Ética y Seguridad Informática

Autor: William Barrios
Editor: Edufuturo
Palabras: 730

La idea de una reglamentación informática comenzó a surgir desde el momento que las personas comenzaron a usar la tecnología para dañar a otras personas. La ética evita que las personas tengan prácticas que dañen a los demás o lastimen la integridad de las cosas que sirven a todos. A raíz de esto muchas empresas y algunos gobiernos han comenzado a implementar códigos o grupos de reglas que los empleados o usuarios de tecnología deben observar y cumplir.

Código Ético:

Estos código son establecidos e implementados por las instituciones o empresas. Los empleados deben regirse a los mismos. A continuación te muestro un ejemplo, no es el único y seguramente puede variar de empresa a empresa, pero te puede servir de guía.

1. No usarás una computadora para dañar a los demás.
2. No interferirás con el trabajo de los demás.
3. No indagarás en los archivos de los demás.
4. No utilizarás una computadora para hurtar o robar.
5. No utilizarás la informática para realizar fraudes.
6. No copiarás o utilizarás software que no hayas comprado.
7. No utilizarás los recursos informáticos ajenos sin la debida autorización.
8. No te apropiarás de los derechos intelectuales de otros. (copy-paste)
9. Deberás evaluar las consecuencias sociales de cualquier código (programas o aplicaciones) que desarrolles.
10. Siempre utilizarás las computadoras de manera que no se violenten los derechos de los demás.

Delitos Informáticos:

En base a la experiencia de estos años de uso de internet, las empresas y los usuario de internet ya pueden hacer un listado de los posibles delitos que cometen las personas no éticas. El listado que se muestra a continuación es un ejemplo de estos posibles delitos.

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
4. Lectura, sustracción o copiado de información confidencial. (Con el fin de dañar)
5. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
6. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa (falsa).
7. Uso no autorizado de programas de cómputo.
8. Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas.
9. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

10. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
11. Intervención en las líneas de comunicación de datos o teleproceso.
12. Programación de instrucciones que producen un bloqueo total al sistema.
13. Destrucción de programas por cualquier método.
14. Daño a la memoria.
15. Atentado físico contra la máquina o sus accesorios.
16. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
17. Secuestro de soportes magnéticos (discos duros o memorias portátiles) entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).
18. Acceso no autorizado: Uso ilegitimo de password's y la entrada de un sistema informático sin la autorización del propietario.
19. Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
20. Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
21. Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
22. Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
23. Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Este listado de posibles delitos está reglamentado en la mayoría de las empresas, pero no en la mayoría de países y es allí en donde radica la debilidad, ya que las empresas y las personas se ven vulnerables ante los ataques de personas que desean dañar y ven como no existen leyes que los puedan proteger. Además, el robo de información (que es el caso más común) es muy difícil de demostrarse ante los entes juzgadores.

Cada año las empresas y las personas invierten mucho dinero en la seguridad de la información, colocando e instalando firewalls, antivirus, y restringiendo a las personas que tienen acceso a los equipos que administran la información.

El uso incorrecto de la información y de las computadoras siempre será vista como no ético.

Referencia:

https://irfeyal.wordpress.com/investigaciones/etica-informatica/

http://bvs.sld.cu/revistas/infd/n809/infd1909.htm