PROCESO DE SANITIZACIÓN DE EQUIPOS DE CÓMPUTO

Comisión Federal de Electricidad®

Dirección Corporativa de Administración
Coordinación de Servicios Tecnológicos
Gerencia de Tecnologías De Información

HOJA DE FORMALIZACIÓN

CLAVE DEL ÁREA: ***K4000***			***COORDINACIÓN DE SERVICIOS TECNOLÓGICOS***
DIA	***MES***	***AÑO***	***GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN***
19	03	2020	

AUTORIZACIÓN

Ing. Marco Antonio López Meléndez Coordinador de Servicios Tecnológicos	Gerente de Tecnologías de Información

REVISIÓN

Ing. Manuel Alejandro Soriano Ferreira Subgerente de Planeación y Servicios	Lic. Álvaro Rafael Rodríguez Garza Jefe de la Unidad de Desarrollo Organizacional y Evaluación

VIGENCIA: A partir de la fecha que señala esta Hoja de Formalización, sin exceptuar los cambios y/o modificaciones sustantivas que se presenten durante el periodo.

OBSERVACIONES: Este documento es de carácter obligatorio para todas las áreas de la CFE, sus Empresas Productivas Subsidiarias y Filiales.

CRÉDITOS:

Nombre(s)	***Cargo***
Ing. Americo Castillo Garza	Jefe de la Unidad de Proyectos

CONTROL DE ACTUALIZACIONES

Revisión No.	Motivo o Causa:	Hoja (s) No.

02	Actualización	Todas

1. INTRODUCCIÓN

La CFE cuenta con una diversidad de equipos de cómputo, infraestructura y sistemas informáticos que deben ser protegidos por una adecuada práctica de seguridad informática.

Para reforzar los mecanismos de protección y cumplir con los lineamientos de seguridad de la información, se tienen desplegados diversos servicios e infraestructura de seguridad que permite detectar equipos con comportamiento anómalo o sospechoso, los cuales deben ser atendidos para llevarlos a un estado de seguridad de la información óptimo.

2. OBJETIVO

Definir un proceso de sanitización de equipos de cómputo que se deberá aplicar en los equipos detectados por los servicios e infraestructura de seguridad de la información, para la protección de la información y uso racional de los recursos y sistemas informáticos de la CFE y sus EPS, reduciendo el impacto de ataques informáticos dirigidos contra la información, equipos e infraestructura informática, sistemas sustantivos, críticos y administrativos.

3. ALCANCE

El presente proceso de sanitización de equipos de cómputo es de aplicación general y de cumplimiento obligatorio para todo el personal, así como terceros que por motivos de proyectos, prestación o contrato de servicios profesionales hagan uso de los recursos informáticos y de información de la CFE y sus EPS y sean detectados por los servicios e infraestructura de seguridad de la información con actividad sospechosa o anómala.

4. POLITÍCA

Definir el proceso de sanitización que debe aplicarse a todos los equipos de cómputo que se conecten a la red de datos de la CFE y que sean detectados fuera de cumplimiento o con actividad sospechosa.

5. NORMAS

Políticas Generales relativas a las tecnologías de información y comunicaciones de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias y Filiales.

El personal que haga uso de la presente guía deberá atender lo dispuesto en los Lineamientos en materia de seguridad de la información de la CFE y sus Empresas Productivas Subsidiarias, Filiales y Terceros.

El personal del corporativo, las empresas subsidiarias y filiales de la CFE deberá atender la presente guía. En caso que por razones técnicas o de operación se requiera un procedimiento o guía distinto u actualizado al presente, la propuesta deberá de garantizar el cumplimiento del estándar de seguridad que se establecen en esta guía y contar con la autorización de la Coordinación de Servicios Tecnológicos.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 ENTRADAS DEL PROCESO

6.1.1 INFRAESTRUCTURA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

La CFE cuenta con una infraestructura de protección contra código malicioso de Symantec instalada en 60,000 equipos de cómputo, que permite detectar:

- Ataques de código malicioso en la red
- Equipos con cliente de antivirus desactualizado
- Equipos infectados con código malicioso
- Equipos que no han recibido un escaneo en el último mes
- Equipos que requieren un reinicio para eliminar completamente código malicioso

6.1.2 INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PALO ALTO NETWORKS

La CFE cuenta con una infraestructura de seguridad perimetral basada en firewalls de siguiente generación de Palo Alto Networks ubicados en las principales zonas regionales y área metropolitana de la CDMX, que permiten detectar:

- Top de aplicaciones usadas
- Top de consumo por usuarios
- Top de categorías de filtrado de URL visitadas
- Top de hosts con acceso sitios con malware
- Actividad maliciosa detectada
- Top de aplicaciones bloqueadas
- Top de categorías bloqueadas por filtrado de URL
- Top de usuarios bloqueados por navegación hacia categorías bloqueadas
- Usuarios con actividad de Comando y Control

6.2 REVISIÓN DE REPORTES DE ACTIVIDAD SOSPECHOSA

Semanalmente se elaboran los distintos reportes mencionados en la sección anterior, los cuales son analizados para determinar acciones en conjunto para abatir los riesgos de perdida de confidencialidad, integridad y disponibilidad de la información en los activos de TIC de la empresa.

Derivado de este análisis, las acciones a seguir son:

- Estrategia de atención
  - Actividades de remediación
  - Atención automática o por equipo
  - Atención conjunta con personal informático del área

- Plan de trabajo para remediar los equipos y/o situaciones que se estén presentando, indicando:
  - Actividad
  - Fecha de atención
  - Responsable

En el análisis mencionado, además del personal de la Unidad de Proyectos podrá participar eventualmente personal que pueda aportar en la solución y actividades definidas, como:

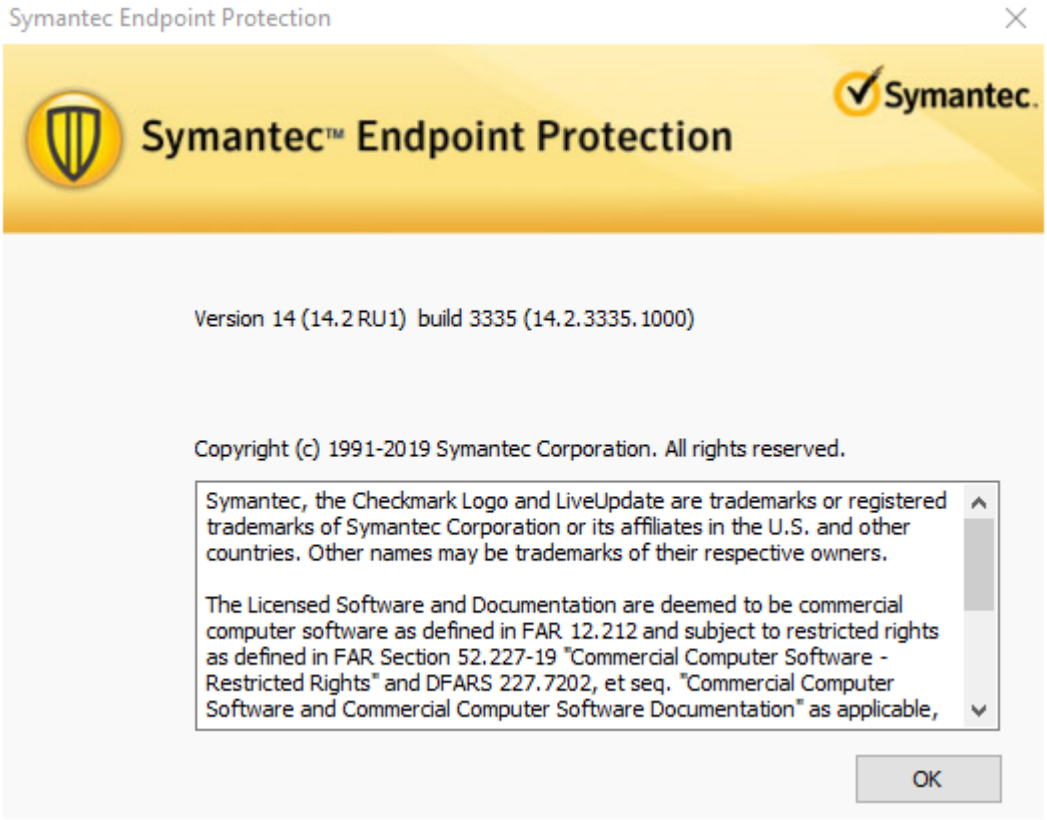
- Personal de redes
- Personal de virtualización
- Personal de TIC regionales

6.3 CHECKLIST DE CONFIGURACIÓN A REVISAR Y ACTIVIDADES POR REALIZAR

6.3.1 ANTIVIRUS CORPORATIVO

Los parámetros a revisar en el cliente de antivirus Symantec Endpoint Protection son los siguientes:

- Versión de antivirus, debe tener instalada la versión 14 (14.2 RU1).



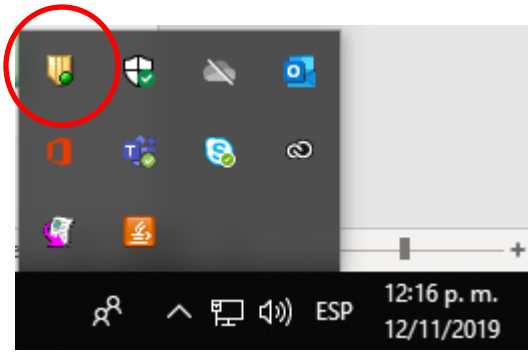
- En caso de no tener instalado el cliente de antivirus o a la versión recomendada, contactar a alguno de los siguientes compañeros:
  - José Flores Landero ext. 48156
  - Rosa Quiroz Dionisio ext. 48274

  Solicitando el paquete de instalación o actualización correspondiente, proporcionando la siguiente información:

  - Direccionamiento IP del equipo
  - Área y proceso
  - Sistema operativo (32 o 64 bits)
  - Tipo de paquete a instalar (PC o servidor)

  Será proporcionada la ubicación para descargar e instalar el paquete que corresponda.

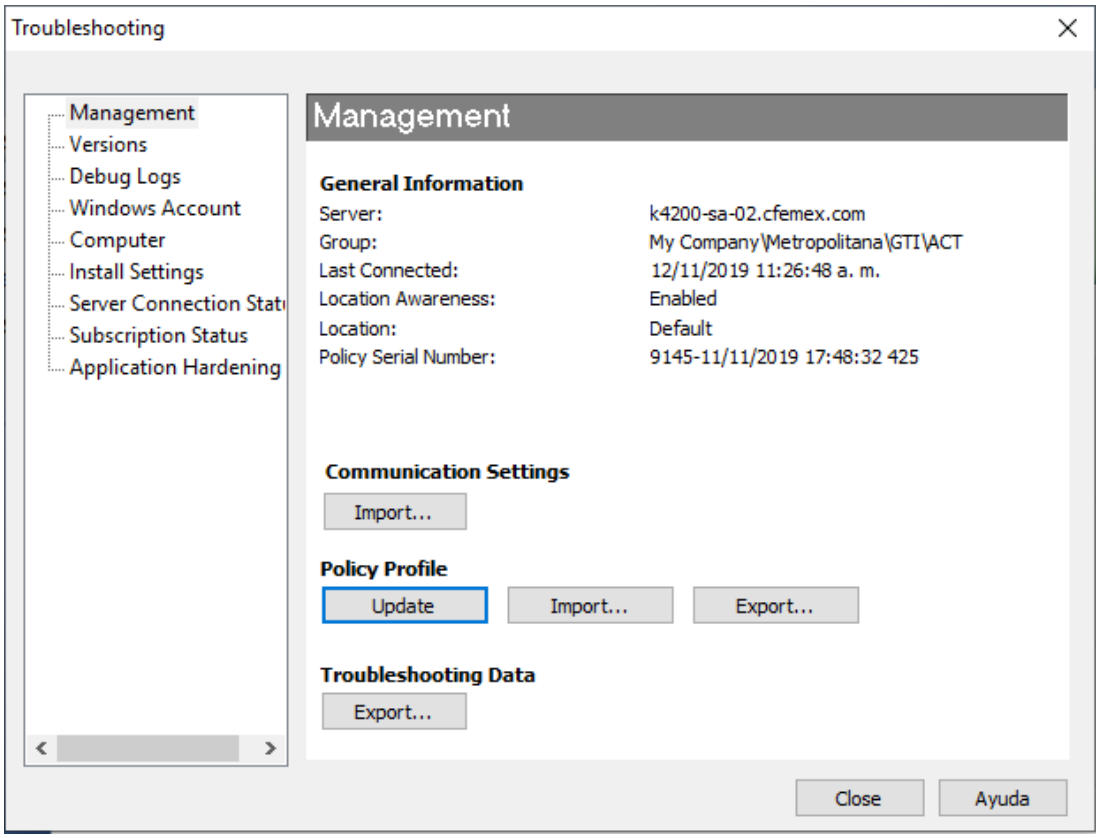
Verificar que el equipo este reportando a la consola de SEP, debe tener un punto verde el icono de SEP en la barra de contexto.



- En caso de no estar reportando a la consola de SEP, realizar las siguientes acciones:
  - Revisar que el equipo no tenga definiciones atrasadas, en caso de tenerlas, hacer la actualización.
  - Se puede hacer descarga manual de actualizaciones bajándolas de la siguiente ubicación ftp://10.55.58.230/Inteligent%20Update/
  - Revisar si alguno de los módulos de protección está en mal funcionamiento, de ser así, será necesario reparar el cliente de antivirus.

Versión de definiciones, deben tener una actualización no mayor a 3 días de retraso.

- En caso de contar con definiciones atrasadas, realizar las siguientes acciones:
  - Actualizar la política para revisar que tenga comunicación con la consola y le sea enviada la actualización.



  - En caso de no actualizar, realizarlo de manera manual.

- Error o mal funcionamiento del antivirus.
  - En caso de que el cliente antivirus no funcione normalmente, realizar las siguientes acciones:
    - Solicitar el paquete de instalación correspondiente y hacer la reinstalación.

- Infección severa de código malicioso.
  - En caso de que el cliente antivirus tenga un problema de infección, realizar las siguientes acciones:
    - Ejecutar la herramienta SymDiag que puede ser descargada de

      ftp://10.55.58.230/Herramientas%20SEP/SymDiag/

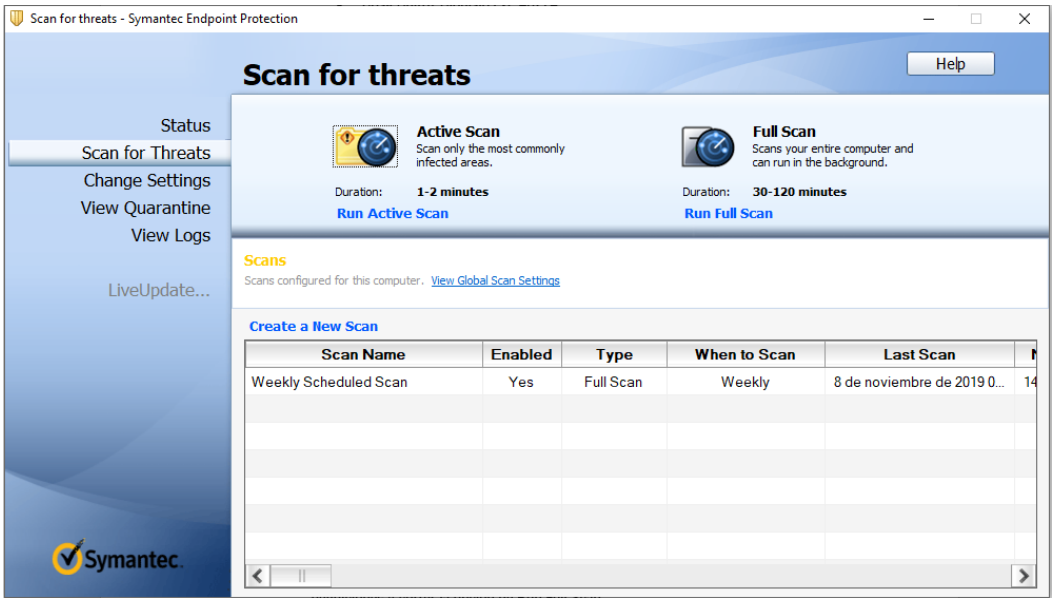
  - Si el código malicioso no es detectado por el cliente de SEP, será necesario solicitar al fabricante la liberación de una firma, actividad que se realiza de manera conjunta con alguno de los siguientes compañeros:

- José Flores Landero ext. 48156
- Rosa Quiroz Dionisio ext. 48274

Proporcionando la siguiente información:

- Medio de infección
- Síntomas del equipo infectado
- Archivo de infección, meterlo en un zip
- Directorio de instalación

- Ultimo escaneo, debe tener al menos un escaneo completo mensual.



- En caso de no haber realizado un escaneo en el periodo recomendado, actualizar las definiciones y correr la opción de Run Full Scan.

6.3.2 ACTUALIZACION DE SISTEMA OPERATIVO Y APLICACIONES

Es necesario ejecutar el servicio de Windows Update y asegurar que se instalen todas las actualizaciones, poniendo especial atención en las actualizaciones de seguridad.

6.3.3 REVISIÓN DE EQUIPO DE CÓMPUTO

- Revisar historial de navegación y de correo recibido en busca de sitios maliciosos visitados recientemente, copiar los enlaces maliciosos si los hay y enviarlos por correo a Mesa de Servicio de la GTI para que se validen y se realice el bloqueo de los mismos en la infraestructura de seguridad perimetral.

- Revisar programas instalados recientemente en busca de programas maliciosos o no deseados, como toolbars. En caso de detectar código no deseado instalado tomar nota de:
    - Nombre de la aplicación
    - Fecha de instalación
    - Ruta de instalación

  Y posteriormente hacer la desinstalación.

- Política de contraseñas
  Validar que el acceso al equipo de cómputo sea a través de usuario y password y que este cuente al menos con las siguientes características de acuerdo a los lineamientos en materia de seguridad de la información de la CFE:
    - Longitud mínima de 12 caracteres
    - Contener al menos un carácter en mayúscula, una minúscula y un carácter no alfabético
    - Vigencia máxima de 3 meses

- Bloqueo de sesión por intentos fallidos en sistemas sustantivos y/o críticos
    - Al tercer intento fallido se deberá bloquear la cuenta del usuario

- Configuración de logs

6.3.4 INGRESO A DIRECTORIO ACTIVO

Para dar cumplimiento al artículo 13 de las políticas generales relativas a las tecnologías de información y comunicaciones de la Comisión Federal de Electricidad y sus empresas productivas subsidiarias y filiales, es necesario que los equipos de cómputo se integren al dominio de servicio de directorio institucional.

7 DIAGRAMA DE FLUJO

NO APLICA

8 MECANISMOS DE CONTROL

Revisión de la atención y seguimiento a notificaciones de equipos con configuración insegura o fuera de cumplimiento, así como la aplicación de la presente guía para ejecutar la remediación correspondiente.

9 FORMATOS

NO APLICA

10 CONTROL DE CAMBIOS

NO APLICA

11 GLOSARIO

NO APLICA

12 LISTA DE DISTRIBUCION

NO APLICA

13 ANEXO (S)

NO APLICA