**AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)**

# GUÍA DE CÓDIGO MALICIOSO

**BOGOTÁ D.C. MAYO DE 2021**

# TABLA DE CONTENIDO

## 1. OBJETIVO

Brindar la información detallada de los aspectos relacionados con las herramientas utilizadas para proteger los equipos de cómputo contra posibles infecciones de programas con código malicioso, ataques o pérdida de datos ocasionados por los mismos.

## 2. ALCANCE

Aplica a toda la infraestructura tecnológica de la Agencia para la Reincorporación y la Normalización (ARN).

## 3. DEFINICIONES

- **ANTISPAM:** es lo que se conoce como método para prevenir el "correo basura". Tanto los usuarios finales como los proveedores de servicios de correo electrónico utilizan diversas técnicas contra ello. El principal objetivo de una herramienta antispam, es lograr un buen porcentaje de filtrado de correo no deseado.

- **ANTIVIRUS:** es un programa que ayuda a proteger los equipos de cómputo contra ataques que pueden provenir de: virus, gusanos, troyanos y otros invasores informáticos indeseados:

    - **Virus:** es un software que tiene por objetivo alterar el funcionamiento normal del equipo de cómputo, sin el permiso o el conocimiento del usuario.
    - **Worm o gusano informático:** es un malware que reside en la memoria del equipo de cómputo y se caracteriza por duplicarse, sin la asistencia de un usuario. Provoca alto consumo de banda ancha o memoria del sistema.
    - **Caballo de Troya o Troyano:** este virus se esconde en un programa legítimo que, al ejecutarlo, provoca daño en el equipo de cómputo. Afecta a la seguridad del equipo, dejándolo indefenso, también puede captar datos que envía a otros sitios, como por ejemplo contraseñas.
    - **Bombas lógicas o de tiempo:** se activan tras un hecho puntual, como por ejemplo con la combinación de ciertas teclas o bien en una fecha específica. Si este hecho no se da, el virus permanecerá oculto.
    - **Hoax**: Son mensajes cuyo contenido no es cierto y que incentivan a los usuarios a que los reenvíen a sus contactos. El objetivo de estos falsos

virus es que se sobrecargue el flujo de información mediante el e-mail y las redes.
  - **De enlace:** estos virus cambian las direcciones con las que se accede a los archivos del equipo de cómputo por aquella en la que residen. Lo que ocasiona es la imposibilidad de ubicar los archivos almacenados.
  - **De sobreescritura:** esta clase de virus genera la pérdida del contenido de los archivos a los que ataca. Esto lo logra sobrescribiendo su interior.
  - **Residente:** este virus permanece en la memoria y desde allí espera a que el usuario ejecute algún archivo o programa para poder infectarlo.

- **CÓDIGO MALICIOSO O MALWARE:** Es un programa informático instalado en el equipo de cómputo sin autorización expresa del administrador o del usuario. El código malicioso crea brechas de seguridad para dañar un sistema informático, puede borrar datos o deteriorar el rendimiento del equipo, auto propagarse, espiar las actividades del equipo. Este código se llama "malicioso" porque sus desarrolladores lo usan para molestar, engañar o dañar los equipos de cómputo.

- **SPAM:** correo electrónico no solicitado, correo basura, mensajes no solicitados, de remitente desconocido y que son sumamente molestosos, habitualmente de tipo publicitario, que se envían de forma masiva y aleatoriamente a varios destinatarios. No es una amenaza directa, pero la cantidad correos electrónicos generados y el tiempo que lleva eliminarlos, representa un factor molesto para los usuarios.

## 4. ASPECTOS A TENER EN CUENTA

Tomar las medidas necesarias para proteger la información previniendo, detectando y recuperando, la intrusión de código malicioso en los equipos de cómputo y Servidores.

Concientizar a los usuarios de la Entidad sobre los controles contra código malicioso con que cuenta la Agencia para la Reincorporación y la Normalización, el uso apropiado de los accesos a sistemas de información y el control de cambios de la infraestructura tanto hardware software y de configuración.

¿Cómo actúa un código malicioso?:

- Afecta los sistemas internos del equipo, por ejemplo, borra archivos o baja el rendimiento.

- Usa el equipo como huésped para retransmitir virus y mensajes de correo electrónico no deseados a los contactos por Internet sin previo conocimiento.
- Espía las actividades para robar información personal con el fin de usarla para robar la identidad.

¿Qué debe hacerse para prevenir?:

- Disponer de un antivirus actualizado que ofrezca garantías.
- Tener actualizado todo tipo de sistemas operativos, ofimática y software licenciado, con los que la entidad cuente como Windows, Linux, contar con paquetes de seguridad que solucionan vulnerabilidades.
- Uso de firewall para bloquear el acceso de intrusos a los equipos de cómputo para evitar la propagación de código malicioso a través de la red de la Entidad.

¿Cómo evitar la descarga de código malicioso?

- Instalar un programa que ofrezca protección antivirus y antispam para servidores, equipos de cómputo, portátiles y equipos de red de comunicaciones de la Entidad.
- No abrir correos de desconocidos en particular los archivos adjuntos.
- Desactivar la vista previa, para evitar la ejecución automática de archivos adjuntos con código malicioso.
- Se prohíbe conectar cualquier equipo de cómputo en la red institucional, que no tenga el antivirus instalado y actualizado.
- Los equipos portátiles que se conectan a la red de invitados de la entidad deberán contar con un antivirus, no deben conectarse por ningún motivo a la red institucional.
- Concientizar a los colaboradores a través de campañas de sensibilización sobre los posibles riesgos de los códigos maliciosos y los cuidados a tener frente a estas amenazas.
- Realizar un monitoreo periódico sobre la consola de la solución de antivirus y de acuerdo a los hallazgos encontrados tomar las acciones pertinentes.

## 5. HERRAMIENTAS DE PROTECCION CONTRA CODIGO MALICIOSO

Existen diferentes soluciones tecnológicas desarrolladas para la prevención de código malicioso.

La Agencia para la Reincorporación y la Normalización cuenta con las siguientes herramientas:

## 5.1 HERRAMIENTA DE GESTIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO

**Características**

- Gestión, registro y presentación de informes.
  - ✓ Modos de gestión básica / avanzada.
  - ✓ Por dominio, administración basada en roles Cuentas.
  - ✓ Actividad completa, configuraciones.
  - ✓ Registro de incidentes y cambios.
  - ✓ Informes.
  - ✓ Módulo de informes incorporado.
  - ✓ Cuarentena centralizada.
  - ✓ Implementaciones a gran escala.
  - ✓ Soporte de SNMP mediante soporte estándar.
  - ✓ IB privada con trampas basadas en umbral.
  - ✓ Servidor de almacenamiento local o externo, Incluyendo dispositivos SCSI.
  - ✓ Soporte de Syslog externo.

- Antispam.
  - ✓ Herramienta de inteligencia de amenazas- antispam:
    - Reputación global del remitente.
    - Comprobación de objetos no deseados.
    - Reglas Heurísticas Dinámicas.
  - ✓ Protección contra spam en tiempo real.
  - ✓ URIs de spam y phishing y direcciones de correo electrónico.
  - ✓ Filtrado de URL de categoría completa.
  - ✓ Listas grises para IPv4, direcciones IPv6 y cuentas de correo electrónico.
  - ✓ Reputación del remitente local (basada en IPv4, IPv6 y End Point ID).
  - ✓ Análisis del comportamiento.
  - ✓ Inspección profunda del encabezado de correo electrónico.
  - ✓ Integración con URL de terceros y listas negras en tiempo real (SURBL / RBL).
  - ✓ Detección de boletines.
  - ✓ Escaneo de PDF y análisis de imágenes.
  - ✓ Bloquear listas seguras a nivel global, de dominio y de usuario
  - ✓ Soporte para estándares de identidad de emisor de empresa:
    - Marco de políticas de remitentes (SPF).
    - Claves de dominio identificadas por correo (DKIM).

- Mensaje basado en el dominio.
- ✓ Autenticación (DMARC).
- ✓ Perfiles de acción y notificación flexibles.
- ✓ Cuarentena de autoservicio del sistema y del usuario.

- Alta disponibilidad
  - ✓ En Escenarios de implementación.
  - ✓ Modo activo-pasivo.
  - ✓ Configuración activa-activa.
  - ✓ Modo de sincronización.
  - ✓ Cuarentena y cola de correo sincronización.
  - ✓ Detección y notificación de fallos del dispositivo.
  - ✓ Estado del enlace, conmutación por error y redundante.
  - ✓ Soporte de interfaz.

- Antimalware.
  - ✓ Detección heurística basada en el comportamiento.
  - ✓ Detección de brotes de malware en tiempo real.
  - ✓ Almacenamiento en la nube y en integración.

- Sistema
  - ✓ Amplia gama de opciones de implementación:
  - ✓ Transparente, Gateway y Modo Servidor.
  - ✓ On-prem o público o privado Despliegue de la nube.
  - ✓ Inspección entrante y saliente.
  - ✓ Varios dominios de correo electrónico con dominio.
  - ✓ Personalización de nivel.
  - ✓ Soporte de direcciones IPv6 e IPv4.
  - ✓ Hosting virtual usando fuentes y / o Puertos de direcciones IP de destino.
  - ✓ Soporte de autenticación SMTP a través de LDAP, RADIUS, POP3 e IMAP.
  - ✓ Enrutamiento de correo basado en LDAP.
  - ✓ Inspección por usuario utilizando.
  - ✓ Atributos de LDAP en una política por (Dominio) Bases.
  - ✓ Interfaz de Webmail Completa para implementaciones de modo de servidor y Gestión de la cuarentena.
  - ✓ Gestión de colas de correo.
  - ✓ Soporte de múltiples idiomas para Webmail y la interfaz de administración.
  - ✓ Conformidad RFC de correo electrónico.

## 5.2 PROTECCIÓN INTELIGENTE

La herramienta de gestión de seguridad de correo electrónico impide que el correo electrónico permita la entrega de mensajes anómalos mediante un filtrado de entrada que bloquea mensajes de spam o malware antes de que pueda obstruir su red y afectar a los usuarios. La tecnología de inspección de salida evita otros accesos antispam de la lista negra bloqueando el spam saliente y el malware, incluido el tráfico móvil.

La flexibilidad de la herramienta proporciona enrutamiento de correo electrónico de alto rendimiento mediante la utilización de múltiples filtros de alta precisión. Junto con antivirus y antispyware proporciona seguridad de correo electrónico rápida y precisa que no afecta a los usuarios finales o retraso en las comunicaciones.

## 5.3 PROTECCIÓN AVANZADA CONTRA AMENAZAS

La herramienta de gestión de seguridad de correo electrónico permite identificar y bloquear archivos sospechosos basados en comportamiento no deseado.
La opción basada en la nube proporciona un entorno que permite frustrar amenazas dirigidas y adaptadas.

## 5.4 DESPLIEGUE

Puede elegirse entre tres modos de despliegue: puerta de enlace, transparente o servidor, para cumplir con los requisitos de seguridad de correo electrónico específicos, minimizando los cambios en la infraestructura y las interrupciones del servicio:

### 5.4.1 MODO DE PUERTA DE ENLACE

La herramienta de gestión de seguridad de correo electrónico recibe mensajes, analiza los virus y el correo basura, y envía el correo electrónico a su destino servidor de correo electrónico para la entrega.
Un simple cambio de registro de DNS redirecciona el correo electrónico a la herramienta de gestión de seguridad de correo electrónico para antispam y análisis antivirus.

### 5.4.2 MODO TRANSPARENTE

La herramienta de gestión de seguridad de correo electrónico analiza los virus y el spam, y luego transmite el correo electrónico al servidor de correo electrónico de destino para la entrega. Esto elimina la necesidad de cambiar el registro DNS, o de cambiar el registro existente configuración de la red del servidor de correo electrónico.
Cada interfaz de red incluye un proxy que recibe y envía correos electrónicos. Cada proxy puede interceptar sesiones SMTP, aunque la dirección IP de destino no sea la herramienta de gestión de seguridad de correo electrónico.

### 5.4.3 MODO DE SERVIDOR

La herramienta de gestión de seguridad de correo electrónico escanea el correo electrónico para detectar virus y spam antes de la entrega. En este modo los externos se conectan a dicha herramienta, lo que funciona como un servidor protegido.
La herramienta de gestión de seguridad de correo electrónico actúa como un servidor de mensajería con una funcionalidad completa de servidor de soporte flexible para acceso seguro a POP3, IMAP y WebMail.

## 5.5 HERRAMIENTA DE INTELIGENCIA DE AMENAZAS

Las amenazas cibernéticas y el delito cibernético están en aumento. Los criminales exploran la complejidad de las redes en expansión para robar datos y sistemas de rescate.
La herramienta de inteligencia de amenazas aborda esta situación actualizando y afinando automáticamente sus herramientas de seguridad, con la última Información sobre amenazas a través de los siguientes controles:

### 5.5.1 Aplicación de próxima generación Control y IPS

Control de aplicaciones e intrusión Prevención (IPS) corresponden a la seguridad fundamental para un cortafuego. Se están creando y cargando firmas para desplegar todos los días.

### 5.5.2 Filtrado Web

Protege la Entidad bloqueando el acceso a sitios web maliciosos, hackeados o inapropiados. El filtrado web es la primera línea de defensa contra los ataques basados en web. Los Sitios web maliciosos o hackeados, son un vector primario

para iniciar ataques ya que pueden activar descargas de malware, spyware o contenido de riesgo.

**Características**

- Mejora la seguridad al bloquear el acceso a sitios web maliciosos y riesgosos.
- Evita las descargas de malware de sitios web maliciosos o hackeados.
- Mantiene la defensa actualizada con herramientas de inteligencia automática, análisis de amenazas específicas y actualizaciones continuas.
- Controla el acceso a través de políticas con bloqueo y filtrado altamente granulares.
- Reduce los costos de entrada y mantenimiento a través de licencias basadas en dispositivos.
- Personaliza la implementación con la flexibilidad de las opciones de actualización de push and pull.

### 5.5.3 Antivirus

La herramienta de inteligencia de amenazas ha identificado y neutralizado cerca de 100.000 programas maliciosos programas dirigidos a los servicios tradicionales, móviles, y plataformas TI.

### 5.5.4 Aplicación web Servicio de seguridad

Ofrece actualizaciones totalmente automatizadas para proteger los datos y contenido confidenciales, desde las últimas amenazas de cada de aplicación. Proporciona actualizaciones sobre las últimas vulnerabilidades de aplicaciones, bots, patrones de URL sospechosos, patrones de tipo de datos y motores de detección heurística para habilitar los dispositivos de seguridad.

### 5.5.5 Antispam

El correo electrónico sigue siendo el vector # 1 para el inicio de un ataque avanzado contra la Entidad, el Antispam detecta correo no deseado y malicioso con spam global filtrado, que utiliza la reputación de IP del remitente.

### 5.5.6 Análisis de vulnerabilidades

La exploración de la vulnerabilidad de la herramienta de inteligencia de amenazas ayuda a la solución FortiClient a identificar y gestionar con precisión las vulnerabilidades de software más recientes en dispositivos endpoint. Identifica el sistema operativo y aplicaciones, y descubre vulnerabilidades conocidas en versiones de software que se ejecutan actualmente en los endpoints. También

proporciona una remediación oportuna e inteligencia para ayudarle a remediar sistemas que han sido identificados como vulnerables.

### 5.5.7 Botnet IP y Reputación del dominio

La herramienta de inteligencia de amenazas cada día bloquea aproximadamente 32.000 ataques botnet. Una parte clave de los ataques botnet es que requiere un dispositivo infectado para comunicarse con un servidor de comandos y control, ya sea para descargar amenazas adicionales o para filtrar datos robados.

### 5.5.8 Control de seguridad de base de datos

La herramienta de inteligencia de amenazas ofrece una gestión centralizada y contenido automatizado de las actualizaciones preconfiguradas, políticas que cubren las situaciones conocidas, debilidades de configuración, problemas de SO, riesgos, privilegios de acceso a los datos y mejores prácticas.

### 5.5.9 Servicio de seguridad móvil

El Servicio de Seguridad Móvil cuenta con la capacidad de proteger contra las últimas amenazas dirigidas a dispositivos móviles. Se emplean motores de detección avanzados para amenazas nuevas y cambiantes.

### 5.5.10 Protección avanzada contra amenazas

El servicio de Sandbox utiliza la base de datos antivirus la herramienta de inteligencia de amenazas, con búsquedas de reputación en la comunidad, independientes de la plataforma, la emulación de código y el sandboxing virtual para identificar amenazas de día cero (0-day) y ataques utilizando nuevas tácticas de evasión.

## 5.6 HERRAMIENTAS DE PROTECCIÓN

La Agencia para la Reincorporación y la Normalización cuenta con las herramientas de protección:

- Antivirus
- Antispyware
- Damage cleanup services
- Behavior Monitoring Components
- Suspicious connections
- Browser exploit solution

### 5.6.1 ANTIVIRUS

Servidores de archivos

Protege sus servidores Windows como parte de un completo marco de seguridad para el puesto de trabajo mediante la consolidación de sus puestos de trabajo bajo una infraestructura unificada.

### 5.6.2 ANTISPYWARE

Es una herramienta que ayuda a proteger los equipos de cómputo contra infecciones por código malicioso, cómo los Spyware, Adware o Troyanos.

- Bloquea archivos infectados.
- Protege los datos contra la corrupción y el robo.
- Detiene los archivos de alto riesgo basados en "tipo de archivo verdadero".
- Evita que las amenazas se propaguen entre los usuarios.

### 5.6.3 DAMAGE CLEANUP SERVICES

Limpia los equipos de cómputo de virus y gusanos (troyanos, entradas de registro y archivos virales). Puede activarse DCS antes o después del análisis de virus / malware, dependiendo del tipo de escaneo.

Limpieza estándar: realiza cualquiera de las siguientes acciones:

- Detecta y elimina troyanos vivos.
- Mata los procesos que los troyanos crean.
- Repara los archivos de sistema que los troyanos modifican.
- Elimina archivos y aplicaciones que dejan troyanos.

Limpieza avanzada: además de las acciones de limpieza estándar, detiene las actividades mediante software de seguridad conocido como FakeAV.

### 5.6.4 BEHAVIOR MONITORING COMPONENTS

Cuenta con las siguientes actividades:

- Patrón de detección de supervisión de comportamiento.
- Controlador de supervisión de comportamiento.
- Servicio de supervisión del comportamiento.
- Modelo de configuración de supervisión de comportamiento.
- Modelo de firma digital.

- Patrón de aplicación de políticas.

### 5.6.5 SUSPICIOUS CONNECTIONS

El servicio de conexión sospechosa administra las listas de IP y supervisa el comportamiento de las conexiones que los puntos finales hacen a los servidores. Las listas de IP aprobadas y bloqueadas definidas por la Entidad permiten un mayor control sobre si los extremos pueden acceder a direcciones IP específicas. La lista Global C & C IP funciona junto con el Motor de inspección de contenido de red (NCIE) para detectar conexiones de red con los servidores confirmados por Trend Micro.

### 5.6.6 BROWSER EXPLOIT SOLUTION

La solución Explorador Exploit consta de los siguientes patrones:

- Patrón de prevención de explotación del explorador.
- Patrón del analizador de secuencias de comandos.

## 5.7 HERRAMIENTA DE MONITOREO Y CONSOLA DE EVENTOS DE SEGURIDAD

SEM (Security Event Manager): Una herramienta SIEM que facilita el uso de registros para seguridad, cumplimiento y detección y solución de problemas.

**Eliminación de las amenazas con detección instantánea de actividad sospechosa y respuestas automatizadas con fines de mitigación y cumplimiento.**

El equipo virtual de SIEM proporciona correlación de eventos en la memoria, en tiempo real, respuestas activas, monitoreo de la integridad de los archivos, inteligencia de amenazas y monitoreo de dispositivos USB.

**Aspectos claves**

- Generación de informes de cumplimiento.
- Respuesta activa: Mitigación de las amenazas al instante con acciones automatizadas que bloquean IP, detienen servicios, deshabilitan usuarios y otras acciones.

- Datos de inteligencia de amenazas: Gestión de alertas sobre eventos de seguridad sospechosos a través de una fuente de inteligencia de amenazas que busca coincidencias con hosts incorrectos conocidos.
- Rastreo de eventos maliciosos: Correlación de datos de eventos de miles de fuentes en tiempo real mediante reglas de eventos de SIEM integradas a fin de proporcionar una solución para las amenazas en menos tiempo.

## 5.8 CORRELACIONADOR DE EVENTOS

### 5.8.1 Características

**Contexto operativo en tiempo real para análisis rápido de seguridad**

- Detecta dispositivos y aplicaciones de red no autorizadas y cambios de configuración.
- Realiza análisis de rendimiento del sistema y aplicaciones junto con datos interrelacionados.
- Presenta contexto del usuario, en tiempo real, con pistas de auditoría de direcciones IP, Cambios de identidad de usuario, ubicación física y geográfica.

### 5.8.2 Arquitectura de bases de datos híbridas feeds de datos estructurados y no estructurados

El correlacionador de eventos aprovecha la información estructurada y adecuada para una base de datos relacional, con un enfoque híbrido en el que los datos se almacenan en bases de datos optimizadas con una lógica única completa y una capa de abstracción de base de datos.

### 5.8.3 Integración de alimentación de amenaza a gran escala

Hay muchas fuentes disponibles para exponerse a las posibles amenazas externas en la red. Esta información es muy robusta y puede contener millones de direcciones IP, dominios de malware, hashes y URL, el ciclo de vida de dicha información es muy corto y puede volverse rápidamente obsoleta.

El proveedor ha desarrollado algoritmos propios que permiten que esta gran cantidad de información se obtenga rápidamente de la fuente, y sea distribuida a varios nodos del correlacionador de eventos para ser evaluada en tiempo real.

### 5.8.4 Notificación y gestión de incidentes

- Marco de notificación de incidentes basado en políticas.
- Posibilidad de activar un script de corrección cuando se especifica la ocurrencia del incidente.
- Integración basada en API a sistemas externos.

### 5.8.5 Integraciones de inteligencia de amenazas externas

- API para integrar inteligencia externa de amenazas – Malware. Dominios, direcciones IP, URL, hashes, nodos.
- Integración de información de fuentes de inteligencia de amenazas populares - ThreatStream, CyberArk, SANS, Zeus.
- Tecnología para manejar grandes amenazas – incrementales, coincidencia de patrones en tiempo real con tráfico de red.
- Centro de inteligencia de amenazas vía Beaconing.
- Las instancias del correlacionador de eventos envían incidentes de estado y anónimos al almacenamiento en la nube del servicio.

La correlación cruzada entre varias instancias de correlacionador de eventos identifica las tendencias emergentes y el desarrollo de malware.