EVIDENCIA DIGITAL E INFORMÁTICA FORENSE
Autor: Lic. Salvador Clemente Beltrán Santana

1.- Globalización y avance tecnológico

- La infraestructura tecnológica disponible y el entorno de globalización han transformado el concepto tradicional de información. El volumen de datos que cruza hoy en día por cualquier organización ha crecido en forma exponencial. La información es la principal mercancía que se intercambia cotidianamente alrededor del mundo. Lo anterior, implica necesariamente la circulación de mayor volumen de información en los intercambios intra e inter institucionales.

- No todos estos intercambios son electrónicos, pero cada vez es más común que la información estratégica y operacional, de cualquier organización, se procese en formato digital y circule por amplias redes informáticas.

- Este entorno sugiere que más que empresas públicas o privadas delimitadas, debamos pensar en la red institucional, local y global, en la que opera la organización –proveedores, subcontratistas, mayoristas, filiales, aliados, competencia, y/o los individuos involucrados en actos delictuosos.

- Cada vez es mayor la necesidad de dar seguimiento puntual a todos los procesos en los que está involucrada la organización y de proteger la información institucional.

- La comunicación por vía electrónica se debe valorar en sus distintas fases: desde la generación, almacenamiento y registro, hasta la administración, envío y validación de la información. Cada uno de estos procesos puede convertirse en ventana de vulnerabilidad para cualquier organización.

- En este contexto se hace necesario analizar no sólo el origen y el destino de la información sino también la vulnerabilidad de los operadores y los medios de transmisión utilizados, el valor estratégico y la legalidad de los mensajes, las características e intereses de los destinatarios, y la capacidad de la organización para controlar la información que fluye desde y hacia ella.

- Dado que la mayor parte de la información se maneja hoy en día en formato digital, es necesario contar con acceso a los equipos y con el capital humano con capacidad para realizar este tipo de análisis de inteligencia con adecuados soportes metodológicos y con técnicos confiables y con experiencia.

2.- Seguridad Informática

- Uno de los hechos más destacados en el actual entorno nacional e internacional es la creciente relevancia de la informática en el funcionamiento cotidiano, tanto de empresas privadas como de agencias gubernamentales.

- Paradójicamente, las organizaciones son cada vez más vulnerables frente a los problemas legales, delictivos y de fuga de información a través de sus sistemas de cómputo. Esta situación puede llegar a ser crítica si consideramos que hoy en día la mayor parte de la información, estratégica y operativa de empresas públicas y privadas, se encuentra en medios electrónicos –según cifras especulativas hasta el 97% de la información que hoy circula se procesa en medios electrónicos aunque su formato final sea impresión en papel y tinta.

- Anualmente el FBI y el Instituto de Seguridad Computacional de EUA realizan un Encuesta sobre Cuestiones de Seguridad Informática. En el estudio de 2002, basado en las respuestas de 503 empresas, instituciones financieras y médicas, universidades y agencias gubernamentales, se encontró lo siguiente:
    - 90% sufrió violaciones a la seguridad informática en el último año.
    - 80% reportó pérdidas financieras asociadas a dichas violaciones
    - 40% detectó penetración por “hackers” externos.
    - 74% reportó intrusión en sus conexiones de Internet.
    - 32% reportó negación de servicios por ataques masivos.
    - 19% experimentó sabotaje en redes de datos.
    - 6% reportó ser víctima de fraude financiero.
    - 85% tuvo incidentes de contaminación por virus.
    - 69% reportó pérdida y robo de computadoras portátiles.
    - el robo de información propietaria ascendió a más de USD 170 millones.
    - Sólo el 34% reportó los incidentes a las autoridades correspondientes.

- ¿Cómo se puede controlar la información que entra y sale de la organización? Existen mecanismos que permiten proteger los equipos de cómputo y restringir la presencia de “hackers” y “visitantes no deseados”; sin embargo, tanto los avances tecnológicos continuos como la fragilidad del factor humano generan ventanas de vulnerabilidad en la organización.

- Algunas organizaciones asignan recursos para salvaguardar las unidades de cómputo y las redes en las que operan; así, construyen barreras (“escudos digitales” y “blindajes electrónicos”) a fin de proteger su información e impedir que personas ajenas a la organización penetren sus sistemas institucionales. Lo que no es tan común es que adopten una

actitud proactiva para detectar filtraciones o mal uso de la información desde el interior de la organización.

- El seguimiento de la información que se procesa dentro de la organización requiere de técnicas y métodos de investigación que permitan explorar, sistemáticamente, las comunicaciones que los empleados realizan a través de computadoras o por cualquier otro medio electrónico.

3.- Informática Forense

- En este contexto se ha venido desarrollando, en años recientes, el concepto de Informática Forense. Esta metodología de investigación sirve para apoyar a las empresas e instituciones gubernamentales cuando surgen problemas de carácter delictivo o de alto riesgo en sus sistemas de cómputo.

- En México el desarrollo de estos procesos de investigación es aún incipiente, razón por la cual **Grupo Coppan S.C.** en asociación con otros especialistas, decidió la creación en México del **Laboratorio de Informática Forense GC, S.C.** para atender las necesidades de informática forense de organizaciones públicas y privadas.

- El **Laboratorio de Informática Forense GC, S.C.** cuenta con la infraestructura y los apoyos necesarios, a nivel nacional e internacional, para realizar sus trabajos con tecnología de punta, el más alto nivel de profesionalismo y, ciertamente, la discreción y confiabilidad que exige la realización de estas tareas.

4.- Desafíos Institucionales

- ***Desconocimiento.-*** Existe un conocimiento limitado sobre qué es la Informática Forense y qué se puede hacer con la evidencia digital. Existe también poca familiaridad con herramientas y procesos que permiten obtener evidencia digital.

- ***Complicidad.-*** Existe siempre la amenaza de una posible complicidad de agentes internos y externos para lograr infiltrarse por vías electrónicas.

- ***Poca credibilidad.-*** Existe poca credibilidad en la obtención de evidencia digital que incrimine a un delincuente o empleado desleal.

- ***Confiabilidad.-*** Existe la urgente necesidad de presentar información confiable y cumplir con estándares a nivel internacional. El seguimiento puntual de los productos informativos puede evitar la pérdida de importantes activos institucionales a través de la comisión de conductas ilícitas como:

    - fraude financiero y fiscal,
    - lavado de dinero y desviación de recursos,
    - robo de propiedad intelectual y secretos comerciales,
    - filtración de información clave a competencia y,
    - fuga de información y espionaje empresarial, entre otros.

- ***Marco Legal.-*** Necesidad de generar un *nuevo marco jurídico nacional e internacional*. La velocidad de los intercambios de información está transformando el entorno jurídico lo que obliga a las organizaciones a adecuarse constantemente a los nuevos parámetros.

- ***Necesidades institucionales.-*** Cada vez es más común tener que presentar información institucional a solicitud de diversas autoridades. Toda organización debe ser capaz de producir la evidencia que se solicite para demostrar la transparencia y legalidad de sus prácticas.

- ***Apego a las normas institucionales.-*** Desconocimiento de herramientas informáticas y procedimientos de búsqueda que permitan verificar que el uso de la información, los equipos, las bases de datos y, en general, los productos informativos de la organización, responden a las normas institucionales.

- ***Seguimiento de flujos de información***.- Es necesario monitorear los flujos de información de la organización ante la sospecha de comportamientos ilícitos, tanto a nivel preventivo como reactivo.

- ***Conflictos de interés***.- En la aplicación indiscriminada de medidas y contramedidas electrónicas avanzadas para obtener evidencia que permita incriminar a un delincuente o empleado desleal que está afectando los intereses de la institución.

5.- Riesgos existentes

Generalmente los riesgos están asociados con acciones u omisiones no-deseadas de parte del personal de la organización:

- **Divulgación de información sensible**
  - ✓ Robo.
  - ✓ Espionaje.
  - ✓ Sustracción.
  - ✓ Mal uso.

- ✓ Ingeniería Social

- **Abuso de privilegios**

  - ✓ Borrado de información.
  - ✓ Fraude (transacciones falseadas).

- **Ataques activos**

  - ✓ Implantación de virus, caballos de Troya, etc.
  - ✓ Provocación de caídas de servidores y/o ruteadores (negación del servicio)

6.- Procesos de investigación y análisis

- La Informática forense se refiere al análisis y evaluación a fondo de la información que circula en los equipos, plataformas y sistemas de una organización. Este trabajo no se circunscribe a recuperar información de un equipo de cómputo, sino también al trabajo de inteligencia para evaluar posibles delitos cibernéticos.

- La informática forense es una disciplina auxiliar en la búsqueda de información estratégica y en el descubrimiento de evidencia en los sistemas y redes informáticas. El análisis de inteligencia, última fase de la informática forense, debe producir informes concretos y concluyentes. Una vez obtenida la información de la fuente cibernética se le debe dar la interpretación adecuada para obtener las pruebas necesarias para la solución del problema.

- En casos judiciales, la información recuperada es inútil a menos que sea admitida en juicio. Es por ello que se requieren expertos forenses para

asegurar que la información obtenida es la adecuada y certificar que no han habido alteraciones en el proceso de recopilación correspondiente.

7.- Evidencia Digital

Es un tipo de evidencia física, menos tangible que otras formas de evidencia (DNA, huellas digitales, componentes de computadores)

Características:

- ✓ Puede ser duplicada de manera exacta y copiada tal como si fuese el original.
- ✓ Con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada, comparada con la original.
- ✓ Aún si es borrada, es posible, en la mayoría de los casos, recuperar la información.
- ✓ Cuando los criminales o sospechosos tratan de destruir la evidencia, existen copias que permanecen en otros sitios del sistema.