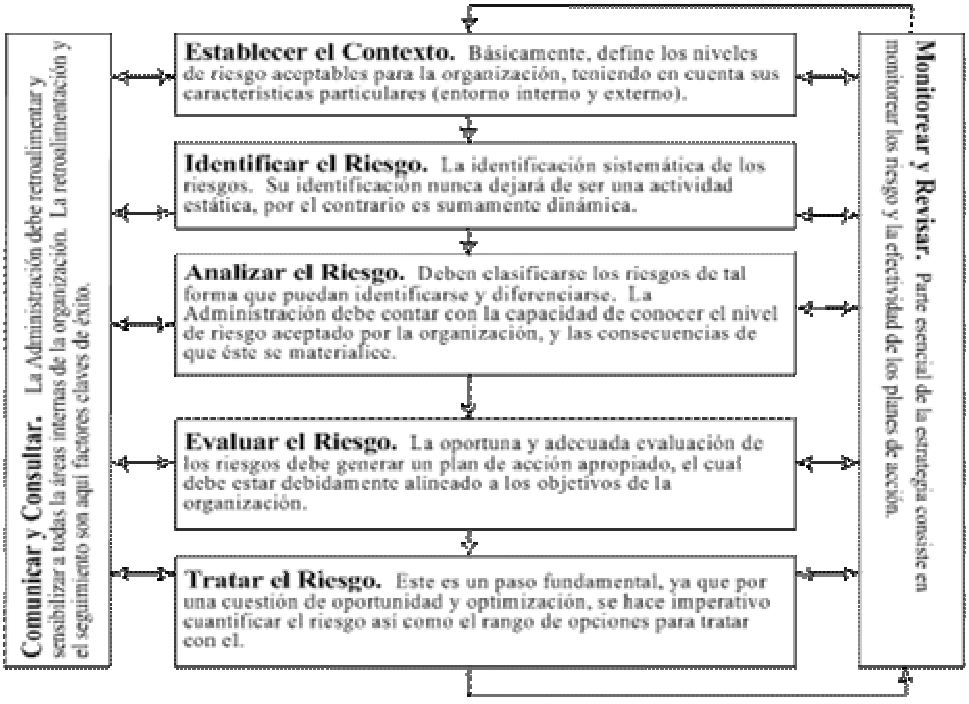
Un día después, con el dinero en su poder, el funcionario volvía a cancelar la póliza a nombre de una persona desconocida, para lo cual tomaba el número de cédula y el nombre de cualquier persona que apareciese en la Base de Datos del Registro Civil.

Para cerrar este "*portillo*" existente en el sistema de información, se procedió a eliminar de la red de cómputo, la posibilidad de reabrir una póliza de vida no vigente.

Es necesario que aprendamos sobre la lamentable situación ocurrida en el INS, la que nos debe llevar al cuestionamiento sobre la existencia de puntos débiles (riesgos) en la infraestructura tecnológica de nuestras organizaciones, que pueden ser aprovechados por individuos inescrupulosos.De aquí que debamos reflexionar seriamente en cómo enfrentar el problema oportunamente.

III Parte: Conclusiones y Recomendaciones

Dentro de este dinámico contexto, la Administración puede considerar la aplicación de la norma **AS/NZS 4360:1999** (para la Administración de riesgos).Para efectos ilustrativos, a continuación se presenta la Matriz de la Administración de Riesgos contenida en la citada norma:



Si bien es cierto que el marco jurídico establece definiciones para calificar y penalizar (esto es después de los hechos) el fraude informático, la mejor estrategia que debe asumir la Administración para minimizar o eliminar eficazmente el crimen o delito informático será siempre el diseño de controles preventivos, detectivos y correctivos.En este sentido, debemos

reconocer la necesidad de realizar un gran esfuerzo para disminuir al máximo la brecha existente entre la creación, adopción y aplicación de leyes en contra del fraude informático, y el avance tecnológico (siempre caracterizado por ser continuo y acelerado).

Un elemento de vital importancia para afrontar este problema, es que los niveles gerenciales se interesen por implementar oportunamente políticas y lineamientos integrales para hacer frente a los ilícitos informáticos, especialmente cuando se tenga evidencia , entre otros, de debilidades en la seguridad lógica y física de la infraestructura tecnológica, insuficiente documentación de los sistemas de información en operación, inconformidades con el servicio de soporte técnico que brinda un determinado fabricante, deficiencias en la asignación y distribución de las responsabilidades del personal, así como en su debida capacitación.

Finalmente, debe tomarse en consideración, que en cada organización, la Administración Superior debe determinar cuáles son los factores de riesgo que comprometen la estabilidad y la continuidad de los servicios que presta., de ahí la importancia enorme de analizar a fondo la ventajas de escoger y utilizar una buena metodología para el control de los riesgos, en especial del fraude informático.