Informática forense – Consejos Prácticos

Infosecurity 2015 - Security is a war

Sheraton Libertado

Ciudad Autónoma de Buenos Aires, septiembre 2015

BDO

Introducción

Para llevar a cabo un fraude, se utilizan los dispositivos electrónicos como medios. Estos no son parte indispensable para su concreción pero necesarios para su diseño y organización.

En este agrupamiento podemos destacar elementos tecnológicos como los teléfonos celulares o herramientas informáticas de comunicación como los correos electrónicos.

Uno de los escenarios más frecuentes en la empresa es el de la comprobación de posibles infracciones e incumplimientos de sus deberes contractuales por los trabajadores, mediante el uso de equipos informáticos o mediante una actividad que deja rastro en archivos almacenados en los mismos.

Estas infracciones podemos clasificarlas en 2 grandes grupos:

✓Utilización de las tecnologías de información como medio.
✓Delitos informáticos.

Introducción

Introducción

No es raro para nosotros al realizar una investigación forense descubrir que la organización solicitante ha destruido o alterado inadvertidamente las pruebas que tenían la esperanza de descubrir

Las acciones del personal sin experiencia en el manejo de evidencia puede dar lugar a una situación en la que queden muy pocos datos relevantes.

Si bien cada caso es único, hemos realizado una listas de las cosas que, si se siguen, nos ayudará a ayudarle.

Que no deben hacer

- No intenten “pegarle una miradita” u operar el dispositivo
- No use a su área de IT a menos que tenga experiencia en el manejo de evidencia digital
- No se demore, cuanto más rápido tome medidas mayores serán las posibilidades de salvar la evidencia
- No levante sospechas, no le diga a nadie a nadie acerca de la investigación a menos que sea estrictamente necesario
- No deje afuera a su departamento de recursos humanos, ellos pueden asesorarlo en los temas legales

Que no deben hacer

- No improvise sobre la mejor acción a realizar, si tiene dudas llame a un especialista en informática forense
- No dude en contactar a la policía si cree que se pudo haber realizado un hecho delictivo
- No se vea tentado a destruir información, eso puede rastrearse y puede tener serias consecuencias legales
- No ejecute nada en el dispositivo o realice actividades que puedan modificar algo del estado actual

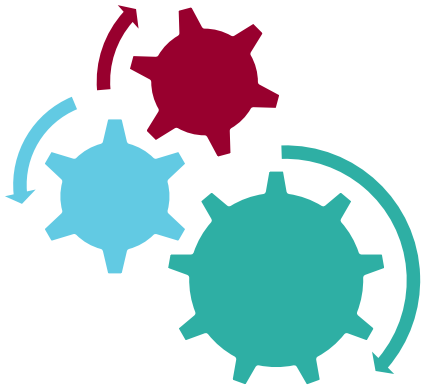
Que pueden hacer

- Asegure el dispositivo para que ninguna persona no autorizada tenga accesos a él
- Si el dispositivo esta apagado, déjelo así!!
- Si esta encendido, dejo así!!
- Si esta encendido, desconecte los cables de red, apague el WIFI y/o BT
- Si no es posible lo anterior, desenchufe el equipo (si es un servidor apáguelo) o saque la batería
- Solo notifique a las personas esenciales que una investigación va a realizarse

Que pueden hacer

- Tome notas sobre la gente involucrada, declaraciones, fechas, etc.
- Reúna todo dispositivo a los cuales tenga acceso que pueda tener información o elementos de pruebas importantes como por ejemplo pendrives, cds, teléfonos, cámaras, etc.
- De ser posible no comente el tema de investigación
- Busque la asesoría de una empresa de computación forense para conocer los pasos a seguir en la investigación

Nuestra metodología de trabajo



1. **AUTORIZACIÓN** -> Se requiere autoridad legal para llevar a cabo una búsqueda o incautación de datos.
2. **CADENA DE CUSTODIA** -> Documentación cronológica de manejo de pruebas para evitar acusaciones de manipulación o mala conducta.
3. **ADQUISICIÓN** -> Debe ser cuidadosamente duplica y luego hash para validar la integridad de la copia.
4. **HERRAMIENTAS** -> Las herramientas que se utilizan deben ser validadas para garantizar la fiabilidad y exactitud.
5. **INDAGACIÓN** -> Técnicas de investigación y análisis para examinar la evidencia.
6. **CALIDAD** -> Los procedimientos y conclusiones del análisis forense debe ser repetible y reproducible por los mismos u otros analistas forenses.
7. **INFORME** -> Documentar su procedimiento analítico y las conclusiones.

Consejos para estar preparado

- Comunicar políticas a la comunidad de usuarios, y asegurarse de su cumplimiento
- Mitigar la ecuación SEGURIDAD versus USABILIDAD
- Defenderse ante las amenaza Ingeniería Social
- La concientización del usuario optimiza el perfil global de seguridad
- Fomentar al uso de hábitos seguros y desalentar los comportamientos riesgosos

Consejos para estar preparado

- Cambiar la percepción del usuario respecto de la Seguridad de la Información
- Informar a los usuarios sobre cómo reconocer y reaccionar ante amenazas potenciales
- Educar a los usuarios sobre técnicas de seguridad de la información que pueden usar

Informática Forense

Aseguramiento de Procesos Informáticos

Diego R. Hvala
Gerente
dhvala@bdoargentina.com

Gustavo L. Amago, CISA
Gerente
gamago@bdoargentina.com

José Rondeau 2664, PB. C1262ABH
Buenos Aires, Argentina
Tel.: 54 11 4106 7000
Fax: 54 11 4106 7255

www.bdoargentina.com