E-COMMERCE

SCP

Firma electrónica

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

open source

Índice

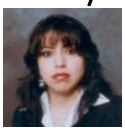
“No se puede usar la ley del siglo XVIII en un mundo digital”

— Andrus Ansip, parlamentario Europeo respecto al uso de firmas electrónicas —

CRÉDITOS:

Revista virtual de comercio electrónico, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre

adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com

Facebook

Twitter

¿Qué es la firma electrónica?

El comercio electrónico se incrementa día a día, de igual forma se desarrolla tecnología que facilite y brinde las seguridades necesarias para poder realizar transacciones virtuales a través de Internet, razón por la cual si usted ¿está comercializando productos a través de Internet? ¿Gestiona o quiere gestionar electrónicamente su negocio desde cualquier lugar? ¿Se relaciona con sus clientes o proveedores a través de medios electrónicos? Si la respuesta es afirmativa en al menos una de las preguntas, sin duda alguna: usted necesita emplear tecnología de firma electrónica o digital.

Esta es la única forma posible de enfrentarse, y superar con éxito, a la gran crítica que el ciudadano hace al comercio electrónico: la falta de confianza en las transacciones económicas. La tecnología de la firma digital está precisamente pensada para eso, para garantizar y dar confianza a todas nuestras actividades empresariales online.

¿Qué es la firma electrónica y para qué sirve?

En realidad, la firma electrónica no tiene nada que ver con nuestra firma física tradicional. No es, al contrario de lo que intuitivamente muchos puedan pensar, nuestra firma personal digitalizada (esto es, escaneada), sino que consiste en la aplicación de una serie de conceptos matemáticos descubiertos en la década de los setenta por dos científicos de la Universidad de Standford y del Instituto Tecnológico de Massachussets.

Se trata, en pocas palabras, de “pegar” a nuestros documentos electrónicos (las facturas, recibos, contratos, etc., digitales) un conjunto de datos en forma de claves que garantizan una serie de cosas a las partes involucradas. Estas garantías son esenciales para dotar de confianza al medio electrónico como entorno de los negocios, y esencialmente son las siguientes:

En primer lugar, el uso de estas claves permite que la información que enviamos por la Red vaya cifrada (encriptada) con la finalidad de que si alguien intercepta dicha comunicación durante su tránsito no sea capaz de leerla. Esto es, le sea incomprensible al igual que lo son los mensajes codificados por los espías o por los servicios secretos. Esa es la función de la encriptación o criptología, la ciencia que se ocupa de ocultar, disimular o cifrar la información.

En segundo lugar, emplear tecnología de cifrado como la que usa la firma electrónica permite garantizar que si alguien intercepta nuestra comunicación e intenta modificarla, y lo logra, su interferencia será técnicamente detectable, esto es: se nos garantiza que la información llegará

intacta a su destinatario porque, de lo contrario, sabremos que ha sido manipulada.

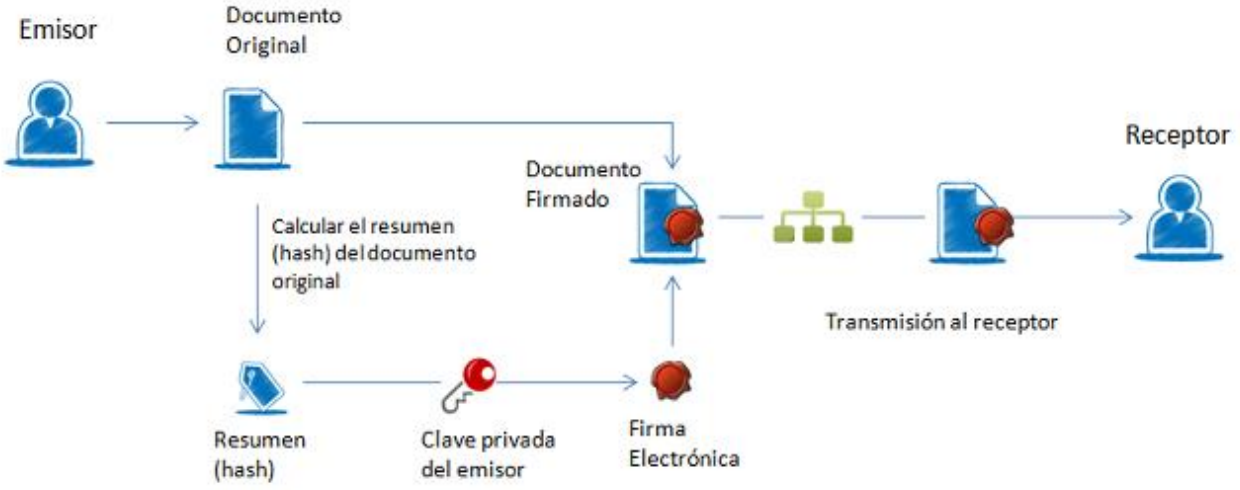
La firma electrónica también nos permite saber o, mejor dicho, tener la certeza de quién es la otra parte con la que estamos interactuando. Es decir, nos da la confianza necesaria para saber que la otra parte es quién dice ser y no un farsante o un impostor que se hace pasar por nuestro interlocutor real.

Y, finalmente, el uso de tecnología de firma digital posibilita garantizar la recepción del mensaje. Esto es, si estoy enviando una documentación legal que estoy obligado a remitir, mi interlocutor no podrá haber negado recibirla si trabajo con esta tecnología.

Estas son pues las importante bases de la firma electrónica: la confidencialidad (la capacidad de mantener accesible un documento electrónico sólo a quien queramos); la integridad (la garantía de que el documento no será manipulado durante su tránsito digital); y la autenticidad (el compromiso de un individuo sobre el contenido del documento electrónico, sobre su autoría, su envío y su recepción).

La Firma Electrónica surge de la necesidad de las organizaciones de reducir sus costos e incrementar la seguridad de sus procesos internos, a través del uso de medios electrónicos que permita agilizar los procesos, reducir los tiempos y evitar el uso de papel.

El Proceso Básico de Firma Electrónica



El proceso básico que se sigue para la firma electrónica es el siguiente:

- El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
- La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
- La aplicación utiliza la clave privada para codificar el resumen.
- La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.
- El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

Recuerda:

La firma electrónica es el archivo o documento electrónico resultante. Este es el documento válido a efectos legales y el que debes conservar.

Cualquier impresión o representación gráfica que se haga de él solo es válido en los términos que determine el destinatario de la firma. En general, en este caso, la firma impresa deberá contener un CSV o Código Seguro de Verificación que permite contrastar la copia impresa con la original electrónica.

Por ello es imprescindible, cuando se quieren hacer negocios online con las mismas garantías de validez y efectos jurídicos que en el mundo físico, atenerse a las especificaciones legales para el uso de tecnología de firma digital.

FUENTES:

- http://www.almiron.org/otros28.html
- http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html

Capacitación en Comercio Electrónico y Gestión Web

"Tu futuro es creado por lo que haces hoy, no mañana."
Robert Kiyosaki

En la actualidad la tecnología avanza a pasos agigantados, incorporándose continuamente en todas nuestras actividades diarias, nuestras compras, consultas, pagos, transacciones, etc. Las realizamos en la comodidad de nuestros hogares, oficinas y/o lugares en los cuales se tenga acceso a Internet, a través de nuestros dispositivos móviles o computadores. Este avance ha permitido y obligado a que las grandes y pequeñas empresas, presenten sus productos y servicios a través del mismo medio, llegando a miles de usuarios en poco tiempo, mejorando sus ventas, así como, reduciendo los gastos en infraestructuras físicas y/o recursos en sus negocios.

Hoy en día las páginas web no se utilizan únicamente para informar, ahora son una vitrina al mundo, por lo que los negocios en línea requieren que sean administrados por personal experto, que realice una planificación y gestión adecuada y garantice el cumplimiento de objetivos y metas establecidas para su productividad.

SCProgress imparte cursos de capacitación en comercio electrónico, para que la creación y presentación de una tienda virtual grande o pequeña, cuente con las características indispensables para que sea rentable, así como, su gestión y seguimiento, mantengan a su negocio en el posicionamiento deseado.

Nuestra metodología se basa en el aprendizaje teórico – práctico, asegurando a los participantes una completa comprensión de las bases fundamentales de la creación y gestión de su negocio en línea.

El personal de capacitación es altamente especializado y goza de la experiencia necesaria para brindar la más completa información en los temas tratados en cada curso.

Esta vez, SCProgress pone a disposición de sus lectores y clientes, cursos de capacitación en los siguientes temas:

Curso de Comercio Electrónico	Curso de Gestión Web
Contenido: • Introducción al Comercio Electrónico • Modelos de negocio en Comercio Electrónico • Uso de embudos multicanal • Modelos de atribución • Seguimiento de eventos en Google Analytics • Analítica de publicidad y marketing en Internet • Redes sociales y Comercio Electrónico • El impacto de las redes sociales • Desarrollo de plan de negocios • Evaluación de caso práctico	**Contenido:** • Introducción a W3C • Principales comando de HTML5 • Diseño con HTML5 y CSS • Evaluación de sitios web • Diferentes tipos de portales web • Gestores de contenidos CMS • Caso práctico de CMS en Drupal • Uso de plantillas para la implementación de sitios web • Evaluación de rendimiento del sitio web • Seguimiento a través de SEO de Google Analytics

Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: **www.scprogress.com**, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

Diferencias entre certificado electrónico, firma digital y firma electrónica

El creciente número de operaciones y de información que se mueve por la red ha hecho saltar las alertas en tema de seguridad y protección de datos. Cualquier acción que realicemos en la web nos exigirá la deposición de una serie de datos personales que, aparentemente, no nos supondría ningún riesgo en nuestra seguridad.

Sin embargo, no somos conscientes de que cada dato que vamos dejando en la red es un rastro que lleva a nuestros datos más personales, como los datos bancarios, de seguros, teléfonos, facturas, etc. Esto nos lleva a preguntarnos, ¿son seguros los portales web que visitamos?

Por tal motivo se diseñó un mecanismo de identificación segura, en la que se relaciona el documento con la persona física o jurídica, el certificado electrónico. Entrando en este terreno, a menudo se confunden los conceptos certificado electrónico, firma electrónica y firma digital, que en muchas situaciones se suelen utilizar como sinónimos. Vamos a intentar aclararlo.

Firma electrónica es el "conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante".

Cuando hablamos de firma electrónica, estamos ante un concepto jurídico, es un método de identificación, como lo es la firma manuscrita, que puede utilizar varios medios electrónicos, como un lápiz electrónico o una firma digital.

Por tanto, la firma electrónica implica que una persona verifica una determinada acción a través de cualquier medio electrónico, quedando un registro de fecha y hora de la firma.

Firma digital son una serie de caracteres que se añaden al final de un documento o cuerpo de un mensaje, y que pretende informar, dar fe o mostrar validez y seguridad. Con la firma digital se identifica la persona que emite el mensaje, la veracidad de que el documento no se ha modificado con respeto al emitido originalmente y no se puede negar haberlo firmado.

Es importante indicar que la firma digital es un proceso de cifrado matemático que permite a cualquiera comprobar la autenticidad de los datos cifrados. Se trata de un sistema de cifrado asimétrico y emplea, por lo tanto, una clave o llave secreta o privada (private key) y otra pública (public key).

La firma digital forma parte fundamental de la firma electrónica segura (legalmente se habla de la firma electrónica avanzada y reconocida). Es decir, la firma digital (el cifrado matemático de datos) permite que la firma electrónica (identificación y muestra de un acto de voluntad) pueda ser atribuida con seguridad a un firmante concreto.

El certificado digital o electrónico es el documento mediante el cual se identifica una persona en Internet. Este fichero informático asocia a una persona física o jurídica a una serie de datos, y es necesario que un tercero de confianza o Autoridad Certificadora autentifique esa asociación de datos.

El certificado electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor.

Todos estos mecanismos tratan de afianzar un sistema seguro a través del cual se puedan llevar a cabo cualquier transacción, operación o gestión a través de la web, de forma rápida, segura y sin costes adicionales.

Se debe indicar también que una **Firma Digitalizada**, no tiene nada que ver con las anteriores ya que se trata de una simple representación gráfica de la firma manuscrita obtenida a través de un escáner, que puede ser "pegada" en cualquier documento. Esta técnica la empezaron a utilizar masivamente los expertos en márketing cuando la publicidad circulaba por correo postal ordinario.

Adicionalmente a lo expuesto, también proporcionaremos conceptos relacionados con la firma electrónica.

¿Qué es la Firma Electrónica Certificada?

En términos legales, la Firma Electrónica Certificada "es aquella que ha sido expedida por la Autoridad Certificadora, consistente en el conjunto de datos electrónicos integrados o asociados al Mensaje de Datos, que permite asegurar la integridad y autenticidad de ésta y la identidad del Titular".

¿Qué es una Autoridad Certificadora?

Una Autoridad Certificadora es "la dependencia de la administración pública que tiene las facultades de autorizar, revocar, suspender o extinguir los certificados de Firma Electrónica Certificada."

La Autoridad Certificadora, por sí misma o a través de la intervención de un Prestador de Servicios de Certificación (Autoridad Registradora), verifica la identidad del solicitante de un certificado antes de su expedición.

La confianza de los usuarios en la AC es importante para el funcionamiento del servicio, ya que legitima ante terceros que confían en sus certificados, la relación entre la identidad de un usuario y su llave pública.

¿Cómo funciona una Autoridad Certificadora?

La Autoridad Certificadora en su función más importante es responsable de verificar la identidad del solicitante de un Certificado de Firma Electrónica Certificada antes de su emisión, así como de almacenar y administrar los certificados que emite.

La operación de una AC se sustenta en una infraestructura tecnológica que le permite la emisión, administración y registro de Certificados Electrónicos, así como de la disposición de herramientas que permitan la consulta de la validez de los mismos en cualquier momento por parte de los servicios que hagan uso de la Firma Electrónica.

Dado lo anterior, y bajo el principio que la confianza que se tenga en la AC es vital para la emisión de documentos y operación de servicios con firma electrónica, es necesario el establecimiento de procedimientos, políticas y lineamientos que estén apegados a estándares reconocidos en términos de seguridad, encriptación, confidencialidad, continuidad, entre otros.

¿Cuáles son las condiciones para considerar un documento electrónico (mensaje de datos) como válido?

Para asegurar la validez de un documento electrónico o mensaje de datos es necesario responder las siguientes preguntas:

- ¿Qué se firmó?
- ¿Quiénes lo firmaron?
- ¿Cuándo lo firmaron?

El contenido del documento electrónico o mensaje de datos es lo que se está firmando, en un acuerdo, los participantes negocian este contenido y una vez aceptado proceden a firmarlo electrónicamente.

Los participantes que aceptaron el contenido del documento electrónico o mensaje de datos y dieron su aceptación utilizando su llave privada para generar su Firma Electrónica Certificada son quienes firman el documento o mensaje de datos.

El Certificado de Firma Electrónica vincula la identidad de los firmantes con su llave pública, que al encontrarse relacionado con su llave privada permite determinar el autor de una Firma Electrónica.

Al ser el Certificado de Firma Electrónica un mensaje firmado electrónicamente, este se puede autentificar y determinar si es integro, que fue emitido por una Autoridad Certificadora confiable y que se encuentra además en su periodo de validez.

Una vez que tenemos un mensaje firmado electrónicamente y conociendo sus correspondientes Certificados de Firma Electrónica, es posible determinar que el mensaje no ha sido alterado, que el mensaje firmado por los participantes fue el mismo, que se tienen elementos suficientes para identificar la autoría de las firmas y que un tercero confiable (AC) verifico la identidad de los firmantes avalando que estos son los poseedores de la llave privada con la que realizaron sus firmas.

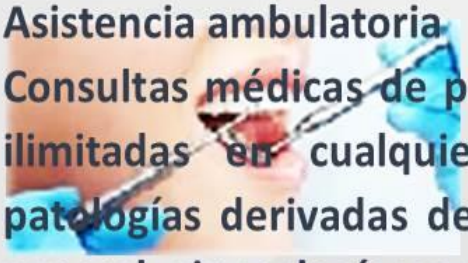
FUENTES:

- http://autoridadcertificadora.guerrero.gob.mx/fec/que-es-la-fec.html
- http://www.axpe-blogs.com/uncategorized/diferencias-entre-certificado-electronico-firma-digital-y-firma-electronica/
- http://www.dpoitlaw.com/nuestros-servicios/soluciones-de-firma-electronica/
- http://www.almiron.org/otros28.html
- http://www.realsec.com/noticias/diferencias-firma-digital-firma-electronica/
- http://www.europapress.es/economia/noticia-diferencias-hay-firma-electronica-firma-digital-certificado-digital-20150421105308.html
- http://blog.segu-info.com.ar/2013/01/diferencias-conceptuales-entre-firma.html
- https://bartolomeborrego.wordpress.com/2007/09/20/diferencias-entre-firma-electronica-firma-digital-y-firma-digitalizada/
- http://blog.a1arte.com/2017/04/13/cual-es-la-diferencia-entre-firma-electronica-y-firma-digital/
- http://www.ecertchile.cl/producto/firma-electronica-simple-certificado-digital

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- Créditos sin garante hasta 3.000 dólares.
- Otorgamos créditos para consumo, emprendedores y microempresarios.
- Las tasas de interés más bajas del mercado.
- Inversiones a plazo fijo.
- Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.



- Asistencia ambulatoria.
- Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.
- Cobertura en asistencia dental.
- Examen clínico y diagnóstico.
- Higiene dental, alivio del dolor.
- Rayos X periapical, profilaxis (Limpieza dental profunda).
- Restauraciones en resina simple.
- Extracciones simples.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204

www.cooprumi.fin.ec

Entidades certificadoras en el Ecuador.

En el Ecuador, al igual que en los países desarrollados, se encuentra adoptando la opción de la firma electrónica, tanto en el sector público, como en el privado y puede ser usado por personas naturales, representantes legales de empresas y funcionarios públicos.

Actualmente podemos firmar electrónicamente documentos para el Servicio de Rentas Internas (SRI), aduanas, en el sector público, toda la documentación elaborada a través del Sistema de Gestión Documental Quipux.

Así también, podemos firmar electrónicamente: correos electrónicos, facturas electrónicas, contratos electrónicos, transacciones electrónicas, trámites tributarios electrónicos, ofertas del Sistema Nacional de Contratación Pública y cualquier tipo de aplicaciones en las que se pueda reemplazar la firma física.

Existen varios tipos de contenedores en los que se puede activar los certificados electrónicos, como son:

- **Token.-** (Dispositivo seguro USB), que es un dispositivo similar a un pendrive que permite el almacenamiento de certificados digitales. Mediante este dispositivo podemos identificarnos así como firmar documentos mediante una clave.

- **Archivo.-** se puede colocar en un servidor o en computador. El usuario debe proteger en todo momento dicho archivo y las copias que realice del mismo, el certificado posee una clave acceso
- **HSM**.- dispositivo de alta seguridad que permite realizar varias transacciones por segundo (transacciones de forma masiva), cumple con altos estándares de seguridad.

- **ROAMING**.- le permite realizar operaciones mediante el uso del applet publicado por la ECIBCE o un aplicativo opcional llamado ESP, este tipo de contenedor se encuentra en el Banco Central del Ecuador.

A continuación, nos permitimos presentar a nuestros lectores un cuadro comparativo de costes de los certificados electrónicos de las instituciones certificadoras en nuestro país.

ENTIDAD / DESCRIPCIÓN	TIPO CONTENEDOR	BANCO CENTRAL DE ECUADOR		REGISTRO CIVIL		SECURITY DATA	
		TIEMPO	VALOR	TIEMPO	VALOR	TIEMPO	VALOR
Certificado Digital	Token	2 años	$30,00	2 años	$27,00	2 años	$65,10 (Incluye Token)
	Archivo	1 año	$15,00			2 años	$42,60 (Bajo volumen) *
	HSM	3 años	$90,00				
	Roaming	2 años	$30,00				
Renovación Certificado Digital	Token	2 años	$15,00	2 años	$18,00	2 años	$37,60
	Archivo	1 año	$15,00			2 años	$42,60 (Bajo volumen)*
	HSM	3 años	$90,00				
	Roaming	2 años	$15,00				
Dispositivo Token			$26,00		$22,00		
Desbloqueo			$00,00		$00,00		$21,51
Soporte técnico y/o instalación			$00,00		$00,00		$60,00

*Bajo volumen.- de 1 a 1000 comprobantes electrónicos emitidos en el mes, se incluye el Sistema de Gestión Documental Gubernamental Quipux y no aplica para el SRI y YO en personas naturales.

Las formas de pago pueden ser mediante transferencias bancarias o en las propias ventanillas de las instituciones certificadoras.

Los lugares donde pueden acercarse a adquirir un certificado electrónico, dependiendo de la institución de su elección, son:

BANCO CENTRAL DE ECUADOR	REGISTRO CIVIL	SECURITY DATA
A través de las agencias del Registro Civil	Ambato, Azogues, Coca, Cuenca, Esmeraldas, Guaranda, Guayaquil Centro, Guayaquil Sur, Ibarra, Lago Agrio, Latacunga, Loa, Macas, Machala, Manta, Portoviejo, Puyo, Quevedo, Quito Matriz, Quito Quicentro Sur, Quito San Blas, Riobamba, Salinas, San Cristóbal, Santo Domingo, Tena, Tulcán Zamora	Quito, Guayaquil, Cuenca, Loja (telconet), Ibarra, Santo Domingo (Cámara de Comercio Santo Domingo), Azogues (Cámara de Comercio e Industrias Azogues), Manta (Fedexport), Tulcán (Cámara de Comercio Tulcán), Salinas (Telconet), Machala (telconet), Esmeraldas (Zalsa) y sus Agentes Móviles en Huaquillas, Latacunga, Riobamba, Ambato y Pillaro.

Requisitos para obtener el Certificado de Firma Electrónica en Ecuador:

Persona Natural

- Digitalizado de cédula o pasaporte a color.
- Digitalizado de papeleta de votación actualizada.
- Digitalizado de la última factura de pago de luz, agua o teléfono.

Persona Jurídica

- Digitalizado de cédula o pasaporte a color.
- Digitalizado de papeleta de votación actualizada.
- Digitalizado del nombramiento o certificado laboral firmado por el representante legal.
- Autorización firmada por el representante legal.

En la mayoría de los casos, se requiere la instalación de software, dependiendo el tipo de contenedor, así como, el tipo de sistema operativo.

SCProgress les recuerda que la seguridad de los certificados electrónicos y las firmas, también se encuentran ligadas estrechamente a las seguridades de su infraestructura tecnológica y de los computadores en los que se ejecutan.

Avira, la galardonada solución alemana, ideal para proteger las empresas y los hogares, no produce molestias al cliente y el altamente eficiente. Previene de amenazas en tiempo real, a través de la detección fundamentada en firmas, el examen heurístico y el análisis basado en la nube le ofrecen una protección completa frente a los programas maliciosos. No dude en comunicarse con nosotros directamente al correo electrónico: avira@scprogress.com

FUENTES:

- https://www.eci.bce.ec
- https://www.registrocivil.gob.ec
- https://www.securitydata.net.ec/
- http://iusdigitalis.blogspot.com/

Rincón de los expertos

Pregunta de un estudiante.

Hace pocos días un alumno en la universidad me formulo una muy interesante pregunta, ¿Por qué requerimos de seguridad en las conversaciones privadas entre amigos o en el intercambio de mensajes entre dispositivos BYOD y Android?

La respuesta más obvia esta en Internet "***las personas fueron especialmente buscadas y victimizadas por grupos delincuenciales o terroristas, no por que hicieron algo malo, sino más bien porque ellos podían ser utilizados en sus planes siniestros***".

Bajo esta concepción, es clara la necesidad de mantener cifradas nuestras comunicaciones entre smartphones, a fin de mantener nuestra información importante lejos del alcance de personas no autorizadas; y para ello existen dos tipos fundamentales de cifrados que son: el que mantiene cifrada la comunicación llamada punto a punto y que se conoce como "data in motion"; y, la segunda que forma, que mantiene cifrados los datos cuando se encuentran en el dispositivo y se conocen como "data at rest".

En el mundo actual el desarrollo de los algoritmos de cifrado garantiza que la comunicación entre dispositivos móviles sea muy difícil de romper, para ello existen algoritmos como AES256, Blowfish, Diffie-Hellman y otros. Por lo tanto los grupos ciberdelincuentes localizan a sus víctimas más frecuentemente por la inseguridad de los datos en reposo, que se encuentran almacenadas en sus respectivos dispositivos.

Es indispensable para las personas hoy en día garantizar la seguridad de las comunicaciones y evitar ser otra víctima de ataques informáticos, y esto tiene tanto que ver con las medidas preventivas que cada persona considera necesarias para su protección, como con la tecnología que utiliza para su uso diario.

Saludos cordiales a todos los alumnos de las asignaturas de seguridad informática y ciberseguridad.

SECaaS Security as a Service

SCProgress brinda el servicio más completo de seguridad informática optimizando los recursos y garantizando la Confidencialidad, Integridad y Disponibilidad de los sistemas.

FireSecure: El primer nivel de servicio que ofrece detalles de evaluaciones a los firewall, manejo de políticas de seguridad, verificaciones de cumplimiento de políticas, fortalecimiento de los Firewall, así como, políticas de remediación.
Con éste servicio se realiza una (1) auditoría por año.

SecurePlus: Una vez realizado el proceso de FireSecure, se brinda a los clientes el servicio SecurePlus, con el cual se ofrecerán reportes mensuales en los siguientes temas:

- Threat Intellicenge (Análisis de Amenazas)
- Breach Detection (Análisis de Vulnerabilidades)
- Event Correlation (Correlación de eventos)
- Incident Response (Respuesta a incidentes)
- Proactive Monitoring (Monitoreo constante de la seguridad de la plataforma)

Vulnerability Assessment & Pen Testing (Evaluación de Vulnerabilidades y Tests de Penetración): El nivel mas alto de evaluaciones de vulnerabilidades de los sistemas en toda la red, se elabora un informe detallado de test realizados y amenazas encontradas.

SCProgress recibe los mensajes automatizados del Centro de Operaciones en los casos de que exista detección de nuevas vulnerabilidades, ransom o amenazas, para coordinar las acciones a tomar con el cliente junto con el equipo de remediación (técnicos).

Inteligencia de amenazas

Alertas de seguridad en tiempo real

Administración de eventos y logs

Análisis y correlación de eventos

Monitoreo 24x7x365

Gestión de respuesta a incidentes

Auditoría y solución de errores del firewall

VAPT

Gestión total del perímetro de seguridad

Novedades

Ganadores de la encuesta de conocimientos SCProgress

"Un niño siempre puede enseñar tres cosas a un adulto: a ponerse contento sin motivo, a estar siempre ocupado con algo y a saber exigir con todas sus fuerzas aquello que desea."

- Paulo Coelho -

SCProgress en homenaje a los niños y para festejar su día, realizó una encuesta de conocimientos sobre sus productos y servicios, las dos puntuaciones más altas fueron los grandes ganadores de dos fabulosas Tablet's de última generación.

Gracias a todos nuestros clientes y seguidores por su fantástica participación, seguiremos organizando promociones para premiar su valiosa confianza, continúen siguiéndonos en la página web www.scprogress.com y redes sociales.

SCProgress, empresa siempre comprometida a satisfacer las necesidades de sus clientes a nivel nacional e internacional, con soluciones de software y hardware en seguridad informática y todo lo necesario para que su infraestructura tecnológica se encuentre a la vanguardia en seguridad y tecnología.

Sr. Daniel Valencia
Ganador de Tablet

Sr. Fernando Cando
Ganador de Tablet

Noticias

Alibaba dispara sus ventas pero gana un 42% menos en el último año

El gigante del comercio electrónico chino supera por primera vez la barrera de los 500 millones de usuarios móviles

Logotipo de Alibaba en su sede en Hangzhou

El grupo Alibaba, propietario de las plataformas de comercio electrónico más grandes del mundo, ganó en el último ejercicio fiscal unos 5.380 millones de euros, una cifra un 42% menor a la registrada el año anterior. La empresa fundada y dirigida por Jack Ma registró un fuerte repunte de las ventas, lo que demuestra la buena salud del sector en el gigante asiático, y logró superar por primera vez la barrera de los 500 millones de usuarios que se conectan a través de dispositivos móviles.

La facturación del grupo alcanzó los 20.660 millones de euros en el último año (la compañía cierra su año fiscal en marzo porque en noviembre celebra el Día del Soltero), un aumento del 56% y mantuvo el crecimiento de los costes por debajo del de las ventas. La caída del beneficio neto se explica por las ganancias anormalmente altas que se registraron el año anterior, derivadas de la desconsolidación de Alibaba Pictures, su división de películas, y la revalorización de su participación en Alibaba Health, la de salud. El beneficio operativo de la empresa creció un 65%, según informó en un comunicado.

Alibaba nació como una compañía de comercio electrónico, aunque se ha expandido en muchas otras áreas para diversificar el riesgo que comporta depender tanto de un sector y de un mercado: el chino. Sin embargo, tres cuartas partes de sus ingresos proceden de las compras online de sus 507 millones de usuarios móviles en el gigante asiático. Las nuevas divisiones de computación en la nube, de entretenimiento o de innovación disparan sus ventas, pero aún no arrojan beneficios. En cuanto a su actividad en el exterior, aunque AliExpress crece y la plataforma Lazada -muy popular en el sudeste asiático- se ha integrado completamente, el negocio en el extranjero no llega al 10% del total.

En el periodo enero-marzo, último del año fiscal y tradicionalmente el más flojo de todos, las ventas de Alibaba crecieron un 60% hasta los 5.040 millones de euros y su beneficio neto alcanzó los 1.290 millones, un 85% más con respecto al mismo trimestre del año anterior. La compañía anunció también un programa de recompra de acciones en los próximos dos años.

El precio de los títulos de Alibaba se ha revalorizado un 56,5% en el último año y toca máximos históricos en torno a los 120 dólares.

Esta subida ha convertido a Jack Ma en el hombre más rico de China, con una fortuna estimada en unos 28.800 millones de euros, superando al magnate del ladrillo y del entretenimiento Wang Jianlin, presidente de Wanda, según cálculos de las revista Forbes. En la apertura de Wall Street justo después del anuncio de resultados, sin embargo, las acciones de la empresa se dejaban más de un 4%.

FUENTE:

- economia.elpais.com/economia/2017/05/18/actualidad/1495112592_321089.html

Qué se puede hacer con 1 bitcoin (o por qué 1฿=1.600€)

La criptodivisa nacida en 2009 vale ahora más que nunca, pero su uso se ha ido alejando de la idea que imaginaron sus primeros impulsores

El bitcoin es una criptomoneda concebida en 2009. El término se aplica también al protocolo y a la red P2P que lo sustenta, y de forma común se denomina como una moneda digital, usados informalmente, se caracteriza por ser descentralizado, es decir, no está respaldado por ningún gobierno ni depende de la confianza de un emisor central, sin embargo se encuentra creciendo aceleradamente.

A mediados de mayo su tipo de cambio superaba por primera vez los 1.600 euros. Llegó a los 1.685 cuando en la primera semana estaba en 1.350. Un ritmo imparable que no se había vivido ni siquiera cuando en 2014 pareció resurgir con el interés de algunas grandes empresas por facilitar este medio a sus clientes.

Microsoft, Dell, Expedia, hasta Paypal, con cuyo sistema de pago rivalizaba, decidió aceptar la criptomoneda, y aún lo hace. En España la web de turismo Destinia era la gran abanderada. El bitcoin era "la moneda de la sociedad civil" y prometía cambiar el comercio a través de Internet. Podemos decir que no ha sido así. Y, sin embargo, su éxito es innegable.

A pesar de su costo y las facilidades que brindaba tras su aparición, "*El interés en utilizar el bitcoin como medio de pago se ha ido perdiendo*", certifica Jorge Ordovás, director del posgrado sobre bitcoin y blockchain de la Universidad Europea de Madrid (UEM) y cofundador de NevTrace, empresa de servicios y laboratorio de ideas en torno a esta tecnología.

En general se ha vivido una paradoja entre oferta y demanda que ha estancado su uso comercial. No había establecimientos que aceptasen el bitcoin porque no había clientes que quisieran pagar con bitcoins. Y los compradores no concebían utilizar este método porque no estaba presente en su día a día y no percibían ventajas en descargar un monedero (el software en el que se almacenan las criptomonedas, para después utilizarlas en comercios digitales o establecimientos físicos que las acepten) y comenzar a convertir euros o dólares en dinero digital. "*Es la pescadilla que se muerde la cola porque al usuario común no le otorga prácticamente ninguna ventaja*", explica Ordovás.

En sí, el bitcoin no abarata los precios, ni acelera las transacciones de forma notable. Pero tiene otras características que explican su uso entre la más notable e importante, la garantía de anonimato.

FUENTE:

- http://elpais.com/elpais/2017/05/15/talento_digital/1494866873_367286.html
- https://es.wikipedia.org/wiki/Bitcoin

Asesoría y consultoría en Comercio Electrónico

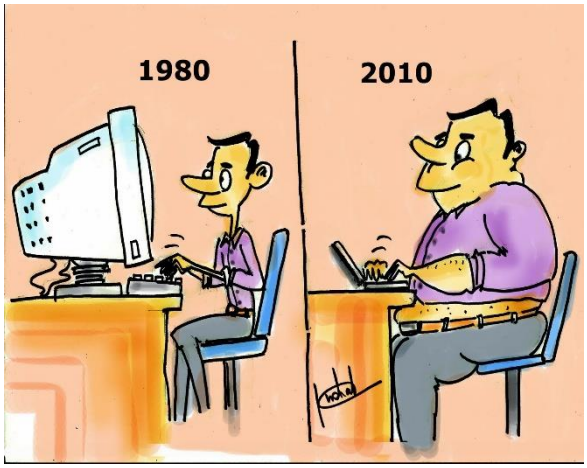
La gestión que marca la experiencia digital de sus compradores, requiere del asesoramiento para mejorar las prácticas de trabajo en su negocio digital, a través de profesionales altamente especializados en temas tan imprescindibles como:

- **Innovación & Design Thinking**
- **Procesos creativos para la creación de productos y servicios de valor**
- **Análisis de Mercados, descubrimiento de necesidades y propuestas de valor**
- **Estrategias de manejo efectivo de clientes**
- **Técnicas de Negociación y Manejo de Reuniones**
- **Emprendimiento tecnológico**
- **Márketing para Pymes de IT**
- **Finanzas del emprendedor**
- **El modelo Canvas y la Planificación estratégica**
- **El modelo Canvas y la Marca Personal**
- **Cultura Corporativa enfocada en los negocios y las personas**
- **Lectura Política, Económica y Social del entorno de negocios**
- **Networking y Asociación Social de negocios para Ejecutivos de IT**

La gestión y administración de su empresa online, en conjunto con el seguimiento adecuado de clientes, pueden mejorar, desarrollar y establecer prácticas y procesos para atraer, retener e incrementar su base de datos de nuevos clientes.

La era digital y los negocios en línea se encuentran en progreso y desarrollo continuo. Contáctenos en el correo electrónico: **camiranda33@hotmail.com**, un asesor le brindará la información necesaria, de acuerdo a sus requerimientos y los de su empresa.

Humor



¿Son seguras las firmas digitales?

Cuando hablamos de firmas digitales, pueden surgir algunas dudas como ¿Son seguras?, si profundizamos un poco en el tema, podemos ver que en realidad es más seguro y más inseguro, dependiendo de cómo entendamos la seguridad.

La firma digital es más segura porque, a diferencia de la firma tradicional, los procedimientos matemáticos y algoritmos asociados a ésta la hacen que sea matemáticamente casi imposible imitar.

Al mismo tiempo es más insegura y vulnerable porque depende de unos procedimientos y algoritmos que el individuo usa pero, en el 99% de los casos, no comprende, mientras que la firma tradicional está completamente controlada por el individuo. Dependiendo de la configuración del dispositivo que se use y del escaso conocimiento de las operaciones que se realizan, puede ocurrir que un dispositivo firme digitalmente por mí y esto tenga trascendencia económica, legal o ambas. Entonces, ¿por qué decimos que la firma digital es tan segura?.

Durante la firma digital se utiliza un documento electrónico conocido como certificado digital X.509. No nos asustemos, X.509 es simplemente el nombre de una norma y un certificado digital, es esencialmente un documento con el que la firma digital obtiene una seguridad criptográfica fuerte. Esta seguridad criptográfica proviene del uso de una serie de claves y de algoritmos de cifrado.

La realidad de los algoritmos criptográficos es bien compleja, pero vamos a intentar aproximarnos a cómo se consigue esta seguridad mediante criptografía. En primer lugar necesitamos dotar a nuestro documento firmado digitalmente de autenticación. Llegue a donde llegue ese documento queremos que pueda comprobarse que quien lo envía es la persona que lo ha firmado digitalmente.

Para dotar de autenticación a la firma digital -que no es más que una serie de bytes asociada al mensaje- se aplican dos tipos de algoritmos criptográficos diferentes al documento que se quiere firmar. Por último, cada uno de estos tipos

de algoritmos depende de una clave concreta y, en el caso del algoritmo más relevante, esa clave es el contenido más importante -pero no el único- del ya famoso certificado digital X.509.

¿Podrían ser falsificadas?

Debido a su naturaleza segura, no se escucha hablar de muchos intentos exitosos de robo de firmas digitales o mal uso de las mismas. Como se basan en mecanismos y algoritmos de cifrado bastante robustos, para ser vulneradas se necesitan de capacidades de cómputo muy grandes que llevan a que sea matemáticamente imposible hacerlo.

La seguridad de una firma electrónica va a estar relacionada con las características que ofrezca para identificar unívocamente al usuario que hace la firma y con la posibilidad de generar una trazabilidad de las transacciones, de tal forma que a través de una auditoría se pueda verificar el usuario y el momento de la transacción.

Por lo tanto, el factor humano se convierte en la principal amenaza para poner en riesgo la información protegida con este tipo de mecanismos. Sin embargo, como sucede con cualquier mecanismo de seguridad, dependiendo del uso que le den los usuarios, podría ser vulnerada, pero no es lo más frecuente.

Garantizando la seguridad

La seguridad de una firma digital se da de la siguiente forma:

- Se calcula el hash de un documento a través de una función hash.
- El documento es cifrado utilizando un algoritmo de clave asimétrica con nuestra clave privada.
- Enviamos el mensaje original y el hash cifrado.
- El recipiente de nuestro mensaje la recibe, calcula su hash y sabe que no hubo adulteración del mensaje, de lo contrario el hash calculado por él no puede ser igual al incluido en el mensaje original.

Con todo esto, el mensaje al que se ha añadido el hash cifrado está firmado digitalmente, su autenticidad está comprobada, el mismo no ha sido alterado y el autor del mismo es reconocido. Esta es una forma bastante segura y utilizada en larga escala globalmente.

3 mecanismos de seguridad necesarios

1. Que la firma pueda ser generada solamente por un usuario
2. Que pueda ser fácilmente verificable por quien la recibe
3. Permitir un fácil uso de la misma para quien las genera y recibe

Para evitar el acceso no autorizado de terceros, es importante contar con software de seguridad que impida el mismo. Además es importante mantener nuestros datos cifrados y agregar una capa adicional mediante la doble autenticación a nuestras redes, sitios y aplicaciones para evitar que un atacante pueda acceder los mismos.

Los riesgos de la firma electrónica

La firma electrónica avanzada es confiable y segura debido a que como ya sabemos hace uso de un cifrado asimétrico, entonces nos preguntamos ¿de dónde vienen los riesgos?. Estos riesgos provienen como siempre del eslabón más débil que es el usuario final que hace uso de la misma.

Para realizar la firma electrónica avanzada se debe hacer uso de dos claves la pública y la privada. La clave pública es la que puede ser mostrada y accedida por un tercero y la privada será la que en ningún caso podrá ser conocida o accedida por otra persona, ya que esta clave lleva integrada nuestra identidad y nuestra firma. Por tanto, aquí podemos encontrar el mayor riesgo, que es la forma en la que se guarda esta clave privada en nuestros sistemas o si la misma es compartida o esta visible para otras personas.

El tener al descubierto la clave privada es un riesgo muy grave, ya que la custodia exclusiva de la misma es la garantía de no repudio de nuestras futuras firmas electrónicas, por lo que cualquier persona que disponga de la misma podrá realizar firmas fraudulentas con el mismo valor legal que si firmara a mano alzada. Por ello, es un riesgo muy grave ya que el conocimiento de una tercera persona de la clave puede traer consigo la suplantación de identidad, se podrá hacer pasar por nosotros y firmar en cualquier sitio.

En caso de haber entregado la firma electrónica, al dejar de trabajar con un proveedor se debe revocar ese certificado y generar uno nuevo que queda vigente desde el mismo momento en el que se genera. En el caso de que sea inevitable el uso de la firma por terceros, lo recomendable es que ese tercero compre su certificado propio y se le da la autorización para que con ese certificado realice los trámites correspondientes, y así de esta forma nunca conocerá ni hará uso de nuestras claves.

FUENTES:

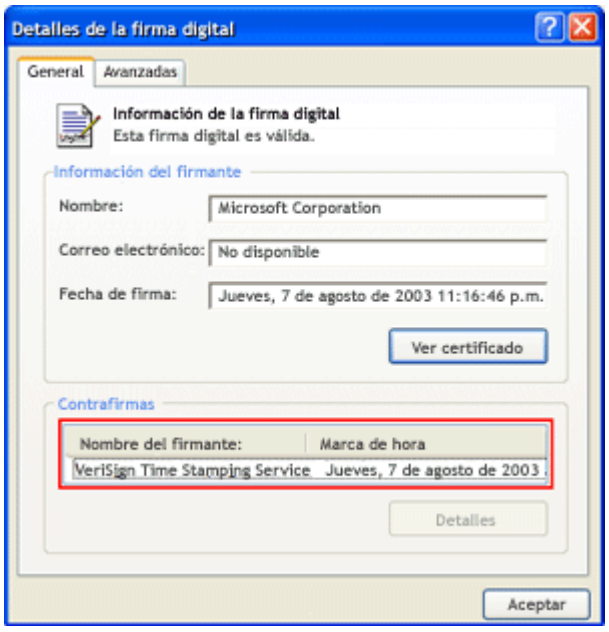
- http://divulgauned.es/firma-digital/
- http://blog.notificaciones060.com/certificadodigital-notificaciones060.html
- https://blogs.deusto.es/master-informatica/los-riesgos-de-la-firma-electronica/
- https://www.welivesecurity.com/la-es/2014/05/12/son-seguras-firmas-digitales/

¿Cómo se sabe si una firma digital es fidedigna en Windows?

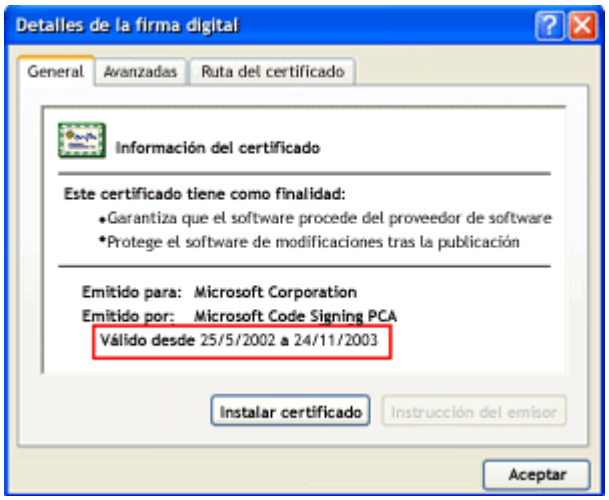
En esta sección, se describe lo que se debe buscar al evaluar la confiabilidad de una firma digital.

La firma digital es correcta

Una firma digital válida se identifica por un mensaje en la parte superior del cuadro de diálogo Detalles de la firma digital que confirma que la firma digital es correcta. También debe observar los detalles de la marca de hora en el campo Contrafirmas. Los detalles de la marca de hora indican que la entidad emisora de certificados, en este ejemplo VeriSign, ha comprobado y aprobado la firma digital.



La fecha de la marca de hora, en este caso 7 de agosto de 2003, debe estar dentro del intervalo de fechas Válido desde del certificado. Para ver el intervalo de fechas de la firma digital, haga clic en Ver certificado.



El editor, en este caso Microsoft Corporation, debe ser un editor de confianza de forma predeterminada en los equipos en los que se ejecute el sistema operativo Microsoft Windows. Los certificados de Microsoft se encuentran en el almacén de las Entidades emisoras raíz de confianza. Si el editor no es de confianza de forma predeterminada, debe confiar explícitamente en él. De lo contrario, el contenido firmado por ese editor no pasa las comprobaciones de seguridad del software.

Buscar la X roja

Una firma digital con problemas muestra la imagen con una X roja.

La X roja puede aparecer por las razones siguientes:

- La firma digital no es válida por alguna razón; por ejemplo, el contenido se ha modificado desde que se firmó.
- Esta firma digital ha caducado.
- El certificado asociado a la firma digital no fue emitido por una entidad de certificación (CA). Por ejemplo, sería un certificado autofirmado creado con Selfcert.exe.
- El editor no es de confianza.

Qué debe hacer si hay un problema con una firma

Cuando haya un problema con una firma digital, en función de la situación, puede hacer lo siguiente:

- Ponerse en contacto con la fuente del contenido firmado y hacerle saber que hay un problema con la firma.
- Ponerse en contacto con el administrador de IT a cargo de la infraestructura de seguridad de la organización.
- Si cree que la macro u otro contenido activo asociado al documento son de confianza, puede guardar el documento en una ubicación de confianza. Los documentos de las ubicaciones de confianza pueden ejecutarse sin someterse a la comprobación del sistema de seguridad del Centro de confianza. El uso de ubicaciones de confianza es una opción mejor que bajar el nivel de configuración del nivel seguridad de todas las macros.
- Puede confiar en el editor explícitamente.

FUENTES:

- https://support.office.com/es-es/article/C%C3%B3mo-se-sabe-si-una-firma-digital-es-fidedigna-0464f8ab-fefa-4bc7-af0d-e07a12f7097e
-

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Junio 2017