Actualización en Seguridad Informática

Cómo la seguridad digital es un elemento estratégico para el crecimiento de las organizaciones y la reducción del riesgo?

John Edinson Martínez G

Ingeniero en Electrónica y Telecomunicaciones
Master en Gestión de Informática

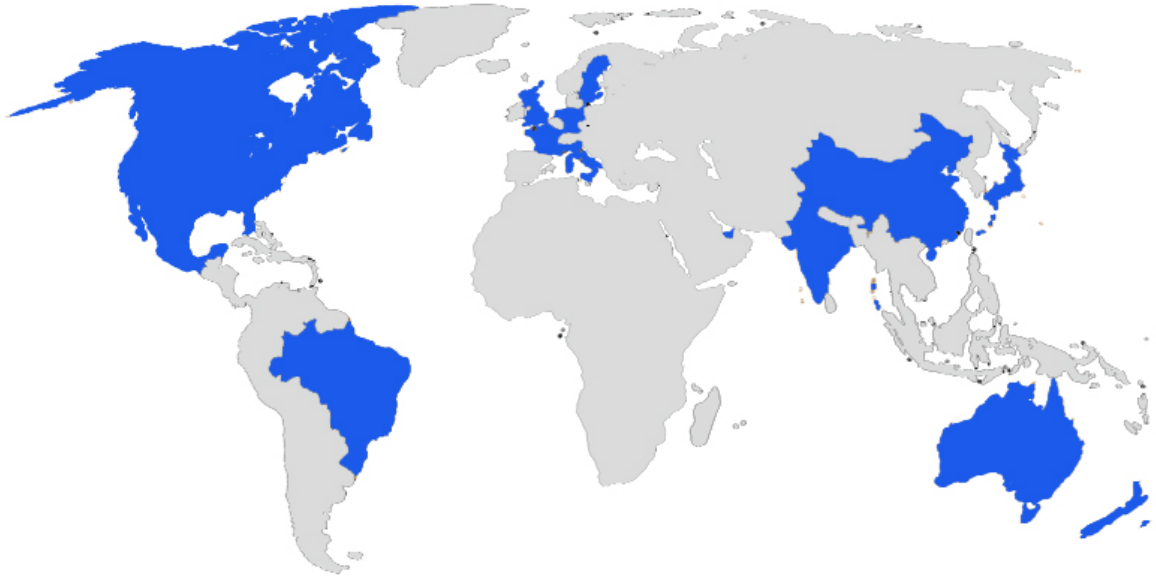
- CISM, Certified Information Security Management – ISACA
- CISA, Certified Information System Auditor– ISACA
- CEH, Certified Ethical Hacking – EC Council
- CSX, Cybersecurity Fundamentals Certificate – ISACA
- Auditor Líder ISO27001
- Auditor Líder ISO31000
- Auditor Líder ISO22301
- COBIT5 Certified
- FIH, Fundamentals Incident Handler – Software Engineering Institute

john.martinez@password.com.co

Agenda

- Gestión estratégica y gobernabilidad de TI
- Seguridad informática vs Seguridad de la información
- Gestión de riesgo informático
- Los principales mitos sobre el aseguramiento digital de su empresa
- Prevención de fraudes informáticos
- Estándares de seguridad y modelos de seguridad fáciles de aplicar
- Conclusiones y recomendaciones

Consumers globally are feeling the danger of cybercrime.



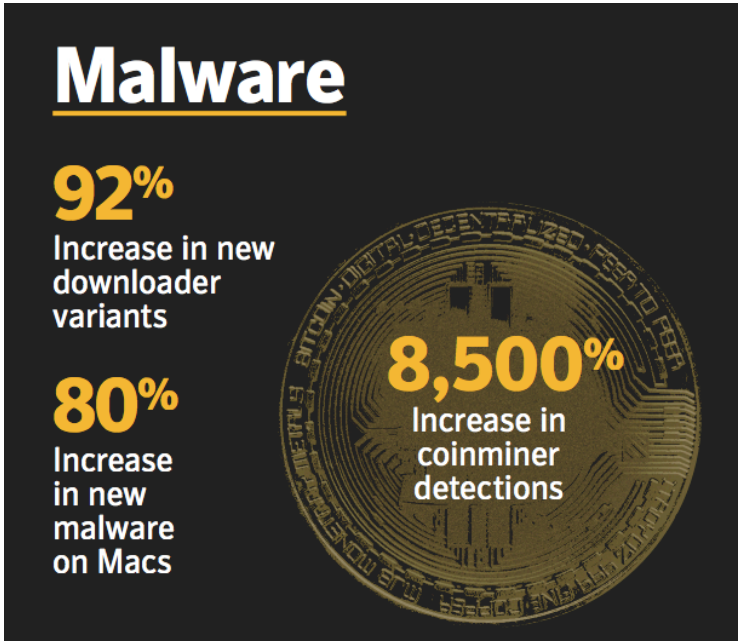
594

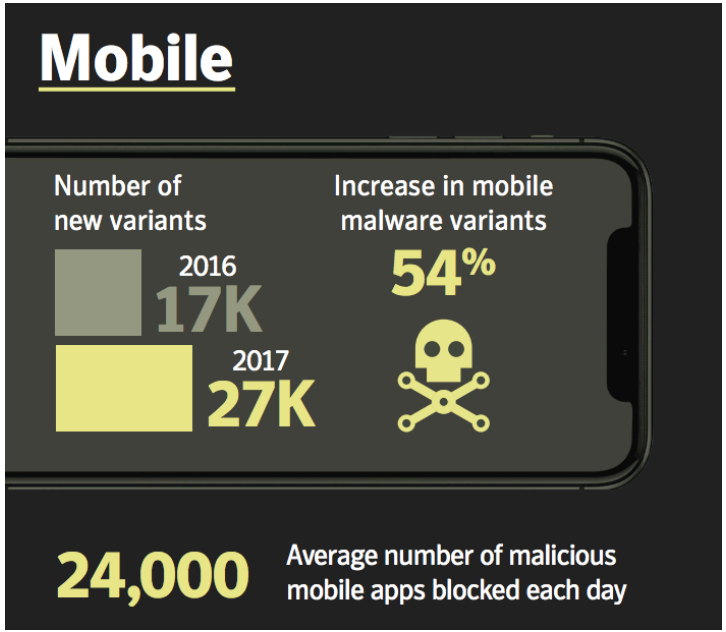
MILLION

AFFECTED BY CYBERCRIME

GLOBALLY

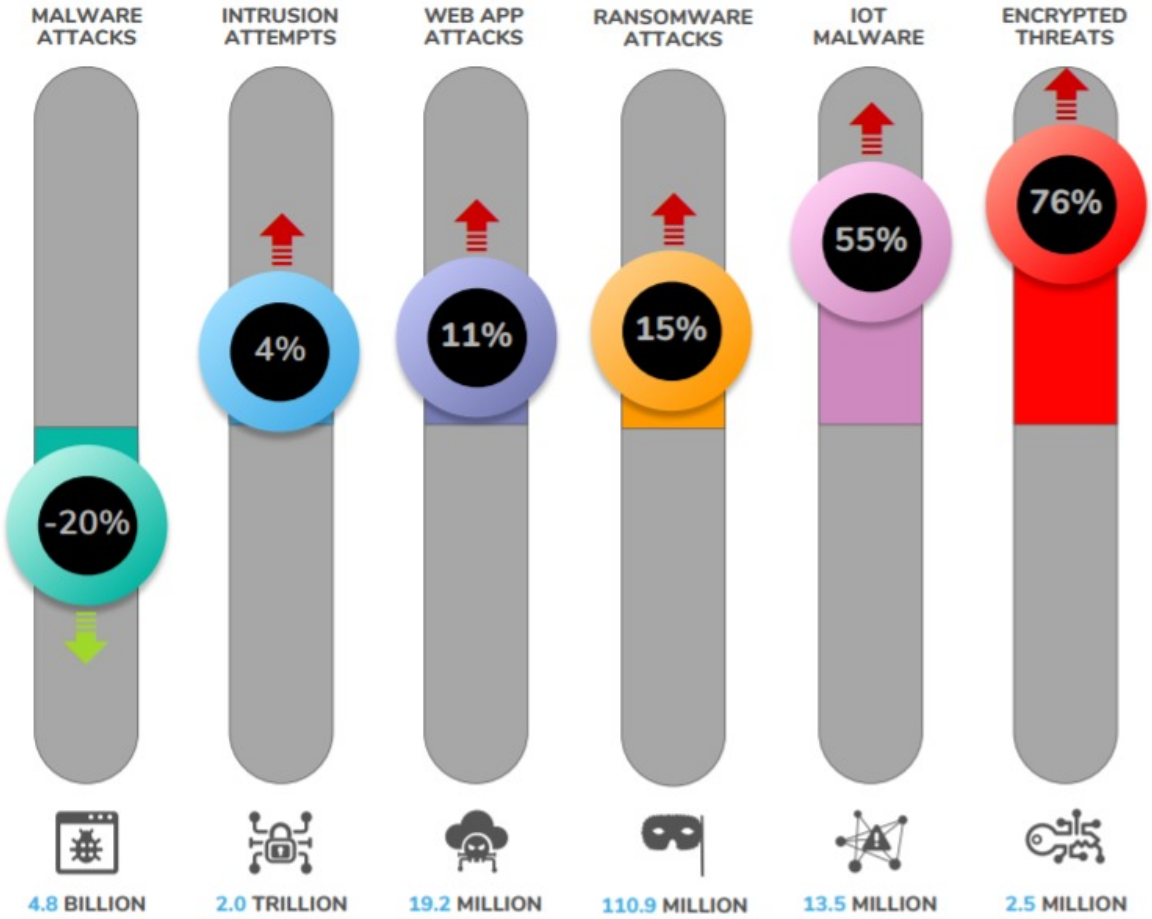
Fuente: https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt





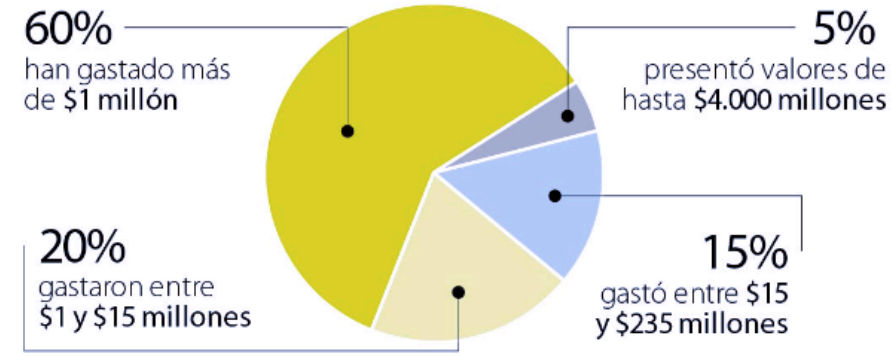
Symantec Internet Security Threat Report

2019 GLOBAL CYBERATTACK TRENDS



Los ataques informáticos ahora se han monetizado

GASTO DE EMPRESAS POR DAÑOS DE CIBERATAQUES



87% DE LAS EMPRESAS NO DENUNCIAN INCIDENTES DIGITALES

VIRUS MÁS FRECUENTES

- Malware
- Exploids
- Cryptojacking
- Phishing
- Adware

Fuente: MinTIC / Centro Cibernético Policial

Gráfico: LR-ER

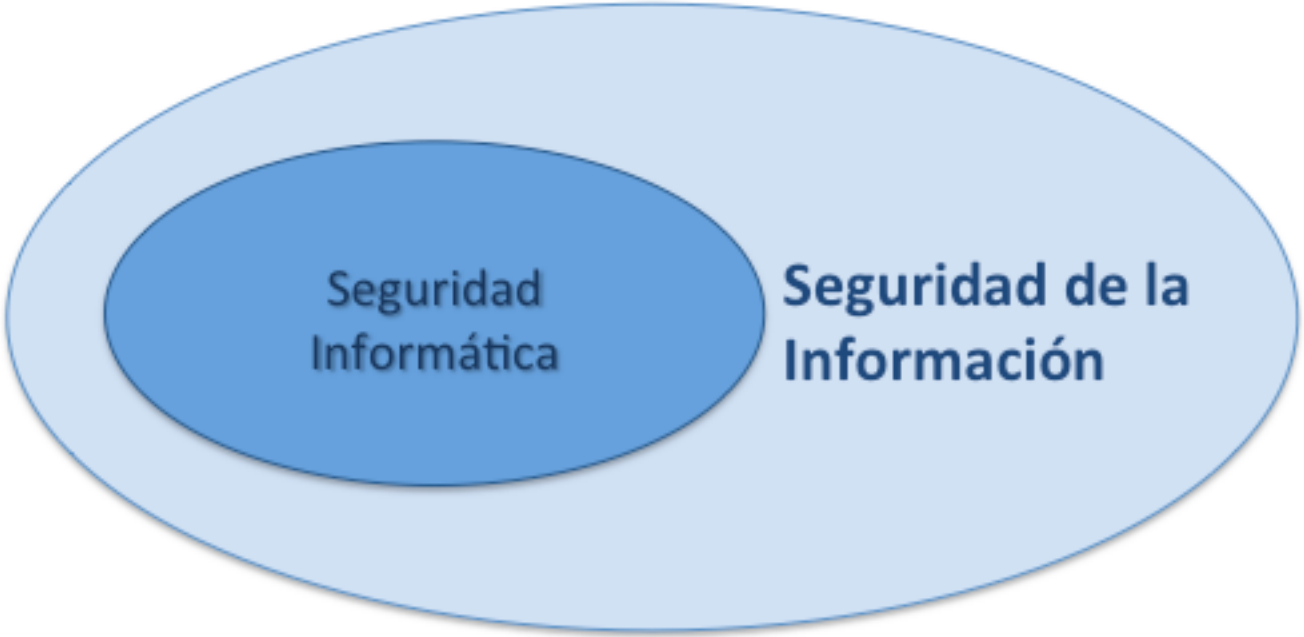
Internet es inherentemente insegura

- Internet funciona en tiempo compartido
- Los protocolos son muy viejos. SMTP fue definido en 1982 y actualizado en 2008
- Requiere capas adicionales de seguridad

Es necesario gobernar la seguridad

Todas las empresas tienen hoy día la información como un recurso de alto nivel (todo esta almacenado en un computador). La seguridad digital debe ser parte de la gestión estratégica de las empresas

Por qué es de interés de toda la organización?


Seguridad Informática
Seguridad de la Información

Y qué tengo que hacer?

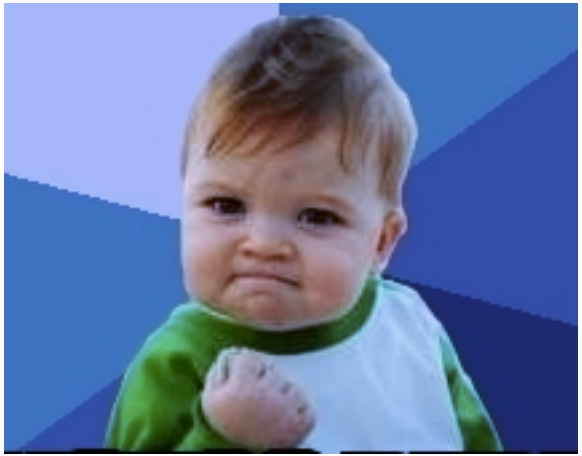
Tener un Plan

Implemente un modelo de gestión de riesgo tecnológico

Implemente controles de acuerdo a esos riesgos

Realice monitoreo periódico de esos riesgos y controles

Estamos listos, a implementar seguridad digital, pero naturalmente no es fácil



Mitos y realidades de la seguridad digital

- Es muy caro
- Es muy difícil
- A mi no me toca
- Fraude informático

Prevenir el fraude

- Ingeniería social
- Virus – Ransomeware
- Ataques informáticos
- Ataques a dispositivos móviles
- Nube


.CO
.CO Internet S.A.S.
+ ENTER.CO LLEVA TU NEGOCIO A INTERNET
Cómo usar las redes sociales para potencializar tu negocio
LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO
Compartir en Facebook
Compartir en Twitter
Compartir en Google+
17 PERSONAS COMPARTIERON
Sabías que, según Digital Guardian, el 97% de los ataques informáticos no aprovechan una falla en el software, sino que usan técnicas de ingeniería social para conseguir las credenciales necesarias para vulnerar la seguridad informática. Por eso, a veces poco importan las medidas de seguridad tecnológicas que implementes si las personas están mandando su clave por correo electrónico. Como parte de la estrategia de seguridad de tu compañía, tienes que hacer un gigantesco esfuerzo para evitar que los criminales informáticos implementen técnicas de ingeniería social para entrar a tus sistemas.
.CO
ENTER.CO
25.07.16 @ 15:30 p.m.
@enterco
COMENTADO 1

SEGURIDAD EN INTERNET ›

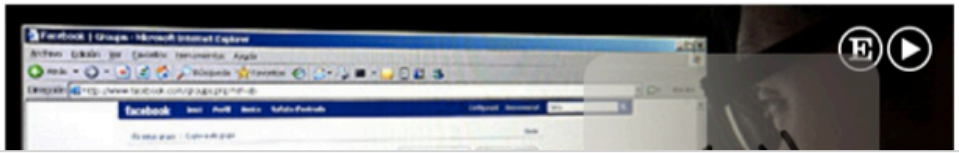
La contraseña más popular del mundo sigue siendo '123456'

Una lista con datos de más de dos millones de usuarios revela la falta de seguridad de la mayor parte de contraseñas que se usan en internet

26

ANDREA ARNAL MARTÍN

25 ENE 2016 - 18:45 CET

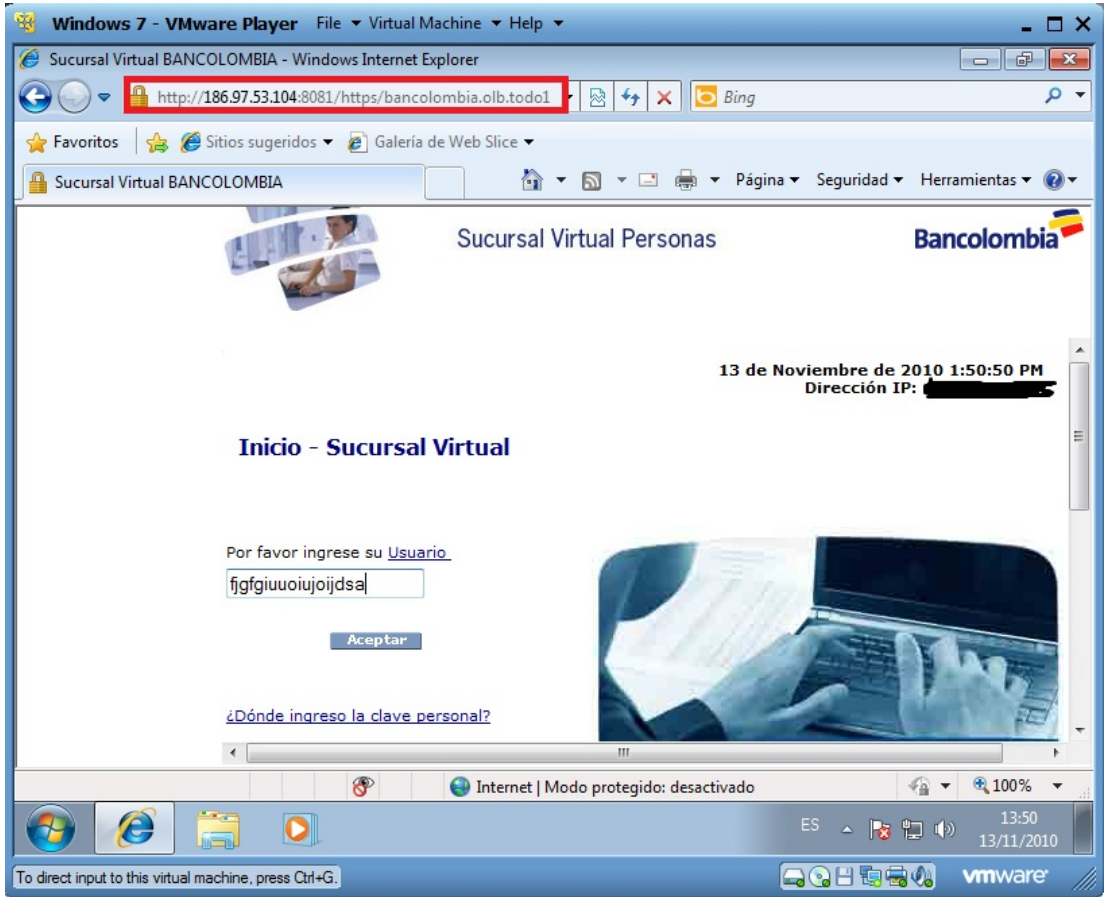


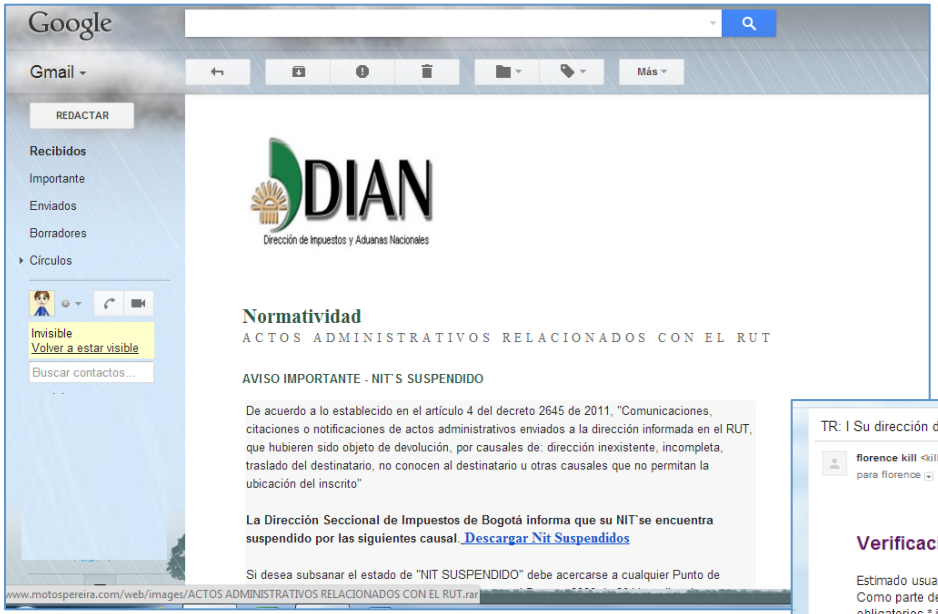
Ingeniería Social

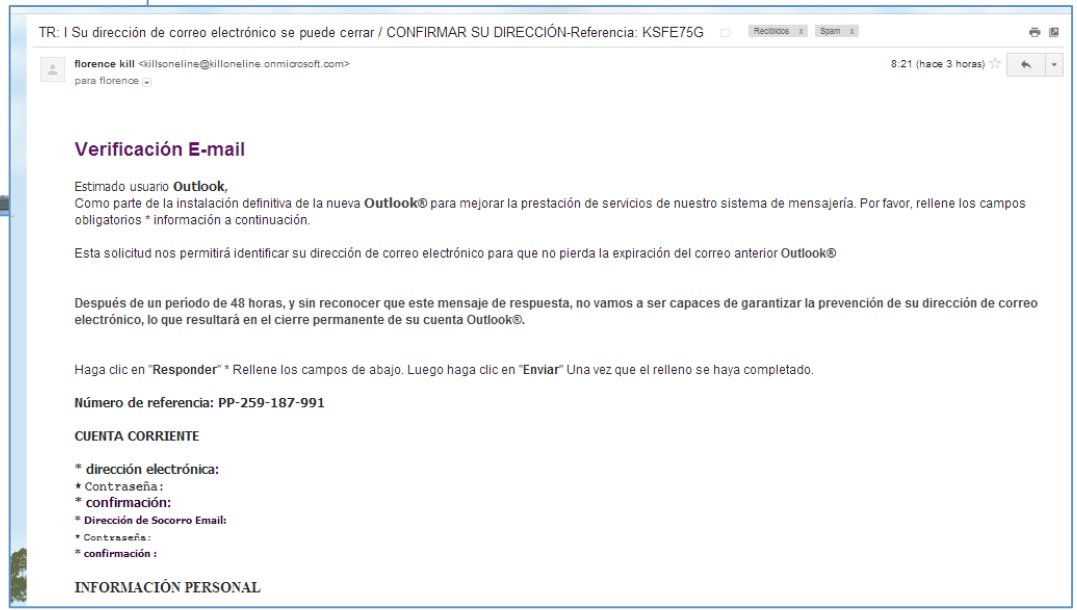
- Phishing
- Fake mail
- Vishing
- Dumpster Diving
- Tailgaiting

50%
Phishing

25%
Fakemail


Windows 7 - VMware Player File Virtual Machine Help
Sucursal Virtual BANCOLOMBIA - Windows Internet Explorer
http://186.97.53.104:8081/https/bancolombia.olb.todo1
Bing
Favoritos
Sitios sugeridos
Galería de Web Slice
Sucursal Virtual BANCOLOMBIA
Página
Seguridad
Herramientas
Sucursal Virtual Personas
Bancolombia
13 de Noviembre de 2010 1:50:50 PM
Dirección IP:
Inicio - Sucursal Virtual
Por favor ingrese su Usuario
fjgfgiuuoiujoijdsa
Aceptar
¿Dónde ingreso la clave personal?
Internet | Modo protegido: desactivado
100%
ES
13:50
13/11/2010
To direct input to this virtual machine, press Ctrl+G.
vmware

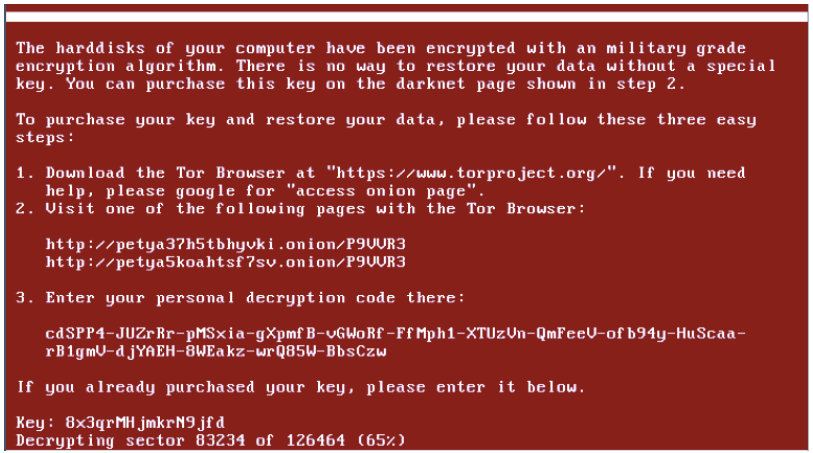

Google
Gmail
Más
REDACTAR
Recibidos
Importante
Enviados
Borradores
Círculos
Invisible
Volver a estar visible
Buscar contactos...
DIAN
Dirección de Impuestos y Aduanas Nacionales
Normatividad
ACTOS ADMINISTRATIVOS RELACIONADOS CON EL RUT
AVISO IMPORTANTE - NIT`S SUSPENDIDO
De acuerdo a lo establecido en el artículo 4 del decreto 2645 de 2011, "Comunicaciones, citaciones o notificaciones de actos administrativos enviados a la dirección informada en el RUT, que hubieren sido objeto de devolución, por causales de: dirección inexistente, incompleta, traslado del destinatario, no conocen al destinatario u otras causales que no permitan la ubicación del inscrito"
La Dirección Seccional de Impuestos de Bogotá informa que su NIT`se encuentra suspendido por las siguientes causal. Descargar Nit Suspendidos
Si desea subsanar el estado de "NIT SUSPENDIDO" debe acercarse a cualquier Punto de
www.motospereira.com/web/images/ACTOS ADMINISTRATIVOS RELACIONADOS CON EL RUT.rar


TR: I Su dirección de correo electrónico se puede cerrar / CONFIRMAR SU DIRECCIÓN-Referencia: KSFE75G
Recibidos
Spam
florence kill <killsoneline@killoneline.onmicrosoft.com>
para florence
8:21 (hace 3 horas)
Verificación E-mail
Estimado usuario Outlook,
Como parte de la instalación definitiva de la nueva Outlook® para mejorar la prestación de servicios de nuestro sistema de mensajería. Por favor, rellene los campos obligatorios * información a continuación.
Esta solicitud nos permitirá identificar su dirección de correo electrónico para que no pierda la expiración del correo anterior Outlook®
Después de un período de 48 horas, y sin reconocer que este mensaje de respuesta, no vamos a ser capaces de garantizar la prevención de su dirección de correo electrónico, lo que resultará en el cierre permanente de su cuenta Outlook®.
Haga clic en "Responder" * Rellene los campos de abajo. Luego haga clic en "Enviar" Una vez que el relleno se haya completado.
Número de referencia: PP-259-187-991
CUENTA CORRIENTE
* dirección electrónica:
* Contraseña:
* confirmación:
* Dirección de Socorro Email:
* Contraseña:
* confirmación :
INFORMACIÓN PERSONAL


ON
THE
AIR
I ran out of hands.

Virus informáticos

- No son ruidosos
- Tienen muchas finalidades: Zombis, Robo de información, robo de capacidad de computo
- Antivirus y sistemas actualizados



chrome

Peligro: se ha detectado software malicioso

Google Chrome ha bloqueado el acceso a esta página en www.elpais.com.co.

Se ha insertado contenido de www.newmediaelpais.com, un distribuidor de software malicioso conocido, en esta página web. Si accedes a ella, es muy probable que tu ordenador se infecte con software malicioso.

El software malicioso provoca daños como robo de identidad, pérdidas financieras y eliminación permanente de archivos.
Más información

Volver Opciones avanzadas

Mejorar detección de software malicioso enviando información adicional a Google cuando reciba advertencias como esta. Política de privacidad

ENTER.CO EMPRESAS


South Summit Bogotá: una ventana para los emprendedores


Facebook capacitará a 4.00 emprendedores colombiano

COLOMBIA, EL PAÍS CON MÁS RANSOMWARE EN LATINOAMERICA, EN 2018

Compartir en Facebook | Compartir en Twitter | Compartir en Google+

DIANA ARIAS
15.05.19 @ 09:00 am
@dianaarias_

Microsoft y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) presentaron su manual de 'Ciber Resiliencia Nacional'. En este se presentan posturas claves que deben adoptar las empresa para desarrollar y responder a las nuevas necesidades digitales. Sin embargo, para esto, es necesario primero reconocer las amenazas que afectan a las empresas.

Ataques informáticos

- Portales Web
- Bases de Datos
- Sistemas Operativos

A1
INJECTION

A2
BROKEN AUTHENTICATION

A3
SENSITIVE DATA EXPOSURE

A4
XML EXTERNAL ENTITIES (XXE)

A5
BROKEN ACCESS CONTROL

A6
SECURITY MISCONFIGURATION

A7
CROSS-SITE SCRIPTING (XSS)

A8
INSECURE DESERIALIZATION

A9
USING COMPONENTS WITH KNOWN VULNERABILITIES

A10
INSUFFICIENT LOGGING & MONITORING

Ataques a móviles

- El teléfono móvil es un computador portátil
- Los tenemos lleno de información confidencial
- No permitir instalaciones de fuentes desconocidas
- Verificar los permisos a las aplicaciones

¿Cómo identificar el nuevo virus informático Agent Smith que ha infectado 25 millones de dispositivos Android?

Publicado: 11 jul 2019 23:57 GMT

Este programa malicioso aprovecha las debilidades de ese sistema operativo y se instala camuflado como una herramienta de actualización de Google.

- La nube es el servidor de alguien más
- Lo que sucede en la nube se legisla en la tierra
- Las responsabilidades y la seguridad deben quedar claramente definidas
- Si son mis aplicaciones son mi responsabilidad

Estándares y modelos

- Conpes 3854 de Ciberseguridad
- ISO27001 – Sistema de Gestión de Seguridad de la Información
- ISO27032 – Ciberseguridad
- COBIT – Auditoria y Control
- Cybersecurity Framework | NIST
- Guías de Mintic – MSPI
- Modelo nacional de gestión de riesgos de seguridad digital
- Ley de protección de datos

Recomendaciones

- ❑ Implemente un modelo de seguridad digital
- ❑ Involucre a toda la organización
- ❑ Capacite y sensibilice
- ❑ Realice análisis de vulnerabilidades al menos dos veces al año
- ❑ Defina políticas para:
  - Manejo de Backups
  - Actualización de su plataforma
  - Uso de dispositivos móviles
  - Manejo y clasificación de información

Recomendaciones

- ❑ Implemente un plan de continuidad del negocio
- ❑ correcto uso de contraseñas e implemente doble factor de autenticación

Preguntas?

John Edinson Martínez G
John.martinez@password.com.co