NOVIEMBRE, 2023

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

5
PASOS PARA AFILIARSE A ASIS INTERNATIONAL

EVENTOS
MEMORIAS DEL XIII SIMPOSIO ANUAL

INCREMENTO DE ATAQUES CIBERNÉTICOS EN EL MUNDO

EGOSURFING: ¿Qué dicen de mí en Internet?

ASIS INTERNATIONAL® | Bogotá Chapter

NOVIEMBRE, 2023

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

CONTENIDO

EDITORIAL

Palabras del presidente

Estamos emocionados de anunciar el lanzamiento de nuestra Newsletter - revista digital para el capítulo 225 de ASIS.

Esta publicación en línea será una fuente inestimable de información, análisis y perspectivas sobre las últimas tendencias y desarrollos en el campo de la seguridad.

Nuestra revista digital está diseñada para mantener a nuestros miembros al día con las mejores prácticas, innovaciones y noticias relevantes en la industria de la seguridad.

¡Esperamos que disfruten de este primer número y que sea de utilidad para seguir siendo líderes en su campo!

DANIEL JIMENEZ
MBA, CPP®,PSP®, CHSS, ESRM

AGRADECIMIENTO ESPECIAL

A Nuestros Patrocinadores:

ORGANIZACIÓN G.D.C
GESTIÓN, DESARROLLO Y CRECIMIENTO EMPRESARIAL

SECURITY COLOMBIA

casmar®

SRR Ltda
SEGURIDAD PRIVADA

PROSINTE
Protección y Selección Integral

TRI CLICK

SICUREX
INSTITUTO DE SEGURIDAD METIS

GRUPO CONSULTOR 360

ANDRÓSS
CAPACITACIÓN ESTRATÉGICA PARA LA PREVENCIÓN DE PÉRDIDAS

SD
SEGURIDAD DIGITAL

CONTRATACIÓN DE SISTEMAS DE SEGURIDAD FÍSICA

Es inaudita la actual forma de contratación de sistemas de seguridad física en las entidades públicas, organizaciones privadas y mixtas

POR: CARLOS A ABONDANO M

Administrador de Empresas,
Asesor & Consultor de Servicios de Vigilancia y Seguridad Privada.
Miembro de ASIS INTERNATIONAL, Capítulo Bogotá

Es absurdo, por decir lo menos, que las organizaciones (públicas, privadas, mixtas, grandes, pequeñas, locales, nacionales, e incluso multinacionales) contraten servicios de vigilancia y seguridad privada para implementar sistemas de seguridad física sin haber realizado previamente los procesos de identificación, análisis y valoración de los riesgos de seguridad física que se deben prevenir o mitigar y sin el diseño previo del correspondiente programa de tratamiento de riesgos. Haciendo una analogía, están comprando el remedio y automedicándose sin asistir a la consulta y al diagnóstico del médico.

Haciendo una analogía, están comprando el remedio y automedicándose sin asistir a la consulta y al diagnóstico del médico.

El concepto de "Administración del Riesgo" se introdujo en las entidades públicas desde la expedición de la Ley 87 de noviembre de 1993, en la que se establecieron normas para el ejercicio del control interno en las entidades y organismos del Estado. En su Artículo 2, Objetivos del control interno, literal a), Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos. Desde entonces ha aumentado para ellas la exigencia para la calidad de la administración del riesgo - con las leyes, decretos, resoluciones etc - y forma parte inherente e ineludible de su sistema de gestión.

Todas las instituciones oficiales, sin excepción, están obligadas a realizar y publicar el análisis de los riesgos, mediante el cual evalúan y tratan o intervienen aquellos eventos, tanto internos como externos, que pueden afectar de manera negativa el logro de sus objetivos institucionales. Los tipos de riesgos en los que se enfoca cada entidad pública dependen de su misión, de las normas que regulan su operación, de los sistemas de gestión que implementen, entre otros aspectos. Hay algunos tipos de riesgos que deben gestionarse obligatoriamente en todas las entidades públicas, como el riesgo de corrupción. Y deberían serlo también, los riesgos de seguridad física. La realidad es que en las entidades, con muy contadas excepciones, no hacen el proceso de evaluación de los riesgos de seguridad física. Sin embargo, y eso es lo inaudito, prácticamente todas abren y realizan licitación pública para la contratación de los servicios de vigilancia y seguridad privada. Y adjudican y contratan así. Contratan a ciegas los sistemas de seguridad física, es decir, sin conocer los riesgos de seguridad física de cada instalación para la que están contratando, a ciegas de cuáles son los riesgos de seguridad de mayor impacto para la entidad, sin una evaluación precisa de cuáles deben tratarse y cómo deben tratarse, sin realizar el programa de seguridad correspondiente, sin tener diseñado el plan de seguridad, sin la realización de manuales de seguridad física para todas las partes interesadas de la entidad, sin planes de contingencia para cuando se presente la materialización de tales riesgos, y varias otras omisiones de las recomendaciones que se encuentran estandarizadas en Normas Técnicas como la ISO 28000 Seguridad y Resiliencia.

Sistemas de gestión de la seguridad. ISO 18788 Sistema de gestión para operaciones de seguridad privada. ISO 31000 Gestión de Riesgos, y otras.

Esa conducta, lleva a que se utilicen importantes sumas de recursos públicos, sin la rigurosidad metodológica que se requiere. ¿Constituye un delito? Por lo menos si constituye una falta de rigurosidad, una irresponsabilidad, utilizarlos como se hace hoy.

Dentro de las muy contadas excepciones vale la pena mencionar una: la Unidad Administrativa Especial de la Aeronáutica Civil, Aerocivil.

El sistema de seguridad física que instala debería ser un modelo para seguir por todas las demás. La Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), como Autoridad Aeronáutica de la República de Colombia, en cumplimiento del mandato contenido en el Artículo 37 del Convenio sobre Aviación Civil Internacional y facultada por el artículo 1782 del Código de Comercio y el artículo 5º del Decreto 260 de 2004 modificado por el Decreto 823 de 2017, ha expedido los Reglamentos Aeronáuticos de Colombia (RAC) de los cuales hace parte el RAC 160 “Seguridad de la Aviación Civil”, el Programa Nacional de Control de Calidad de la Seguridad de la Aviación Civil, el Programa Nacional de Instrucción en Seguridad de la Aviación Civil, el Plan de seguridad de cada aeropuerto y el Plan de seguridad de cada explotador de aeronaves, entre otros.

Cuando cada explotador de un aeropuerto realiza la selección y contratación de una empresa de vigilancia y seguridad privada, tienen absolutamente claro el objetivo del sistema de seguridad de la aviación civil que va a instalar. La Seguridad de la Aviación - AVSEC - es uno de los servicios especializados de apoyo terrestre a la operación de aeronaves. Se encarga de prevenir, mitigar y controlar los riesgos asociados con los actos de interferencia ilícita para la gestión de la seguridad hacia los pasajeros, las aeronaves e infraestructura asociada.

Lamentablemente, el mismo inadecuado e irresponsable comportamiento para la contratación de sistemas de seguridad física que hacen la mayoría de las entidades oficiales, se presenta en las organizaciones privadas. La diferencia es que ellas no están obligadas legalmente a implementar un sistema de administración del riesgo.

Las empresas de vigilancia y seguridad privada cotizan o participan de las licitaciones, se comprometen contractualmente a manejar y tratar unos riesgos de seguridad física que desconocen. Riesgos de seguridad que van a descubrir y enfrentar una vez que han instalado el servicio. Un servicio que puede estar sobredimensionado, o por el contrario, insuficiente para enfrentar los riesgos de seguridad reales de esa entidad. ¿Cómo saberlo si no se realizó el análisis correspondiente?

Solo cuando se materializan los incidentes de seguridad - siempre con costosas consecuencias, inclusive en pérdidas de vidas, o lesiones personales y otros tipos de afectaciones a las personas, como las afectaciones a la salud mental que deja el enfrentarse a hechos traumáticos como asaltos, secuestros, asonadas, agresiones físicas, o graves daños a instalaciones o pérdida o daño de costosos equipos por hurto, robo, vandalismo etc. – es que vienen a conocerse realmente las amenazas, los agentes perpetradores de las amenazas y las vulnerabilidades que facilitaron los ataques y que con antelación debieron haberse identificado , analizado y diseñado las medidas preventivas y correctivas correspondientes.

Cuando se presentan los incidentes, los contratantes, los que contrataron a ciegas, se descargan por las orejas – como dice el refranero popular – trasladando a las empresas de vigilancia y seguridad privada contratadas la responsabilidad del siniestro, como si de ellas hubiera sido la responsabilidad de hacerles la tarea que han debido realizar antes de contratar. Y asumen que las empresas de vigilancia y seguridad privada son las "propietarias de los riesgos de seguridad" que debe enfrentar la entidad. Craso error. De absoluta ignorancia en la administración de los riesgos de una organización. Y no en pocas ocasiones, esas empresas contratadas resultan sancionadas, pagando los platos rotos, tanto con sanciones económicas, como con vetos a su contratación por esas mismas y otras instituciones. Y el personal de la operación de seguridad correspondiente, destacado para prestar el servicio, también resulta afectado con malas evaluaciones y calificaciones de su desempeño profesional, culpados por las consecuencias de las omisiones de los contratantes.

Una de las varias razones detrás de ese comportamiento de contratación totalmente antitécnico, que sorprende y causa extrañeza, se debe a que las organizaciones no cuentan con el personal competente para realizar la evaluación de riesgos. Saben que lo deben hacer, pero no disponen de los recursos necesarios.

No es extraño que en las instituciones públicas no haya asignado y de planta un jefe de seguridad o que si lo hay sea alguien cuyo único mérito sea el de ser ahijado político de algún cacique electoral. En algunos casos es alguien con las competencias necesarias, pero sin los recursos suficientes para realizar una actividad que desborda su capacidad. Y en las organizaciones privadas, invierten generalmente los recursos en el análisis de riesgos estratégicos, legales, financieros, de mercado, de recursos humanos (SST), ambientales, y no asignan los recursos para el análisis de riesgos de seguridad.

Todas, oficiales, privadas, mixtas, quejándose de la inseguridad y simultáneamente cerrando los ojos a la tarea que les corresponde.

Lo grave es que las empresas de vigilancia y seguridad privada no pueden exigir a las entidades y empresas contratantes que hagan y que hagan bien la parte que les corresponde para el tratamiento de los riesgos de seguridad. Para que realicen, previo a la contratación la evaluación de los riesgos de seguridad, el plan de tratamiento de esos riesgos, y el programa de seguridad que se debe implementar.

Son la ciudadanía, de una parte, y los propietarios o accionistas, de otra, los que deben tomar esa responsabilidad y exigir que se inviertan debidamente las enormes cifras que hoy se invierten en el país en la implementación de sistemas de seguridad física.
¡Billones al año!

Lo que ocurre por el lado de los dineros públicos, es que las instituciones llamadas a ejercer control de las formas de contratación también contratan igual de mal. Y por el lado de los propietarios y accionistas, en las privadas, hay ignorancia de lo que representan los sistemas de seguridad en su cadena de valor y por eso poca o ninguna atención le prestan a su forma de contratación.

Es curioso que los gremios del sector, no hayan tomado acciones en el asunto. Mientras tanto, la regla para las empresas de vigilancia y seguridad privada es: "si le sirve así licite y contrate así y asuma las consecuencias y si no le sirve así no lo haga, que hay muchas empresas detrás de ese contrato".

5 pasos para afiliarse

Afiliarse a la mayor asociación de profesionales de la seguridad del mundo es muy fácil y aquí compartimos hoy el paso a paso para lograrlo:

1. Cree una cuenta
Para lo cual visite el siguiente enlace:

https://external.asisonline.org/eWeb//DynamicPage.aspx?WebCode=verify&Site=asis

2. Llene el formulario
Trate de ser BREVE PERO PRECISO, haga click en continuar, después del catpcha (verificar que no es un ROBOT),

Complete la información a continuación para crear un perfil en línea. La información que envíe se utilizará para ayudarlo a personalizar su experiencia en línea, lo que incluye unirse a ASIS, gestionar suscripciones, configurar alertas, descargar notas técnicas de la industria, actividades de centros de carreras profesionales y según se describe en nuestra Política de privacidad.

3. Cree la contraseña (password)
Incluya entre 8 y 18 caracteres, y al menos un numero y continúe:

4. Hecho!!!
Se ha registrado.....

5. Cierre
Vuelva abrir su cuenta EN 8 DIAS, vaya a My Account Links/ My invoices, allí encontrará el monto a pagar . Para que pague su empresa con la tarjeta de crédito empresarial, imprima el invoice que le llegó al email que inscribió, y empiece a disfrutar los beneficios.

INCREMENTO DE ATAQUES CIBERNÉTICOS EN EL MUNDO,

¿cuáles son los más comunes y qué grupos de hackers son los más peligrosos?

CORTESÍA UNIDAD DE ANÁLISIS POLÍTICO Y SEGURIDAD CORPORATIVA, 3+ SECURITY COLOMBIA

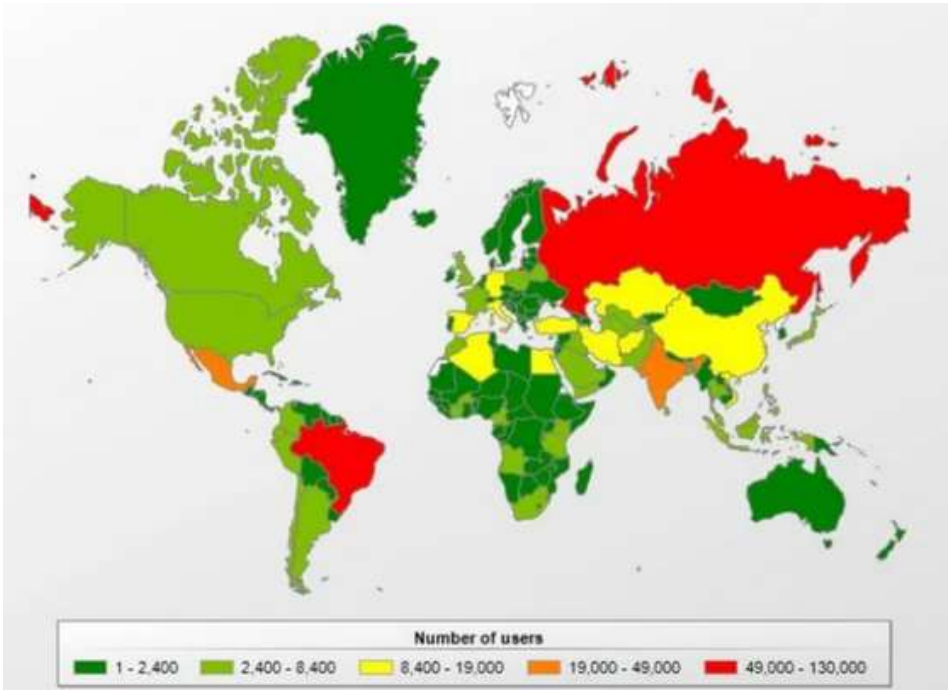
Los ataques cibernéticos son accesos no autorizados a sistemas o redes informáticas por parte de terceros. Quienes incurren en estas prácticas son denominados ciberdelincuentes o "hackers"

Los ataques cibernéticos son accesos no autorizados a sistemas o redes informáticas por parte de terceros. Quienes incurren en estas prácticas son denominados ciberdelincuentes o "hackers" (Interbel, 2023). Estos últimos realizan dichas acciones con diversos fines, principalmente para robar información, manipular los sistemas de empresas u organizaciones específicas y pedir dinero a cambio del restablecimiento de las plataformas (La Tercera, 2023). Los ataques cibernéticos implican la posible vulneración, pérdida o manipulación de datos, lo que trae como consecuencia un impacto negativo para quien es víctima del delito (Interbel, 2023). Según Immanuel Chavoya, estratega de detección y respuesta ante amenazas, "los ciberataques suponen un peligro constante para las empresas de todos los tamaños, poniendo en jaque sus operaciones y su reputación" (Revista Semana, 2023).

En 2023 los ataques cibernéticos han experimentado un incremento del 87% a nivel global (Revista Semana, 2023). Actualmente se producen aproximadamente 1.700 ataques informáticos por segundo (SER, 2023) y el 66% de organizaciones en el mundo ha sido víctima de este tipo de delitos (La República, 2023). Estados Unidos, Alemania, Francia, España y Reino Unido son los países con mayor número de casos por ciberataques (20 Minutos, 2023).

Mapa de los países más afectados por modalidad de ciberataque "Troyanos Bancarios"

Fuente: *Infobae, 2023.*



En el caso de Latinoamérica, Brasil y Colombia lideran la lista de países afectados (Revista Semana, 2023). En Colombia se han registrado más de 15 millones de intentos de acceso no autorizados a plataformas contra grandes y medianas empresas (La República, 2023).

Si bien existen diferentes modalidades, hay dos estrategias principales utilizadas por los "hackers" para cometer ciberataques. El primero es el "Malware", que en español hace referencia al "virus de software malicioso". El "Malware" contagia una red a través de una ruptura o una vulnerabilidad, es decir, cuando el usuario abre un enlace peligroso o descarga un archivo que contiene el virus. Este tipo de ataque contiene varias subcategorías, por ejemplo: el "Ransomware", el "Spy Loan" y el "Virus Troyano". El "Ransomware" bloquea el acceso a las claves de red, el "Spy Loan" es un software que roba datos sin conocimiento del usuario por medio de su teléfono móvil y el "Virus Troyano" "se disfraza de software legítimo" para darle confianza al usuario y que este le permita, por consiguiente, ingresar a la plataforma. El segundo tipo de ciberataque es el "Phishing" que consiste en enviar correos electrónicos que parezcan confiables y de esta forma engañar a la víctima para que los abra y su dispositivo se contamine.

Otras modalidades de delincuencia informática son: el "Ataque de Contraseñas", el "Man-in-the-Middle" y la "inyección SQL" (Interbel, 2023).

Entre las organizaciones criminales que se dedican a este delito se encuentran "REvil", "Dragonfly", "Lazarus" y "Lapsus$". "REvil" es un grupo ruso dedicado a piratear sistemas y cifrar archivos para bloquear plataformas para luego exigir sumas de dinero a cambio del restablecimiento de las estructuras informáticas. Existen desde el año 2019 y en el 2021 "fueron los responsables del 37% de los ataques de "Ransomware" en el mundo. La organización "Dragonfly", nacida en 2010 y también de procedencia rusa, se dedica a realizar labores de ciberespionaje a instituciones norteamericanas y europeas. Se presume que esta vinculada con el Servicio Federal de Seguridad de Rusia. No hay información certera cobre el grupo "Lazarus", sin embargo, parece ser que sus miembros estarían vinculados con el régimen de Corea del Norte y que entre sus actividades estaría el espionaje a enemigos ideológicos del régimen de Kim Jong-Un.

Por último, "Lapsus$" es una organización inglesa, creada en 2021, dedicada a extorsionar por medio del robo de datos (La Tercera, 2023).

Los delitos informáticos van en aumento y el avance de la inteligencia artificial acelera aún más este proceso. Es por ello, por lo que resulta pertinente tomar las medidas necesarias para proteger "las redes, los sistemas informáticos y sus componentes del acceso digital no autorizado", esto se denomina ciberseguridad (Interbel, 2023).

Utilizar software antivirus, mantenerse alerta y evitar ingresar a enlaces sospechosos, actualizar los sistemas operativos y navegadores con regularidad, realizar copias de seguridad y diseñar planes de contingencia capaces de responder efectivamente a situaciones de riesgo cibernético son algunas de las pautas para evitar y mitigar daños con respecto a los ataques informáticos (20 Minutos, 2023).

3+ Security Colombia:
www.3securitycol.com

MEMORIAS DE NUESTRO SIMPOSIO ANUAL

Agradecemos a todos los participantes en nuestro exitoso XIII Simposio Anual: “Convergencia de la Academia y la Seguridad Organizacional”

RECONOCIMIENTOS

recibidos por nuestros asociados

Martín Tarazona, reconocido por la revista internacional CIO Review como uno de los TOP 10 Risk Management Solutions Providers en Latinoamerica.

Cesar Suarez, condecorado por el ejército de Paraguay, acompañan agregados de defensa del ejército de USA para el cono sur.

EGOSURFING: ¿QUÉ DICEN DE MÍ EN INTERNET?

"Internet es el mayor banco de información de la historia y puede haber contenido privado o inapropiado sobre nosotros circulando por la red, aunque no seamos conscientes de ello" (OSI)

POR: YELENA CASTAÑEDA

Administradora de Empresas,
CEO TriClick.co

Todo lo que publicamos en Internet: fotos, vídeos, opiniones, etcétera, e incluso lo que otros publican sobre nosotros, incluyendo documentación o publicaciones oficiales, donde aparece información sobre nosotros, permanece en la red. El conjunto de esos datos son los que forman la huella digital personal y puede verse dañada en función del tipo de información que se encuentra sobre cada uno.

Además del riesgo reputacional, la privacidad también corre el riesgo de ser vulnerada. Por ejemplo, al exponer datos personales que se acaban filtrando como el número de cédula, la dirección, los vehículos, la actividad profesional e incluso asuntos privados como implicación en casos jurídicos, se corre el riesgo de que lleguen a manos de ciberdelincuentes y sean usados para suplantaciones, fraudes chantajes y otros tipos de delitos.

Entonces, así como periódicamente vamos al médico a hacernos un chequeo es importante revisar y chequear periódicamente la información que hay sobre nosotros en internet, ya sea publicada por nosotros o por terceros, de forma legítima o ilegítima y esto se puede hacer a través del *Egosurfing*.

El *Egosurfing* consiste en utilizar las redes sociales y los buscadores de Internet, como Google, Bing y otros utilizando términos de búsqueda relativos a nosotros, como nuestro nombre, apellidos, identificación, etc., para localizar información sobre nosotros en páginas webs y otras plataformas.

Los ataques cibernéticos son accesos no autorizados a sistemas o redes informáticas por parte de terceros. Quienes incurren en estas prácticas son denominados ciberdelincuentes o "hackers"

Aplicando esta práctica podemos saber qué se dice de nosotros, cómo se dice, quién lo dice y con qué objetivo, y sobre todo identificar la información que no debería estar publicada y que queremos que sea eliminada.

> Todo lo que publicamos en Internet, permanece en la red.

¿Cómo hacer egosurfing?

Para hacerlo debemos introducir los términos de búsqueda relativos nosotros o a nuestra empresa en las redes sociales y los buscadores de internet, pueden ser datos como nombre, apellidos, número de identificación, placas de los vehículos o números de seguridad social, así se localiza la información que aparece sobre uno en los sitios web, redes sociales y plataformas, y esto se puede hacer con diferentes herramientas.

Webmii. Es una plataforma que ayuda a averiguar la presencia de cualquiera en internet, ya sea alguien conocido o popular o simplemente un nombre anónimo y corriente, mostrando fotografías, etiquetas, redes sociales y resultados relacionados con la persona a encontrar o con contactos afines.

Buscadores (Google, Bing, DuckDuckgo, etc.) Se puede realizar una monitorización similar en un momento puntual que interese, de una manera más sencilla y con los mismos términos utilizados en la opción anterior. Tan solo hay que escribir en la barra del buscador el dato que se quiera encontrar, como se realiza cualquier otra búsqueda de manera común.

Imágenes de Google. También podemos buscar imágenes concretas en Google Imágenes y ver dónde aparece nuestra imagen, tanto en perfiles propios e identificar si también han sido compartidas o publicadas por otras personas.

Redes sociales, foros y otras plataformas. En ellas es donde más información se comparte y si no está bien configurada la privacidad de los perfiles, todos esos datos pueden quedar expuestos a terceros, lo que podría llevar a que fueran utilizados con mala intención. Para hacer Egosurfing en ellas se debe introducir el nombre completo, el nombre de usuario o el correo electrónico, así veremos qué información ofrece públicamente la plataforma, qué han publicado sobre nosotros otras personas, ex empleados o ex clientes, y descubrir si existen perfiles falsos que suplantan nuestra identidad o la de nuestra empresa.

Google Alertas. Con esta funcionalidad de Google podemos recibir en el correo electrónico notificaciones sobre un tema de interés. Para este caso, podemos indicar a la herramienta los datos que queremos tener monitoreados, introduciendo en la barra de búsqueda esas palabras claves, entre comillas, para que aparezca con exactitud lo que buscamos y seamos notificados oportunamente.

¿Y qué hacer si encontramos información no deseada en Internet?

Para eliminar datos o imágenes sobre uno mismo que no se quieren mantener en la red, se puede hacer uso de distintas herramientas según las características de la información, dónde y cómo aparece.

Si la información no ha sido publicada por nosotros mismos, se puede solicitar al administrador de la red que rectifique o elimine dicho contenidos, demostrando la inexactitud de los datos o que ellos afectan nuestra reputación.

Incluso, si la difusión de nuestros datos empresariales pudiera ser constitutiva de delito, se podría interponer una denuncia por afectar el buen nombre de nuestra empresa.

Si la información la publicamos nosotros mismos es cuestión de ir a la fuente y eliminar esas publicaciones, y configurar las opciones de privacidad de las redes sociales.

Si se encuentra un perfil falso, se debe denunciar a la red social a traves de los canales de soporte para que sea eliminado cuanto antes.

Ejercer el derecho al olvido si los datos o imágenes han sido publicadas por terceras personas e instituciones y afectan de manera negativa a la identidad digital y la reputación.

Como vemos, el *Egosurfing* más que una práctica de vanidad es una práctica de seguridad que se debe hacer periódicamente para mantener el control de nuestra información expuesta en la Red, conocer nuestra huella digital y la imagen que proyectamos, y saber a tiempo si estamos siendo suplantados.

Triclick | Agencia de Marketing Digital
triclick.co

Síganos y comparta con sus contactos las publicaciones de **ASIS COLOMBIA,**

+57 310 477 0280

secretario@asiscolombia.org.co

www.asiscolombia.org.co

asis-colombia

asiscolombia

¡Unidos somos más fuertes!