Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

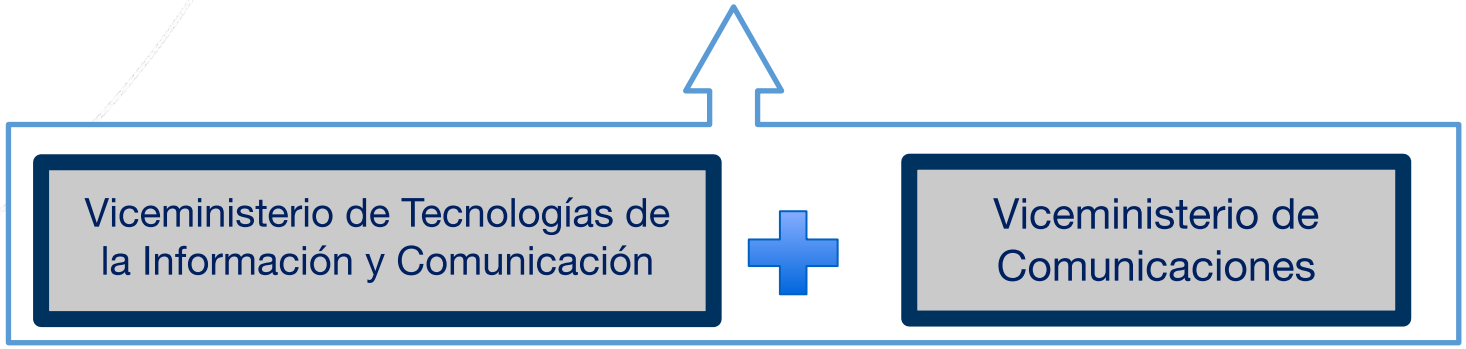
SEGURIDAD EN LA ERA DE LOS MEDIOS DIGITALES

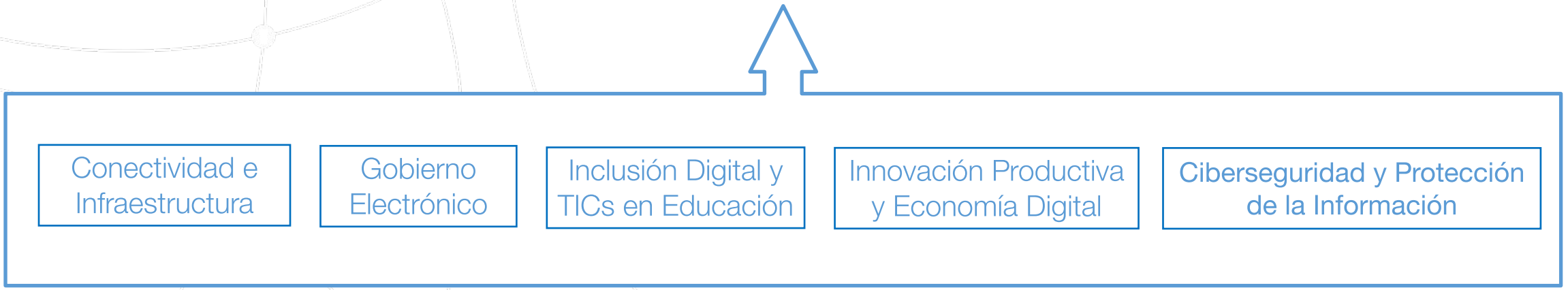
CERT-PY

MITIC - Nuevo rol, nuevas atribuciones

Secretaría
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

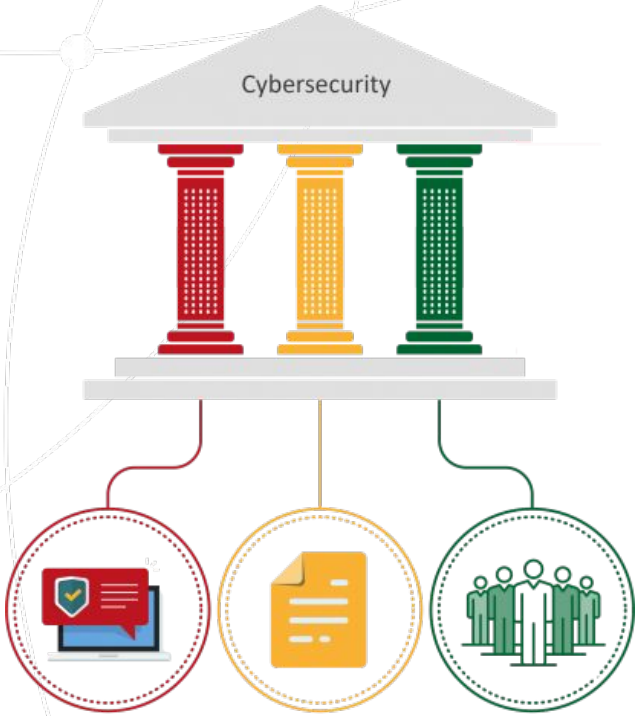
Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN





Pilares de Ciberseguridad y Protección de la Información

Tecnología
Prevención y Detección



Formación de
Capacidades

Políticas y
Gobernanza

Objetivos Estratégicos

- Proteger los sistemas de información del Gobierno y la Infraestructura crítica
- Crear un ecosistema e industria de ciberseguridad
- Construir la capacidad de hacer frente a las ciberamenazas
- Fomentar la concienciación y construir capacidades en ciberseguridad

CERT-PY

PROTEGE TU INFORMACIÓN

SEGURIDAD EN LA ERA DE LOS MEDIOS DIGITALES

¿Por qué preocuparnos?

- Uso de internet para tareas tradicionalmente “offline”.
- Mayor cantidad de riesgos, más sofisticados, más silenciosos.
- Redes sociales para fines laborales.
- Límite difuso entre el ambiente personal, social y laboral.
- Mayor interconexión de los servicios.
- Muchos puntos de entrada para atacantes.

¿Por qué preocuparnos?

CERT-PY

Ciberseguridad

Es la protección de los activos digitales.

Seguridad de la Información

Preservar la confidencialidad, integridad y disponibilidad de la información.

CERT-PY

Control de Acceso Credenciales

Autenticación

CERT-PY

¿Qué es la autenticación?

Sistemas basado en usuario y contraseña

Ataques de contraseña:

350 mil millones de contraseñas por segundo

	Números	Minúsculas	Minúsculas + números	Minúsculas + Mayúsculas + números
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

Contraseñas robustas

CERT-PY

Longitud

¿Son suficiente 8 caracteres?

NO!

Mínimo 12 caracteres!

En una contraseña compuesta solo por minúsculas, 1 carácter adicional significa una contraseña 16 veces más difícil de crackear

Contraseñas robustas

Combinación de tipo de caracteres

No limitarse a usar minúsculas!

- Minúsculas
- Mayúsculas
- Números
- Caracteres: $ # % & ! . , * -

DATO: En una contraseña de 8 minúsculas, 1 carácter adicional significa una contraseña 35% más difícil de crackear

Contraseñas robustas

CERT-PY

Frases

- **¿Por qué usar palabras si podemos usar frases?**

EJEMPLO:

“Esta frase es solo un ejemplo”
“Est4.fr4s3-3s.s0l0-un.Ej3mpl0”

NO usar palabras de diccionario

- Palabras o nombres conocidos, propios del lenguaje
- Contraseñas comunes y conocidas: admin, root, qwerty, etc..

DATO:
Contraseñas más comunes:

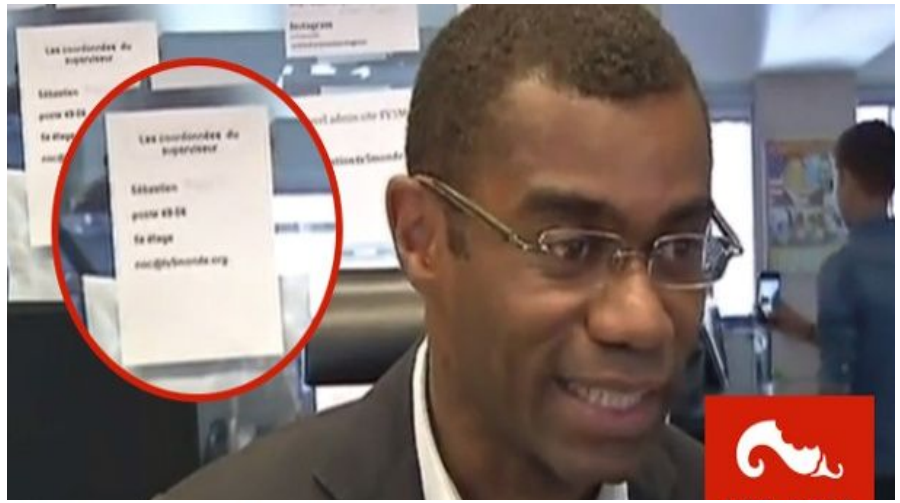
1) **123456**
2) **password**
3) **12345678**
4) **qwerty**
5) **12345**
6) **123456789**

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL
Paraguay de la gente

Buenas prácticas

- No uses la misma contraseña para todo.
- Cambia tu contraseña regularmente.
- Cambia las contraseñas por defecto.
- No la escribas en papeles o documentos accesibles.
- No la introduzcas en sitios o programas desconocidos – cuidado con el PHISHING!
- No la introduzcas en equipos poco seguros – cuidado con los KEYLOGGERS!
- No uses herramientas online para crear contraseñas



Tv5Monde revealed his own passwords in an interview

April 10, 2015 By Pierluigi Paganini

A TV5Monde staffer accidentally revealed a password used to access the social media account of the broadcaster in an interview.

Following the successful attack against the network of the TV French Channel TV5Monde, law enforcement and French Intelligence started to investigate the attach chain.

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

Autenticación de doble factor

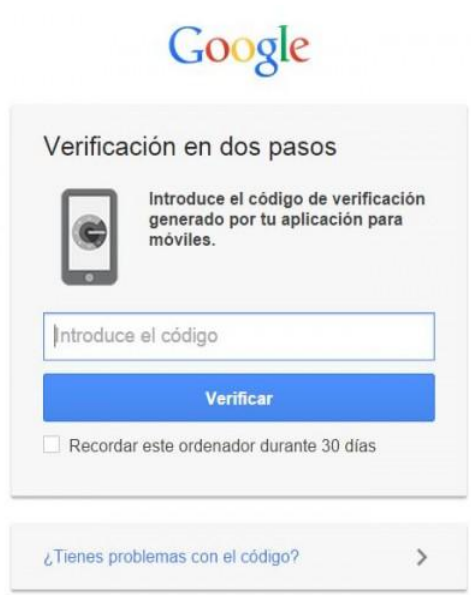
CERT-PY

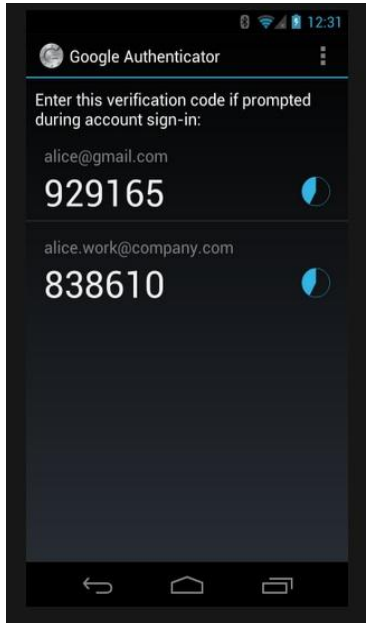
¿Es suficiente? ...

Medida de seguridad adicional al usuario y contraseña

Usuario + Contraseña + CÓDIGO DE SEGURIDAD

1) Algo que el usuario sabe → contraseña
2) Algo que el usuario tiene → teléfono
3) Algo que el usuario es → huella dactilar





TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

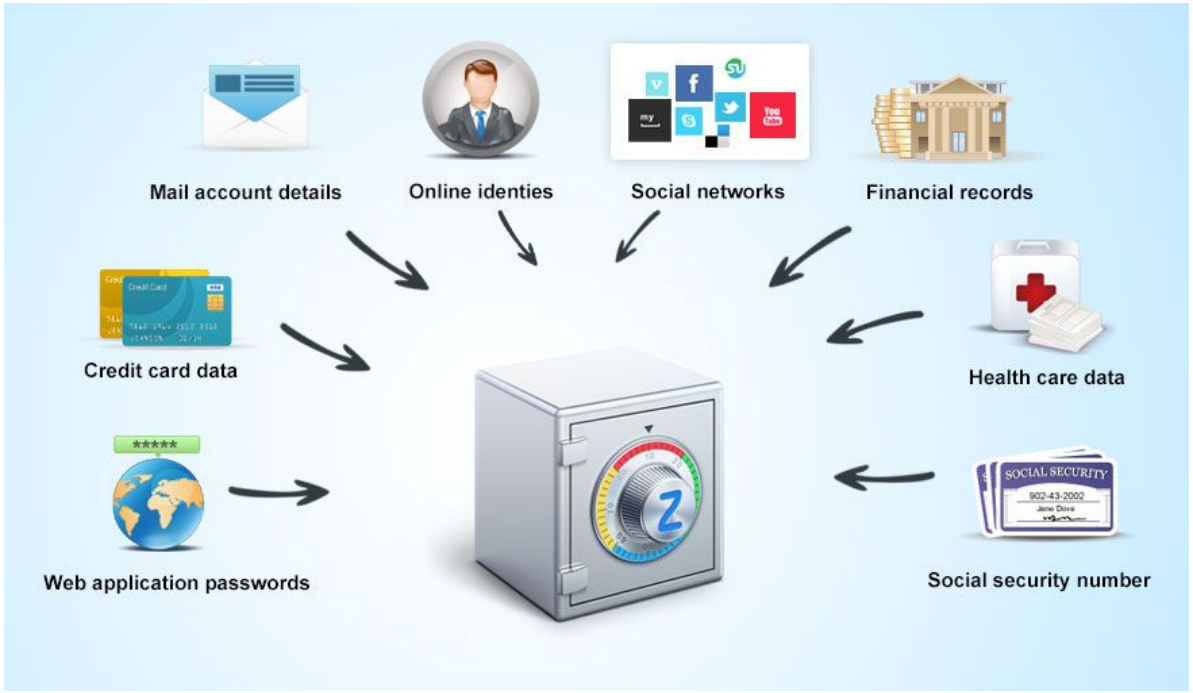
GOBIERNO NACIONAL

Paraguay de la gente

Gestores de contraseña

CERT-PY

¿Cómo acordarnos de tantas contraseñas?



Offline:

1Password

Kaspersky Password Manager

KeePassX

KeePass

Norton Identity Safe

Online:

McAfee LiveSafe

LastPass

Dashlane

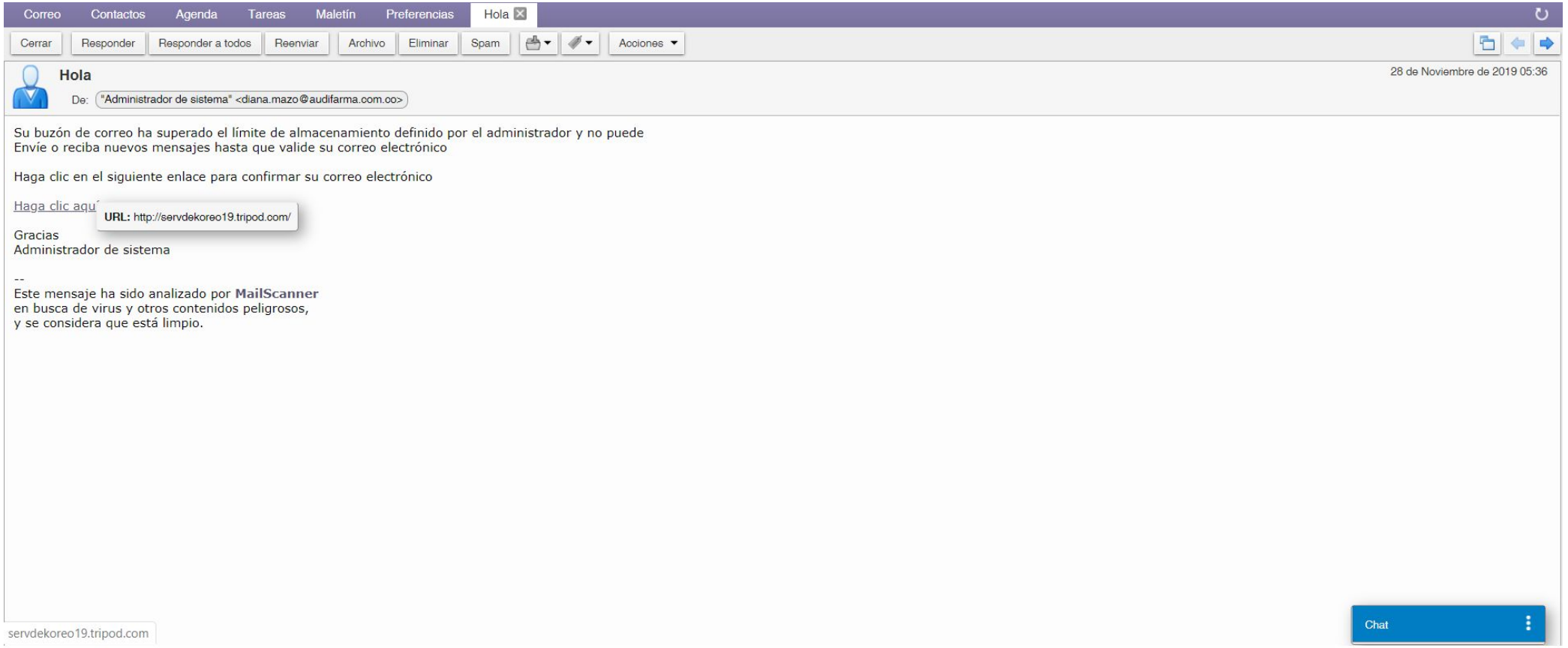
Avast Easy Pass

Zoho Vault

CERT-PY

Correo Electrónico

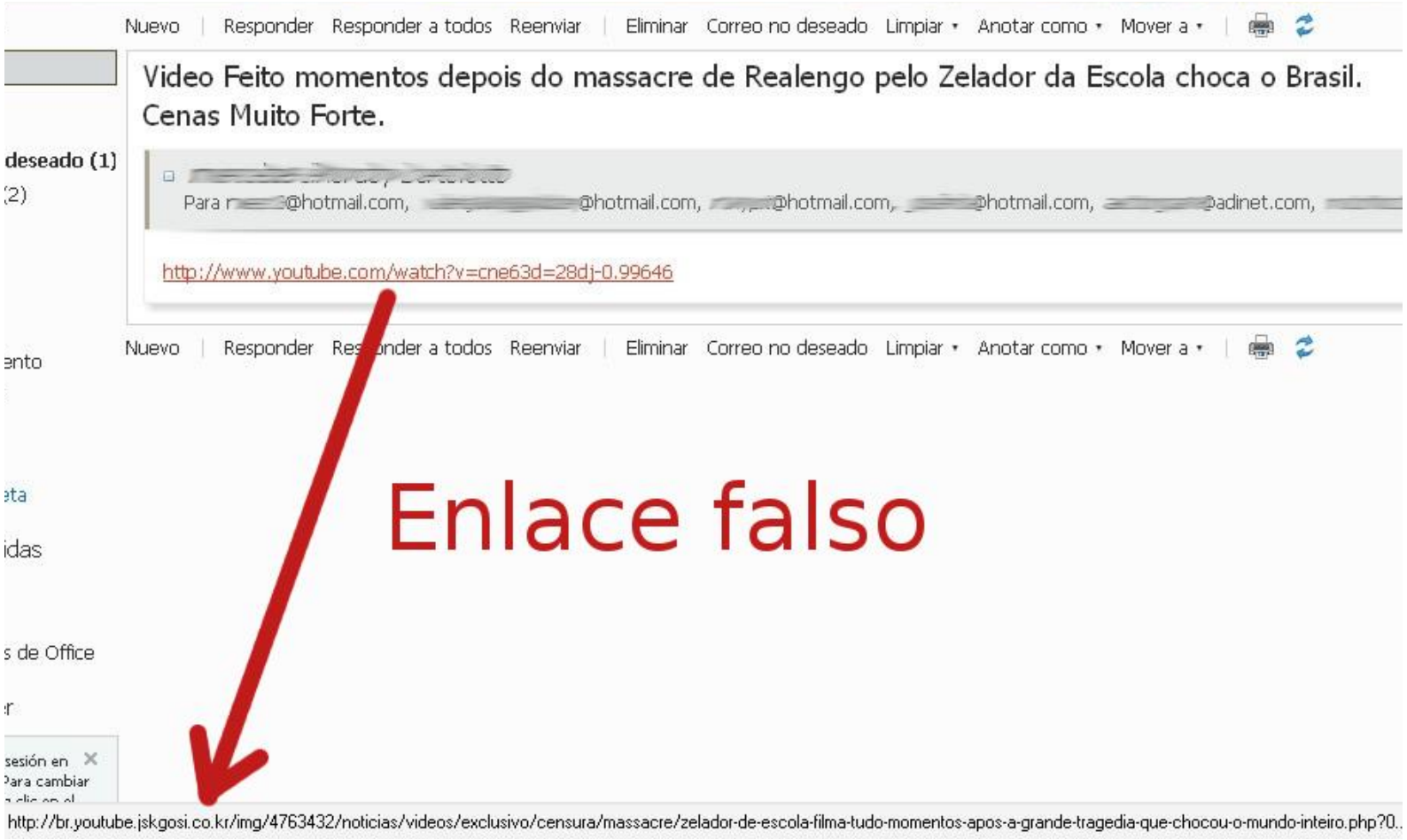
Spam


Correo
Contactos
Agenda
Tareas
Maletín
Preferencias
Hola
Cerrar
Responder
Responder a todos
Reenviar
Archivo
Eliminar
Spam
Acciones
Hola
28 de Noviembre de 2019 05:36
De: "Administrador de sistema" <diana.mazo@audifarma.com.co>
Su buzón de correo ha superado el límite de almacenamiento definido por el administrador y no puede
Envíe o reciba nuevos mensajes hasta que valide su correo electrónico
Haga clic en el siguiente enlace para confirmar su correo electrónico
Haga clic aqu
URL: http://servdekoreo19.tripod.com/
Gracias
Administrador de sistema
--
Este mensaje ha sido analizado por MailScanner
en busca de virus y otros contenidos peligrosos,
y se considera que está limpio.
servdekoreo19.tripod.com
Chat

Spam

BUILD A FREE WEBSITE
OF YOUR OWN ON
TRIPOD.
Home
Rellene y envie el formulario
Nombre de usuario
Email
Contrasena
Confirmar contrasena
Submit

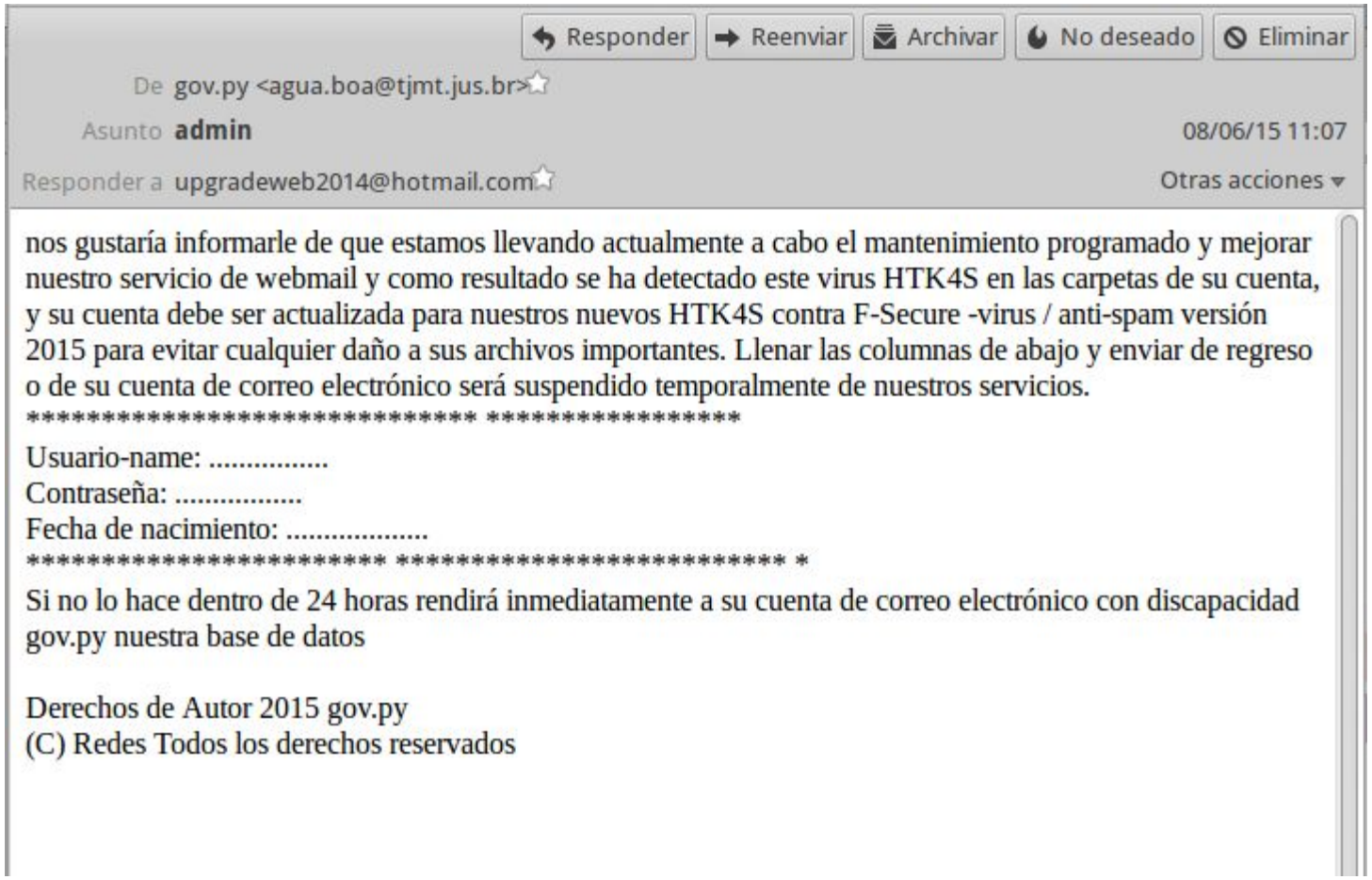
Spam



TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente



Responder | Reenviar | Archivar | No deseado | Eliminar

De gov.py <agua.boa@tjmt.jus.br>

Asunto **admin** 08/06/15 11:07

Responder a upgradeweb2014@hotmail.com Otras acciones

nos gustaría informarle de que estamos llevando actualmente a cabo el mantenimiento programado y mejorar nuestro servicio de webmail y como resultado se ha detectado este virus HTK4S en las carpetas de su cuenta, y su cuenta debe ser actualizada para nuestros nuevos HTK4S contra F-Secure -virus / anti-spam versión 2015 para evitar cualquier daño a sus archivos importantes. Llenar las columnas de abajo y enviar de regreso o de su cuenta de correo electrónico será suspendido temporalmente de nuestros servicios.

********** **********

Usuario-name: .....

Contraseña: .....

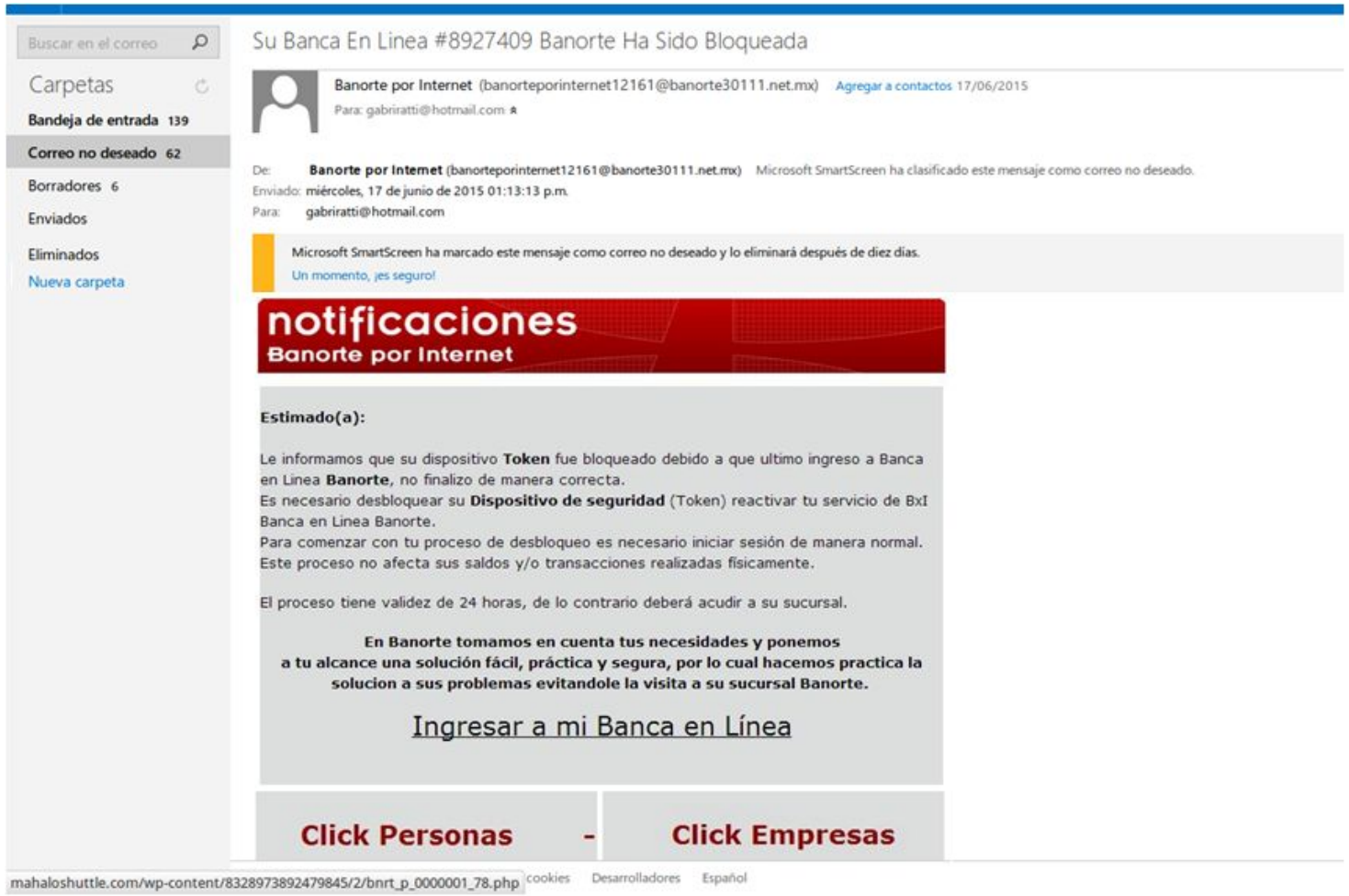
Fecha de nacimiento: .....

********** ********** *

Si no lo hace dentro de 24 horas rendirá inmediatamente a su cuenta de correo electrónico con discapacidad gov.py nuestra base de datos

Derechos de Autor 2015 gov.py
(C) Redes Todos los derechos reservados

CERT-PY



TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

¿Cómo cuidarnos del Spam?

- Cuidado con los archivos adjuntos
- Bloquear imágenes y contenido remoto de los correos
- Proteger la dirección de correo
- Filtros anti-spam
- No responder jamás el spam
- No entrar a enlaces
- Buenas prácticas para las contraseñas
- No reenviar cadenas
- Utilizar la opción “Con Copia Oculta” (CCO)
- No enviar un correo a más de 10 ~ 15 contactos.
- Reportar el spam!

¿Y del phishing? ...

¿Cómo cuidarnos del Phishing?

- No proporcionar nunca información confidencial por correo
- Asegurarse de que la URL comience con HTTPS
- Verificar el remitente del correo, en caso de duda, comunicarse personalmente
- Examinar periódicamente la actividad en las cuentas (bancarias, de correo, de redes sociales, etc.)

CERT-PY

Ingeniería Social

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

¿Qué es la ingeniería social?

Es el **arte del engaño** que busca que la víctima revele información confidencial o realice acciones que brinden al atacante un **punto de entrada** a sus sistemas informáticos.

CERT-PY

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

YouTube

Ingeniería social - Otros medios

CERT-PY

¿Qué hay de las redes sociales? ...

¿Y si el engaño no es a través de internet? ...

- **Curiosidad**
- **Empatía**
- **Miedo**
- **Vanidad**
- **Vergüenza**

CERT-PY

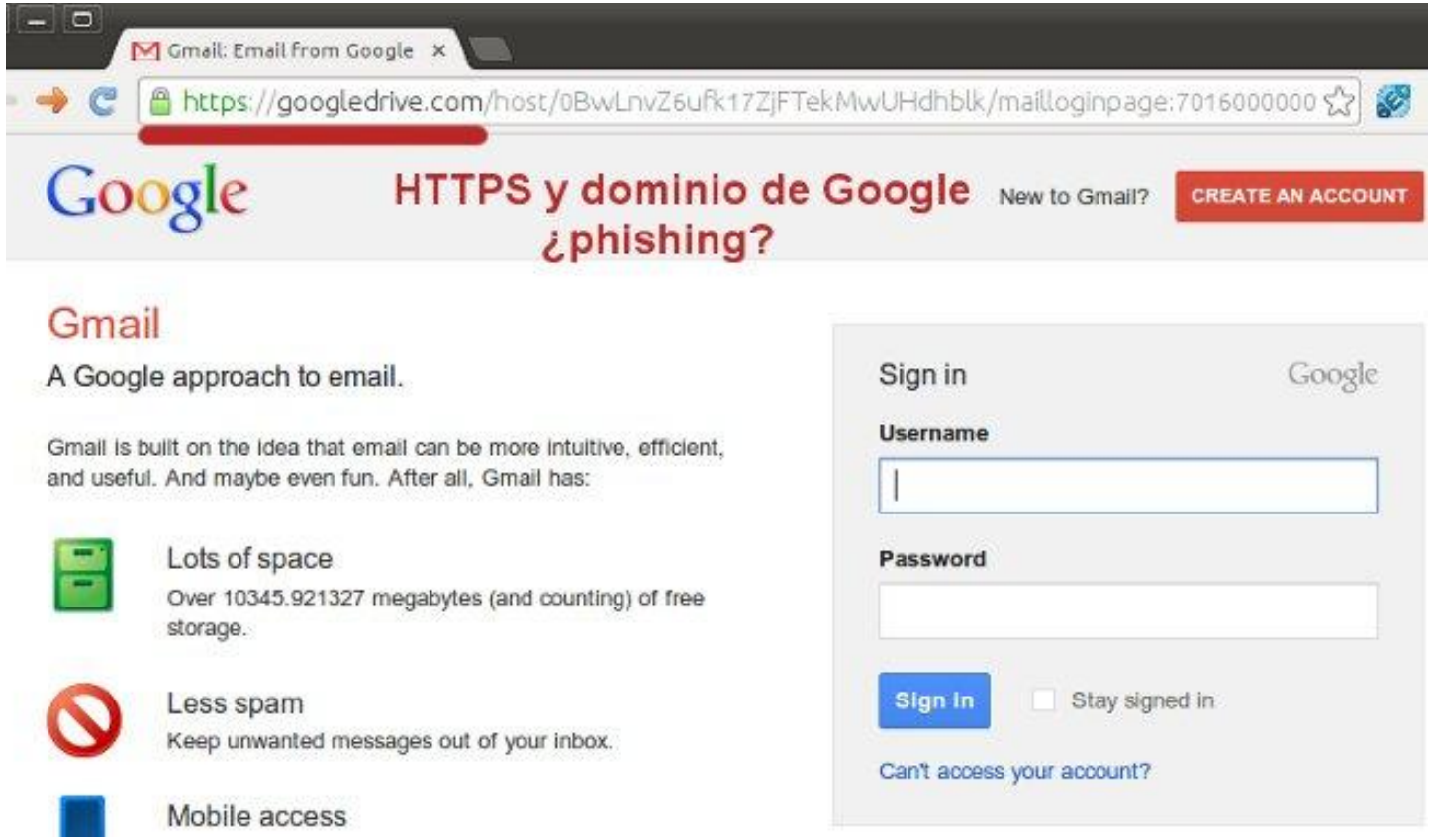
Navegación Segura

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

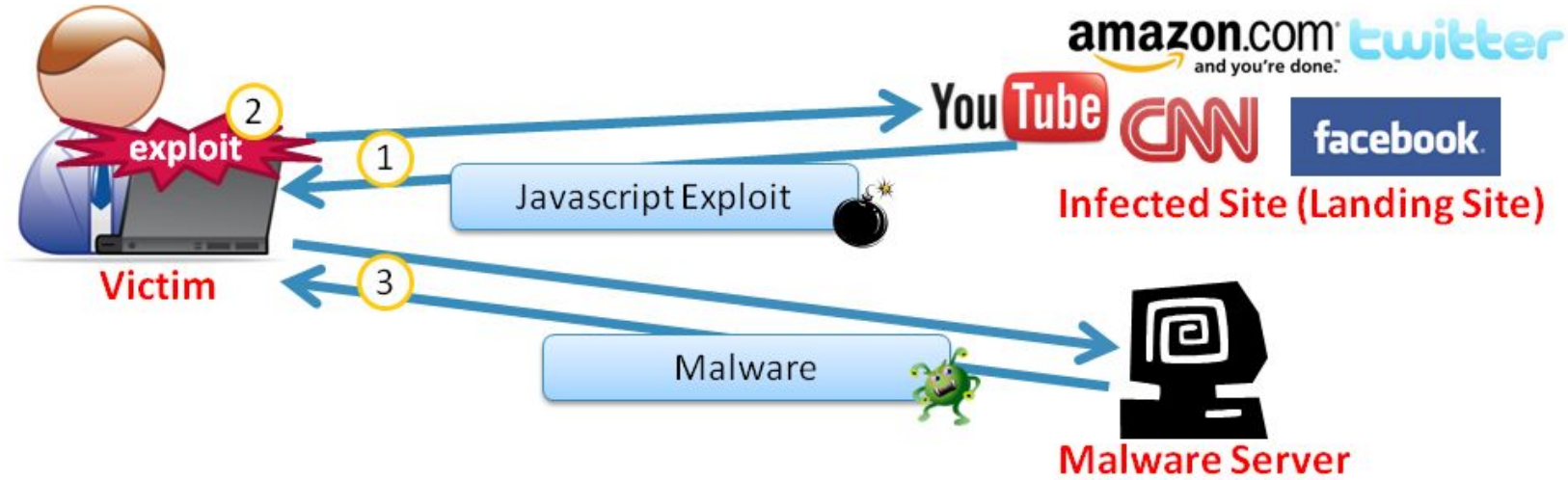
Paraguay de la gente

Las buenas prácticas no bastan



Las buenas prácticas no bastan

Existen técnicas a través de las cuales sólo se requiere que un usuario abra una página web en el navegador para infectarlo.

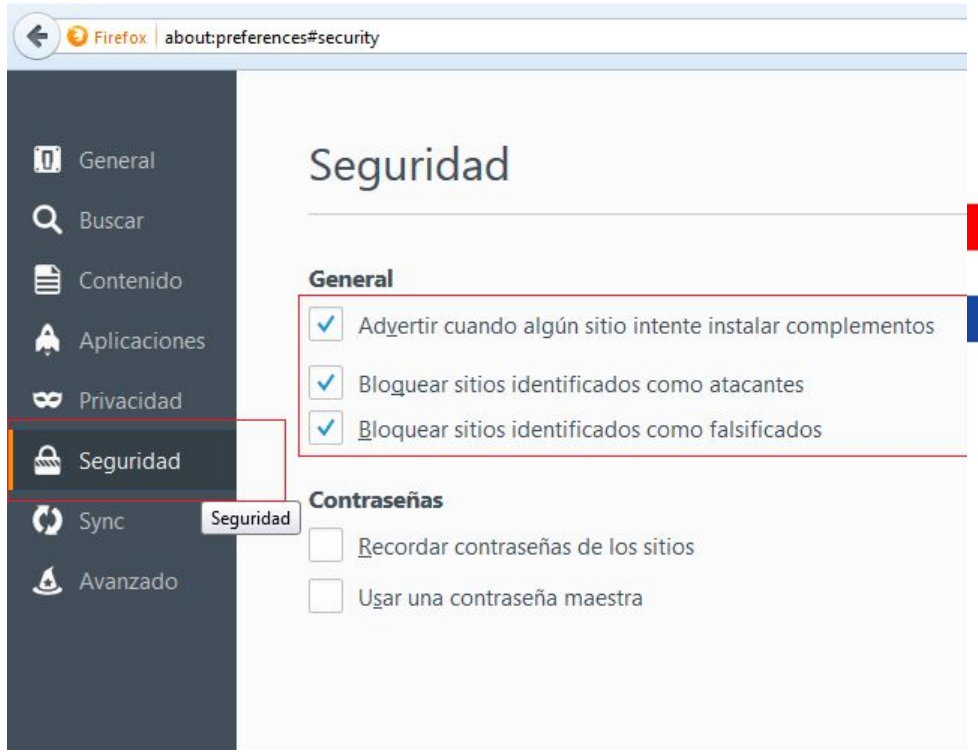


Securizando el Navegador

Protección anti-phishing y anti-malware

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Safari

Protección anti-phishing y anti-malware - Configuración



TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

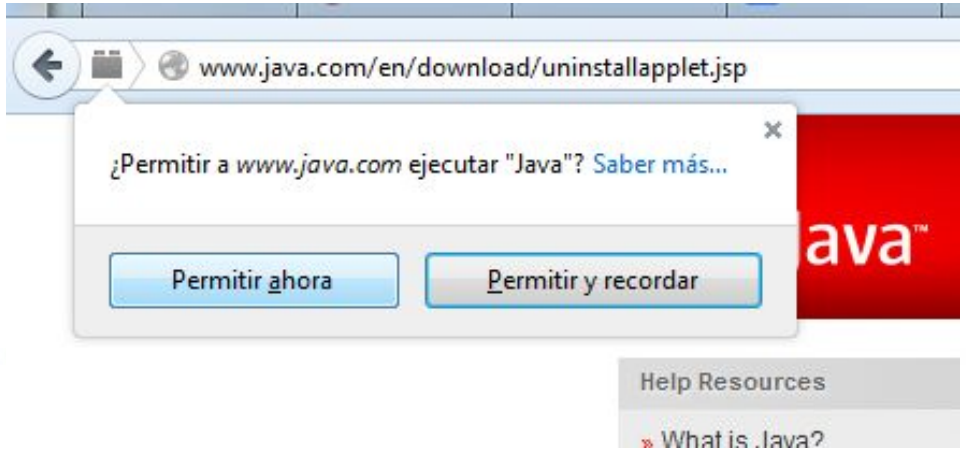
Paraguay de la gente

Securizando el Navegador

CERT-PY

Plugins

- Adobe Flash Player
- Visor de PDF
- Java
- Decodificadores de audio
- Silverlight
- Decidir cuándo otorgar permiso de ejecutar
- Mantenerlos actualizados
- No instalar ni autorizar plugins de sitios dudoso – **cuidado con los plugins**



- **Complementos de seguridad**
  - AdBlock-Plus
  - No-Script
  - ScriptSafe
  - HTTPS Everywhere
  - Ghostery

REPÚBLICA DEL PARAGUAY

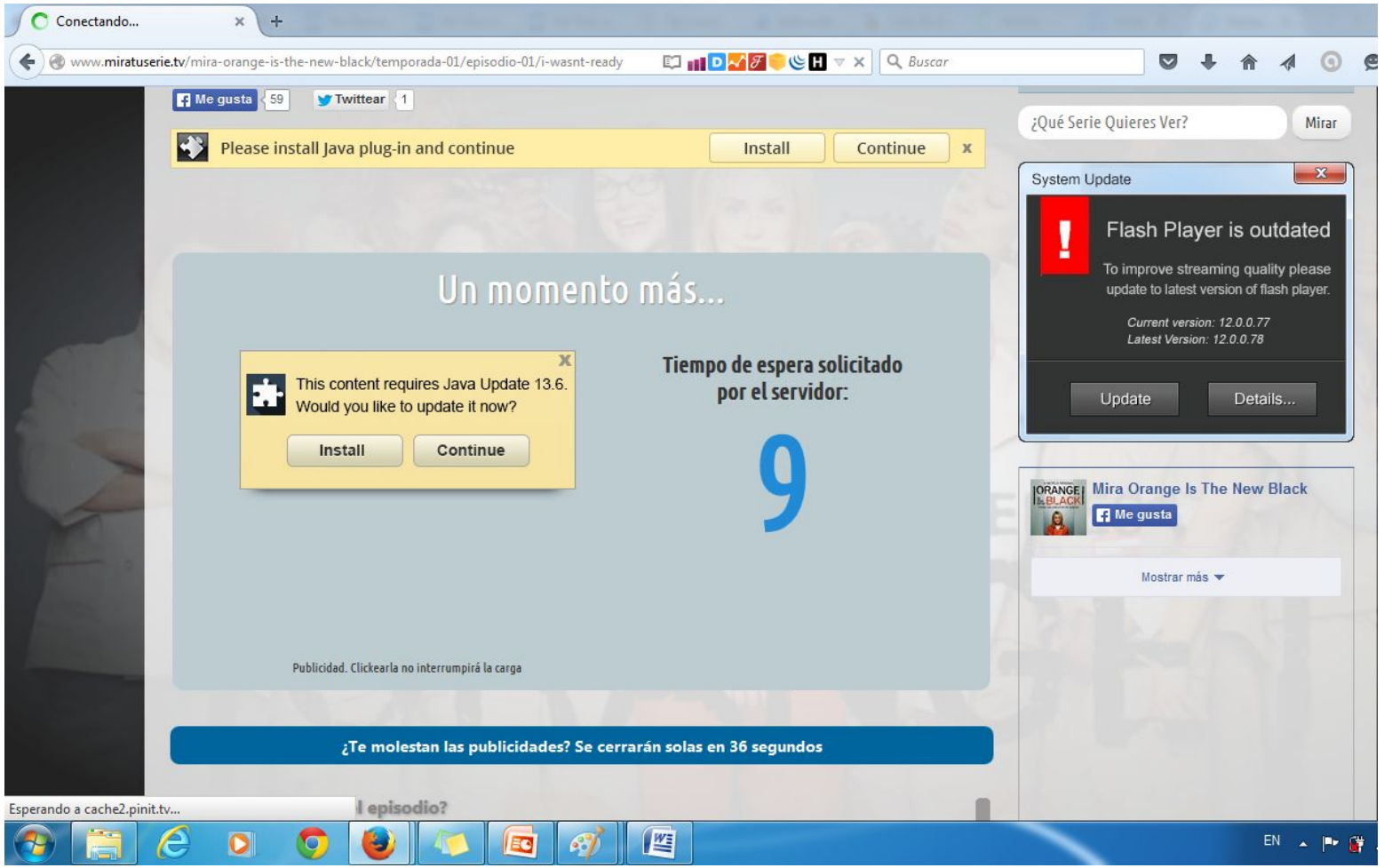
TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

¿Qué tan efectivo es?

CERT-PY



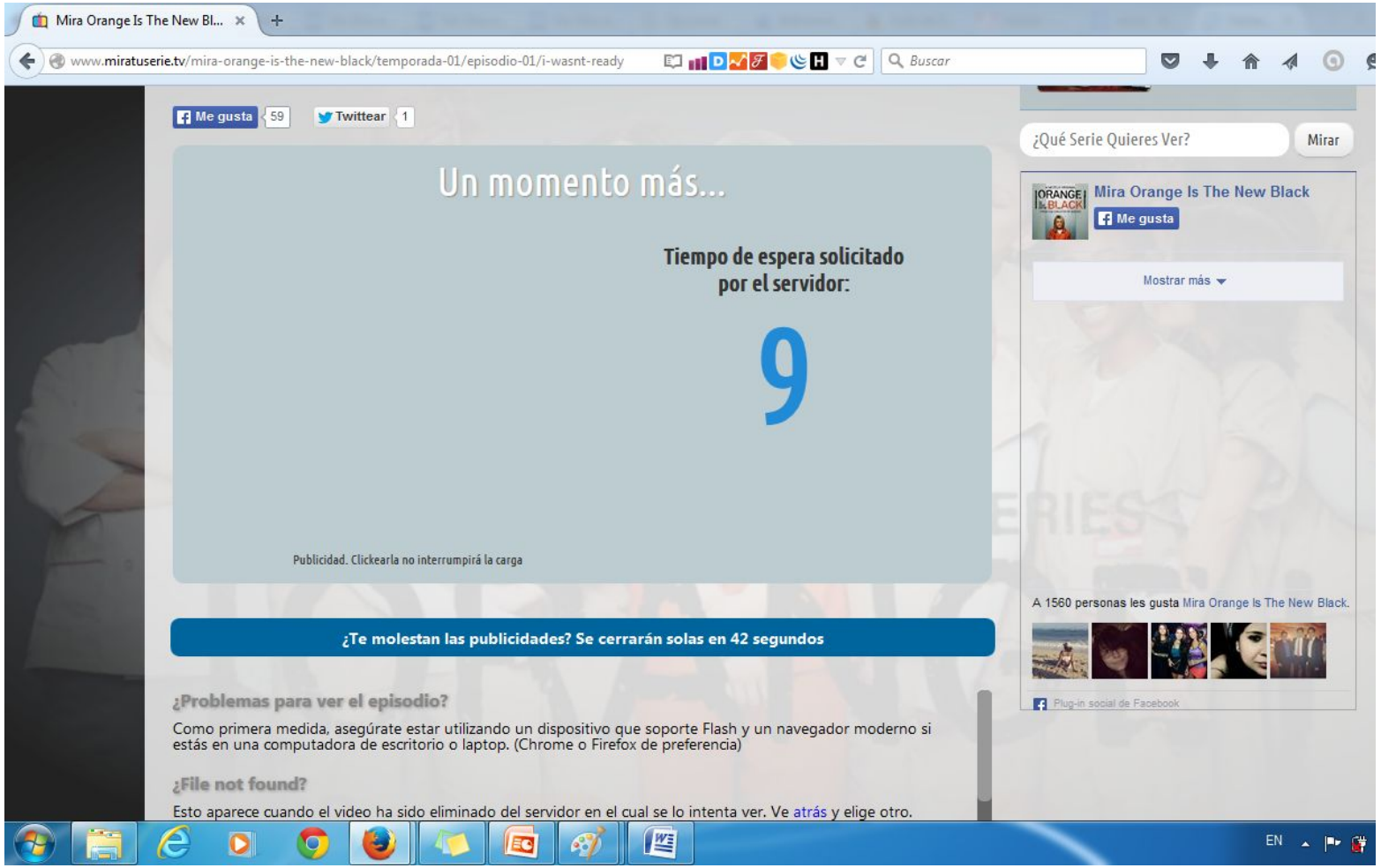
TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

¿Qué tan efectivo es?

CERT-PY



TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

¿Qué tan efectivo es?

CERT-PY

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

CERT-PY

Seguridad en Equipos

Los riesgos

- Virus
- Gusanos
- Spyware
- Troyanos
- Ransomware

¿Cómo entran? ...

CERT-PY

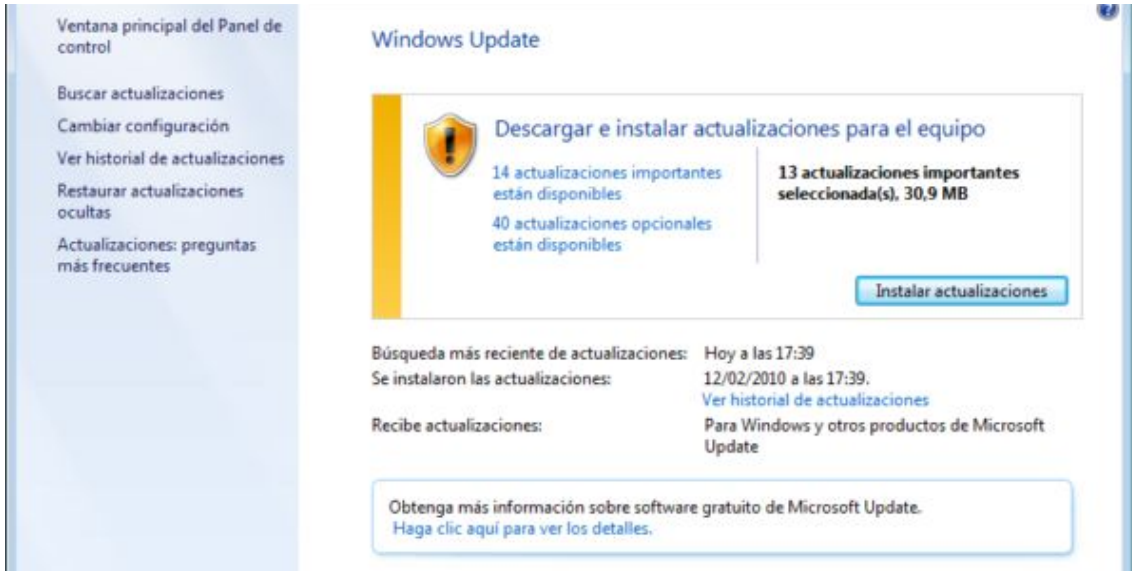
Vulnerabilidades

- Sistema operativo:
  - Windows
  - Linux
  - OS X
  - Android
- Programas o aplicaciones:
  - Office
  - Java
  - Navegadores

CERT-PY

¿Cómo protegernos del malware?

- Actualización permanente del sistema operativo y aplicaciones
- Usar software legal
- No descargar programas de dudosa reputación
- Deshabilitar la ejecución automática de dispositivos USB
- Contar con software de seguridad



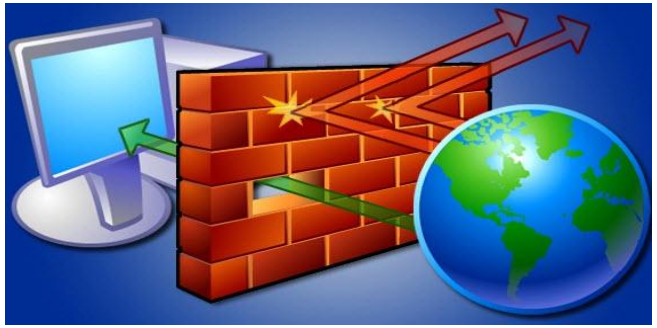
TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

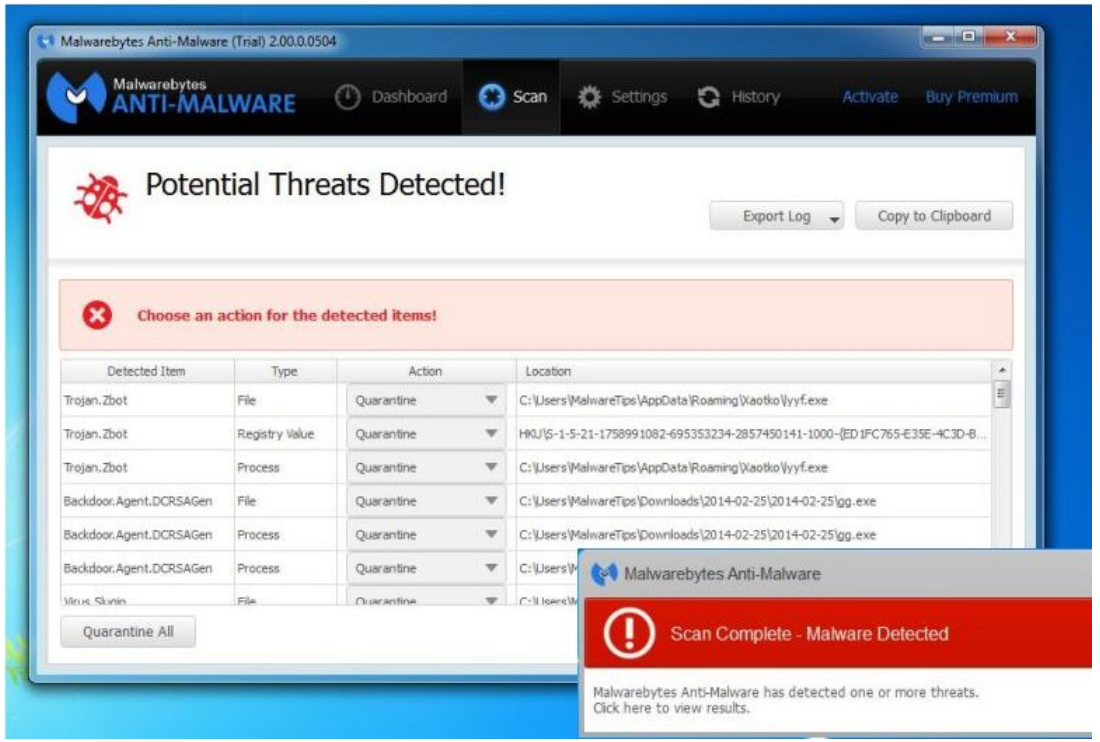
Paraguay de la gente

CERT-PY

Software de seguridad



- Antivirus
- Antimalware
- Firewall



VIPRE from SUNBELT SOFTWARE · TREND MICRO · pctools · McAfee · KASPERSKY lab · ca · eset · AVG · G DATA · PANDA SECURITY · AhnLab · avast! · Norton from symantec · F-Secure · Microsoft Security Essentials · webroot · Quick Heal · RISING · bitdefender

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

CERT-PY

Free vs. Premium

Malwarebytes Anti-Malware Key Features	Free	Premium
REAL-TIME PROTECTION	✗	✓
MALICIOUS WEBSITE BLOCKING	✗	✓
AUTOMATIC UPDATES	✗	✓
FAST HYPER SCANS	✗	✓
SCHEDULED SCANS	✗	✓
ADVANCED MALWARE DETECTION	✓	✓
ADVANCED MALWARE REMOVAL	✓	✓

CERT-PY

Ransomware

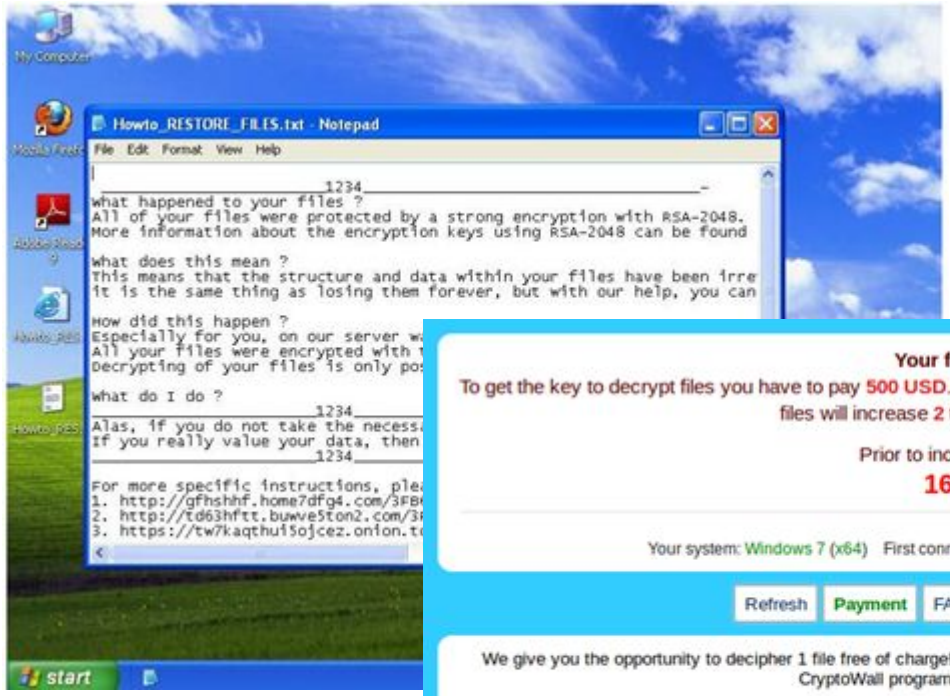
TEMBIPORU MARANDU HA IÑEMOAÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

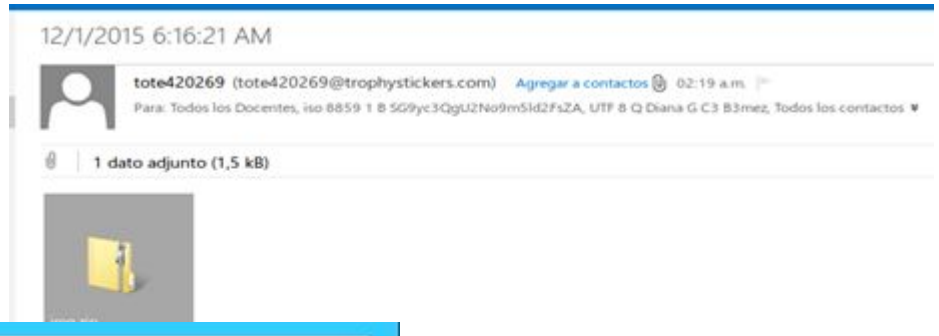
GOBIERNO NACIONAL

Paraguay de la gente

CERT-PY

Ransomware (1)





TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

CERT-PY

Protección de Datos

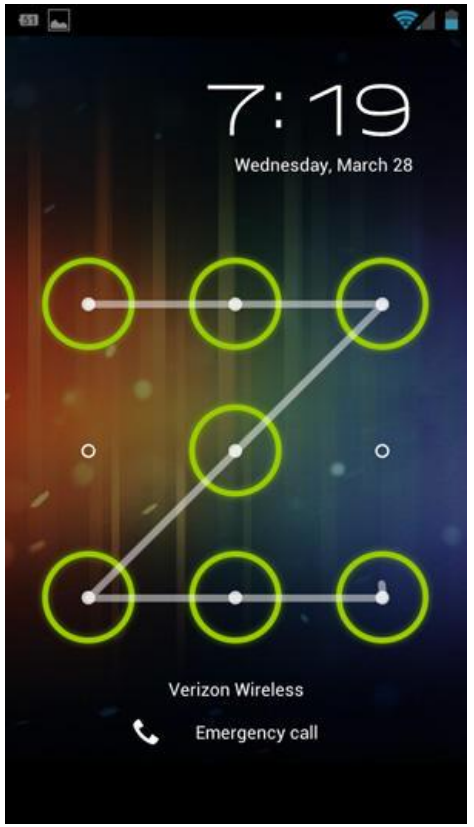
TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

- Robo de equipos
- Daños
- Pérdida de equipos
- Malware (Ransomware)
- Intrusiones

- **Contraseña de inicio de sesión**
- **Pantalla de bloqueo**



CERT-PY

Backup

Más importante que nunca ..

Ransomware

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

CERT-PY

Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

www.cert.gov.py

@CERTpy

/CERT-Py

denuncias: abuse@cert.gov.py
contactos: cert@cert.gov.py

REPÚBLICA DEL PARAGUAY

TEMBIPORU MARANDU HA IÑEMOASÃIRÃ
Motenondeha
Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente