CIBERSEGURIDAD

SCP

Seguridad de las Comunicaciones en los Dispositivos Móviles

Cyberoam

Avira

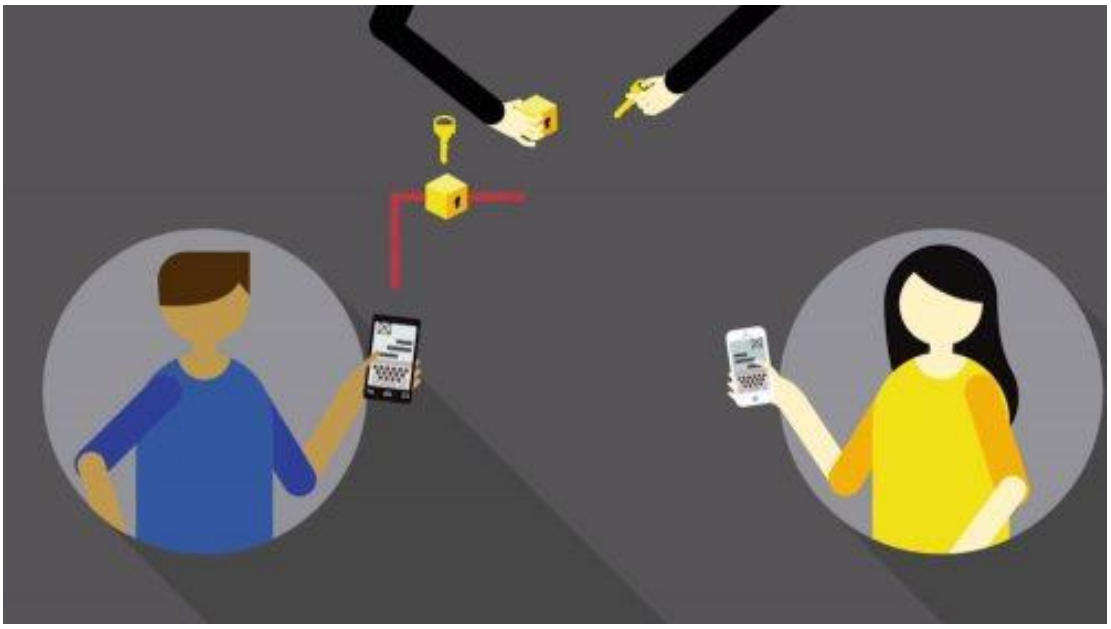
NEXXT SOLUTIONS

CRYPTOPHONE™

Cloud24x7

open source™

Índice



“Un sistema no es bueno por el hecho de que se pueda confiar en los usuarios del

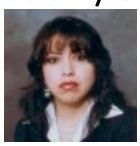
mismo, un sistema necesita ser robusto ante intrusos”

— Robert Morris, Director científico de la NSA —

CRÉDITOS:

Revista virtual de seguridad informática, 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:

SCProgress

www.scprogress.com

Facebook

Twitter

La Seguridad en los Dispositivos Móviles

Con el pasar de los años, los teléfonos móviles han experimentado una intensa evolución que ha llevado a utilizar desde gigantescos equipos hasta los actuales smartphones, estos dispositivos que poseen características similares a las de una computadora portátil son utilizados por las personas para trabajar en forma más eficiente y eficaz.

El desarrollo socioeconómico depende de estar comunicado. Las empresas necesitan buenos enlaces con sus proveedores, clientes, empleados. Por lo que estos teléfonos inteligentes permiten hacer cada vez más tareas, como: conectarse a Internet y compartir en redes sociales, navegar en la web, revisar el correo electrónico, y realizar trámites bancarios en línea, entre otros.

Los usuarios almacenan cada vez más información personal y sensible, que además de estar expuesta al robo físico del dispositivo, puede resultar valiosa para los ciberdelincuentes que buscan obtener ganancias ilícitas utilizando códigos maliciosos u otras amenazas. Pese a que no todos los sistemas operativos del mercado móvil son igual de atacados por códigos maliciosos, existen varias recomendaciones generales que aplican a todo tipo de casos, dispositivos y usuarios.

Los teléfonos celulares, así como, en cualquier otro equipo tecnológico, requieren contar con los cuatro principios básicos de seguridad de la información: confidencialidad, integridad, autenticación y no repudio.

En la actualidad existen diversos tipos de ataques y/o riesgos que puedan existir para los usuarios de smartphones: malware, phishing, fraudes y robo o pérdida del dispositivo. Cada uno de estos riesgos perjudica al usuario de diferentes maneras.

Por lo general, el éxito en la propagación de cualquier tipo de amenaza informática (exceptuando la pérdida del teléfono) radica principalmente en las estrategias de Ingeniería Social que el cibercriminal utilice. Para este tipo de dispositivos es común que se usen temáticas específicas para este segmento, como troyanos que se expanden con la excusa de ser algún determinado juego mobile, o incluso se han llegado a reemplazar códigos QR legítimos por otros que no lo son, para dirigir al usuario a un sitio que descarga alguna clase de código malicioso.

Una vez que el ciberdelincuente ha escogido una temática, procede a expandir masivamente alguna amenaza.

Aunque hace algunos años la problemática de los códigos maliciosos afectaba predominantemente a equipos estándar como PC de escritorio o

portátiles, en la actualidad también representan un riesgo para los usuarios de smartphones.

Actualmente, la mayoría de las familias de códigos maliciosos para Android y otras plataformas tienen como objetivo la suscripción a servicios SMS premium y el control del dispositivo. En menor cantidad, geolocalizar a la víctima a través del GPS o instalar más amenazas en el sistema.

Las redes sociales permiten un nivel de interacción impensado antes de su invención, además han logrado un gran impacto y alcance en poco tiempo. De esta forma, sus características hacen que estos servicios sean muy apetecidos por los usuarios. Sin embargo, lo mismo ocurre con los cibercriminales quienes invierten tiempo y recursos en crear códigos maliciosos que se propaguen por esta vía. Por otro lado, una incorrecta configuración de la cuenta de la red social puede exponer información del usuario a terceros, facilitando el robo y suplantación de identidad.

¿Cuáles son las principales amenazas que afectan a los dispositivos móviles? ¿Qué medidas puede adoptar el usuario para mitigar el impacto de este tipo de ataques y peligros?, entre otras preguntas, son realizadas con mucha frecuencia, por lo que SCProgress, en esta edición, realiza una recopilación de información para solventar este tipo de interrogantes, de tal forma que nuestros lectores puedan hacer un uso seguro y consciente de estos dispositivos móviles.

FUENTES:

- https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_6).pdf
- http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion4/leccion4.html
- http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf
- https://cartilla.cert.br/fasciculos/dispositivos-moviles/fasciculo-dispositivos-moviles-slides.pdf
- http://www.monografias.com/trabajos11/telcel/telcel.shtml#ixzz4klmUMdDM
- https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf

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

Principales Riesgos y Amenazas de los Dispositivos Móviles.

Cada vez más los dispositivos móviles se asemejan a las computadoras personales o portátiles, su funcionalidades son similares, por lo que, los riesgos también son similares, como por ejemplo: código malicioso, phishing, acceso a contenidos impropios u ofensivos, contacto con personas mal intencionadas, pérdida de información, dificultad para proteger la privacidad entre otros. Sin embargo las características de los teléfonos celulares inteligentes, los hacen mucho mas atractivos a los ojos de los atacantes.

Con los dispositivos móviles cada vez más presentes en nuestro lugar de trabajo, es imprescindible conocer las principales amenazas de seguridad que traen consigo, además de enseñar a prevenir que se produzcan las temidas brechas de seguridad.

Hace ya 13 años de la llegada del primer programa malicioso para dispositivos móviles, en 2004, pero ha sido durante los últimos años cuando estos programas realmente se han convertido en una amenaza para los usuarios. De hecho, el rápido crecimiento en el uso de teléfonos inteligentes y tabletas durante los dos últimos años ha conducido inevitablemente a que estos dispositivos se conviertan en objetivo prioritario de los ciberdelincuentes.

El crecimiento exponencial de los dispositivos ha provocado un aumento de programas maliciosos dirigidos a estos. Cuando pensamos en las tendencias de seguridad en el campo de las tecnologías de la información, suelen venirnos al pensamiento los firewalls, los dispositivos de seguridad, políticas y amenazas como malware, ransomware y troyanos. Pero eso era seguridad antes de la invasión móvil.

Con este antecedente, ponemos en su conocimiento los principales ataques cibernéticos a los dispositivos móviles con mayor impacto durante este año:

Phishing.- es una modalidad de fraude electrónico. Consiste en el envío de un email aparentando ser remitido por una empresa o institución fiable, con el fin de obtener datos confidenciales del usuario. El phishing es uno de los métodos favoritos de los hackers, que envían tres de cada cuatro campañas de malware por email. Es, además, uno de los que más ha crecido y lo seguirá haciendo en los siguientes años.

Ransomware en móviles.- (software malicioso que encripta archivos y luego pide el pago de un rescate) aumentó más de tres veces durante los primeros meses del año, el 86 por ciento de estos archivos tuvieron relación con la familia de troyanos Congur, que se encargan de cambiar la contraseña de acceso del dispositivo o establecen una propia si no había y así consiguen los derechos de administrador en el dispositivo.

El ransomware dirigido a dispositivos móviles se disparó y nuevas familias, así como modificaciones, siguen proliferando. Las personas deben tener en cuenta que los atacantes pueden —y lo harán cada vez más— bloquear el acceso a sus datos no sólo en una PC, sino también en su dispositivo móvil.

Debemos considerar que los correos electrónicos fraudulentos no solo sirven para el robo de identidades, también pueden contener ransomware.

Wifi inseguro.- Se ha convertido en algo cotidiano utilizar nuestros dispositivos móviles en las cafeterías y otros lugares que ofrecen conexión inalámbrica gratuita, pero cuando nos conectamos a esos puntos de acceso gratuitos, pueden producirse transmisiones inseguras de datos. Es fundamental que sepamos que esta práctica es sumamente peligrosa y que solo debemos conectarnos de forma segura a este tipo de Wifi utilizando una VPN, pues de otra manera nuestra conexión puede ser espiada mediante el conocido MIT (hombre en medio).

Software desactualizado.- Casi un tercio de los dispositivos presentes en el mercado hoy en día están ejecutando una versión obsoleta de Android, haciendo que estos Smartphones sean mucho más sensibles a ataques externos y otras vulnerabilidades.

Los dispositivos móviles necesitan que su software y su sistema operativo sean actualizados con la mayor frecuencia posible. Algunos Smartphones contienen datos aún más sensibles que algunas redes corporativas, como pueden ser los números de teléfono, números de tarjetas de crédito, cuentas bancarias, ubicaciones y contraseñas. Por tanto, el uso de software obsoleto puede crear riesgos de seguridad para esos datos.

Software malicioso.- Nunca debes de permitir que se instalen en tu Smartphone programas de fuentes desconocidas. Estas aplicaciones ilegítimas pueden fácilmente extraer datos personales y/o corporativos, y transmitirlos a terceros. Los juegos y las aplicaciones de redes sociales siempre son los más deseados, y los usuarios en muchos casos se apresuran a descargarlos de fuentes no seguras para obtenerlos con más celeridad, lo que les puede acarrear más de un dolor de cabeza.

Educación tecnológica deficiente.- Los usuarios de ordenador saben que no deben abrir archivos adjuntos o facilitar contraseñas en formularios. Por el contrario, muchos usuarios móviles han dejado a un lado esas preocupaciones, simplemente porque piensan que sus teléfonos inteligentes son inmunes a los hackers. Pero nada más lejos de la realidad. Las plataformas móviles son más vulnerables que los ordenadores, por lo que los usuarios no pueden dar por sentado la seguridad de la información que contiene su Smartphone.

Autenticación.- El hackeo de tus redes sociales o de tu nube se produce principalmente debido a contraseñas débiles, pero los atacantes pueden

hackear incluso contraseñas fuertes. Para evitar este tipo de problemas de autenticación, es fundamental implementar la autenticación de dos factores.

Ataques a dispositivos móviles.- (smartphones y tablets).- En los últimos años, el uso de smartphones y tablets han crecido exponencialmente, por este motivo, los ataques a dispositivos móviles con malware seguirá en aumento. Check Point señala que el 20% de los empleados de una empresa será responsable de alguna brecha de seguridad poniendo en riesgo los datos corporativos. Esto lo harán sin saberlo, ya que será a través de malware en el propio dispositivo móvil o porque se han conectado a un Rogue AP y un cibercriminal ha conseguido sus credenciales mediante ataques MIT (hombre en medio).

Recientemente algunos países han atacado a móviles de periodistas, lo que pone de manifiesto que los ataques a dispositivos móviles están a la orden del día.

FUENTES:

- https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_6).pdf
- http://www.fundacionctic.org/sat/articulo-seguridad-en-los-dispositivos-moviles-smartphones-y-tablets
- https://eventosti.net/blog/2017/03/16/ataques-dispositivos-moviles-se-mantiene-principal-amenaza/

Capacitación en Ciberseguridad y Antimalware

"La necesidad de capacitación surge por la diferencia entre lo que uno debería saber y lo que sabe realmente"

El personal responsable de las áreas de sistemas, así como los usuarios, deben conocer sobre la infinidad de ataques informáticos amenazas, ataques a la información y a las infraestructuras tecnológicas, los mantienen como áreas vulnerables permanentes, facilitando las actividades fraudulentas de hackers, quienes han visto como un gran negocio lucrativo, la sustracción de datos, ya sea personal, financiera, confidencial, etc.

La capacitación en seguridad informática, se vuelve relevante e importante para evitar que las empresas e instituciones, se vean afectadas ante este tipo de amenazas.

SCProgress cuenta con asesores altamente especializados a nivel internacional, lo que nos permite brindar cursos de capacitación en diversos temas tecnológicos, especialmente en el área de seguridad informática, su amplia experiencia y conocimientos, les ha permitido participar en eventos nacionales e internacionales como la conferencia organizada por la CEPOL Research & Science Conference (Organismo acreditado de la Unión Europea), realizada en Budapest el año 2016.

En esta ocasión SCProgress, consiente de la importancia que prestan las instituciones a la seguridad de la información, y ante el incontrolable crecimiento de las amenazas, ha organizado y pone a disposición de sus lectores y clientes, capacitación en los siguientes temas:

Certificación en Ciberseguridad de la RED	Introducción al análisis y comportamiento del malware
Contenido: • Fundamentos de red de computadoras y defensa • Amenazas, vulnerabilidades y ataques a la red • Controles, protocolos y equipos para la seguridad de la red Diseño e implementación de políticas de seguridad en la red • Seguridades físicas • Seguridades en los Host • Configuración y administración segura de Firewalls • Configuración y administración segura de IDS • Configuración y administración segura de VPNs • Protección de redes inalámbricas • Monitoreo y análisis del tráfico de la red • Gestión de riesgos y vulnerabilidades • Data backup y recuperación de datos • Respuesta y manejo de incidentes	**Contenido:** • Análisis de malware • Indicadores de infección • Malware signatures • Categorías de malware • Mass vs Targeted malware • Metodología de análisis de malware • Herramientas Antimalware • Malware empaquetado y oculto • DLL Hijacking • Magic labels • Formatos de archivos • Dynamic Link Libraries • Detección de virtualización de malware • Dependency Tracing • Modificación de registros • Manipulación de archivos del sistema • Análisis de tráfico de la red • Sandboxes

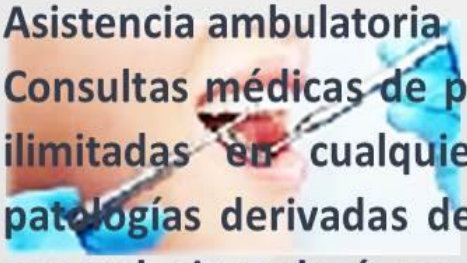
Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

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

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

CryptoPhone. Dispositivos Móviles Seguros Desde su Diseño.

Como hemos visto en los temas anteriores, la seguridad en los dispositivos móviles debe ser considerada como la principal prioridad, para mantener nuestra información segura contra ciberataques.

Los usuarios, deben observar los mecanismos de seguridad disponibles para los diferentes modelos y fabricantes de teléfonos celulares, principalmente debemos seleccionar el más seguro para nuestra información y de las empresas.

La empresa alemana GSMK CryptoPhone, es la primera en desarrollar, producir y comercializar teléfonos móviles blindados contra todo tipo de ataques como troyanos, virus y malware, y, por sobretodo espionaje. Sus equipos de telefonía cifrada fijos y celulares, utilizan sistemas de encriptación de VoIP, ofreciendo una protección móvil de 360 grados.

Las principales características de estos dispositivos móviles son:

- La primera y única solución completamente confiable para comunicaciones confidenciales de telefonía móvil.
- Son fáciles de usar y proveen una adecuada seguridad sin complicaciones.
- Son cifradas con llaves de 256 bits utilizando AES y Twofish como "counter mode stream ciphers", ofreciendo seguridad a largo plazo. No poseen backdoors para nadie y pueden ser verificados por investigadores independientes.
- Ofrecen una protección mundial para sus llamadas confidenciales.

Estos dispositivos móviles son completamente seguros, ya que al cifrar con AES y Twofish resulta en un cifrado mucho más seguro que al utilizar un solo algoritmo. Dada el muy improbable caso en que se descubra una debilidad en uno de los algoritmos, el uso del segundo algoritmo provee un buen margen de seguridad. La utilización de dos algoritmos fuertes es una propiedad única de Cryptophone. La llave utilizada es creada mediante un intercambio de llave secreta Diffie-Hellman de 4096 bit.

¿De qué amenazas protege CryptoPhone?

Cryptophone se encuentra diseñado para ofrecer protección contra todo aquel que intente escuchar conversaciones, tanto en la red fija como la de aire. Cryptophone provee seguridad punta a punta encriptando todo el camino entre ambos teléfonos.

Es importante destacar que para realizar espionaje a teléfonos celulares, hoy en día existe un dispositivo llamado IMSI-Catcher que permite que cualquier persona pueda escuchar llamadas en redes móviles, los mismos están disponibles en el mercado y se utilizan cada vez más con mayor frecuencia. Todas estas intromisiones se pueden controlar fácilmente, si utiliza los dispositivos móviles de Cryptophone.

SCProgress es la única empresa autorizada en el Ecuador, para la venta y distribución de los teléfonos Cryptophone, contáctenos a ventas@scprogress.com, para una demostración y proporcionarle asesoramiento, sobre la mejor opción para usted y su empresa.

FUENTES:

- http://www.scprogress.com/cinco/?q=GSMK_Cryptophone
- http://www.cryptlab.com/cryptophone/qa/technical/index.html
- http://www.cryptlab.com/cryptophone/qa/index.html
- https://www.welivesecurity.com/la-es/2016/12/20/dispositivos-moviles-seguros-diseno/

Rincón de los Expertos

Teléfonos Celulares, el Gran Riesgo para su Negocio

Los teléfonos celulares se han convertido en computadores de bolsillo, consecuentemente son mayormente vulnerables a los virus, troyanos y todo tipo de malware. Actualmente, son el principal objetivo de ataque por parte de grupos cibercriminales inescrupulosos que intentan someter a personas buenas a través de la extorsión y amenazas. Para conseguir estos objetivos buscan instalar agentes de software (backdoors) en los teléfonos celulares que una vez conectados a redes de datos, transfieren toda la información de los mismos a servidores pertenecientes a estos grupos delincuenciales.

Hoy en día, es importante comprender que los teléfonos celulares inteligentes (smartphones) tienen las mismas capacidades que los computadores; tienen procesadores de 1Ghz y varios cientos de megabytes en memoria RAM. Por lo tanto, los mismos tipos de ataques que se hacen contra los computadores se pueden realizar en contra de los teléfonos celulares, con el mayor inconveniente que a través de los celulares se maneja información más confidencial de las personas e instituciones, y a la vez, si no se toman todas las medidas de protección necesarias, el ciber riesgo existente puede convertir a los celulares, en una arma de geolocalización, espionaje y ciberataque.

Por todo lo antes indicado es importante considerar las siguientes medidas como básicas, para la protección de la información existente en los teléfonos celulares y la privacidad de las personas.

1) Tener un teléfono celular que incluya un sistema operativo endurecido, que entre una de las principales características tenga un firewall.
2) Maneje varios niveles de servicios dependiendo de la persona que lo vaya a utilizar.
3) Un sistema que pueda ser manejado y operado a escala global, independiente del prestador de servicios de Internet, ya sean estos operadores o empresas de telefonía celular.
4) Sistemas de cifrado de alto nivel para la “data in motion” y la “data in rest”.
5) Un producto que cumpla con los más altos estándares de calidad y desde su origen no esté involucrado en temas globales de espionaje.

Bueno, además capacitar a los usuarios en temas de ciberseguridad, seguro contribuirá a mejorar nuestros niveles de Seguridad, Confidencialidad y Productividad.

Les recordamos que hay una versión gratuita de AVIRA antivirus para los sistemas operativos Android y IOS.

Novedades

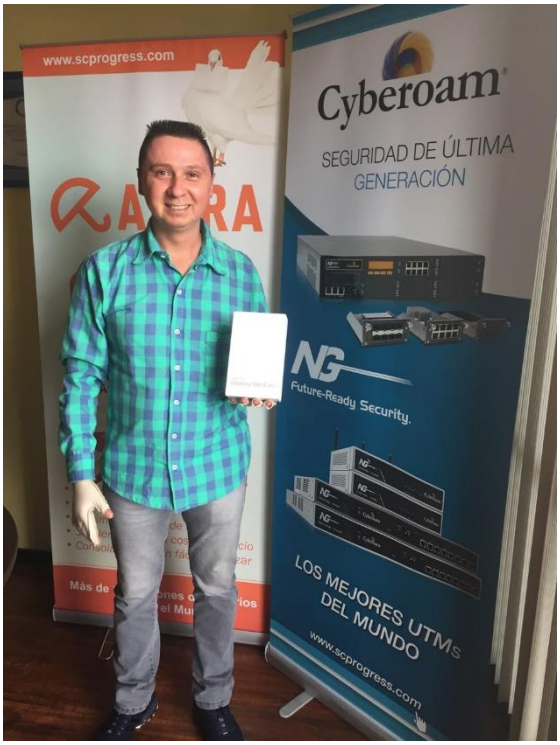
SCProgress Festeja el Día del Padre.

”Un papá es un hijo que parece duro y espinoso por fuera, pero es puro y dulce en su interior”

- Anónimo -

SCProgress para homenajear al padre en su día, realizó una encuesta de conocimientos, en la cual se entregarían fabulosos premios a las tres personas con mejor puntuación, entre los premios se encontraba una Tablet Samsung de última generación para el primer lugar.

Al no existir participantes que hayan respondido correctamente las preguntas y obtengan la puntuación necesaria para la entrega de premios, la empresa SCProgress, en su continua labor social y actuando de forma solidaria y comprometida con la sociedad ecuatoriana, procedió a realizar la entrega de la Tablet, al señor César Augusto Bora Cárdenas, en reconocimiento a su valor y voluntad para salir adelante a pesar de las circunstancias impredecibles que le presentó el destino.



Agradecemos a todos nuestros lectores, clientes, amigos y seguidores por su confianza en todos nuestros productos y servicios, así como, les recordamos que contamos con todo lo necesario en hardware y software, para hacer que su infraestructura tecnológica sea la más segura, con tecnología de vanguardia e innovación, en las marcas más reconocidas a nivel nacional e internacional, y proporcionando el mejor soporte técnico con personal altamente calificado.

Continúen siguiéndonos en nuestra página web y redes sociales, donde podrán encontrar información sobre nuestra empresa, productos, cursos de capacitación y servicios.

Respuestas al Cuestionario Realizado por SCProgress, en Homenaje al Día del Padre.

A continuación presentamos a nuestros lectores las preguntas y respuestas de la encuesta de conocimientos que realizó la empresa SCProgress, para festejar el día del padre, y que se encontró publicada los días 14 y 15 de junio del año en curso en la página web www.scprogress.com y redes sociales.

1. Cuáles son los módulos de Internet Protection (Seguridad en Internet) de Avira?

   Firewall, Web protection, Mail Protection

2. Latin American Quality Institute (LAQI) reconoció y premió a la empresa SCProgress, por sus altos estándares de calidad, productos y servicios a nivel Latinoamérica.

   Verdadero

3. Qué aplicativo de Avira le permite gestionar diferentes contraseñas en cada uno de los medios tecnológicos y redes sociales que dispone.

   Avira Vault

4. De qué curso de capacitación que brinda SCProgress son los temas: El uso de plantillas para la implementación de sitios web; la evaluación de rendimiento del sitio web; y, el seguimiento a través de SEO de Google Analytics.

   Gestión Web.

5. Dentro del curso de certificación en Ciberseguridad de la RED se encuentran los temas: Configuración y administración segura de IDS, configuración y administración segura de VPNs, protección de redes inalámbricas, monitoreo y análisis del tráfico de la red y Gestión de riesgos y vulnerabilidades.

   Verdadero.

6. Enumere todos los algoritmos de cifrado que utilizan los Cryptophone para la “data inmotion”

   Para garantizar la integridad se utiliza Diffie Hellman y SHA 256
   Para garantizar la confidencialidad Twofish y AES256

7. El servicio de SecurePlus, proporcionado por SCProgress, requiere obligatoriamente que se realice primero el servicio de:
   a. Vulnerability Assessment
   b. Pen Testing
   c. FireSecure
   d. No requiere ningún servicio con anterioridad.

8. ¿En qué servicio de seguridad proporcionado por SCProgress, se realiza las evaluaciones de vulnerabilidades, se toman acciones contra nuevas amenazas y se presenta informes mensuales de los test realizados y amenazas encontradas?

   Vulnerability Assessment & Pen Testing.

9. Son temas del curso de Comercio Electrónico proporcionado por SCProgress:
   a. **El impacto de las redes sociales, desarrollo de plan de negocios, evaluación de casos prácticos.**
   b. Evaluación de sitios web, gestores de contenidos CMS, caso práctico de CMS en Drupal.
   c. Todas las anteriores.
   d. Ninguna de las anteriores.

10. Avira antivirus for EndPoint, es un software diseñado exclusivamente para proteger equipos servidores de gama alta.

    Falso.

11. ¿Cuál es el sitio recomendado para leer sobre la evolución de las tecnologías de IoT?

    En la revista No. 39 página 12 en el apartado "El Rincón de los Expertos" se recomendó el URL: https://www.statista.com/topics/2637/internet-of-things/

12. Cyberoam NGFW ofrece inspección y control de:
    a. Aplicaciones en línea y Filtrado Web
    b. Inspección HTTPS y Sistema de prevención de intrusos
    c. VPN (IPSec y SSL) y controles de ancho de banda granulares.
    d. Todas las anteriores

13. Cuál es el último modelo de equipo móvil presentado por Cryptophone en el Mobile World Congress Barcelona 2017?

    CP 600G

14. SCProgress brinda el servicio SECaaS, el cual consta de:
    a. FireSecure, SecurePlus, Vulnerability Asesseent & Pen Testing.
    b. Treat Intelligence, Breach Detection, Event Correlation.
    c. Event Correlation, Incident Response, Proactive Monitoring.
    d. Ninguna de las anteriores.

Humor

Aspectos a Tener en Cuenta en la Seguridad de tu Aplicación de Mensajería Instantánea

WhatsApp, Messenger, Facetime, iMessage, Allo, Telegram, Hangouts, Skype; en la actualidad tenemos docenas de aplicaciones de mensajería instantánea entre las que elegir, cada una con decenas o cientos de millones de usuarios en todo el mundo y con funciones que satisfagan las necesidades de estos en el entorno de la comunicación.

Sin embargo, tal y como sucede en multitud de aspectos relacionados con la tecnología, uno de los apartados que más preocupa a la comunidad es todo aquello que esté relacionado con la seguridad y privacidad de los datos que vayamos a transmitir en este caso. Es por ello que no todas estas aplicaciones de mensajería son igual de fiables a la hora de garantizar nuestra privacidad y seguridad.

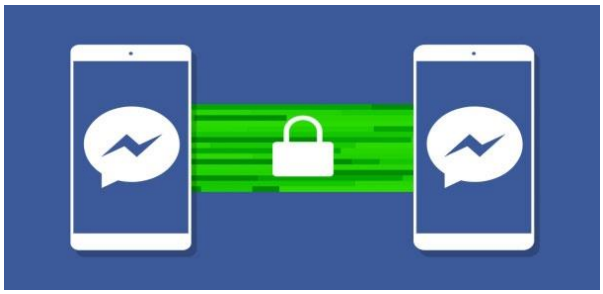
A pesar de todo, usamos todo tipo de aplicaciones de mensajería para intercambiar grandes cantidades de información sensible, ya sea personal, política o relacionada con nuestros negocios. Llegado el caso, en la mayoría de las ocasiones damos por sentado que las medidas de seguridad implementadas en estas aplicaciones son más que suficientes, pero eso es falso, ya que desde el punto de vista de los posibles atacantes, éstos pueden usar nuestra información personal de muchas maneras, llegando incluso a la extorsión.

Es por ello que a continuación vamos a hablar de algunos temas importantes a tener en cuenta a la hora de valorar la seguridad que nos proporciona realmente nuestra app de mensajería instantánea, válidos para todo tipo de sistemas operativos móviles como Android o iOS.

Cifrado:

En primer lugar vamos a referirnos al cifrado que se debería hacer de los datos que transmitimos por estas vías, sean del tipo que sean. Este sistema se centra en el uso de determinados algoritmos matemáticos que se utilizan para

codificar los datos compartidos en estas redes, por lo que se consideran como una de las mejores maneras de evitar que elementos no deseados puedan dar sentido a los mensajes que enviamos. Es precisamente por ello que la gran mayoría de las principales aplicaciones de mensajería usan algún tipo de cifrado para proteger nuestra privacidad.



Sin embargo hay que tener en cuenta que no todos los métodos de cifrado se realizan de la misma manera, de hecho hay algunos de estos servicios que deliberadamente mantienen las llaves para descifrar los mensajes previamente cifrados para poder acceder a su contenido. Esto es algo que se utiliza en algunos casos para, por ejemplo, analizar nuestra información y así poder crear anuncios mejor orientados a cada caso, o para «alimentar» a sus algoritmos de aprendizaje máquina y así mejorarlo. Llegados a este punto cabe mencionar que por esto las aplicaciones de este tipo consideradas como más seguras son aquellas que utilizan un sistema encriptación de extremo a extremo, también conocido como E2EE. Así se usa una forma de cifrado que asegura que solo el remitente y el destinatario de un determinado mensaje podrán leer su contenido. Además con E2EE ni siquiera el proveedor del servicio que almacena los mensajes en sus servidores, podrá descifrarlos ni leerlos.

Código abierto:

Por otro lado diremos que en los últimos años, la transparencia ha surgido como un elemento crítico para el desarrollo de software seguro, por lo que la mayoría considera que los desarrolladores que «abren» el código fuente de sus propios proyectos para que otros lo vean, son mucho más fiables. Decir que el Open-sourcing de una aplicación no lo hace intrínsecamente seguro, sin embargo también es cierto que ofrece la oportunidad a los expertos de seguridad de revisar el código y así poder encontrar posibles bugs o puertas traseras en la nueva herramienta.

Por el contrario, aquellas aplicaciones que hacen uso exclusivo e interno de su propio código fuente dejando al resto de expertos en el tema en la más total oscuridad, obligan a los usuarios de sus desarrollos a confiar en que la propia empresa haya probado de manera conveniente a la vez que efectiva y depurado su propio código contra posibles ataques externos.

Eliminación de mensajes:

En el desafortunado caso de que nuestro teléfono móvil caiga en otras manos indeseadas y no lo tengamos convenientemente protegido, o por alguna razón nuestra cuenta de usuario de la aplicación de mensajería instantánea se vea comprometida, hay que tener muy en consideración que ningún tipo de cifrado será capaz de proteger nuestra información confidencial llegado el momento. Es por todo ello que el hecho de ser capaz de eliminar los mensajes almacenados en la propia herramienta, se le puede considerar como una medida extra relacionada con la seguridad.

Precisamente por estas razones, la mayoría de las aplicaciones nos permitirán eliminar mensajes individuales o chats completos de nuestras propias cuentas y, por lo tanto, de los dispositivos móviles. Sin embargo estas mismas aplicaciones de mensajería segura deben permitir a los remitentes borrar todos los mensajes confidenciales de los dispositivos pertenecientes a todas las partes involucradas en una misma conversación.

Almacenamiento de metadatos:

Además del contenido de nuestros mensajes, cada servicio de mensajería almacena un conjunto de información propia que alberga datos como la hora a la que se envió un mensaje, a quién se le mandó, etc; lo que se suele denominar como metadatos o "datos sobre datos". Aunque a primera vista el contenido de estos metadatos podría no ser tan sensible como el mensaje real, sí que se puede deducir bastante de los mismos como los contactos que tenemos, los patrones de uso o nuestra ubicación, entre otras cosas. A esto hay que sumarle que los metadatos nunca están encriptados o protegidos como sucede con el contenido del mensaje.

De hecho para algunos expertos los metadatos son mucho más íntimos incluso que nuestras conversaciones, ya que muestran dónde vamos, nuestros intereses, relaciones o quiénes somos en realidad.

Por lo tanto es información que se podría considerar como de extrema importancia y muy perjudicial si llega a caer en manos equivocadas. De este modo podemos llegar a la conclusión de que cuantos menos metadatos almacene una aplicación de mensajería instantánea, más segura será en este sentido. Así es recomendable revisar las políticas de almacenamiento de esta información que la aplicación de mensajería que usemos de manera habitual haga, para que al menos seamos conscientes de todo ello.

Estos son algunos de los aspectos más importantes a la hora de evaluar la fiabilidad de cada una de las aplicaciones de estos entornos que usemos, lo que no significa que debemos descartarla si no se ajusta a los criterios anteriormente mencionados. Sin embargo sí que nos puede servir para no dar por sentados ciertos hechos relacionados con la privacidad y seguridad de nuestros datos y tomar las medidas necesarias en cada caso.

FUENTES:

- https://www.softzone.es/2017/06/19/seguridad-aplicaciones-mensajeria-instantanea/

6 Aplicaciones de Mensajería Segura que Debes Conocer

En un mundo interconectado, en donde la privacidad de nuestras comunicaciones es cada día más vulnerable, es fundamental utilizar aplicaciones de mensajería seguras.

En la actualidad existe una diversidad de aplicaciones para comunicarnos, sin embargo no todas son seguras, por lo que a continuación, les presentamos, a nuestro criterio, las seis aplicaciones más seguras:

1. Signal

Es una aplicación de la organización Open WhisperSystems, que permitirá cifrar totalmente sus llamadas y evitar escuchas ilegales o intromisiones contra su intimidad. Signal nos permite hacer llamadas y enviar mensajes de texto privadas, protegiendo la confidencialidad de nuestras comunicaciones.

Al igual que con la versión de iOS, en cualquier texto, vídeo o imagen de la versión de Android la señal se cifra antes de salir de su teléfono, lo que significa que Open Whisper no puede ver lo que estás enviando.

2. Wickr

Es otra destacada opción de mensajería segura, con la que se puede cifrar mensajes de texto, voz o vídeos, y transmitir de forma cifrada de extremo a extremo.

Este servicio de mensajería instantánea nos garantiza un grado de seguridad muy alta al enviar y recibir mensajes. Los mensajes cifrados con este sistema desaparecen tras un plazo de tiempo determinado. En la actualidad algunas empresas extrajeras trabajan para establecer este tipo de servicios y evitar el espionaje industrial.

3. WhatsApp

Con más de 1.000 millones de usuarios en todo el mundo, y en aumento. WhatsApp, también garantiza en la actualidad la privacidad, ofreciendo un servicio de cifrado de extremo a extremo basado en la misma tecnología de Signal.

El cifrado de extremo a extremo en WhatsApp asegura que solo tú y el receptor puedan leer lo que se envía, y que nadie más, ni siquiera WhatsApp lo pueda hacer. Tus mensajes se aseguran con un candado y solo tú y el receptor cuentan con el código/llave especial para abrirlo y leer los mensajes. Para mayor protección, cada mensaje que envías tiene su propio candado y código único. Todo esto pasa de manera automática; sin necesidad de realizar ajustes o de crear chats secretos para asegurar tus mensajes. Adicionalmente cuenta con una opción para PC.

4. iMessage - sólo para iOS

La aplicación de mensajería por defecto de Apple también utiliza un protocolo criptográfico, el cifrado que utiliza iMessage está diseñado por la propia Apple, el cifrado es bastante bueno, sin embargo, algunos expertos creen que Apple va a cambiar su protocolo a algo parecido a Signal, pero con más de mil millones de dispositivos que utilizan iMessage, es más fácil decirlo que hacerlo. Lo mejor de iMessage es que viene preinstalado en todos los iPhone, es decir, el envío de mensajes cifrados es tan fácil como mandar un mensaje de texto normal.

5. Telegram

Con telegram puedes enviar mensajes y hacer llamadas totalmente gratis, además de crear grupos hasta de 5000 personas para chatear al mismo tiempo, programar Chats Secretos con cifrado especial para que solo tú y la persona con la que estés hablando vea los mensajes y se destruyan automáticamente si así lo deseas, y lo mejor de todo es que tiene capacidad de 1GB para enviar vídeos.

La mejor característica son sus chats secretos encriptados de dispositivo a dispositivo e incluso se pueden autodestruir. Está disponible en multitud de plataformas y también tiene una opción para computadores personales, además de servicio web.

6. Threema

Es una aplicación de mensajería instantánea para Android y iOS. Es similar a Whatsapp y te permite enviar mensajes, fotos, vídeos o tu posición, pero en este caso encriptados y totalmente seguros. Preserva tus datos fuera del alcance de empresas, hackers y cualquier atacante, y puede usarse de manera completamente anónima

Threema utiliza la librería de criptografía de dominio público NaCl de código abierto para el cifrado. Las claves de cifrado se generan y almacenan de forma segura en los dispositivos del usuario para impedir el acceso a puertas traseras.

Al iniciar Threema por primera vez, se genera un código de 8 dígitos (Threema ID). Este código se genera fuera de cualquier servidor. Para utilizar Threema no necesitas ni el número de teléfono, ni una dirección de correo electrónico, una característica única que permite a los usuarios permanecer 100% anónimos.

Adicionalmente, podemos indicar que existen muchas más aplicaciones para mensajería, en las cuales también se habla sobre seguridades en el envío de mensajes, dejamos a tu decisión para

utilizar las recomendadas, o seleccionar una de las más variadas mensajerías instantáneas existentes, pero siempre debes utilizar el mejor criterio, en cuanto a la seguridad en la transmisión de la información a través de cualquiera de dichas aplicaciones.

FUENTES:

- http://www.periodismociudadano.com/2017/01/20/3-aplicaciones-de-mensajeria-segura-que-debes-conocer/
- http://es.gizmodo.com/las-aplicaciones-de-mensajeria-mas-seguras-que-puedes-i-1782483162
- http://www.androidpit.es/mejores-aplicaciones-mensajeria
- http://www.semana.com/tecnologia/articulo/whatsapp-o-telegram-cual-es-la-aplicacion-mas-segura/476254
- http://www.como-espiar.com/threema-mensajeria-mas-segura-whatsapp/

¿Cómo proteger Nuestros Smartphones y Tablets?

La mayoría de las personas vivimos con un teléfono móvil bajo en la mano. Hoy en día estos dispositivos no solo se utilizan para mantener el contacto con los amigos, se los utiliza también para almacenar datos o llevar el día a día de una agenda personal y profesional. Además, gracias a los smartphones cualquiera con conexión a Internet podrá gestionar sus redes sociales, así como, echar un vistazo al estado de sus cuentas bancarias con tan solo un par de clicks.

Todas estas funcionalidades y ventajas que nos brindan estos dispositivos, nos obligan a tomar medidas de seguridad, para proteger nuestra información, a continuación te proporcionamos algunas medidas básicas:

- **Observar mecanismos de seguridad**.- Cuando adquieras un teléfono celular, escoge el que consideres del más seguro. No compres equipos de dudosa procedencia o desbloqueados ilegalmente, si es de segunda mano, restablece la configuración de fábrica.

- **Configurar el bloqueo automático.** Después de un tiempo de inactividad es conveniente que el dispositivo se bloquee.

- **Protegerlo con una contraseña o pin**. Parece algo elemental y lo es pero aún se puede ver que mucha gente no lo hace. En caso de pérdida o robo lo único que perderíamos sería el equipo.

- **Registrar el IMEI.-** El IMEI se obtiene pulsando *#06# deberíamos registrar este código pues en caso de robo o extravío podremos llamar a nuestra operadora e inutilizar el dispositivo para evitar que accedan a la información.

- **Instalar aplicaciones de control remoto**.- Estas aplicaciones deben permitirnos geolocalizar el dispositivo desde una cuenta vinculada y saber en el momento en que haya desaparecido, donde se encuentra nuestro teléfono. Las versiones más actuales se incorporan estas herramientas, pero si no, se pueden descargar de las respectivas tiendas

de aplicaciones. Además deben dejarnos borrar de manera remota todo el contenido de nuestros dispositivos en caso de robo o extravío de los mismos.

- **Realizar copias de seguridad.-** Hoy en día existen numerosas herramientas para respaldar en la nube la información que contienen los dispositivos móviles, para poder restaurar de manera instantánea en otro dispositivo, sin problema alguno.

- **Controlar instalación de las aplicaciones.-** Se deben tratar con precaución las aplicaciones que se instalen en el sistema, intentando bajarlas de fuentes de confianza y con una reputación positiva. También hay que revisar los permisos que estas aplicaciones requieren para su funcionamiento.

- **Mantener el software actualizado**.- Con el fin de corregir lo mejor posible los problemas de seguridad, es importante mantener tanto las aplicaciones como el sistema operativo actualizados. Además, si es posible, hay que configurarlos para que realicen la actualización automáticamente.

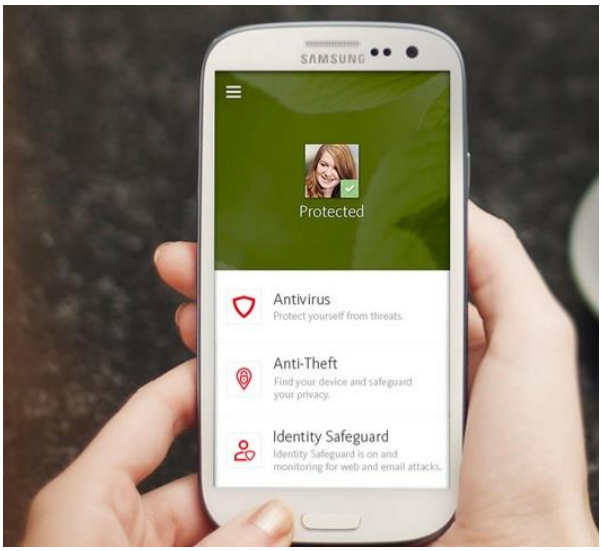
- **Cifrar la información delicada.-** Este cifrado puede realizarse tanto utilizando los servicios que ofrece el sistema operativo como mediante aplicaciones confiables de terceros.

- **Monitorizar el uso de recursos.-** Se pueden detectar anomalías realizando un control de la utilización de los recursos del dispositivo móvil por parte de las aplicaciones. Esto incluye revisión de la factura telefónica para detectar posibles usos fraudulentos.

- **Deshabilitar los sistemas de comunicación cuando no se utilicen**.- Además de reducir el consumo energético, deshabilitar los sistemas de comunicación cuando no se utilizan puede evitar ataques. Los sistemas de comunicación únicamente se deben utilizar en redes de confianza.

- **Eliminar la información confidencial antes de desechar el dispositivo.-** Al deshacerse del dispositivo, no sabemos en qué manos puede caer, por lo tanto es importante eliminar toda la información que contiene.

- **Instalar un antivirus.-** Sí, también existen virus que afectan a los sistemas operativos móviles y sí existen herramientas de antivirus desde la tienda oficial del sistema operativo y descargar un antivirus **Avira,** que cuenta con una versión gratuita para dispositivos móviles, que permite protegerlos contra troyanos bancarios, Ransomware y bloquea las llamadas no deseadas. Comunícate con SCProgress al correo electrónico avira@scprogress.com y te asesoramos.



- **Cuidado con las redes públicas**.- Debemos tener cuidado con las redes a las que nos conectamos. Si vemos una red abierta o con seguridad básica debemos saber que no solo estamos obteniendo acceso a internet cuando nos conectamos, sino que también entramos a formar parte de esa red local, por lo que es conveniente cuidarnos con las

aplicaciones que ejecutamos y los controles de acceso que tiene nuestro dispositivo. Esto aplica también a las conexiones bluetooth como puede ser un manos libres o cualquier otro, que suelen usar contraseñas muy básicas de emparejado de dispositivos por defecto.

En resumen podemos indicar que debemos tomar las mismas precauciones que con los computadores personales, cuando tratamos con archivos adjuntos a correos electrónicos, enlaces desde SMS y, en general, navegación por Internet, y utilizar permanentemente el sentido común para proteger la información.

FUENTES:

- https://www.gestiontpv.com/blog/alertan-sobre-nuevo-virus-que-ataca-los-tpv
- http://muyseguridad.net/2015/12/05/malware-en-tpv/
- http://cso.computerworld.es/cloud/las-brechas-de-seguridad-llegan-a-los-tpv-conectados-a-la-nube
- http://searchdatacenter.techtarget.com/es/cronica/Mejores-practicas-en-seguridad-de-aplicaciones-moviles-para-proteger-datos-corporativos

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