CONTRALORÍA

GENERAL DE LA REPÚBLICA

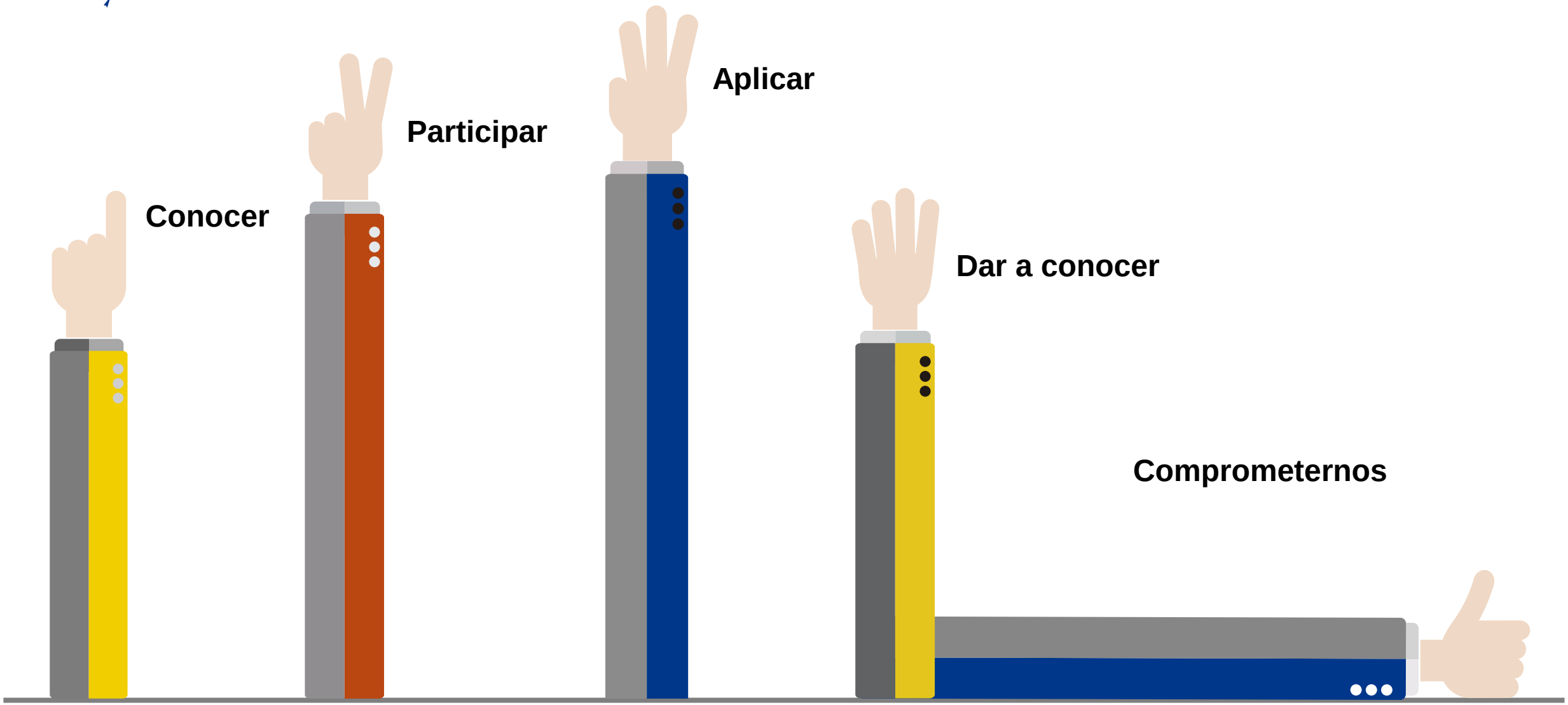
SINERGIA

Gobierno de TI para TODOS

Políticas de Seguridad

Septiembre 12 de 2017

¿Qué vamos a hacer?



Nuestro objetivo

Dar a conocer las políticas del Sistema de Gestión de Seguridad de la CGR y la importancia del rol del tecnólogo como parte activa de la seguridad en la Entidad.

Los avances tecnológicos proporcionan grandes ventajas para la humanidad

… pero traen consigo grandes retos para la seguridad.

Veamos algunos incidentes de seguridad ocurridos recientemente

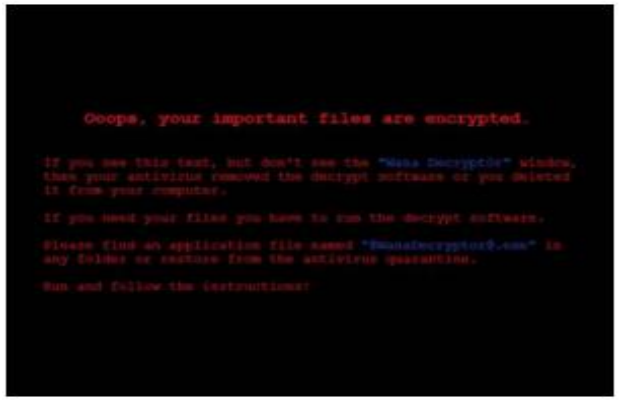
SINERGIA
Gobierno de TI para TODOS

Colombia también es víctima del ataque global informático

74 países reportaron episodios de 'ransomware'. De España, China y EE. UU. hay confirmación.

Los equipos de respuesta a incidentes cibernéticos de varios países están alerta por ataques de 'ransomware'.
Foto: Chubb Seguros

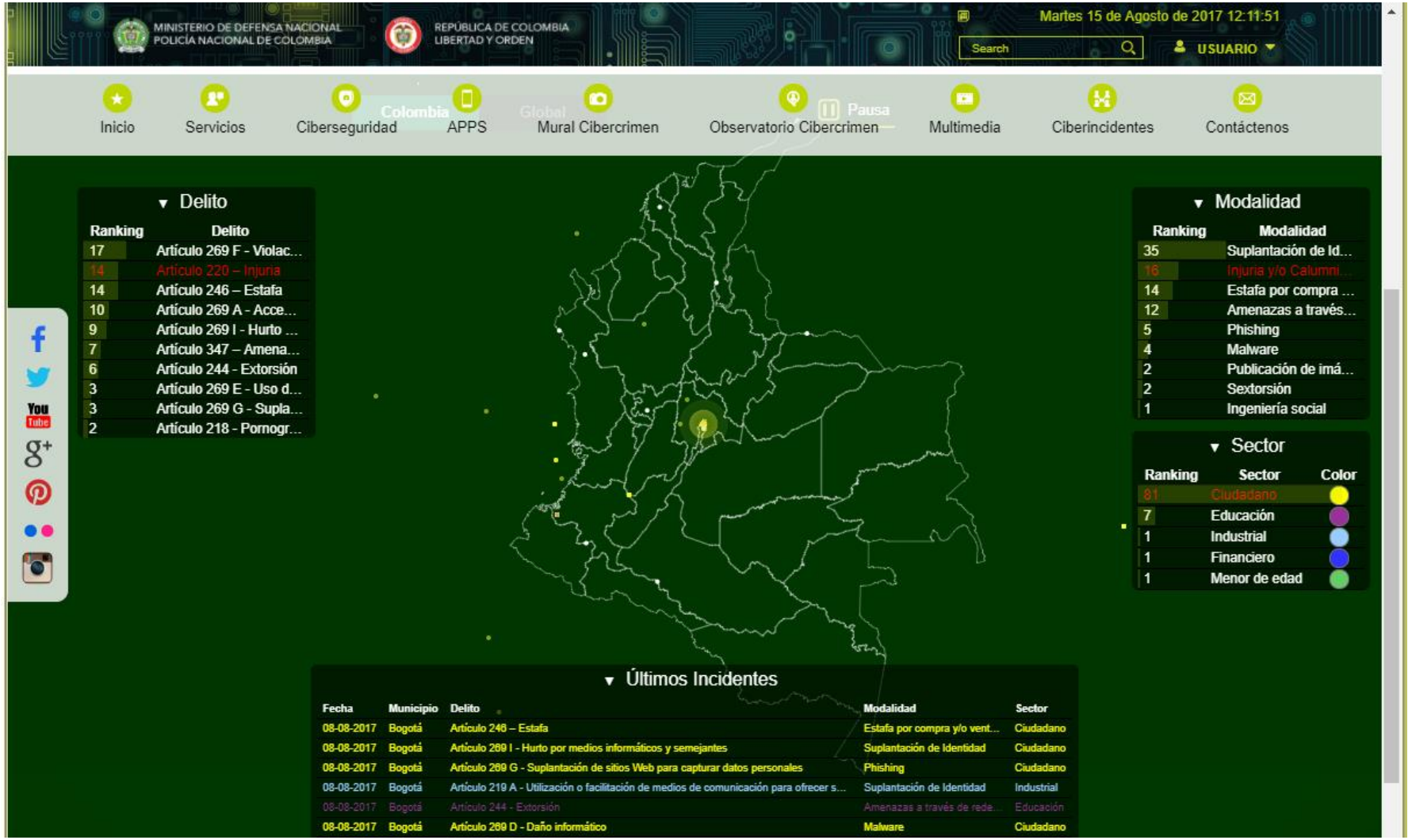
Por: **Tecnósfera** | 13 de mayo 2017 , 08:20 a.m.



Cuando el virus infecta el ordenador, esta imagen aparece ebn el fondo de escritorio.

CIBERATAQUES ACTUALES WANNACRY

CIBERATAQUES ACTUALES PETYA



https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real
https://cybermap.kaspersky.com/es/
http://map.norsecorp.com/#/

SINERGIA
Gobierno de TI para TODOS

¿ En la CGR a qué estamos expuestos?

¿ Cómo nos podríamos ver afectados?

¿Qué podemos hacer para evitarlo?

…Gestión de riesgos de seguridad

Un riesgo es…

La posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.

Un **riesgo de seguridad** se da ante la posibilidad de que una **amenaza** aproveche una **vulnerabilidad** para la que no se tienen controles.

Amenazas	Vulnerabilidades
•Virus •Ingeniera social •Phishing •Robo o extravío de PC's •Ransomware •Acceso indebido a documentos impresos •Violación de contraseñas •Robo de información •Destrucción de soportes documentales •Incumplimiento de leyes y regulaciones	•Falta de conciencia acerca de la seguridad •Uso incorrecto de software o hardware •Descargas de archivos sin precaución

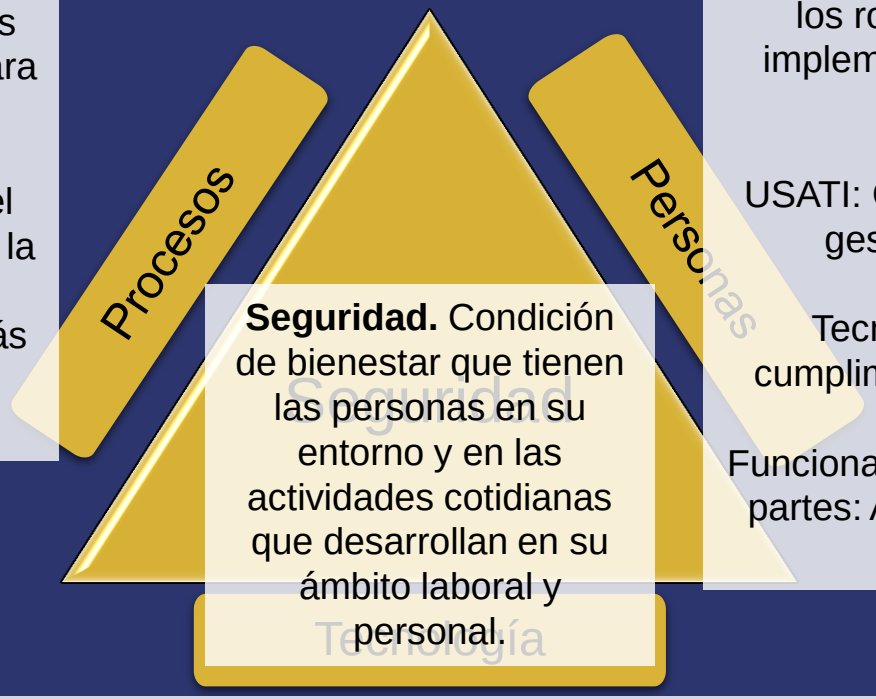
Riesgo de seguridad

¿La CGR cómo gestiona los riesgos de seguridad?

Gestión de riesgos de seguridad

Normatividad

Procesos. Mecanismos formales e informales para realizar las tareas. Identifican, miden, gestionan y controlan el riesgo, la disponibilidad, la integridad y la confidencialidad, además de asegurar la responsabilidad.



Seguridad. Condición de bienestar que tienen las personas en su entorno y en las actividades cotidianas que desarrollan en su ámbito laboral y personal.

Personas. Recursos humanos y los aspectos de seguridad que los rodean. Define quién implementa cada parte de la estrategia:

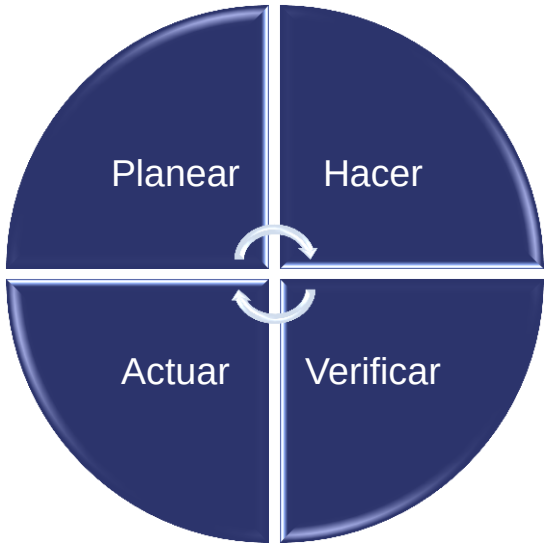
USATI: Gestiona el sistema de gestión de seguridad

Tecnólogos: Apoyan el cumplimiento de las políticas.

Funcionarios/contratista/terceras partes: Aplicamos las políticas de seguridad.

Tecnología. Conformada por herramientas, aplicaciones e infraestructura que incrementa la eficiencia de los procesos.

Sistema de gestión de seguridad - SGS



Creado mediante Resolución Organizacional OGZ-0531-2016

El SGS establece lineamientos para minimizar los riesgos de seguridad de las personas, la información y los bienes de la Contraloría General de la República.

Consúltelo en: http://clic-online/USATI/Paginas/default.aspx

Política de seguridad de personas

Propósito

Establecer el compromiso en la CGR para coordinar la protección de los derechos a la vida, la libertad, integridad y seguridad de los servidores públicos y contratistas de la Entidad cuando estén en riesgo extraordinario derivado del ejercicio de su cargo

¿Cómo?

Con la prevención y mitigación de riesgos extraordinarios

Definiendo, elaborando, implementando y manteniendo procedimientos internos de seguridad de personas

Atendiendo los principios de: Consentimiento, causalidad y reserva legal.

Política de seguridad de bienes

SGS-B-PO-001

Propósito

Establecer el compromiso en la CGR para velar y garantizar la seguridad de los bienes a su cargo

¿Cómo?

Con la prevención y mitigación de riesgos para garantizar la continuidad de la operación

Definiendo, elaborando, implementando, manteniendo y mejorando los procedimientos de seguridad de bienes

Política de seguridad y privacidad de la información

SGS-I-PO-001

Propósito

Declaración que representa la posición de la administración de la CGR con respecto a la protección de activos de información.

La seguridad de la información se relaciona con el cumplimiento de los principios de: Confidencialidad, Integridad y Disponibilidad.

¿Cómo?

La CGR debe elaborar, implantar, mantener y mejorar las estrategias, con una asignación equilibrada de recursos dirigidos a lograr un nivel elevado de la seguridad.

Principios de la seguridad y privacidad de la información

¿Qué pasaría si los datos de los informes de auditoría llegan a manos de personas no autorizadas antes de ser liberados oficialmente?

¿Cómo afectaría que los datos registrados en los sistemas de la CGR estén incompletos?

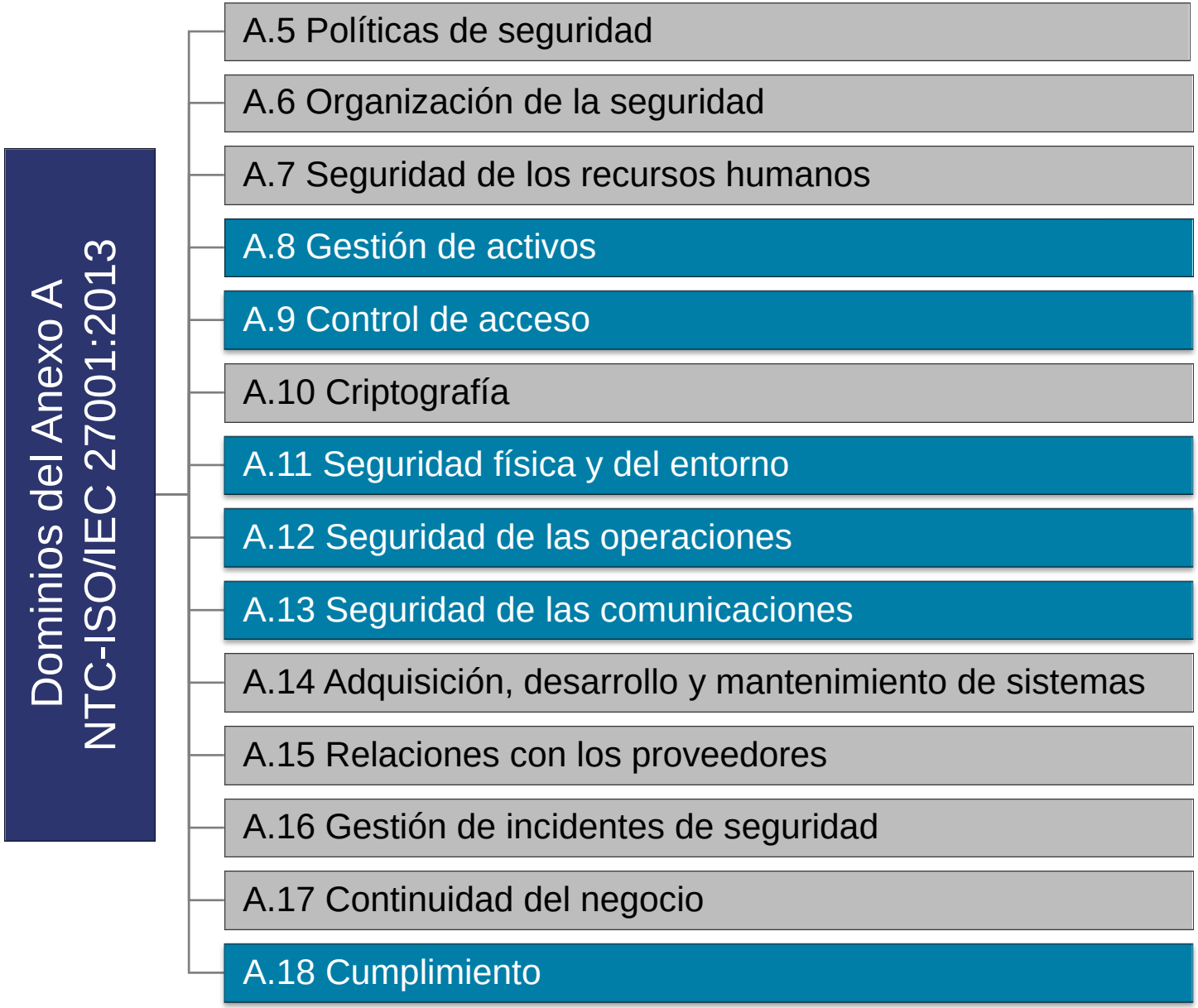
¿Qué pasaría si el aplicativo de registro del proceso auditor se encuentra fuera de servicio?

Para garantizar la confidencialidad, integridad y disponibilidad de la información en la CGR nos basamos en una buena práctica

Norma Técnica Colombiana NTC-ISO/IEC 27001:2013

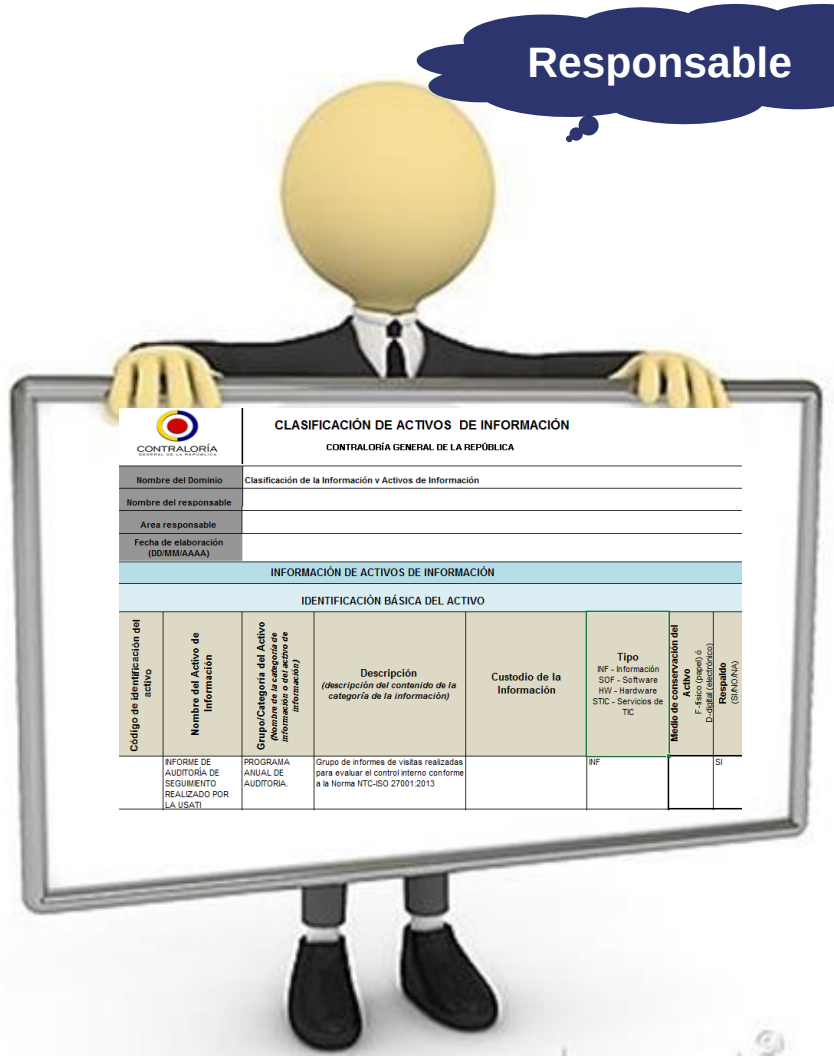
Anexo A	
Dominios	14
Objetivos de control	35
Controles	114

- Entendimiento de la organización y su contexto.
- Liderazgo y compromiso de la alta dirección; Políticas; Roles y responsabilidades.
- Tratamiento de riesgos y definición de objetivos de seguridad.
- Recursos; Competencias; Toma de conciencia; Comunicación; Información documentada.
- La organización debe implementar las acciones para lograr los objetivos de la seguridad.
- Realizar seguimiento, medición, análisis y evaluación del SGSI; Realizar auditorías internas; Revisión por la dirección.
- Identificar no conformidades e implementar acciones para corregirlas.


Dominios del Anexo A
NTC-ISO/IEC 27001:2013
A.5 Políticas de seguridad
A.6 Organización de la seguridad
A.7 Seguridad de los recursos humanos
A.8 Gestión de activos
A.9 Control de acceso
A.10 Criptografía
A.11 Seguridad física y del entorno
A.12 Seguridad de las operaciones
A.13 Seguridad de las comunicaciones
A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.15 Relaciones con los proveedores
A.16 Gestión de incidentes de seguridad
A.17 Continuidad del negocio
A.18 Cumplimiento

Política de responsabilidad por los activos (de información)

Vs.



Política de responsabilidad por los activos (de información)

SGS-I-A8-PO-001

Propósito

Otorgar la responsabilidad sobre la Información a los funcionarios, contratistas, proveedores y terceros.

¿Cómo?

Se debe elaborar, documentar y mantener el inventario de activos de información

Todos los activos de información deben tener un responsable que garantice su protección en todo momento

Los activos de información deben ser devueltos al final de la relación laboral

Hacer uso responsable de los activos de información

Política de control de acceso

Vs.

Política de control de acceso

SGS-I-A9-PO-001

Propósito

En la CGR debe implementar controles con el fin de evitar la pérdida, alteración, consulta, uso o acceso no autorizado o fraudulento a los activos

¿Cómo?

- Limitar la asignación y uso de privilegios
- El acceso a áreas seguras debe estar restringido mediante perímetro de seguridad
- Se deben asignar roles y perfiles a grupos de usuarios con niveles de acceso
- Utilizar contraseñas fuertes (mínimo de ocho caracteres, mayúsculas y minúsculas, números y caracteres especiales)
- No escribir las contraseñas en papel
- Cuidar el usuario y contraseña, es personal e intransferible

Política de seguridad física y el entorno

Vs.

Política de seguridad física y el entorno

SGS-I-A11-PO-001

Propósito

Se debe evitar el acceso físico no autorizado a las instalaciones de procesamiento de la información y a sus áreas circundantes

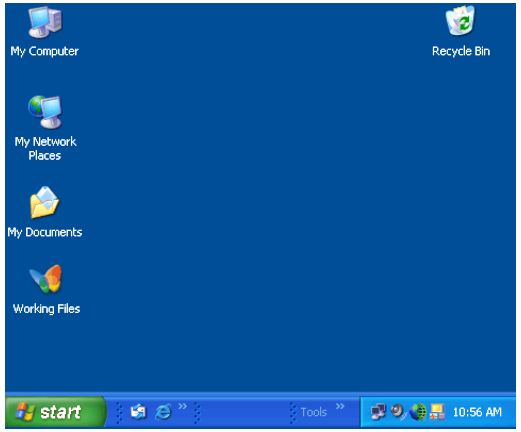
La política busca proteger el entorno de procesamiento y producción de información de la entidad

¿Cómo?

- Portar el carné en lugar visible, no prestarlo y evitar su pérdida
- Bloquear la pantalla del computador al levantarse del puesto
- Proteger los documentos en lugar seguro
- Destruir los documentos que se envían a la basura
- Reportar eventos que se observen como inseguros

Política de escritorio limpio y pantalla limpia

Vs.



Política de escritorio limpio y pantalla limpia

SGS-I-A11-PO-002

Propósito

Gestionar el riesgo asociado al acceso no autorizado, pérdida, daño, modificación o exposición de la información, tanto física como electrónica

¿Cómo?

En ausencias temporales del puesto de trabajo el equipo debe ser bloqueado

Evitar el uso no autorizado de fotocopiadoras, equipos de reproducción o impresión de documentos como escáneres, cámaras digitales, video grabadores, impresoras

En caso de ausencia guardar en lugar seguro los documentos

Política de seguridad de equipos

Vs.

Política de seguridad de equipos

SGS-I-A11-PO-003

Propósito

Garantizar la seguridad de los equipos de cómputo y de infraestructura para prevenir la interrupción de las operaciones de la CGR así como la pérdida, el daño, el robo o el compromiso de los activos de información.

¿Cómo?

Aplicando controles de seguridad de equipos y activos de infraestructura tecnológica de la Entidad dentro de su ciclo de vida: adquisición, utilización u operación, mantenimiento y retiro o renovación.

Bloqueando la pantalla del computador al levantarse del puesto

Política para uso y licenciamiento de software

Vs.

Política para uso y licenciamiento de software

SGS-I-A12-PO-003

Propósito

Definir, implantar, mantener y mejorar las estrategias y procesos que permitan un marco de trabajo seguro

¿Cómo?

No se harán ni usarán copias no autorizadas de software

No descargar, intercambiar, usar, copiar, reproducir ni instalar software no autorizado

Política de protección contra códigos maliciosos

Vs.

Antivirus

Software de aseguramiento de equipos

Política de protección contra códigos maliciosos

SGS-I-A12-PO-002

Propósito

Definir y aplicar procedimientos operacionales y programas de instrucción y concientización sobre código malicioso

Contar con una plataforma de hardware y software con herramientas para detección, prevención y recuperación de amenazas

¿Cómo?

Contar con un servicio especializado para detección y contención de código malicioso con el apoyo de herramientas

Mantener instalado y actualizado el antivirus y el software de aseguramiento de equipos (PC-SECURE)

Revisar con el antivirus los archivos descargados y los dispositivos que conectemos al computador

Política de la gestión de las redes

Vs.

Política de la gestión de redes

SGS-I-A13-PO-001

Propósito

Preservar la confidencialidad, integridad y disponibilidad de la información transmitida y/o transportada por las redes de comunicaciones

¿Cómo?

Aplicar procedimientos para la administración de los equipos de redes y comunicaciones

Las conexiones remotas no están permitidas. Las excepciones requieren autorización

Se debe atender el principio del mínimo privilegio

Política de uso del correo electrónico

Vs.

Política de uso del correo electrónico

SGS-I-A13-PO-003

Propósito

Contemplar los controles para preservar la confidencialidad, integridad y disponibilidad de la información trasmitida y/o transportada a través del correo electrónico de la Entidad.

¿Cómo?

Garantizar la seguridad de los correos electrónicos incluyendo los adjuntos contra la interceptación, exposición, copiado, modificación, desviación o destrucción de la información.

Ser cuidadoso al abrir archivos adjuntos del correo

Abrir correos sólo de fuentes conocidas o confiables

Política de uso de internet

Peligros del Internet

Vs.

Política del uso de internet

SGS-I-A13-PO-004

Propósito

Preservar la confidencialidad, integridad, disponibilidad y privacidad de la información accedida, consultada, trasmitida, almacenada y utilizada por medio de este servicio.

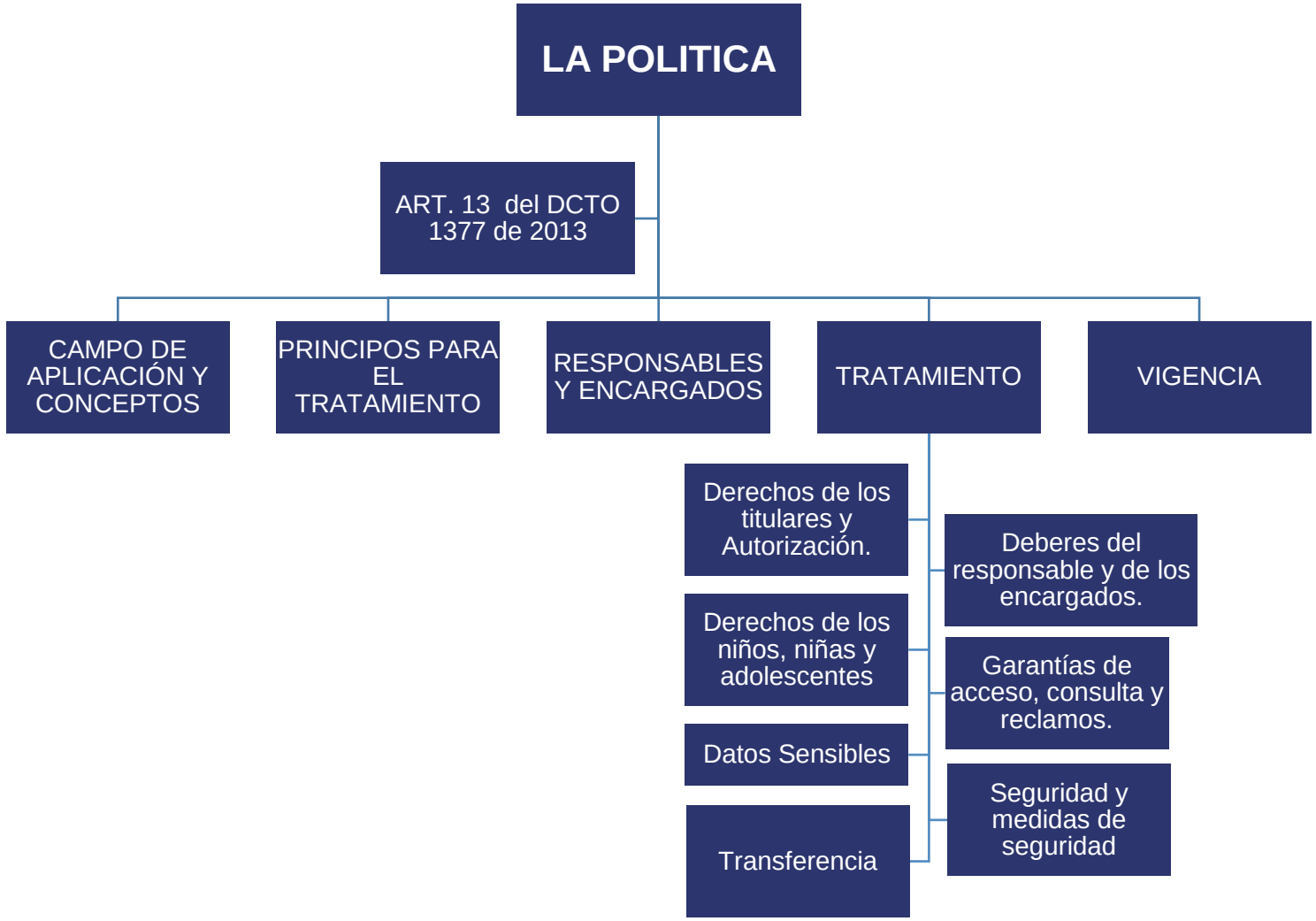
¿Cómo?

Usar el servicio de internet para realizar actividades que tengan relación con el quehacer institucional.

Las redes sociales, acceso a sitios de difusión de contenido comercial, streaming, radio, TV en vivo y fotografías y la descarga de información y otros servicios serán autorizados previa justificación del objetivo y necesidad.

Utilizar con precaución los sitios web, pueden contener código malicioso

Política de tratamiento de datos personales



Política de tratamiento de datos personales

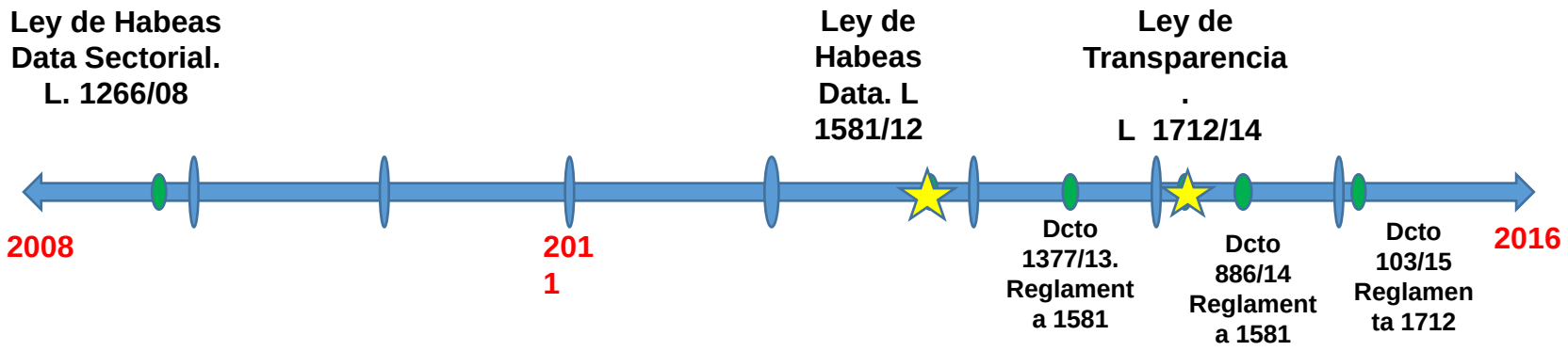
SGS-I-A18-PO-001

CONSTITUCIÓN POLÍTICA:

- Art. 15: Derecho de Habeas Data.
- Art. 20: Derecho de Acceso a la Información Pública.

JURISPRUDENCIA:

- C-748 de 6 de octubre de 2011. Constitucionalidad de la Ley de Habeas Data.
- C-274 de 9 de mayo de 2013. Constitucionalidad de la Ley de Transparencia.



Política de tratamiento de datos personales

Ley 1581 de 2012 y sus decretos reglamentarios.

Criterio Objetivo:
Aplicable a cualquier base de datos.

Derecho a la intimidad y al buen manejo de su información: **principio de circulación restringida.**

VS

Ley 1712 de 2014 y su decreto reglamentario.

Criterio Subjetivo:
Aplicable a los sujetos obligados.

Derecho de acceso a la Información publica: **principio de máxima divulgación.**

La seguridad es responsabilidad de todos

Seguridad física

- Portar el carné en lugar visible, no prestarlo y evitar su pérdida
- Bloquear la pantalla del computador al levantarse del puesto
- Proteger los documentos en lugar seguro
- Destruir los documentos que se envían a la basura
- Reportar eventos que se observen como inseguros

Gestión de activos

- Hacer uso responsable de los activos de información

Control de acceso

- Utilizar contraseñas fuertes (mínimo de ocho caracteres, mayúsculas y minúsculas, números y caracteres especiales)
- Cuidar el usuario y contraseña, es personal e intransferible
- No escribir las contraseñas en papel

Seguridad de las operaciones

- No descargar, intercambiar, usar, copiar, reproducir ni instalar software no autorizado
- Mantener instalado y actualizado el antivirus y el software de aseguramiento de equipos (PC-SECURE)
- Revisar con el antivirus los archivos descargados y los dispositivos que conectemos al computador

Gestión de las comunicaciones

- Ser cuidadoso al abrir archivos adjuntos del correo
- Abrir correos sólo de fuentes conocidas o confiables
- Utilizar con precaución los sitios web, pueden contener código malicioso

Protección de datos personales

- Salvaguardar los documentos que contengan datos personales (semiprivados, privados o sensibles)

Toma la seguridad como un hábito

SINERGIA

Gobierno de TI para TODOS

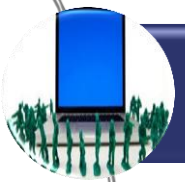
Listas blancas en Ciberseguridad

La importancia de PCSecure

Septiembre 12

Introducción

A quién afectó WannaCry y Petya?



Pero, ¿por qué no funcionó la ciberdefensa en las grandes corporaciones?

Los ciberataques han crecido, sus blancos también.

Las defensas tradicionales son ineficaces.

Las organizaciones deben considerar nuevos enfoques.

Nuevo enfoque

Enfoques tradicionales, la lista negra, heurística.

Deficiencias de este enfoque.

Nuevo enfoque: La técnica de lista blanca sirve para detener malware avanzado.

Lista blanca

La técnica de Lista Blanca es recomendada por algunas de las más importantes autoridades de ciberseguridad en el mundo.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Homeland Security

Lista blanca

THE SEVEN STRATEGIES

1. IMPLEMENT APPLICATION WHITELISTING

Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of some systems, such as database servers and human-machine interface (HMI) computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.

Example: ICS-CERT recently responded to an incident where the victim had to rebuild the network from scratch at great expense. A particular malware compromised over 80 percent of its assets. Antivirus software was ineffective; the malware had a 0 percent detection rate on VirusTotal. AWL would have provided notification and blocked the malware execution.

https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Lista blanca

Homeland Security

Seven Strategies to Defend ICSs

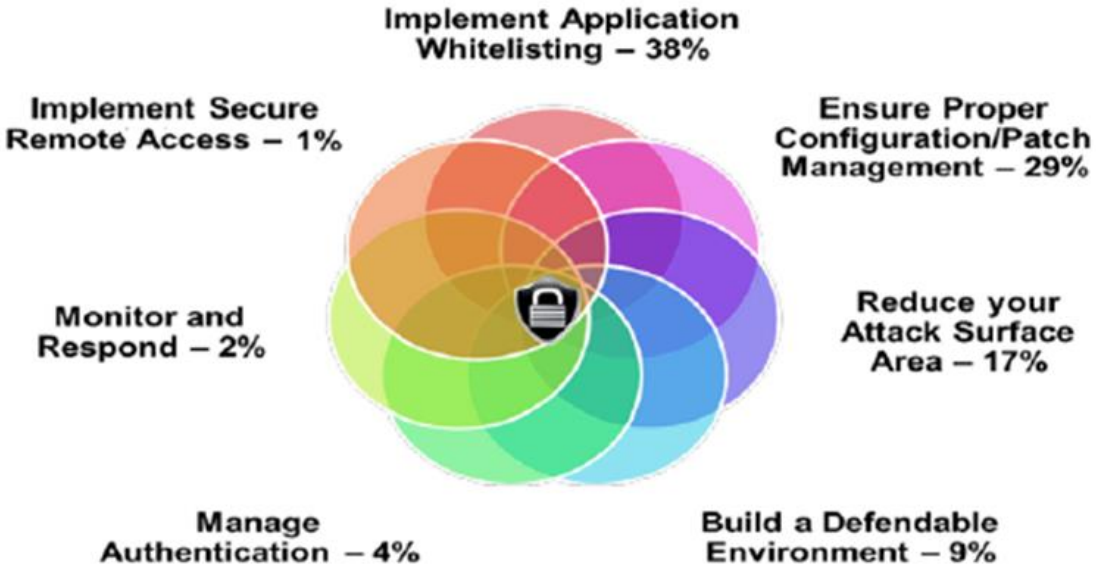


Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

Ventajas de la lista blanca

Protección contra el malware, aún el desconocido, pues impide que se corran ejecutables no autorizados.

Mejora la productividad, porque no se instalarán ni ejecutarán programas no deseados.

Impide la instalación de software ilegal o no licenciado.

Evita el uso ineficiente de recursos de la organización

Lista blanca en la CGR

La CGR, desde diciembre de 2013, cuenta con una aplicación de lista blanca: **Pcsecure**.

Pcsecure es un aplicativo de seguridad para equipos de usuario final que aplica la tecnología de lista blanca.

Pcsecure debe estar instalado y activo en todos los computadores (de usuario final) de la Entidad.

PC Secure

- ✓ Reducción de Riesgos Informáticos
  - ✓ (Evita acceso no autorizado a los equipos; instalación de software malicioso o virus; daño en la información y programas improductivos).
- ✓ Aseguramiento y control de fuga de Información sensible
  - ✓ (Copias de respaldo y cumplimiento sobre manejo de información de terceros. Control de extracción de información privada).
- ✓ Cumplimiento de Normas Legales
  - ✓ (Evita instalación de software sin licencia, música y videos con derechos de autor).
- ✓ Aplicación de Herramientas de medición y uso de la Tecnología
  - ✓ (Estadísticas, tendencias, productividad).

Módulos de PC Secure

PC Secure

Facilita algunas tareas de soporte, entre las que destacan:

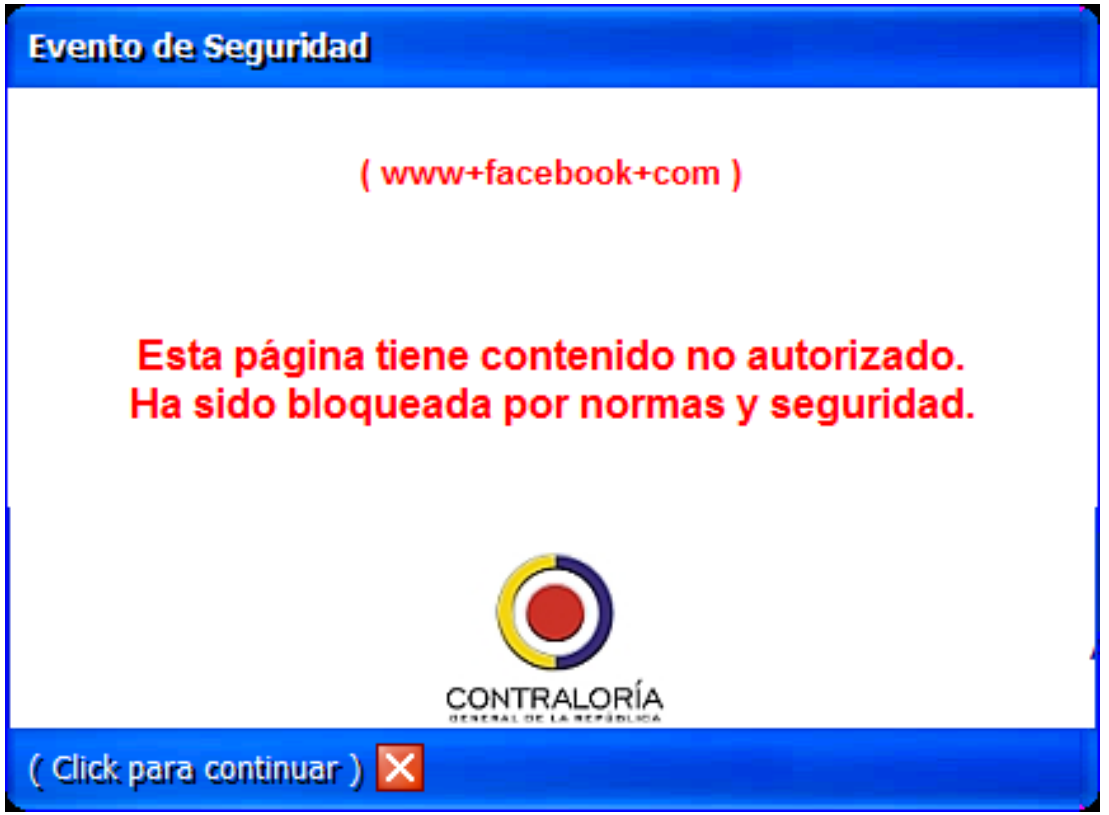
- Control remoto para realizar capacitación o soporte a usuarios.
- Instalación y/o ejecución masiva de cualquier aplicativo.
- Ejecución de tareas de administración sin necesidad de cerrar sesión en los usuarios.
- Obtención de inventario de hardware y software.
- Programación de copias de respaldo personalizadas.
- Envío de mensajes a los PC de la Gerencia.
- Alertas de cambios de hardware.
- Apagado remoto de los equipos, entre otros.

Top 5 – Lo que no sabemos y nos molesta

1. Mensaje de “List index out of bounds (0)”.
2. Bloqueos a instalación de aplicativos autorizados.
3. Bloqueos de ejecutables autorizados.
4. Bloqueos a página web autorizadas.
5. No se reportan algunos equipos a mi consola.

PC Secure

Si el bloqueo de un programa o página web lo hace Pcsecure, se despliega un aviso como este:



PC Secure

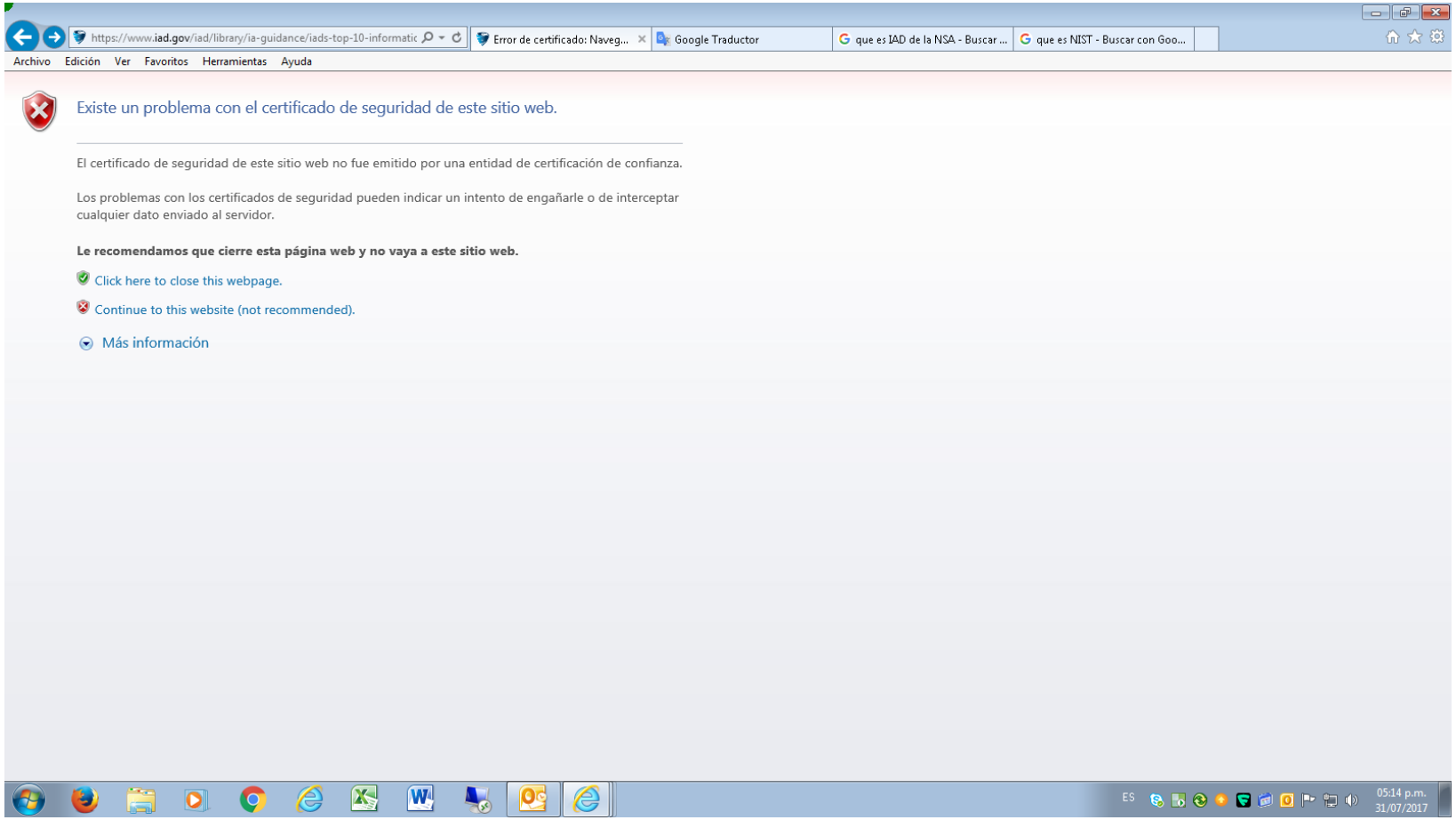
También el filtrado web, administrado desde la OSEI, puede bloquear páginas de Internet. En este caso, el mensaje es como este:

PC Secure

Mensajes de bloqueo del filtrado web.

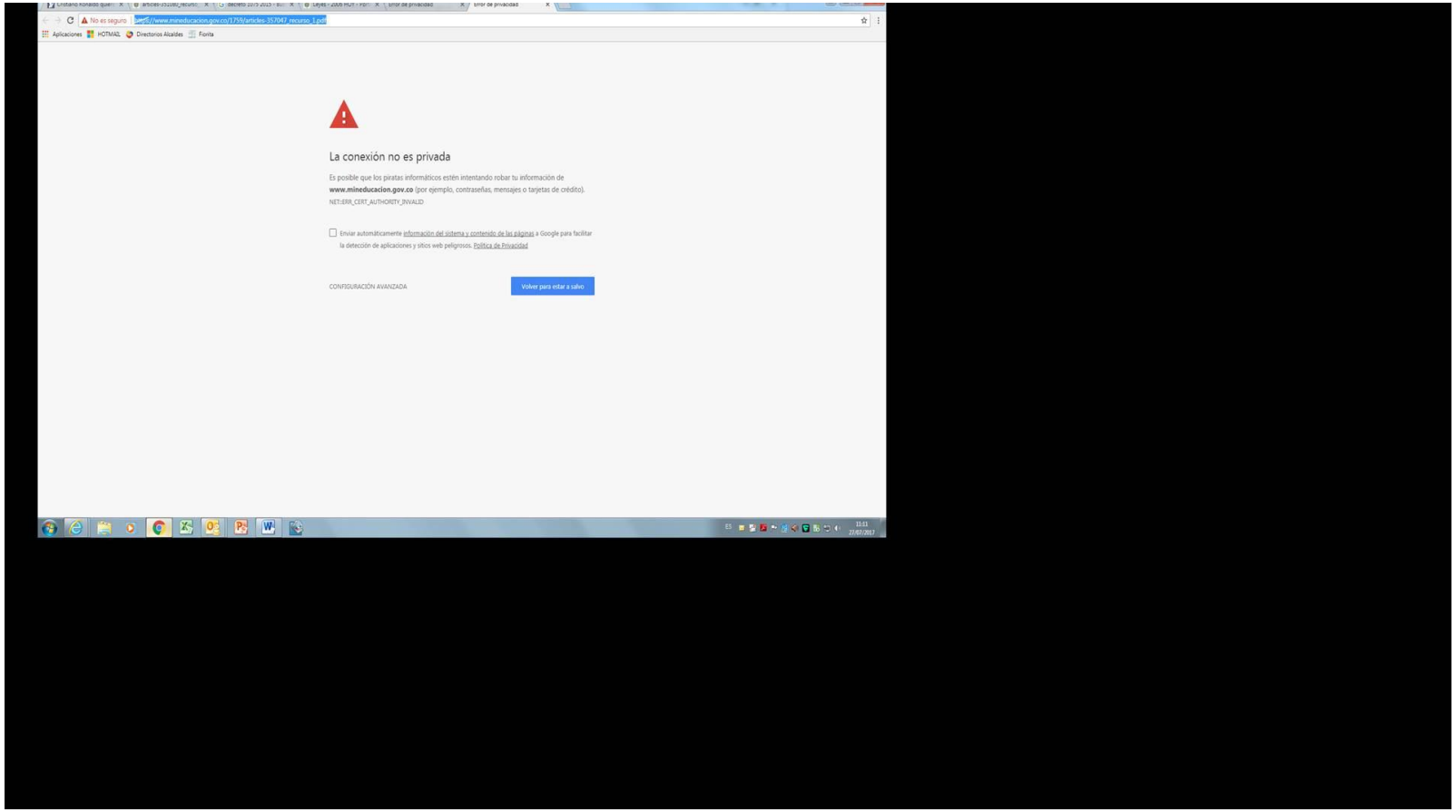
PC Secure

Otros mensajes de bloqueo, navegadores.



PC Secure

Otros mensajes de bloqueo, navegadores.

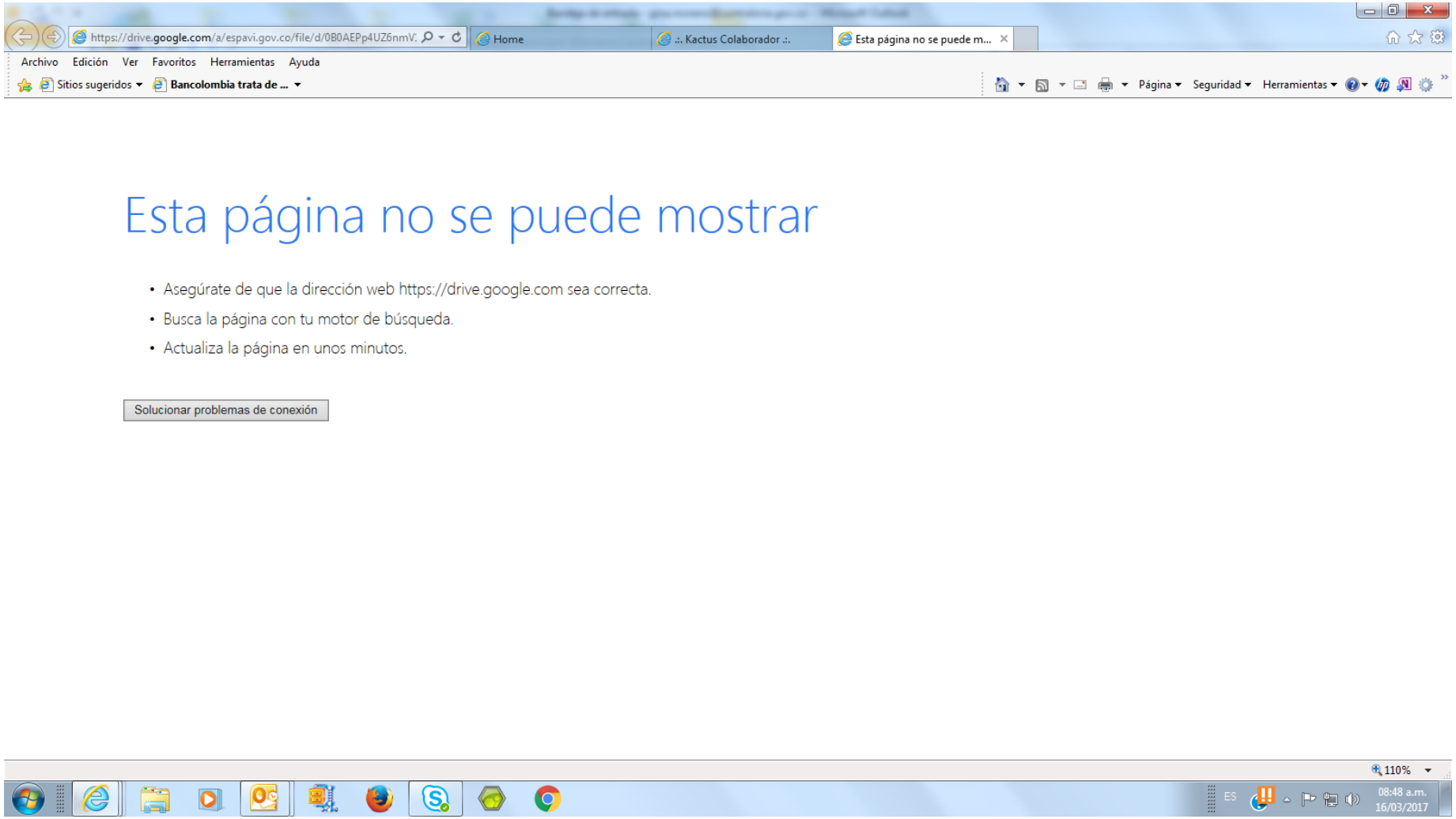


PC Secure

Otros mensajes de bloqueo

SINERGIA
Gobierno de TI para TODOS

PC Secure



Qué hacer en caso de bloqueo

1. Determinar si el bloqueo es legítimo.
2. Si el bloqueo no es legítimo, tomar una imagen del bloqueo.
3. Crear una incidencia en la Mesa de Ayuda, describiendo la situación, adjuntando la imagen, indicando la IP del equipo, así como el nombre y usuario de red del funcionario. Es necesario justificar la solicitud.
4. Si se trata de una página web restringida, la solicitud debe ser enviada por un directivo de la dependencia.

Conclusiones y recomendaciones

1. Es necesario tener un complemento al antivirus en el equipo de usuario final.
2. Tener Pcsecure instalado y activo en cada equipo.
3. Comunicar cualquier anomalía o desviación.
4. Los Tecnólogos de las Gerencias son administradores de Pcsecure y guardianes de la seguridad en su Gerencia.
5. No apagar la consola junior.
6. Socializar el uso de Office 365.
7. Pcsecure es fundamental para la seguridad en la CGR.

La seguridad es responsabilidad de todos

IMPORTANCIA DEL ROL DE TECNÓLOGO PARA LA SEGURIDAD

❖Enlace para apoyar el cumplimiento de las políticas de seguridad impartidas por la CGR, de acuerdo a los lineamientos del Sistema de Gestión de Seguridad – SGS de la Entidad.

❖Apoyar en la sensibilización y apropiación del Sistema de Seguridad SGS de la Entidad en su dependencia de acuerdo a las directrices establecidas.

❖Reportar los incidentes de seguridad

CONCLUSIÓN

La seguridad es un proceso esencial para la prestación de servicios de la Entidad, todos debemos ser conscientes de su importancia y participar activamente aplicando prácticas y comportamientos que permitan mitigar los riesgos a los que estamos expuestos.