NORMA DE METRICOS DE SEGURIDAD PARA LOS SISTEMAS INFORMATICOS DE LA AUTORIDAD DEL CANAL DE PANAMA (IMXI-NO-04-006 / Rev. 04.09.24a)

1. INTRODUCCIÓN

Este documento define los métricos de seguridad informática a implementar en la red informática de la Autoridad del Canal de Panamá (ACP), de acuerdo a solicitud del Director de Informática y Tecnología (IM) hecha a la Oficina de Seguridad de Sistemas de Informática (IMXI). Para cada métrico se ha definido los mecanismos de recolección de datos, fórmula a utilizar y fuente de la información.

IMXI será responsable de coordinar y producir periódicamente los métricos, de acuerdo a la información recolectada de los sistemas informáticos y sus administradores. También deberá actualizar periódicamente este documento para incluir otros métricos que ayuden a determinar la efectividad de los controles y mecanismos de seguridad utilizados en la ACP.

2. METRICOS PARA PROTECCIÓN CONTRA CODIGO MALICIOSO

Se ha seleccionado el sistema informático de protección contra código malicioso para implementar los primeros métricos de seguridad en la ACP. Los métricos se han definido a partir de lo expuesto en documento borrador "Directriz para la Protección de los Recursos Informáticos en la ACP de Ataques por Código Malicioso". Este documento está sujeto a la aprobación de IM para la posterior firma del Administrador de la ACP.

No existe fundamento jurídico en la República de Panamá para la creación de mecanismos que permitan medir la efectividad de controles de seguridad. El Decreto Ejecutivo No. 273 del 27 de diciembre de 2000 "Por el cual se reglamenta el uso de programas de computadora en las entidades estatales" sólo menciona en sus consideraciones "Que el gobierno debe... prevenir virus...". Sin embargo no se definen requisitos específicos para prevenir infecciones por virus.

El Departamento de Operaciones Marítimas (MR) fue certificado bajo la norma de calidad ISO 9001. Este proceso incluyó la definición de la Instrucción de Trabajo SCI-16-002 (Rev. 2) para los administradores de red en donde se detalla la protección antiviral de datos y así mantener la integridad de los mismos. Los métricos definidos en este documento buscan adicionalmente medir el impacto del trabajo definido en el documento SCI-16-002.

Se han definido tres métricos de seguridad para el sistema informático de protección contra código malicioso en la ACP: uno para determinar la actualización del programa antiviral, uno para determinar el grado de

implementación de la detección pro-activa de código malicioso y uno para determinar el número de casos de computadoras infectadas en la ACP.

La información necesaria para elaborar los métricos se puede obtener con relativa facilidad, por medio de los sistemas o administradores de los mismos. Un aspecto que mejoraría considerablemente la recolección de los datos necesarios para al menos dos de los tres métricos sería la implementación del sistema de generación de reportes McAfee ePO. Este sistema también mejoraría la integridad de los datos necesarios. Por estas razones se recomienda la implementación del sistema ePO en el lapso menor de tiempo.

2.1 METRICO: ACTUALIZACION PERIÓDICA DE ARCHIVO DE ACTUALIZACION

Elemento Crítico	Es actualizado y activado el programa de detección y eliminación de código malicioso?
Pregunta Subordinada	Son periódicamente actualizados los archivos de actualización de firma de virus?
Métrico	Porcentaje de sistemas con actualizaciones automáticas de los archivos de definición de virus (dat files) y motores de búsqueda (scan engine)
Propósito	Determinar el grado de protección contra virus informáticos en los sistemas informáticos de la Autoridad del Canal de Panamá
Evidencia de Implementación	1. ¿Mantiene la ACP un inventario actualizado de las computadoras existentes? Sí _____ No _____ 2. Si la respuesta es afirmativa, cuántas computadoras existen en la ACP? _____ 3. ¿Cuántas computadoras utilizan alguna versión del sistema operativo Microsoft Windows? _____ 4. ¿Cuántos sistemas existen en la unidad u oficina bajo tu administración con sistema operativo Microsoft Windows? _____ 5. ¿Cuántos sistemas actualizan periódicamente su archivo de definición de virus? Manual ____ + Automático _____ = _____ (Total)

	6. ¿Con qué frecuencia se actualizan los archivos de definición de virus? - Diaria _____ - Semanal _____ - Bi-semanal _____ - Mensual _____ - Otro _____
Frecuencia	Semi-anual
Fórmula	Número de computadoras con sistema operativo Microsoft Windows y actualizaciones al menos semanal (pregunta No. 6) / Número de computadoras con sistema operativo Microsoft Windows en inventario (pregunta No. 3)
Fuentes de la información	1. Encuesta a la División de Atención al Cliente (IMCD) y administradores de red de distintos departamentos 2. Registros del sistema de administración remota de recursos Microsoft (SMS) 3. Registros de configuración del programa McAfee VirusScan en computadoras (muestra) de la ACP
Indicadores	La actualización periódica del archivo de actualización de firmas permite que los programas contra código malicioso puedan detectar las nuevas amenazas de virus, gusanos y demás problemas similares. La actualización automática con periodicidad menor a una semana garantiza que la búsqueda y limpieza de código malicioso se realice con la base de firma más reciente. Las mejores prácticas de seguridad indican que este métrico debe ser igual a 100%. Si existe una periodicidad mayor a una semana para actualizar el archivo de firmas o es necesaria la intervención manual de un usuario para realizarla, esto aumentaría significativamente el riesgo de que una computadora sea infectada.

2.2 METRICO: BÚSQUEDA AUTOMATICA DE CODIGO MALICIOSO

Elemento Crítico	Es actualizado y activado el programa de detección y eliminación de código malicioso?
Pregunta Subordinada	Se realizan búsquedas automática de código malicioso?
Métrico	Porcentaje de sistemas con búsquedas automáticas de virus en los recursos accedidos desde una computadora.
Propósito	Determinar el grado de protección contra virus informáticos en los sistemas informáticos de la Autoridad del Canal de Panamá.
Evidencia de Implementación	1. ¿Cuántas computadoras utilizan alguna versión del sistema operativo Microsoft Windows? _____ 2. Se realizan búsquedas automáticas de código malicioso en las computadoras con protección contra código malicioso? (colocar número de computadoras que cumplen) Sí _____ + No _____ = Total _____ 3. Si la respuesta es afirmativa, en qué instancias ocurre la búsqueda? - Al conectarse a la red o a un recurso de la misma _____ - Al iniciar la computadora _____ - Al insertar un disquete o dispositivo externo de almacenamiento _____ - Al bajar archivos del Internet _____ - En intervalos de tiempo programados _____
Frecuencia	Semi-anual
Fórmula	Número de computadoras con sistema operativo Microsoft Windows y programa contra código malicioso con búsquedas automáticas (pregunta No. 2) / Número de computadoras con sistema operativo Microsoft Windows en inventario (pregunta No. 1)
Fuente de la información	1. Encuesta a la División de Atención al Cliente (IMCD) y administradores de red de distintos departamentos

	2. Registros de configuración de programa McAfee VirusScan en computadoras (muestra) de la ACP 3. Registros del sistema de generación de reportes para programa anti-viral (McAfee ePO, pendiente de implementación) Se recomienda que la implementación del sistema McAfee ePO se realice antes de iniciar el uso de este métrico. Las otras dos fuentes, encuesta y registros de configuración, pueden producir resultados no confiables o que toman mucho tiempo para desarrollar. Esto es contraproducente ya que pueden producir un sentimiento falso de los mecanismos de protección utilizados.
Indicadores	La configuración de búsqueda automática al acceder algún recurso informático permite que los programas contra código malicioso puedan detectar las nuevas amenazas de virus, gusanos y demás problemas similares. La configuración de búsqueda automática al mayor número de dispositivos y componentes garantiza la protección de los archivos almacenados en la computadora. Las mejores prácticas de seguridad indican que este métrico debe ser igual a 100%. Como mínimo, toda computadora debe mantener activo la búsqueda automática de código malicioso para todo evento en donde se guardan temporal o permanentemente archivos dentro de ella. Es importante mencionar que en una futura versión de este métrico es importante incluir la medición del número de dispositivos que son incluidos en la búsqueda automática y no sólo si una computadora hace uso de esta herramienta.

2.3 METRICO: CASOS DE INFECCIONES POR CODIGO MALICIOSO EN LA ACP

Elemento Crítico	Es actualizado y activado el programa de detección y eliminación de código malicioso?
Pregunta Subordinada	Han ocurrido casos de infecciones en las computadoras de la ACP?
Métrico	Número de casos en que una computadora de la

	Autoridad del Canal de Panamá es infectada por un código malicioso.
Propósito	Determinar el grado de protección contra virus informáticos en los sistemas informáticos de la Autoridad del Canal de Panamá.
Evidencia de Implementación	1. Número de usuarios existentes en la red informática de la ACP o bajo su administración. _____ 2. Ha ocurrido algún incidente de computadora infectada en la red informática bajo su administración? De ser afirmativo, indicar el número de incidentes. _____
Frecuencia	Semi-anual
Fórmula	Número de incidentes de computadoras infectadas por
Fuente de la información	1. Encuesta a la División de Atención al Cliente (IMCD) y administradores de red de distintos departamentos 2. Registros trimestrales del sistema de detección de intrusos (IDS), Unidad de Interconexión de Redes (IMTI). 3. Registros del sistema de generación de reportes para programa anti-viral (McAfee ePO, pendiente de implementación) Se recomienda que la implementación del sistema McAfee ePO se realice antes de iniciar el uso de este métrico. Las otras dos fuentes, encuesta y reporte del IDS, pueden producir resultados incompletos al no poder detectar todos los casos que ocurren en la red de la ACP. Usualmente los usuarios no desean reportar estos casos para que sean identificados como fuente de infección. Esto es negativo ya que puede producir un sentimiento falso de los mecanismos de protección utilizados.
Indicadores	El reporte de incidentes de infección ayuda a determinar los puntos de entrada de código malicioso en la red informática de la ACP. También ayuda a verificar los otros métricos de

	seguridad definidos para código malicioso. Las mejores prácticas de seguridad indican que este métrico debe ser igual a cero (0).

4. BIBLIOGRAFÍA

National Institute of Standards and Technologies. (2003). *Security Metrics Guide for Information Technology Systems* (Special Publication 800-55). Retrieved September 1, 2004, from NIST website: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

National Institute of Standards and Technologies. (2001). *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26). Retrieved September 1, 2004, from NIST website: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

National Institute of Standards and Technologies. (1998). *Guide for Developing Security Plans for Information Technology Systems.* Retrieved September 1, 2004, from NIST website: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

5. HISTORIAL

Revisión	Autor(es)	Descripción
04.09.24a	GMHoward	Documento original