MEDIDAS PREVENTIVAS CONTRA LA FUGA DE INFORMACION

· Estimule la destrucción de todo el papel desechado.
· Adquiera destructoras de documentos apropiados a sus necesidades.
· Use destructoras de corte cruzado para altos niveles de seguridad.
· Las formas continuas de computación y altos volúmenes requieren de una destructora industrial de alta capacidad.
A los husmeadores les encanta cuando los papeles confidenciales se esconden en sitios previsibles en la oficina, si no los necesita más destrúyalos. No dependa la destrucción a los compradores de papel reciclable.

Destrúyalos antes de venderlos. No se olvide de tener destructoras al lado de las fotocopiadoras y en las casas de los ejecutivos que también trabajan desde sus casas.

Este elemento que puede ser usado como un símbolo de estatus puede tener un efecto positivo hacia la empresa. Algunas empresas aluden el empleo de destructoras para proteger la privacidad de sus clientes. Un servicio que no ofrecen sus competidores.

Verifique y fotocopie, las credenciales con las órdenes de trabajo de cualquiera que este efectuando trabajos técnicos como sub-contratado en sus oficinas. Haga un doble chequeo. Verifique que el trabajo ha sido requerido y sea necesario.

Verifique sus cerraduras y el sistema de alarma periódicamente. Asegurase que cada componente este trabajando. Se sorprendería al saber cuanta confianza se tiene sobre cerraduras malas y sensores de alarmas defectuosos. Si el control sobre las llaves se ha perdido hace tiempo, ataje el problema inmediatamente. Cambie las cerraduras e implemente un sistema de control que realmente sirva. Considere las tarjetas de control de acceso.

EN EQUIPOS DE COMPUTO

· Desarrolle un sentido comunal de responsabilidad en materia de seguridad.
· Limite el acceso físico a las computadoras por extraños.
· Limite el acceso por software. Use claves no convencionales.
· Nunca deje un terminal activo. Siempre cierre su sesión.
· Reporte las intrusiones sospechosas y/o datos alterados.
· Remueva los datos sensitivos de la computadora cuando no se necesiten más.
· Proteja los medios de respaldo disquetes, CD-DISCOS DUROS ETC
· Los comandos de copiar pueden mover datos sensibles inadvertidamente.

· No confíe en los comandos de borrado, Déle formato si es posible.
· Borre los discos antes de desecharlos o transferirlos para otro uso o usuario.
· Desconecte la PC de la red cuando no se use.
· Las computadoras con acceso vía teléfono necesitan protección de acceso.
· No use software prestado o no solicitado.

· Haga un respaldo de sus datos periódicamente.
· Reformatee los discos duros antes de retirar las computadoras obsoletas.
· No hable sobre la seguridad de su sistema con nadie que usted no conozca, sin importar lo que ellos le digan.

EN TELEFONOS

· Restringa el acceso directo por llamada hacia la central telefónica, característica empleada por los técnicos de mantenimiento remoto.
· Algunos peligros de estos accesos no autorizados son:
· Completa desprogramación de la central.
· Reprogramación secreta que permita acceder a...
· Llamadas gratis,
· Correo de voz,
· Características ejecutivas de invalidación (que permiten el acceso forzado sobre las líneas ocupadas),
· Creación de puentes (permite el monitoreo silencioso desde otros teléfonos),
· Intercomunicador y manos libres (permite el monitoreo del cuarto desde otros teléfonos),
· Y monitoreo del registro de todas las llamadas salientes efectuadas.