Algunos análisis, situaciones, riesgos y prevención delespionaje industrial. Si bien es cierto que la palabra espionaje se asocia directamente al secreto de los Estados, y la forma de conseguir información clasificada relacionada con fines militares, también es cierto que está directamente asociada a los secretos que tienen las industrias para realizar sus actividades y operaciones comerciales.
Con el devenir del tiempo, esta forma de espionaje ha tenido un crecimiento relativamente alto en todo el planeta y ha sido blanco de ello casi cualquier tipo de industria o comercio. Una labor de espionaje considerada como aceptable dentro de los negocios se esconde dentro del oficio llamado mercadeo, donde de formas variadas y dentro del marco legal, se tratan de conocer y obtener secretos de comercialización, fórmulas, estrategias de fabricación y otros factores que permitan ser competitivos en el mercado.
En este artículo se exponen ciertos factores que le ayudaran a prevenir y combatir los intentos de espionaje a los cuales pueda estar expuesto, y de acuerdo a cómo usted se considere como un posible candidato a ser espiado.

Espionaje Industrial

Este es un tema que se puede considerar como Tabú dentro de cualquier conversación empresarial o corporativa, ya que implica muchos factores como los son: la confianza, la responsabilidad, la moral, la prevención, la seguridad, etc.
Cuando las corporaciones se sienten amenazadas, se efectúan reuniones de alto nivel, y comparten o no sus inquietudes con el Jefe de seguridad. Buscan asesorías con las empresas que puedan estar relacionados con este tipo de labor, como son las agencias de detectives, empresas de vigilancia, abogados, o con personas allegadas que les pudieran orientar al respecto.
Finalmente logran contactar con alguien que les pueda dar una respuesta a sus inquietudes, que dispongan de los medios tecnológicos para determinar la existencia de posibles micrófonos, y que les den la certeza si están o no siendo espiados. Lamentablemente no existen muchas empresas o personas que tengan un conocimiento profundo sobre el tema, o que se dediquen dentro de sus actividades en el mundo de la seguridad a la contra inteligencia electrónica.
Son muchos los factores que se deben tomar en cuenta al momento de efectuar un levantamiento de este tipo de seguridad, para determinar el cómo ha sido la fuga de información, pero principalmente hay que hablar con la o las personas que se sientan espiadas, para conocer que fue lo que lo indujo a pensar en ello. Para esto es necesario establecer una confianza plena entre ambas partes, ya que es importantísimo conocer ciertos factores de operatividad, incluso de la vida privada, para ir filtrando las diversas posibilidades que conducen a una fuga de información.
En conclusión, si usted se siente predispuesto a ser atacado por alguna forma de espionaje, encontrara a continuación una serie de tips que le permitirán minimizar estos riesgos, y como contactar a empresas especializadas en la materia.

¿Que hace atractivo el espionaje?

· Bajo riesgo, altas ganancias. · Bajos niveles de moralidad. · Bajos niveles de responsabilidad.
· Aumento de la competencia en el mercado.
· La tecnología para el espionaje es de bajo valor y fácil de adquirir.

· La escucha furtiva y el espionaje son en algunas culturas moralmente aceptado.

¿Quién es un probable espía?

No hay una respuesta exacta, pero una buena descripción ha sido elaborada por la Asociación de Control del Espionaje Industrial y sus Contramedidas.

· De 21 a 35 años de edad. Mujer u hombre. · Graduado de Bachiller con baja puntuación académica. · Liberal, con empleos de corta duración. · Con problemas monetarios – sueldo bajo, mal administrado.
· Experiencia en Inteligencia Militar.
· Conocimiento policial o similar.
· Considerado un extraño o solitario.
· Excluido de una carrera policial o militar.
· Romántico, con algún hobby o interés. (Escritor, fotógrafo, buceo, etc.)
· Colecciona literatura paramilitar.
· Un activo interés en armamentos, a veces con entrenamiento.
· Reclutado por medio de un aviso de alguna agencia de detectives.
· A veces un empleado de bajo nivel o sin oficio.
· Habilidades musicales, Ajedrez, Matemáticas, etc. - ...que están asociadas con rompimiento de claves o espionaje.

Tenga en mente esta lista, pero recuerde… Cualquiera puede ser un fisgón.

¿Quiénes son esos fisgones?

Competidores, vendedores, investigadores, consultores de negocios, colegas buscando escalar posiciones, jefes de producción, socios sospechosos, la prensa, negociadores empresariales, sindicatos, agencias gubernamentales. La lista es larga.

¿Porque puedo ser un blanco posible?

El Dinero y el Poder son las dos mayores razones que están detrás de las actividades ilegales de la vigilancia. Si cualquier cosa que usted dice o escribe puede aumentar en otros su riqueza o estatus, usted es un posible blanco..

¿Es común el Espionaje?

Sí. Las noticias están llenas de historias acerca de información robada en el ámbito mundial. En verdad, muchas de las noticias tienen un comienzo debido a un proceso de escape de información. El más famoso: Watergate

¿Me puedo Proteger?

Si, el espionaje se puede prevenir. Si se conocen las debilidades, puede tomar las medidas correspondientes de precaución. Algunos trucos de espionaje son obvios, si uno se para a pensar en ello. A veces son a través de claros abusos de la tecnología con la que convivimos a diario. Todas son devastadoras. El tiempo ha demostrado que muchos de los trucos han sido empleados en forma reiterada, y satisfactoriamente. Prepárese para contra-atacarlas

A continuación podrá leer unas maneras simples, pero efectivas para conseguir información sensible y como protegerse de este tipo de situaciones.

Téngalas presentes en sus actividades diarias con la finalidad de minimizar estas debilidades, así estará mejor protegido contra la fuga de información.

1 – Rastrear la Basura

El husmear entre la basura es uno de los principales objetivos y métodos empleados en la actualidad para el espionaje industrial.
Increíblemente, pero robar la basura es una actividad legal en muchos países. Según algunas decisiones tomadas en materia de leyes, no hay una expectativa de propiedad privada o de pertenencia, una vez que el objeto esta dispuesto en la basura para que lo recojan. Mucho de los fragmentos de información sin importancia están estrechamente conectados.
El proceso del contraespionaje tiene como objetivo el reducir estas partes del rompecabezas. La desintegración de la documentación es parte fundamental de ese proceso.
Tips y Recomendaciones · 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.

El error de comprar una sola maquina grande...
El adquirir una sola maquina grande para destruir la documentación de todos es un error. La Razón: Hay personas tan ocupadas que no se preocupan de ese detalle. La mejor opción es la de comprar pequeñas maquinas tipo papelera con corte cruzado.
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.

2 – El espía ocasional

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. Esto incluye: · Técnicos en Telecomunicaciones ·
Técnicos de Computación
· Técnicos de Equipos de Oficina
· Personal de Mantenimiento
· Personal de Limpieza
· Electricistas
· Técnicos de Alarmas y/o CCTV
Haga que alguien de confianza que represente sus intereses, acompañe a estos trabajadores mientras estén en su propiedad. Si es posible, que terminen sus labores durante el horario normal de oficina. Las personas sub-contratadas y empleados de empresas no autorizadas nunca se les deben permitir que ingresen en áreas que contengan información sensible.
Solo un espía profesional se puede jactar que cualquier edificio es penetrable a cualquier hora, simplemente presentándose como el reparador del sistema de aire acondicionado. Su soporte

incluirá una tabla con documentación y un termostato industrial, como artículo opcional, un radio transmisor y una gorra. Si se le traba el ingreso, podrá aducir que no regresara sino en dos semanas, ya que tiene mucho trabajo, tú sabes… Nadie querrá responsabilizarse por no dejar entrar a este reparador.

Otros consejos...
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.

Aunque la mayor parte en la búsqueda de información involucra otros métodos listados en este resumen, la escucha electrónica es la más devastadora. Los más privados e irrefutables secretos son sus blancos de ataque.
Es un error común el decir… “Cielos, me estoy volviendo paranoico”, cuando se comienza a sospechar de una escucha electrónica. Piense... Usted no tendría sospechas si todo esta bien. Algo esta mal.
Acciones a tomar... · No hable de sus sospechas con otros a menos que ellos realmente lo necesiten saber. · No hable de sus sospechas en las áreas sospechosas. · No intente una solución hecha por usted mismo.
· No malgaste su dinero comprando juguetes anti-espías.
Solicite la ayuda de un profesional sin demora. Contrario a lo que se ve en la televisión, en las películas, o los catálogos, la detección de los micrófonos y transmisores es un trabajo intenso de conocimiento y equipamiento. Es altamente factible que un grupo profesional de rastreadores tenga invertidos en equipos cerca de $50.000,00 dólares o más.
Este personal tendrá un profundo conocimiento y experiencia en seguridad, investigaciones, electrónica y comunicaciones. No se moleste en buscarlos en las páginas amarillas. Contacte a un Director de Seguridad Corporativo o una organización profesional de seguridad para una recomendación con conocimiento. Vale la pena el esfuerzo.

4 – Información Digital
El espionaje enfocado hacia las computadoras, Laptops, PDA, redes y puertos de acceso remoto esta en ascenso. Explique enfáticamente a todo el mundo que contenga datos sensitivos en sus equipos, el porque es necesario tomar precauciones de seguridad. Por ejemplo: La regla de “proteja su Laptop siempre”.
El costo de reemplazo no es la única perdida, considere lo siguiente... · Los invaluables datos de confidencialidad y competitividad.
· El tiempo y esfuerzo que tomo en recabar esa información.
· El tiempo que tomara en reconstruir los datos perdidos.
· Los teléfonos de los módems de la oficina y claves de acceso a las redes están en el disco duro.
Cuando esta información se pierde, la empresa estará vulnerable a...
· Robo de mercancía
· Corrupción de la base de datos del Servidor
· Sabotaje por Troyanos, Virus, puertas traseras, etc.

Por lo tanto habrá: · Menos ingresos o ganancias.· Perdida de la confianza de sus clientes.
Algunos tips adicionales... · 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. · Asegure los materiales relacionados: discos, cintas, disquetes, etc. · 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-ROM, DAT.
· 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.

5 – Tecnologías Amigables

Los avances tecnológicos nos ofrecen muchas alternativas a la comodidad en las comunicaciones, como ejemplo los teléfonos portátiles. Pero desgraciadamente también proveen de oportunidades a los fisgones.
Algunas de las vulnerabilidades que debe conocer...
· Contestadotas Telefónicas. Los mensajes dejados en muchas de estas máquinas pueden ser accesadas remotamente usando un código de dos o tres cifras, fácil de hackear. La mayoría de las personas nunca cambian el código de fabrica que viene en las nuevas maquinas. Algunas poseen la característica de escucha remota. Léase el manual con detenimiento y cambie lo que sea necesario para aumentar su protección.· Correo de Voz. Es la versión ejecutiva del contestador telefónico, este también puede ser monitoreado. Emplee una clave lo mas larga posible. Cámbiela a menudo. · Monitor de Bebes. Son en realidad, micrófonos de alta sensibilidad que transmiten las 24 horas continuas. Son monitoreadas por ladrones para darse cuenta si la casa esta vacía, y también por vecinos entrometidos. Use estos monitores con moderación. Colóquelos con un rele actuado por reloj. Mantenga el cuarto del bebe cerrado en su ausencia.
· Equipos de Fax I. Algunas maquinas usan rollos desechables de película negra para sus procesos de impresión. Estos rollos usados contienen una copia de todos los faxes recibidos. Deseche apropiadamente estos rollos. El recibir faxes después de horas laborales es como recibir cartas sin sobres. Los mensajes pueden ser leídos rutinariamente por los empleados que matan el tiempo dando vueltas por la oficina y por guardias que están aburridos. La solución, guarde estas maquinas en una caja de seguridad que permitan su operación.
· Micrófonos Inalámbricos. A los presentadores en las conferencias les encanta usarlos. Desdichadamente, estos micrófonos tienen la suficiente potencia para radiar con claridad a unos 400 metros a la redonda. No los utilice en cualquier reunión en la cual se presenten

asuntos de la alta gerencia y donde no se invitaría a cualquiera.
· Maquinas Dictadoras. Usted puede destruir documentos, cerrar las copias de los archivos, y enviar los originales en sobres de seguridad… pero la cinta con el dictado esta en la maquina de la secretaria, esa cinta puede ser fácilmente reemplazada llevándose esos documentos importantes.

6 – Telefonía portátil
Los teléfonos inalámbricos y los celulares están catalogados como los blancos más fáciles para su interceptación. Contrario a la creencia popular, la recepción de las conversaciones es generalmente muy nítida, sin estática o interferencia. Cada una de las palabras puede ser entendida. Úselos con discreción. La recepción de las comunicaciones de los celulares puede ser recibida a varios kilómetros de distancia. Adicionalmente de ser un provecho para el espía, se ha convertido en un pasatiempo de personas sin escrúpulos que pueden también vender sus hallazgos.
El monitorear las transmisiones telefónicas es un acto ilegal. No confíe en las leyes para proteger su privacidad, Generalmente no son casos concluyentes.Las nuevas técnicas de monitoreo sobre celulares incluyen sistemas computarizados totalmente automatizados. Esto permite el monitoreo durante las 24 horas, de celda a celda, sin la intervención humana.
Para proteger las conversaciones... · Llame al número que no identifique a la compañía o que de otro tipo de información pertinente. · Use el nombre de pila y palabras en código para identificar los proyectos especiales.
· Hable generalizadamente y en términos sin interés. Los teléfonos inalámbricos pueden recibirse hasta un kilómetro de distancia. Úselos convenientemente para contestar las llamadas, luego devuelva la llamada por el teléfono normal para una mayor – no absoluta – privacidad.
Si usted debe obligatoriamente usar los teléfonos inalámbricos, compre de los que operan a la frecuencia de 900 MHz y que empleen la tecnología de dispersión digital en el espectro (digital spread spectrum technology).
Otros teléfonos que pueden ser interceptados incluyen: · Teléfonos comerciales de las aerolíneas y transporte terrestre o marítimo.
· Llamadas de larga distancia transmitidas vía satélite.
· Llamadas de larga distancia transmitidas vía enlaces de microondas.
· Llamadas telefónicas usando las computadoras (VoIP).
· Llamadas usando la red Lan o Wan por frame relay.

7 – Ataque a las líneas telefónicas
Los teléfonos comerciales ricos en características amigables le proveen al espía de una gran variedad de métodos de escucha. Los teléfonos en si proveen de la energía eléctrica, tienen micrófonos y parlantes incorporados que pueden servir para dobles propósitos, y tienen el suficiente espacio para esconder artilugios electrónicos de espionaje o efectuar puentes internos. Inclusive mediante comandos generados desde la computadora que verifica el proceso de la central telefónica.
Lista de verificación sobre telefonía... · Tenga un alto grado de seguridad en los cuartos donde esta la central telefónica. · 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.
Recomendación: Remplace el MODEM de acceso normal – el cual conecta la central con la línea externa – con uno que tenga la característica de call back. Con esta configuración, las conexiones del PBX están limitadas a números telefónicos autorizados. · Asegure los terminales que programan la central.
· Este seguro de la honestidad del Administrador del Sistema.
· Conduzca inspecciones regulares buscando conexiones alámbricas sospechosas.
· Efectúe auditorias sin aviso de las configuraciones del software.
· Elimine los cables no usados en las áreas sensibles.
· Asegurarse que las claves del correo de voz y permisos de acceso a la central sean de alta calidad. Dígales a los usuarios de teléfonos, que reporten inmediatamente al departamento de seguridad, sobre cualquier llamada sospechosa, o funcionamiento irregular del correo de voz. Adicionalmente de los escuchas, estas pueden ser indicaciones de hackers tratando de entrar para robarse el servicio telefónico.

8 – Reuniones Peligrosas
Las reuniones fuera de las oficinas, convenciones, shows comerciales, seminarios, etc. Le presentan al espía excelentes oportunidades para infiltrarse y recolectar información importante. Alerte a su gente de estos problemas.
Una simple reseña debe incluir las siguientes advertencias...
· Reuniones fuera de las oficinas atraen a los fisgones. · Los métodos de espiar pueden ser ilegales y sin ética. · La seguridad tomara el control de acceso a la sala las 24 horas.
· La detección de emisiones radioeléctricas serán empleadas.
· Los que atienden a la reunión deberán usar sus carnets de identificación todo el tiempo.
· Nunca deje su laptop o maletín desatendido.
· Deje la información propietaria escrita con la gente de seguridad en sobre cerrado.
· La información y los datos propietarios deberán estar en el área asegurada.
· No hable sobre el negocio en áreas públicas. · Sea suspicaz con los extraños que se interesen en usted.
· Reporte cualquier actividad sospechosa al personal de seguridad inmediatamente.
Defina lo que es la información propietaria con sus empleados. Es aquella información que no es de conocimiento general y esta relacionada con los productos de la empresa, métodos, clientes, planes, etc. Es cualquier información que pueda causar perdidas de ganancias, o una desventaja competitiva, si cae en las manos equivocadas.

9 – La Bandeja de Plata

A veces dejamos que la información se escape. ¿Cuáles de los siguientes casos se aplican a alguien que usted conoce?· Oficinas sin cerradura, escritorios o archiveros. · Documentos confidenciales sin guardar en la noche.
· Claves compartidas, simples o escritas en un papelito auto adhesivo.
· Directorio telefónico con notas explicitas.
· Tarjetas de créditos, identificaciones, notas con números telefónicos y tarjetas Rolodex sin guardar encima del escritorio.
· Respondiendo preguntas por teléfono a personas que no conoce realmente.
· Hablando temas sensitivos con chismosos conocidos. · etc., etc., etc.
La lista puede crecer a medida que piense más en el asunto. La solución: Reflexione sobre el asunto, entonces la lista decrecerá.

10 – Traición
Otro tipo de espía, el “empleado de confianza”; es uno de los más peligrosos y difíciles de detectar. Los candidatos más apropiados son los empleados que pueden... · están descontentos, posiblemente por estancamiento en los puestos de trabajo, falta de promociones, etc. ·
Hayan caído en grandes deudas por hábitos de juego, circunstancias personales inevitables, o uso de drogas.
· Estar involucrado en disputas sobre asuntos laborales o gerenciales.
· Tener personalidad de emprendedor.
Tips de Protección...
· Inspeccione buscando equipos de escucha. Esta clase de gente tiene la oportunidad y el tiempo para implantarlas y monitorearlas. · Selectivamente deje caer información falsa y espere a ver por donde aparece de vuelta. · Conduzca verificación personal de todos los empleados nuevos y de aquellos que tienen acceso a información sensible.
· Verifique los empleos anteriores cuidadosamente.
· Revise sobre los periodos sin empleo no mencionados.
· Verifique los periodos sin empleo.
· El vivir más allá del sueldo puede significar un ingreso extra de dinero proveniente del receptor de los secretos de su negocio.
Buenas noticias...
El espionaje puede ser prevenido, y el tener conocimiento sobre las tácticas empleadas para ello es el primer paso para obtener la protección. Usted ahora tiene el suficiente conocimiento para comenzar con ese proceso con confianza...