Política de Seguridad de la Autoridad Independiente de Responsabilidad Fiscal (AIReF).

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 23 de septiembre de 2016 por el Presidente de la Autoridad Independiente de Responsabilidad Fiscal.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Autoridad Independiente de Responsabilidad Fiscal (AIReF) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se -

La Autoridad Independiente de Responsabilidad Fiscal (AIReF) nace con la misión de velar por el estricto cumplimiento de los principios de estabilidad presupuestaria y sostenibilidad financiera recogidos en el artículo 135 de la Constitución Española.
Contacto AIReF:
C/José Abascal, 2, 2º planta. 28003 Madrid. Tel. + 34 91 701 79 90
Email: Info@airef.es.
Web: www.airef.es

adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las Divisiones deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes Divisiones deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC.

Las Divisiones deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo previsto en el art. 7 del ENS.

2.1. PREVENCIÓN

Las Divisiones deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, las Divisiones deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, las Divisiones deben:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el art. 9 del ENS.

La monitorización es especialmente relevante cuando se fijan líneas de defensa de acuerdo con el art. 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Las Divisiones deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, las Divisiones deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de la AIReF y a todos los miembros de la organización, sin excepciones.

4. MISIÓN

La Autoridad Independiente de Responsabilidad Fiscal (AIReF) tiene por objeto velar por la sostenibilidad de las finanzas públicas como vía para asegurar el crecimiento económico y el bienestar de la sociedad española a medio y largo plazo.

Su misión es garantizar el cumplimiento efectivo por las Administraciones Públicas del principio de estabilidad presupuestaria previsto en el art. 135 de la Constitución Española, mediante la evaluación continua del ciclo presupuestario y del endeudamiento público.

La AIReF dispone de un equipo profesional de dilatada experiencia que aspira a cumplir los objetivos encomendados, mediante la publicación de Informes, Opiniones y Estudios de manera periódica en su ámbito de responsabilidad.

El ámbito de actuación de la AIReF impacta en elementos clave de todas las Administraciones Públicas y, por tanto, afecta de lleno las decisiones en torno a las cuentas públicas y a los principales capítulos de gasto e inversión, como Educación, Sanidad y Obra Pública, entre otros. Por ello, la Comunicación se convierte en parte esencial de la actividad de la AIReF.

En numerosos países de nuestro entorno, ya existen o se están creando Instituciones Fiscales Independientes, con la finalidad de disponer de un Organismo independiente que garantice la sostenibilidad de las finanzas públicas.

5. MARCO NORMATIVO

Los hitos legales que han hecho posible la creación de una autoridad fiscal independiente en España comenzaron con la modificación del art. 135 de la Constitución, el 27 de septiembre de 2011, con el objetivo de garantizar el principio de estabilidad presupuestaria, así como la sostenibilidad financiera de nuestro país.

En un segundo paso, una modificación en la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera propició la creación de un Organismo independiente de control fiscal como una de las medidas de garantía del último mandato constitucional. Así, por Ley Orgánica 6/2013, de 14 de noviembre, se creó la Autoridad Independiente de Responsabilidad Fiscal (AIReF), cuya actividad también está regulada en su Estatuto Orgánico, aprobado por Real Decreto 215/2014, de 28 de marzo.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC estará formado por: (i) un representante de la División Jurídico-Institucional; (ii) otro de la División de Análisis Económico; y (iii) otro del Gabinete del Presidente.

El Secretario del Comité de Seguridad TIC será Patricia Flores Cerdán, adscrita a la División Jurídico-Institucional, y tendrá como funciones las siguientes:

- Convocar las reuniones del Comité.

- Elaborar y distribuir las actas.

- Comunicar a la organización las modificaciones sustanciales de la Política de Seguridad.

El Comité de Seguridad TIC reportará al Director de la División Jurídico-Institucional.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Evaluar la aplicación de la Política de Seguridad y, en su caso, los incidentes de seguridad acaecidos desde la última reunión.

- Evaluar los riesgos potenciales.

- Estudiar las nuevas medidas a adoptar en función de nuevas amenazas o cambios en los procesos de trabajo de la institución.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

La información necesaria para el desempeño de la actividad de la AIReF se obtiene de diversas fuentes, entre otras, de la Plataforma de información del Ministerio de Hacienda y Función Pública. También se recibe información directamente de las Entidades Locales y Comunidades Autónomas.

La información es tratada por cada una de las Divisiones, existiendo un responsable por División y un responsable global de toda la información que se almacena el servidor de ficheros de la institución para su posterior uso y elaboración de los informes y estudios.

En los sistemas de información de la AIReF se definen los siguientes roles:

- Responsable de la información: Ignacio Fernández-Huertas.

- Responsable del servicio: Mª Rosario Gálvez Vicente.

- Responsable de la seguridad: Emilio Arribas Peces. Las funciones del responsable de seguridad son las siguientes:

    - Definir las políticas de seguridad de los sistemas de información.
    - Monitorizar la aplicación de las mismas.
    - Revisar semestralmente las políticas.
    - Mantener la interlocución con el Comité de Seguridad, proponiendo actuaciones que se deriven de amenazas para la seguridad y que deban ser canalizadas por el Comité de Seguridad.

En relación con los datos de carácter personal, la Resolución 21/2016, de 19 de septiembre de 2016, del Presidente de la Airef, aprueba el Documento de Seguridad para el desarrollo y cumplimiento de la normativa sobre Protección de Datos.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN.

El Responsable de Seguridad de la Información será nombrado por el Director de la División Jurídico-Institucional, a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Presidente de la AIReF y difundida para que la conozcan todos los afectados.

7. DATOS DE CARÁCTER PERSONAL.

La AIReF trata datos de carácter personal. El Documento de Seguridad, al que tendrán acceso solo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de la AIReF se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Las personas autorizadas para acceder al Documento de Seguridad son las siguientes:

- Fichero de Nóminas: Enrique García Galende, Jefe de Sección del Área de Gerencia de la AIReF. Nivel de seguridad ALTO.

- Fichero de Gestión de recursos Humanos: Francisco Manuel Soriano Llano, Jefe de Servicio del Área de Gerencia de la AIReF. Nivel de seguridad ALTO.

- Fichero de Proveedores y colaboradores: Joaquín Martín Sánchez, Jefe de Servicio del Área de Gerencia de la AIReF. Nivel de seguridad BÁSICO.

- Fichero de suscripción de Newsletters: Mª Rosario Gálvez Vicente, Gerente de la AIReF. Nivel de seguridad BÁSICO.

8. GESTIÓN DE RIESGOS.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año

- Cuando cambie la información manejada

- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la AIReF en diferentes materias:

- Política de Seguridad de los Sistemas de Información de la AIReF, desarrollada por Tragsatec. Se adjunta como Anexo I.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet:

http://intranet.airef.es

10. OBLIGACIONES DEL PERSONAL

Todos los empleados y directivos de la AIReF tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los empleados y directivos de la AIReF atenderán a una sesión de concienciación en materia de seguridad TIC, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la AIReF, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando la AIReF preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando La AIReF utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se prevé en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Será necesaria la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

ANEXO I

Política de Seguridad de los Sistemas de Información de la AIReF

Versión 2016

Índice

Introducción

El presente documento detalla las medidas y políticas de seguridad informática que serán implantadas en las infraestructuras informáticas y por el personal de AIReF, de cara a prevenir infecciones o ataques por programas informáticos malintencionados.

Las medidas preventivas a adoptar se basarán en las siguientes medidas y herramientas:

- Configuración de reglas de protección de acceso específicas en la consola ePO de McAFee para su despliegue en todos los puestos de trabajo de AIReF.
- Configuración de servicios de filtrado de contenidos (CFS), prevención de intrusiones y anti-malware en el firewall NSA 220
- Listas de control de acceso a las estructuras de directorios.
- Restricción de los permisos de administración de los puestos de trabajo.
- Ejecución trimestral de herramientas de detección y limpieza de virus y malware
- Actualización permanente de parches de seguridad y firmas de virus en las bases de datos del antivirus.
- Realización de copias de seguridad de la información disponible.
- Información periódica a los usuarios de AIReF sobre buenas prácticas frente a ataques malintencionados.
- Auditorías de seguridad por empresas externas.

Para el diseño de estas medidas se han tenido en cuenta las recomendaciones del Centro Criptológico Nacional (informes CCN-CERT IA-01/16, CCN-CERT ID-07/16), del Intel Security Group (Protecting against ramsonware) y documentación técnica del Sonicwall CFS suite.

Configuración de reglas en la ePO McAfee

El producto ePO McAfee es una consola de gestión centralizada para el despliegue de productos antivirus y anti-malware. Permite la implantación de políticas de forma centralizada y funcionalidades tales como la programación automática de actualizaciones de firmas de virus y despliegues de políticas.

Con base en las recomendaciones desarrolladas por el Intel Security Group, en su documento "Protecting against ramsonware, revisión H" se ha procedido a implementar políticas de protección de acceso para el producto Viruscan Enterprise, versión 8.8, que es la instalada en AIREF. Como anexo 1 se adjunta este documento.

En esencia, se implantan reglas de protección de acceso de bloqueo de escritura y de ejecución de ficheros que puedan contener códigos malignos del tipo ramsonware, en concreto:

- Cryptolocker v.1, v.2, v.3, v.4
- Cryptowall
- Teslacrypt v.1, v.2, v.3 y v.4
- Locky v.1

Adicionalmente a las reglas anteriores y como medida de protección frente a cualquier tipo de infección se han implantado las siguientes reglas de protección de acceso:

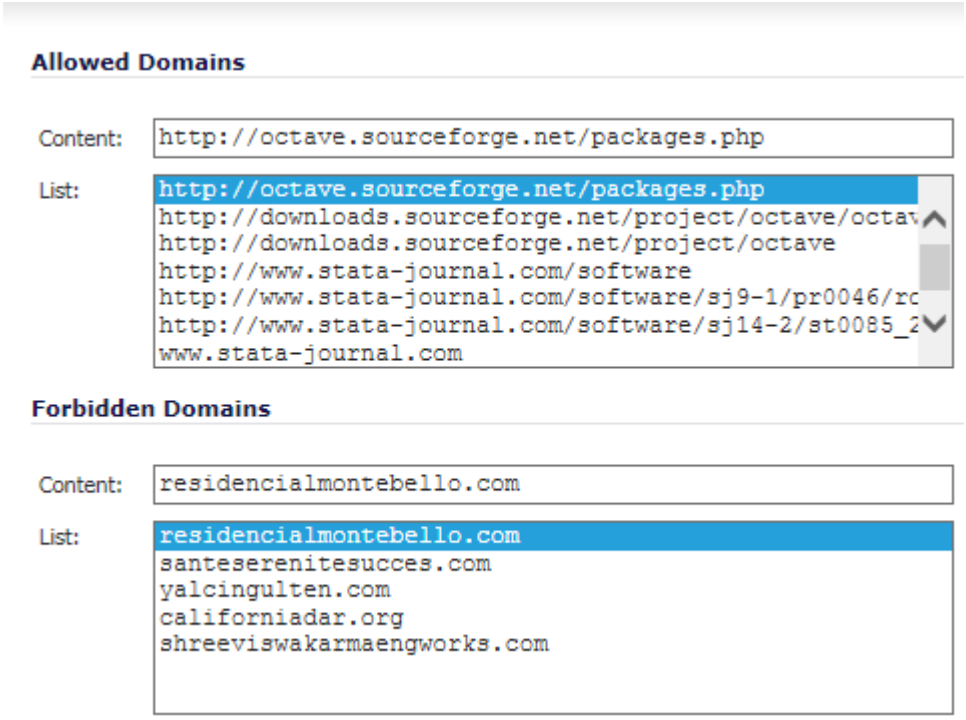
- Imposibilidad de instalar ejecutables fuera de la carpeta de archivos de programa.
- Reglas de protección contra modificaciones de configuración y favoritos de IE.
- Reglas de protección frente a modificaciones de configuración de Mozilla y Firefox.
- Análisis de adjuntos de mails con varias extensiones.
- Creación de una carpeta de trabajo personal (c:\WTRAB) para la generación de árboles de directorios por parte del usuario.

Servicios de seguridad del firewall

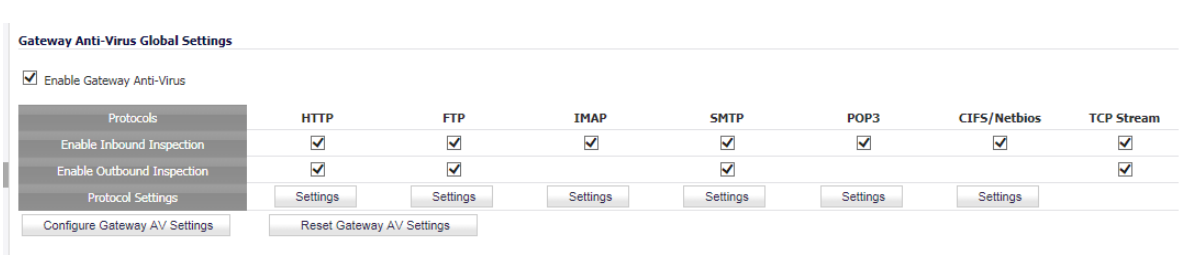
En AIReF se dispone de un firewall Sonicwall NSA 220 que realiza el filtrado de las comunicaciones entrantes y salientes de Internet. Funciona como puerta de enlace para Internet y permite la conexión de las varias VLAN's existentes y de las dos redes wifi desplegadas.

Se han configurado los siguientes servicios de seguridad:

- Políticas de filtrado de contenidos (CFS). Se ha configurado una política en la que se impide el acceso a páginas web clasificadas como peligrosas y se han añadido específicamente páginas de hackers desde las que se pueden lanzar ataques o descargar códigos malignos.



- Antivirus de puertas de enlace. Virus que atacan al firewall directamente.
- Prevención de intrusiones. Ejecución de códigos malignos que aprovechan las vulnerabilidades de



diferentes programas. Se configura protección contra ataques altos y medios para no penalizar el rendimiento del firewall y de la velocidad de internet.

Tragsatec
GrupoTragsa

SEPI

IPS Global Settings

☑ Enable IPS

Signature Groups	Prevent All	Detect All
High Priority Attacks	☑	☑
Medium Priority Attacks	☑	☑
Low Priority Attacks	☐	☐

Configure IPS Settings Reset IPS Settings & Policies

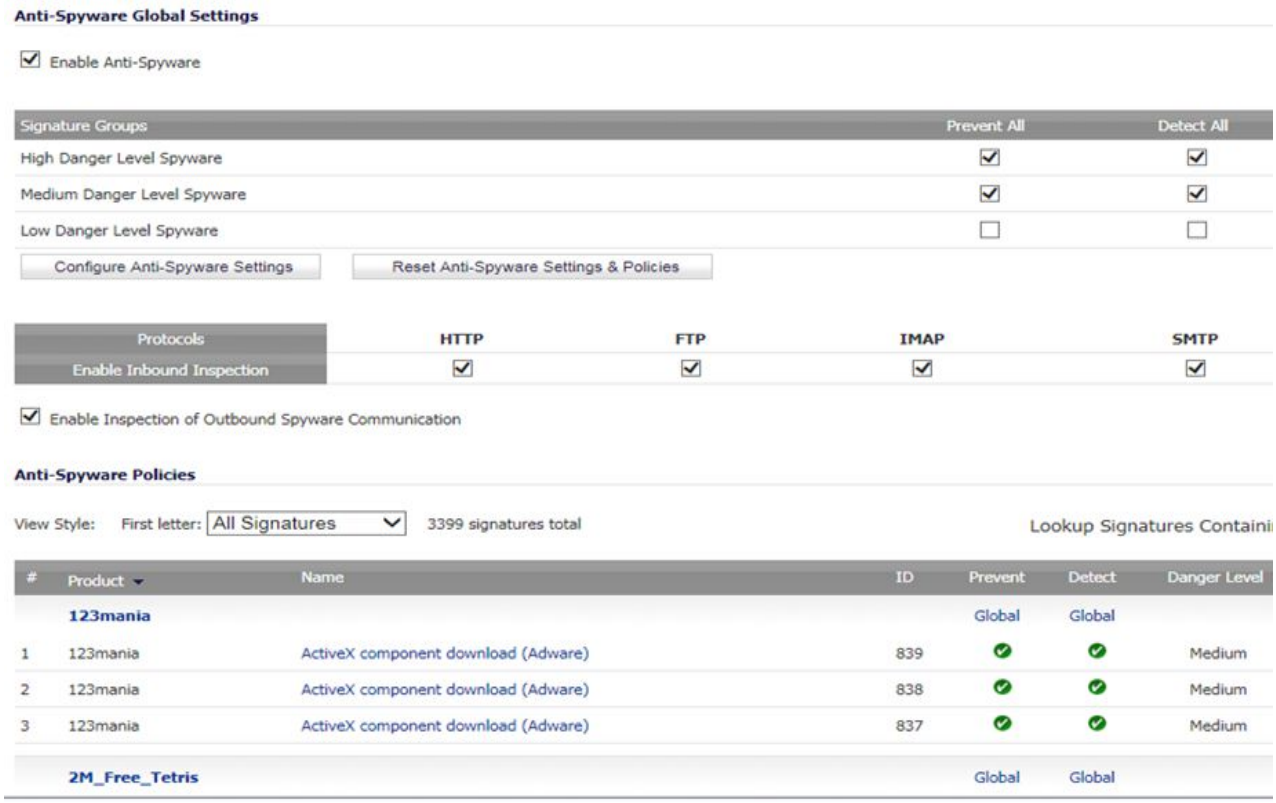
IPS Policies

View Style: Category: All categories Priority: All

#	Category	Prevent	Detect	Comment
	ACTIVEX	Global	Global	
	BACKDOOR	Global	Global	
	BAD-FILES	Global	Global	
	COMPROMISED-CERTS	Global	Global	
	DB-ATTACKS	Global	Global	
	DNS	Global	Global	
	EXPLOIT	Global	Global	
	EXPLOIT-KIT	Global	Global	
	FTP	Global	Global	
	ICMP	Global	Global	
	IMAP	Global	Global	
	INFO	Global	Global	

-

– Protección anti-spyware. Programas que recopilan información de los sistemas para después utilizarla de forma malintencionada.



Anti-Spyware Global Settings

Enable Anti-Spyware

Signature Groups	Prevent All	Detect All
High Danger Level Spyware	☑	☑
Medium Danger Level Spyware	☑	☑
Low Danger Level Spyware	☐	☐

Configure Anti-Spyware Settings | Reset Anti-Spyware Settings & Policies

Protocols	HTTP	FTP	IMAP	SMTP
Enable Inbound Inspection	☑	☑	☑	☑

Enable Inspection of Outbound Spyware Communication

Anti-Spyware Policies

View Style: First letter: All Signatures 3399 signatures total Lookup Signatures Containi

#	Product	Name	ID	Prevent	Detect	Danger Level
	123mania			Global	Global	
1	123mania	ActiveX component download (Adware)	839	✔	✔	Medium
2	123mania	ActiveX component download (Adware)	838	✔	✔	Medium
3	123mania	ActiveX component download (Adware)	837	✔	✔	Medium
	2M_Free_Tetris			Global	Global	

Recomendaciones aplicadas

Listas de control de acceso

En el caso de infecciones por virus de los tipos ramsonware, la infección se propaga a todos los archivos para los que el usuario tiene permisos de acceso/escritura. Esto puede provocar la pérdida de toda la información en el disco duro o en discos de red donde se disponga de acceso.

Para limitar este efecto, en AIReF se han adoptado las siguientes políticas en cuanto a listas de acceso:

- Acceso con permiso de lectura para todos los archivos en el servidor de ficheros.
- Acceso con permisos de lectura y escritura para los usuarios de su respectiva división.
- Acceso con permisos de lectura y escritura para la carpeta Z:\AIREF.

Estas listas podrán tener excepciones por motivos de trabajo entre diferentes Divisiones o en proyectos comunes.

Privilegios de Administrador

Salvo casos muy concretos, ningún usuario podrá instalar software en sus equipos, debiéndose dirigir a un técnico de informática para la instalación de un software adicional a la configuración estándar que pueda necesitar.

Para determinados usuarios, se generará un usuario local con perfil de administrador para realizar pruebas e instalaciones de todo tipo de software en su equipo, de forma que se validen los cambios o la idoneidad de las nuevas instalaciones, sin comprometer al resto de usuarios en red.

Medidas preventivas globales

A un nivel inferior, se aplicarán las siguientes políticas de prevención:

Ejecución trimestral de herramientas de detección y limpieza de virus y malware.

Con periodicidad trimestral, se ejecutarán herramientas de detección y eliminación de virus para garantizar el buen estado de los sistemas.

Para este efecto se utilizará el software Spyhunter versión 4.

Actualización permanente de parches de seguridad y firmas de virus en las bases de datos del antivirus.

Las actualizaciones se harán con diferentes frecuencias en función del software donde se aplican:

- Antivirus: actualización diaria de bases de datos de virus detectados
- Windows: descarga semanal en el servidor de actualizaciones críticas e importantes. Instalación semanal en clientes, previo reinicio del sistema.
- Firewall: Actualización continuada de firmas de código maligno de los servicios de seguridad configurados.

Información periódica a los usuarios de AIReF sobre buenas prácticas frente a ataques malintencionados

De forma periódica y con recordatorios semanales, se realizarán sesiones de formación al personal de AIReF sobre los métodos utilizados por los "hackers" para infectar los equipos y que medidas adoptar en caso de aparecer mails o páginas web sospechosas.

Copias de seguridad

Dado que la aparición de nuevos códigos malignos es continua, es preciso que en cualquier caso, es posible recuperar la información que se haya podido ver afectada.

Para ello, se dispone del paquete Veritas backup con el que se implementa la política de copias de seguridad definida por AIReF.

Se realizan copias totales semanales, copias incrementales diarias y copias totales mensuales, guardando la información por un periodo de 6 meses.

A corto plazo, se procederá a migrar las infraestructuras de AIReF a una nube híbrida, dejando la práctica totalidad del sistema de ficheros en la nube, con lo que las copias de seguridad serán prácticamente online.

En cualquier caso, se dispondrá de una copia asíncrona de la información ubicada en la nube, de forma local, funcionado esta como copia de respaldo.

Medidas reactivas

En el momento en que se produce una infección por virus se comenzarán a infectar los ficheros del equipo y los mapeados en las unidades conectadas, tanto dispositivos físicos (usb's, discos duros externos, etc.) como unidades de red.

En la gran mayoría de situaciones se es consciente de la infección cuando el virus ha finalizado su ejecución y todos los ficheros se han dañado, sin embargo existe la posibilidad de que este aún no haya terminado su ejecución, permitiéndonos recuperar información sobre el virus.

Se recomienda seguir los siguientes pasos generales en el momento de la detección de un virus:

1. **Desconectar las unidades de red**, esto supone "tirar del cable" de red (o desactivar las interfaces inalámbricas). De este modo se podría llegar a evitar la infección de ficheros en unidades de red accesibles, en el caso de que el virus aún no hubiera finalizado su ejecución.

2. **Comprobar si el proceso dañino aún sigue ejecutándose**. Esta tarea no es sencilla en muchos casos ya que el proceso dañino podría haberse inyectado en otro legítimo o simplemente podría haber finalizado su ejecución. Sin embargo, en caso de identificarse el proceso en cuestión (usando herramientas como Process Explorer de Sysinternals), desde el Administrador de Tareas de Windows (Taskmanager) se realizará un dump (volcado de la memoria) del proceso dañino, para ello hay que hacer click derecho sobre el proceso y seleccionar la opción "Crear archivo de volcado" (se guardará en %TMP%). Una vez volcado el fichero hay que guardarlo a buen recaudo en un sistema aislado.

3. **Finalizar la ejecución del proceso dañino.** Para ello existen dos alternativas:

    a. En caso de haberse identificado el proceso simplemente bastará con parar su ejecución desde el Administrador de Tareas de Windows: click derecho sobre el proceso y seleccionar la opción "Finalizar el árbol de procesos".
    b. Si no se ha podido identificar el proceso se recomienda **apagar el equipo de manera manual e inmediata.**

4. **Comunicar el incidente de seguridad a la persona/equipo de informática.**

Buenas prácticas

Las medidas enumeradas anteriormente proporcionan una mayor protección frente infecciones o ataques del tipo de virus encriptadores, que eran los que por su constante evolución y forma de actuar no tenían suficiente protección con las herramientas de seguridad que teníamos instaladas en AIREF.

Estas mayores medidas no eliminan la necesidad de prestar atención frente a situaciones que puedan resultar sospechosas.

Aunque en muchos casos los ataques son cada vez más difíciles y detectar, existe una serie de buenas prácticas que todo el personal de AIReF debería tener en cuenta para evitar nuevas incidencias:

1- Es complicado, porque se hace de manera inconsciente, cuando se hace una búsqueda por Internet, muchas veces los primeros resultados son Anuncios por los cuales pasas antes de llegar a la página oficial, mirarlos bien antes de "clickear" a esos enlaces porque pueden ser una vía de acceso a la propagación del virus.

2– No descargar ficheros ejecutables (.exe, .bat, .bin, .msi, .dat) que no sean de absoluta confianza u origen conocido y confirmado.

3– En el caso de descargar hojas Excel de procedencia no garantizada, **no grabarlos con la extensión que permite la ejecución de macros.**

4- Existen e-mails suplantando a Correos, los hay también de la Agencia Tributaria, Dirección General de La Policia, que llevan archivos adjuntos, incluyendo el virus. No abrirlos NUNCA

http://www.elconfidencial.com/tecnologia/2015-04-16/criptolocker-virus-troyano-espana_760146/