ADMINISTRACIÓN DE PARCHES PARA SISTEMAS INFORMÁTICOS DE LA AUTORIDAD DEL CANAL DE PANAMÁ (IMXI-NO-04-004 / Rev. 04.07.19)

1. OBJETIVOS

1.1 Establecer las bases y mecanismos para corregir vulnerabilidades en el código utilizado por los sistemas informáticos de la ACP.
1.2 Proteger los recursos informáticos de la ACP contra vulnerabilidades existentes y que pueden impactar la operación del Canal.
1.3 Mejorar el rendimiento del código utilizado en los sistemas.

2. INTRODUCCIÓN

Este documento establece las bases para la administración de parches en los sistemas informáticos de la Autoridad del Canal de Panamá (ACP). La Oficina de Seguridad de Sistemas de Informática (IMXI) ha sido asignada por el Director del Departamento de Informática y Tecnología (IM) como la responsable de coordinar la instalación y verificación de los parches en los sistemas de la ACP, trabajando con los distintos grupos de soporte y administración de estos sistemas.

Para realizar la administración de parches, se ha divido el proceso en tres fases: detección, ejecución y verificación. Esta división permite controlar el número de parches a instalar o cambios de configuración que se le pueden solicitar a un administrador, al tiempo que también se establecen los mecanismos para una respuesta ordenada y efectiva que mitigue la vulnerabilidad detectada.

La fase de detección establece la creación de grupos de vigilancia dentro de IMXI, que servirán de monitor ante las nuevas vulnerabilidades que puedan surgir. Estos grupos realizarán un análisis del riesgo e impacto a los sistemas de la ACP para determinar si es necesario o no la instalación de los parches involucrados. Los grupos de vigilancia contarán con el apoyo de especialistas de cada producto para determinar el impacto y la importancia del parche. La suma de todos los grupos de vigilancia y de los especialistas de productos recibirá el nombre de Equipo de Vulnerabilidades y Parches (ACP-EVYPA).

La fase de instalación establece la necesidad de adquirir los parches sólo de fuentes autorizadas, la obligatoria verificación del código adquirido y la correspondiente instalación en sistemas de prueba, antes de pasar a la instalación en los sistemas de producción. Finalmente, la fase de verificación permitirá determinar la correcta aplicación de los parches y consecuente mitigación de la vulnerabilidad detectada.

La creación de un plan de administración de parches responde al elevado número de vulnerabilidades detectadas comúnmente en los sistemas [CERT], la realidad de que todo programa está sujeto al problema de que típicamente se encuentran 1 a 7 defectos por cada 1000 líneas de código [DAVIS] y el hecho de que resulta más barato parchar un sistema o recurso a no hacerlo [INFOSEC]. Esta iniciativa es un elemento más dentro de la estrategia de protección contra código malicioso y ataques a los sistemas de la ACP. Es responsabilidad de todos los involucrados cumplir con los roles asignados para la exitosa protección de los sistemas.

Este documento ha sido desarrollado con información adquirida principalmente de procedimientos y recomendaciones del Instituto Nacional de Normas y Tecnología de los Estados Unidos y de la Organización Internacional de Estándares [NIST01, NIST02, ISO01].

En caso de tener algún comentario o pregunta sobre este documento, favor dirigirse a los teléfonos 272-4630 ó 272-4159 o al correo electrónico cert@pancanal.com.

3. PERFIL INFORMÁTICO DE ACP

La red informática de la ACP está compuesta de una gran variedad de programas o software para apoyar la operación del Canal. Esto hace necesario priorizar cuales programas deben ser verificados continuamente para determinar si requieren la instalación de parches. De esta forma, se utilizan adecuadamente los recursos humanos y tecnológicos que son limitados.

La prioridad de los programas está definida por el impacto que pueda tener sobre la red informática o la operación de la ACP el no instalar los parches. El impacto puede ser clasificado en uno de cuatro niveles: alto, alto-medio, medio y bajo y ha sido basado en [NIST01]:

- El nivel alto posee un costo elevado para la ACP e implica (1) una pérdida tangible de los principales recursos o datos de la Autoridad, incluyendo las medidas de seguridad corporativa; (2) puede significativamente violar, lastimar o impedir la misión, reputación o interés de la Autoridad; o (3) puede resultar en serias lesiones o muertes humanas.
- El nivel alto-medio posee un costo elevado para la ACP e implica (1) una pérdida significativa de las operaciones por medios informáticos, incluyendo la infraestructura que la soporta (2) puede significativamente violar, lastimar o impedir la misión, reputación o interés de la Autoridad; o (3) puede resultar en lesiones humanas.
- El nivel medio posee un costo considerable para la ACP e implica (1) una pérdida de las operaciones por medios informáticos; (2) afecta algún recurso cuyo soporte ha expirado según el fabricante o la ACP; o (3) puede afectar la misión, reputación o interés de la Autoridad.
- El nivel bajo posee un costo pequeño para la ACP e implica (1) una pérdida de algún recurso informático o datos de la Autoridad; o (2) puede afectar la misión, reputación o interés de la Autoridad.

La lista que se presenta a continuación es el resultado de una evaluación de los riesgos encontrados en los últimos años en los productos o programas utilizados por la ACP y de los datos propiedad de la Autoridad que se almacenan en estos productos:

TABLA NO. 1: IMPACTO E UTILIZACIÓN DE SOFTWARE EN LA ACP

Software	Cantidad*	Utilización	Impacto
Microsoft Win2K Server	300	Dominio windows PANCANAL, correo-e corporativo, base de usuarios corporativo, almacenamiento de archivos de unidades/deptos., Compaq Insight Manager, autenticación remota, GIS, SMS	ALTO
Microsoft SQL 2000		Aplicaciones departamentales (MR, IM, FM)	ALTO
McAfee VirusScan 7.1	3000	Protección anti-viral corporativa	ALTO

TABLA NO. 1: IMPACTO E UTILIZACIÓN DE SOFTWARE EN LA ACP			
Software	**Cantidad***	**Utilización**	**Impacto**
Sun Solaris 8	28	Sistema financiero, recursos humanos, DNS, EVTMS	ALTO
Sun Solaris 2.6	9	Sistema financiero, recursos humanos, EVTMS, datawarehouse	ALTO
Oracle 8 y 9i	25	Base de datos para sistema financiero, recursos humanos	ALTO
Oracle 11i	10	Aplicación de sistema financiero, recursos humanos	ALTO
Sun ONE Web Server x.x		Web corporativo	ALTO
Oracle iAS 1.x	1	Licitaciones en línea	ALTO
Cisco PIX (firewall)	2	Protección corporativa	ALTO
Netscreen NS-500-ES	2	Protección a redes EDCS	ALTO
Cisco IOS: routers, switches	100	Infraestructura de red (VLANs)	ALTO - MEDIO
Sun ONE Directory Server	2	Directorio EDCS	ALTO - MEDIO
Microsoft WinNT4 Server (inclye Terminal Edition)	100	Metaframe, DHCP interno, SNA, Ship Data Bank, Planilla, EVTMS	ALTO - MEDIO
Citrix Metaframe 1.8	10	Herramientas (internas) de sistema financiero	ALTO - MEDIO
Microsoft Win2K Professional	2000	Computadoras de escritorio, portables	ALTO – MEDIO
Microsoft WinXP Professional	500	Computadoras de escritorio, portables	ALTO - MEDIO
Microsoft Internet Explorer (5.5 y 6)	3000	Acceso al Internet e aplicaciones web	ALTO - MEDIO
Microsoft Win9x	100	Computadoras de escritorio	MEDIO
Microsoft WinNT4 Workstation	500	Computadoras de escritorio	MEDIO
Microsoft SQL 7		Base de datos departamentales?	MEDIO
Microsoft Office 2000	2500	Documentos de oficina, cliente de correo-e	BAJO
Microsoft Office 2002	500	Documentos de oficina, cliente de correo-e	BAJO

* Cantidades aproximadas

3.1 INCLUSIÓN DE PROGRAMAS

La inclusión de nuevos programas o reemplazo de existentes deberá ser coordinado entre los administradores de los respectivos recursos y la Oficina

de Seguridad de Sistemas de Informática (IMXI). En el caso de recursos o licencias corporativas, la División de Atención al Cliente (IMC) fungirá como administrador y notificará a IMXI. IMC establece las versiones de uso permitido para los programas corporativos en la ACP. Para recursos o licencias departamentales, los Oficiales de Automatización estarán encargados de informar a IMXI.

IMXI deberá revisar esta lista cada seis (6) meses para garantizar la efectividad de la administración de parches en los programas que está siendo utilizados y son críticos para la ACP.

Los programas o software no incluidos en esta lista y que son utilizados en los sistemas informáticos de la ACP, son responsabilidad de sus respectivos administradores. IMXI proveerá soporte a estos recursos por medio de análisis de vulnerabilidades, según lo soliciten los administradores. Se recomienda también que los administradores contacten a los fabricantes de los productos utilizados y establezcan canales de comunicación para recibir actualizaciones de los mismos.

3.2 EXCLUSIÓN DE PROGRAMAS

Debido al historial de fallas de seguridad encontrado en algunos productos, se puede tomar la decisión de excluir algunos productos y recomendar el no uso de los mismos. Al seleccionar programas es importante que el evaluador o quien finalmente administrará el mismo, tome en consideración la madurez en términos de seguridad que haya alcanzado el producto y el hecho de que el producto tenga un periodo de soporte útil según el fabricante. Usualmente, el periodo de soporte debe ser de al menos tres (3) años al momento que lo adquiere la ACP.

Actualmente, estos son los productos que no deben ser utilizados para aplicaciones corporativas en la ACP:

- Microsoft Internet Information Server (IIS) 4.0
- Microsoft Internet Information Server (IIS) 5.0

3.3 PERÍODO DE VIDA Y SOPORTE PARA PROGRAMAS

Todo producto tiene un período de soporte limitado, lo que debe ser considerado al momento de determinar la disponibilidad de parches. A continuación se detallan los períodos típicamente establecidos por los fabricantes utilizados por ACP. Estos valores deben servir de referencia, para cada producto en específico se debe consultar los enlaces web que se ofrecen a continuación:

TABLA No. 2: PERIODO DE VIDA Y SOPORTE TIPICO, SEGÚN FABRICANTE		
Fabricante	**Período(*)**	**Mayor Información**
Microsoft	10 años	http://support.microsoft.com/default.aspx?scid=fh%3Ben-us%3Blifecycle&LN=ES-PA&x=11&y=14 En el caso de Internet Explorer, el período de soporte termina 2 años después de la publicación del siguiente Service Pack (SP) o al final del período de vida del producto, lo que ocurra primero.
Sun	7 años	http://wwws.sun.com/software/solaris/fcc/lifecycle.html Puede ser extendido, previo contrato, por cinco (5) años más desde el momento que salió el producto al mercado.
Cisco	3-4 años	http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin09186a00801a1349.html
Oracle	*¿? años*	*Disponible en Oracle Metalink*
Citrix	2 años	http://www.citrix.com/site/SS/supportThird.asp?slID=5107&tlID=5110

(*) Caso típico, puede variar.

4. NORMA

La administración de parches estará coordinada por IMXI, oficina que debe trabajar con los administradores de los programas incluidos en esta norma para garantizar que los sistemas informáticos de la ACP son actualizados de forma oportuna, diligente y con procedimientos claros.

El proceso de administración de parches puede ser dividido en tres pasos: detección de las alertas, instalación de los parches y verificación de los cambios. La responsabilidad de IMXI será detectar y analizar las alertas de seguridad publicadas por fabricantes de software, determinar que acciones se deben tomar, informar a las unidades correspondientes y verificar la aplicación de las medidas o parches.

IMXI coordinará la instalación de parches con todo el personal responsable de la administración de los programas, según se indica en la Tabla No. 3 de este documento.

4.1 DETECCIÓN

4.1.1 Equipo de Vulnerabilidades y Parches (EVYPA)

IMXI creará grupos de detección o vigilancia dentro de su unidad que servirán de monitor ante las posibles publicaciones de nuevas alertas y el descubrimiento de vulnerabilidades en los productos utilizados por ACP. Utilizando la Tabla No. 1 de este documento y considerando la experiencia de los últimos años en cuanto al número de parches para cada producto, se han identificado cinco (5) grupos: Cisco, McAfee, Microsoft, Oracle y Sun.

Cada uno de los grupos contará con dos personas, una que servirá de punto de contacto y otra que hará de respaldo. Ambas personas serán igualmente responsables de servir de monitor para detectar la publicación de nuevas vulnerabilidades para cada uno de los productos asignados.

Actualmente, estos son los miembros de cada uno de los grupos:

TABLA No. 3: GRUPOS DE VIGILANCIA DE IMXI

Grupo	Principal	Respaldo
Cisco	Gaspar Modelo Howard gmhoward@pancanal.com Ofic. 272-4159 Res. 317-0774	Manuel Varela mvarela@pancanal.com Ofic. 272-4151 Res. 277-4783
McAfee	Eduardo Thomas ethomas@pancanal.com Ofic. 272-4142 Res. 233-0666	Juan Víctor Chong jvchong@pancanal.com Ofic. 272-4131 Res. 230-6864

Microsoft	Manuel Varela mvarela@pancanal.com Ofic. 272-4151 Res. 277-4783	Juan Víctor Chong jvchong@pancanal.com Ofic. 272-4131 Res. 230-6864
Oracle	Juan Víctor Chong jvchong@pancanal.com Ofic. 272-4131 Res. 230-6864	Eduardo Thomas ethomas@pancanal.com Ofic. 272-4142 Res. 233-0666
SUN	Gaspar Modelo Howard gmhoward@pancanal.com Ofic. 272-4159 Res. 317-0774	Eduardo Thomas ethomas@pancanal.com Ofic. 272-4142 Res. 233-0666

Cada grupo tendrá adicionalmente, representantes de las unidades responsables por la administración de los productos y que forman parte del Departamento de Informática y Tecnología (IM). Estos representantes servirán como expertos o especialistas de productos, ayudando a los grupos de vigilancia en la planificación e instalación de parches:

TABLA No. 4: ESPECIALISTAS DE IM, SEGÚN PRODUCTO

Fabricante	Productos	Puntos De Contacto	
		Principal	Respaldo
Cisco	PIX firewall	Howard Phelps	Miriam Gallardo
	routers, switches	Belisario Tejada	Emilio Barria, Pacha
McAfee	VirusScan	Juan Cedeño	Jorge Vergara
Microsoft	sistema operativo y aplicaciones para Servidores	Paolo Angeloni	Angel Sing, Kathy Bermúdez
	sistema operativo y aplicaciones para estaciones de trabajo	Juan Cedeño	Jorge Vergara
Oracle	Base de datos y aplicaciones	Miguel Díaz	José Luis Urriola
SUN	sistema operativo	Miguel Díaz	Jose Luis Urriola
		Leyla Raymondo	Miriam Gallardo
	Servidor web	Leyla Raymondo	

A la suma de los grupos de IMXI y los especialistas de productos se le definirá como el Equipo de Vulnerabilidades y Parches (ACP-EVYPA). El diagrama No. 1 presenta el trabajo entre los grupos de vigilancia de IMXI y los especialistas de productos (en colores), así como el trabajo que debe realizarse con el personal involucrado en la instalación y verificación de los parches con los administradores y proveedores (sin colores):

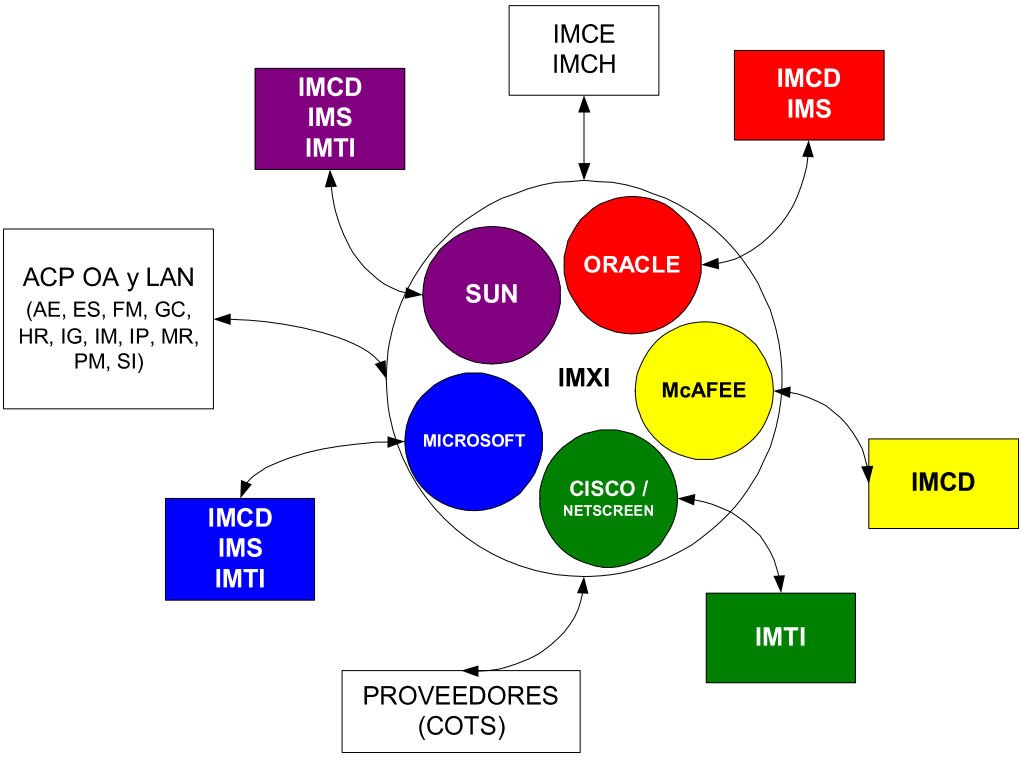


DIAGRAMA No. 1: Interacción para detección, instalación y verificación de parches

IMXI establecerá mecanismos de comunicación con representantes de los cinco fabricantes, lo que permitirá verificar la información sobre nuevas vulnerabilidades y parches para sus productos. Esta comunicación se podrá establecer utilizando los canales existentes dentro de los contratos de mantenimiento con cada uno de ellos. Actualmente, se han establecido los siguientes puntos de contacto para cada fabricante de software:

TABLA No. 5: PUNTO DE CONTACTO, SEGÚN REPRESENTANTE LOCAL

Fabricante	Punto De Contacto Local
Cisco	José Troitiño Cargo Telefono

TABLA No. 5: PUNTO DE CONTACTO, SEGÚN REPRESENTANTE LOCAL	
Fabricante	**Punto De Contacto Local**
	Correo-E
McAfee	Arturo Newland Cargo Telefono Correo-E
Microsoft	Ventura Pérez Cargo Telefono Correo-E
Oracle	¿? Cargo Telefono Correo-E
SUN	¿? Cargo Telefono Correo-E

4.1.2 Suscripción a sistemas de alertas

El principal medio de notificación de nuevas alertas será el Internet, particularmente el correo electrónico. Todo miembro de EVYPA deberá estar suscrito a la lista de seguridad de su respectivo fabricante. Para suscribirse, es necesario visitar el sitio web del fabricante y dar (usualmente) su dirección de correo electrónico. Estas son las direcciones para suscribirse a cada una de las listas:

TABLA No. 6: NOTIFICACIONES DE ALERTAS, POR FABRICANTE	
Fabricante	**Dirección**
Cisco	Enviar un mensaje de correo electrónico a la dirección majordomo@cisco.com. En el cuerpo del mensaje, escribir "subscribe cust-security-announce" sin las comillas. Tomado de http://www.cisco.com/en/US/products/products_security_advisory09186a00801d44a6.shtml#Subscribing

McAfee	http://vil.nai.com/vil/default.asp → presionar "Subscribe to AVERT Virus News" (ubicado al final de la página) Usualmente, McAfee publica cada miércoles las actualizaciones de sus programas anti-virus.
Microsoft	http://www.microsoft.com/technet/security/bulletin/notify.mspx Microsoft publica sus boletines de seguridad cada segundo martes de cada mes.
Oracle	http://profile.oracle.com/jsp/reg/RegisterUser.jsp?src=1376097&Act=4 Requiere primero la creación de una cuenta de usuario y contraseña para acceder el sitio.
SUN	Enviar un mensaje de correo electrónico a la dirección security-alert@sun.com. En el título del mensaje, escribir "subscribe cws your-email-address" sin las comillas y reemplazando your-email-address por tu dirección de correo electrónico. Tomado de http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec

Adicionalmente, los miembros de IMXI deberán suscribirse en al menos una de las siguientes listas:

SANS @RISK: The Consensus Security Alert. Enviado cada lunes por la mañana, @RISK primero resume las tres a ocho vulnerabilidades que mayor impacto tienen mundialmente, indica cuál es el daño que causan y cómo puede protegerse de ellas. Añade una característica adicional: un resumen de las acciones que han tomado 15 organizaciones mundiales para proteger a sus usuarios. Finalmente, @RISK presenta un catálogo completo de todas las vulnerabilidades de seguridad descubiertas durante los últimos siete días. Para suscribirse, favor visitar http://www.sans.org/newsletters/risk/

BUGTRAQ: Lista de seguridad de alto volumen de mensajes en donde se publican de forma voluntaria las vulnerabilidades encontradas. Para suscribirse, favor visitar http://www.securityfocus.com/archive → seleccionar BUQTRAQ.

US-CERT NATIONAL CYBER ALERT SYSTEM: Alertas enviadas por el Equipo de Emergencias Computacionales del Departamento de Seguridad de la Nación (Homeland Security) de los Estados Unidos. Hay dos opciones, las alertas (Cyber Security Alerts) y los boletines (Cyber Security Bulletins). Las alertas están disponibles en formato para usuarios regulares y para usuarios técnico-administrativo. Los boletines son publicados cada quince días y resumen las vulnerabilidades, su impacto, parches así como otras acciones para mitigar el riesgo. Para suscribirse, favor visitar http://www.us-cert.gov/cas/signup.html

Para el grupo de IMXI encargado de vigilar la aparición de nuevos virus, es recomendable suscribirse a otra lista de notificaciones de algún fabricante. Por ejemplo, se puede suscribir a la lista de Trend Micro, cuya suscripción está disponible en http://www.trendmicro.com/subscriptions/default.asp

4.1.3 Clasificación de vulnerabilidades

Toda vulnerabilidad que afecte a un recurso o programa utilizado en la ACP, deberá ser clasificado para ayudar a los administradores a detectar la importancia de instalar el parche correspondiente. La clasificación permitirá también que los administradores identifiquen el tiempo de respuesta necesario para corregir la vulnerabilidad en sus sistemas.

Para clasificar las vulnerabilidades y sus respectivos parches, se utilizará una escala de cuatro niveles basado en [CVA]: crítica, alta, media y baja. El objetivo de esta escala es diferenciar las vulnerabilidades que deben ser corregidas inmediatamente de las que pueden ser programadas dentro de los procedimientos de mantenimiento de los administradores. Es importante recordar que se espera alcanzar un balance entre la seguridad que es necesaria y la continuidad de la operación.

A continuación se detalla los distintos niveles, sobre la base de cuán crítico puede ser una vulnerabilidad para las operaciones y los datos de la ACP:

TABLA No. 7: ESCALA DE VULNERABILIDADES

Nivel De Vulnerabilidad	Tiempo De Respuesta	Descripción
CRITICA	Horas	Vulnerabilidad que afecta una instalación por defecto de un software ampliamente instalado o algún sistema informático de impacto alto en la ACP. La información o código necesario para aprovechar la vulnerabilidad está ampliamente disponible; por ejemplo, es publicado en el Internet. El resultado es acceso administrativo no

TABLA No. 7: ESCALA DE VULNERABILIDADES		
Nivel De Vulnerabilidad	**Tiempo De Respuesta**	**Descripción**
		autorizado de los servidores o equipos de infraestructura. Si el código disponible es de fácil operación, usualmente el atacante no requiere credenciales especiales de autenticación, conocimiento detallado de la configuración de la víctima o realizar ingeniería social.
ALTA	Días	Vulnerabilidad que típicamente tiene el potencial en convertirse de nivel CRITICA, pero tiene uno o más factores que mitigan el riesgo y hace menos atractivo su uso por parte de los atacantes. Por ejemplo, si el código para aprovechar una vulnerabilidad es difícil de ejecutar, el resultado puede ser de un acceso sin privilegios elevados o administrativos o incluso impactar a un grupo pequeño de víctimas. Una vulnerabilidad ALTA que posee una deficiencia sobre el detalle de cómo ejecutarla puede convertirse en una vulnerabilidad CRITICA en cuanto los detalles estén disponibles. Por precaución, se podrán considerar vulnerabilidades ALTAS como CRITICAS para suponer que los atacantes poseen información no pública para realizar el ataque.
MODERADA	Normalmente semanas. Se notificará según caso.	Aplica aquellas vulnerabilidades que no producen un acceso remoto o local administrativo no autorizado, requiere que el atacante esté en la misma red local, afecta configuraciones no por defecto o requiere ingeniería social. Un ejemplo es una vulnerabilidad que produce rechazo de servicio. También incluye aquellos casos en donde se puede mitigar el riesgo por medio de algún control existente. Por ejemplo, la vulnerabilidad de un sistema que reside en la red interna de ACP puede ser controlado

TABLA No. 7: ESCALA DE VULNERABILIDADES		
Nivel De Vulnerabilidad	**Tiempo De Respuesta**	**Descripción**
		por medio de la muralla de fuego o sistema de protección antiviral, impidiendo la amenaza proveniente del Internet.
BAJA	Normalmente meses. Se notificará según caso.	Posee poco impacto sobre la infraestructura o sistemas de la ACP. Este tipo de vulnerabilidad usualmente requiere acceso físico o local al sistema o puede resultar en un problema de privacidad de los datos almacenados o en un ataque tipo rechazo de servicio. También puede incluir una fuga de información referente a la configuración y programas utilizados en sistemas o infraestructura de red.

Es posible que una vulnerabilidad previamente identificada bajo un nivel, suba o baje dependiendo de nueva información adquirida o publicada. Es importante que cada grupo de IMXI, mantenga un verificación constante de la información que está disponible de forma que se mantenga actualizado a los administradores.

En ocasiones puede ser difícil determinar el nivel de una vulnerabilidad, aún con las definiciones de la tabla de arriba. La mejor forma de determinar el nivel, es exponer toda la información al grupo y llegar a un consenso de las partes. El Gerente de IMXI será quién publicará la información, por lo que debe ser consultado para determinar si el nivel seleccionado es el apropiado.

A continuación se listan doce (12) preguntas que pueden ser utilizadas de base para determinar el nivel de una vulnerabilidad. La respuesta a cada pregunta es un sí o no. Cada pregunta posee un puntaje que será sumado en caso de que la respuesta sea sí:

TABLA No. 8: CUESTIONARIO PARA DETERMINAR NIVEL DE VULNERABILIDADES	
Pregunta	**Puntaje (si respuesta es afirmativa)**
1. Afecta a recursos de alto valor (ej. base de datos, planilla, comercio electrónico, operación del Canal)?	1 punto
2. Afecta la infraestructura de red (ej. conmutadores, murallas de fuego, DNS)?	1 punto
3. Afecta a un producto ampliamente instalado en la ACP?	1 punto
4. Afecta instalaciones por defecto de un producto?	1 punto

5. Existe código disponible públicamente que aproveche la vulnerabilidad?	1 punto
6. Está siendo ejecutada ampliamente en el Internet?	0.5 punto
7. La vulnerabilidad se puede acceder remotamente?	0.5 punto
8. La vulnerabilidad se puede acceder sin credenciales?	1 punto
9. Se han publicado detalles técnicos de la vulnerabilidad?	0.5 punto
10. El resultado permite acceso administrativo o con privilegios?	1 punto
11. Se requiere de ingeniería social (ej. visitar un sitio, hacer clic sobre un enlace web) para aprovechar la vulnerabilidad?	0.5 punto
12. Existen registros de auditoria en la ACP que demuestran intentos o ataques utilizando la vulnerabilidad?	1 punto

Si el puntaje final es entre 10 a 7.0 puntos, entonces la vulnerabilidad se puede considerar CRITICA. Si el puntaje es entre 6.0 y 5.0, la vulnerabilidad es ALTA. De 4.0 a 3.0, MODERADA y de 2.0 a 0 es BAJA. Aunque esto no es un sistema científico ni puede ser utilizado como método final para determinar el nivel, sí ayuda a aclarar posibles dudas y conflictos. Es importante recordar nuevamente que la decisión final será tomada entre el grupo responsable y el Gerente de IMXI.

IMXI llevará a cabo reuniones semanales entre todos los grupos de vigilancia y el Gerente con el objetivo de repasar las vulnerabilidades encontradas en los últimos siete (7) días. Cada grupo de vigilancia deberá presentar un resumen de las vulnerabilidades encontradas durante este lapso de tiempo para los productos bajo su responsabilidad. El resumen incluirá el nivel de vulnerabilidad determinado para cada caso por el grupo de vigilancia. Esto permitirá que los otros grupos se informen de las vulnerabilidades encontradas en las otras aplicaciones y productos utilizadas en ACP. Las reuniones se celebrarán todos los lunes a las 8:00AM.

4.2 EJECUCIÓN

4.2.1 Adquisición de los Parches

Los parches deben ser adquiridos de fuentes confiables como por ejemplo, directamente del representante local o del sitio en Internet del fabricante. Es necesario que también se verifique la integridad de los archivos adquiridos. Usualmente, los fabricantes publican un compendio de cada archivo de forma que se pueda verificar la integridad. Típicamente se utiliza el algoritmo Message Digest 5 (MD5) o el sistema Pretty Good Privacy (PGP). Este último, permite verificar no sólo la integridad del archivo sino también la fuente.

IMXI se encargará de bajar los archivos y verificar la integridad de los mismos. Para verificar los compendios MD5, se puede utilizar la herramienta MD5SUMS (disponible en http://www.pc-tools.net/win32/freeware/md5sums). Para verificar los compendios firmados con PGP, se puede utilizar PGP (http://www.pgp.com) o GPG (http://www.gnupg.org).

A continuación se detalla una tabla de los fabricantes y sus respectivas llaves PGP, utilizadas para crear el compendio de los parches y archivos de seguridad publicados:

TABLA No. 9: LLAVES PGP, SEGÚN FABRICANTE

Organización, Responsable	Llave PGP (fingerprint)	Mayor Información
Cisco, Product Security Incident Response (PSIRT)	8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590	http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x32B6B590 http://www.cisco.com/warp/public/707/sec_incident_response.shtml
McAfee, Anti-Virus Emergency Response Team (AVERT)	No tiene	http://vil.nai.com/vil/content/alert.htm http://www.networkassociates.com/us/security/home.asp
Microsoft, Security Notificaton Service	5E39 0633 D6B3 9788 F776 D980 AB7A 9432	http://www.microsoft.com/technet/security/bulletin/notify.mspx
Oracle	No tiene	http://otn.oracle.com/deploy/security/alerts.htm
SUN, Security Coordination Team	1D15 D561 2C8E 4871 E284 E4BD C503 D21E	http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec
US-CERT	7046 C9D4 7F23 3254 A8FC CBE2 5E5B CD47 1024 1560	http://www.us-cert.gov/pgp/encryptmail.html

Todo parche debe ser inspeccionado por un programa antivirus antes de ser publicado en la ACP para su instalación. Se conocen de casos en donde fabricantes, de forma involuntaria, han distribuido parches infectados.

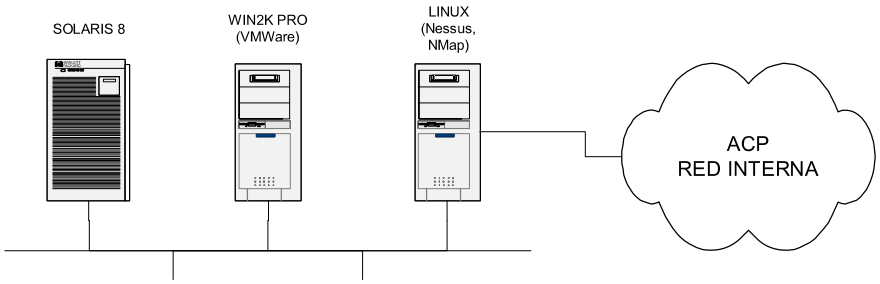
Para verificar el archivo o parche, IMXI utilizará el programa McAfee VirusScan con la última actualización disponible.

El uso de fuentes de confianza para la adquisición de parches, así como la verificación de integridad por medios criptográficos es sumamente importante para evitar trojanos o código malicioso en los parches. Esto es particularmente importante para los sistemas o productos que distribuyen los parches en código fuente. Un ejemplo de esto son los parches distribuidos por la compañía Sun.

4.2.2 Pruebas a Parches o Cambios de Configuración

Todo parche que va a ser instalado en un sistema de producción de la ACP, debe ser instalado primero en un sistema de prueba o desarrollo, según sea el caso. Inicialmente, IMXI deberá realizar estas pruebas en los equipos que tiene asignado para este uso. Si IMXI no posee el equipo necesario, los administradores correspondientes deberán coordinar con el grupo de IMXI para garantizar que se posee suficiente certeza de que el parche corrige la vulnerabilidad detectada y no ocasiona efectos secundarios en el comportamiento del sistema parchado.

IMXI utilizará una red aislada de la red interna de la ACP para realizar las pruebas de instalación de nuevos parches. Esta red contará de una computadora Sun con sistema operativo Solaris 8, una computadora con sistema operativo Windows 2000 Professional y una computadora con sistema operativo Linux.



La computadora con Windows 2000 Professional contará con la aplicación VMWare, lo que servirá para instalar las versiones Windows 2000 Server y Windows XP Profesional. Adicionalmente tendrá instalado la aplicación McAfee VirusScan, que se utilizará para detectar si los parches no están infectados.

La computadora con Linux tendrá instalado herramientas de seguridad (Nessus y Nmap) para realizar las pruebas sobre los parches. Además tendrá dos tarjetas de red, lo que permitirá que sea utilizada para bajar o copiar los parches y herramientas necesarios desde el Internet.

Existen varios productos que no pueden ser probados en el laboratorio de IMXI ya que no se cuenta con el equipo necesario. En estos casos, IMXI deberá coordinar con los especialistas del producto afectado para que se realicen las pruebas del parche sobre los sistemas de desarrollo o pre-producción, según se haya definido previamente.

En los casos que no exista un parche para mitigar una vulnerabilidad publicada o no se conozcan todas las implicaciones de la vulnerabilidad, IMXI podrá esperar para recibir más información o la publicación del parche antes de enviar una alerta al personal responsable de la ACP. Sin embargo y para llegar a esta decisión, IMXI deberá verificar que otras medidas de seguridad están activas. Por ejemplo, podrá solicitar a la Unidad de Interconexión de Redes (IMTI) una tabla actualizada de las reglas de la muralla de fuego o un reporte de la última actualización del programa anti-viral a las estaciones y servidores de ACP.

4.2.3 Creación de alertas

Cada ocasión en que se determine que una vulnerabilidad es crítica o alta, IMXI deberá publicar una alerta o advertencia a todo el personal involucrado en la administración de los sistemas afectados. Este documento debe presentar de forma resumida a los administradores sobre lo que implica la vulnerabilidad y como debe ser mitigada.

La alerta deberá comenzar con un encabezado, que incluye el título de la alerta, los puertos TCP o UDP que son utilizados para aprovechar la vulnerabilidad, el código del documento de acuerdo a la nomenclatura de IMXI, el número de la última revisión y la fecha y hora en que fue actualizada por última vez. Es importante colocar la hora local de Panamá por lo que se utilizará la expresión de referencia al meridiano de Greenwich. Por ejemplo, para una alerta sobre múltiples vulnerabilidades encontradas en el programa Microsoft Outlook Express y que fue actualizado por última vez a las 6:38PM del 20 de abril de 2004, el encabezado sería el siguiente:

> **MULTIPLES VULNERABILIDADES EN OUTLOOK EXPRESS (PUERTOS UDP/135, 137, 138, 445 Y TCP/135, 139, 445 Y 593)**
> **(IMXI-AD-04-058 / Rev. 04.04.20)**
> Actualizado al: 04/20/2004 06:38 p.m. (GMT -05:00)

Toda alerta deberá incluir de forma obligatoria ciertas secciones, para que ofrezcan la información necesaria y respondan las preguntas típicas que se hace un administrador a la hora de informarse sobre una nueva vulnerabilidad:

TABLA No. 10: SECCIONES DE ALERTA

Sección	Tipo	Descripción
Distribución	Obligatorio	Responde a la pregunta: ¿A quién está dirigida esta alerta?

TABLA No. 10: SECCIONES DE ALERTA		
Sección	**Tipo**	**Descripción**
		Se deberá listar a todo el personal de ACP a quienes está dirigido este documento.
Sistemas Vulnerables	Obligatorio	Responde a la pregunta: ¿Qué sistemas son vulnerables? Se debe listar todos los programas o sistemas que están bajo riesgo crítico o alto debido a la vulnerabilidad publicada.
Mitigación	Obligatorio	Responde a la pregunta: ¿Qué debo hacer para mitigar o eliminar la vulnerabilidad? En los casos en que se requiera la instalación de parches, se deberá especificar el sitio exacto de dónde bajarlo. Adicionalmente, se debe detallar de forma individual, el parche para cada uno de los sistemas o programas afectados. Si es necesario instalar un programa o software antes de aplicar la medida o parche, se deberá incluir también en esta sección.
Nombre e Identificador de la Vulnerabilidad	Obligatorio	Responde a la pregunta: ¿Es esta vulnerabilidad similar o distinta a otra que me informaron antes? Usualmente, una misma vulnerabilidad puede recibir distintos nombres, dependiendo de quién la está reportando. Para evitar confusiones es necesario detallar en esta sección el nombre asignado por el fabricante del software. Adicionalmente se debe colocar entre paréntesis, el código asignado a la vulnerabilidad por parte de [CVE].

TABLA No. 10: SECCIONES DE ALERTA		
Sección	**Tipo**	**Descripción**
		Los códigos siguen la nomenclatura [CVE / CAN]-[año]-[no. Secuencial]. Ejemplos de códigos CVE son CAN-2000-0071 y CVE-2001-0500 Para verificar el código CVE con una vulnerabilidad dada, se debe utilizar el índice de vulnerabilidades del NIST [ICAT].
Resumen	Obligatorio	Responde a la pregunta: ¿Qué hace esta vulnerabilidad? Se detalla una pequeña descripción, usualmente no más de seis (6) líneas, de la vulnerabilidad, que componente dentro de la aplicación posee el problema, y el impacto que puede tener sobre la aplicación o las operaciones de la ACP.
Referencias	Opcional	Responde a la pregunta: ¿Dónde puedo encontrar mayor información? Se debe ofrecer al menos dos referencias, una proveniente del fabricante del software utilizado en la ACP y otra de una fuente tercera de confianza como US-CERT.
Mayor Información	Obligatorio	Responde a la pregunta: ¿Cómo contacto a los autores de este documento? En esta sección se debe detallar la dirección de correo electrónico y teléfonos para contactar a IMXI. En los casos de instalación remota de parches o software, como el uso del Microsoft System Management Server (SMS), se debe también incluir los puntos de contacto del mismo.

El documento debe ser conciso y sólo ofrecer la información que es necesaria. Usualmente el documento debe tener entre dos y tres páginas. La información adicional que se puede ofrecer, debe ser indicada por medio de referencias de forma que la audiencia del documento decida si desea utilizarla.

Para los casos de vulnerabilidades de tipo moderada o baja, no será necesario crear una alerta ni informar a los administradores. IMXI podrá esperar a la publicación de grupos de parches para informar a los administradores de la instalación requerida. Por ejemplo, Microsoft publica periódicamente grupos de parches llamados Service Packs que permiten a los administradores actualizar su sistema contra múltiples problemas o vulnerabilidades.

4.2.4 Publicación de Alertas

La publicación de las alertas deberá realizarse utilizando dos medios de comunicación, por medio del correo electrónico y del sitio web interno de la ACP. Adicionalmente, antes de publicar la alerta se deberá notificar por teléfono al menos a uno de los especialistas de IM encargado del producto afectado. En los casos en que se involucra la instalación remota de parches, se deberá también contactar telefónicamente al personal de SMS.

El Centro de Ayuda Técnica (IMCH) debe ser notificado de todas las alertas que sean publicadas por IMXI de forma que pueda dar un soporte a las unidades de ACP que posean los productos afectados. El personal de IMCH deberá entonces estar incluido en las listas de distribución utilizada por IMXI para el envío de alertas por los correos electrónicos.

Para la publicación de la alerta por correo electrónico se debe utilizar las listas de distribución disponibles en el sistema de correo. El mensaje que se enviará a los grupos, deberá ser autorizado previamente por el Gerente de IMXI.

Existen varias listas de interés y que deben ser usados al momento de publicar la alerta:
- 'Distribution OA/LAN': contiene a todos los administradores de red y oficiales de automatización, junto al personal de IM que coordina el trabajo corporativo con estas personas. La lista actualizada de personas que deben formar parte de esta lista se encuentra en la sección 'Automatización de Oficina' de la División de Atención al Cliente (IMC) en el sitio web de la ACP (http://imcd-fsw-01.acp/im/imc/imcs/oa/index.html).
- 'Distribution Lista Soporte IM': contiene todo el personal de soporte informático de cada una de las divisiones y unidades de IM.
- 'Distribution Centro de Ayuda Técnica': contiene todo el personal del Centro de Ayuda Técnica (helpdesk).

IMXI deberá verificar cada seis (6) meses que las listas utilizadas incluyan los cambios de personal ocurridos desde la última actualización.

Para la publicación en el sitio web interno de ACP, el grupo de vigilancia deberá publicar la alerta en la sección de seguridad del producto correspondiente de forma que sirva también de registro histórico de las distintas actualizaciones o parches que requiere el mismo. El sitio también deberá ser actualizado cuando los fabricantes actualicen los parches o publiquen actualizaciones que reemplacen a un grupo de parches. Un ejemplo de esto es cuando Microsoft publica un Service Pack para alguno de sus productos, lo que reemplaza a múltiples parches individuales que se publicaron previamente.

4.2.5 Instalación de parches

La instalación de parches deberá ser realizada por los administradores de cada uno de los programas o equipos afectados, siguiendo las recomendaciones de tiempo establecidas en la alerta y de acuerdo al nivel de la vulnerabilidad (ver Tabla No. 7). La instalación del parche implica usualmente la interrupción del servicio ofrecido por el recurso, por lo que el administrador también deberá programarlo dentro de un lapso de tiempo que impacte de menor forma el servicio, a partir del momento en que el administrador recibe la alerta de IMXI.

4.3 VERIFICACIÓN

El grupo de vigilancia de IMXI deberá verificar la correcta instalación del parche y la consecuente mitigación de la vulnerabilidad. El grupo deberá utilizar los mecanismos necesarios, previa coordinación con los administradores de los productos, para hacer las verificaciones luego de que haya pasado el tiempo establecido para instalar los parches.

El resultado de la verificación deberá ser presentado al gerente de IMXI en forma de reporte, indicando la cantidad de computadoras afectadas por la vulnerabilidad y el número o porcentaje de computadoras que han recibido el parche o cambio de configuración. Adicionalmente, el reporte debe incluir una lista de los equipos y su estado referente a la vulnerabilidad.

5. APÉNDICE A
REGISTRO DE ADMINISTRACIÓN DE PARCHES
IMXI-FO-04-031 / Rev.040719

Nombre de la Vulnerabilidad: _____

_____

Código/número del boletín de seguridad: _____

Código: CVE:_____ BUGTRAQ: _____

Producto(s) o sistema(s) afectado(s): _____

_____

DESCRIPCIÓN	SECCION	RESPONSABLE	FECHA / HORA
Recepción de alerta del fabricante y/o sistema de tercero: CERT, SANS, etc.	4.1.2		
Clasificar vulnerabilidad	4.1.3		
Resultado	☐ Crítica ☐ Alta ☐ Media ☐ Baja		
Si la vulnerabilidad recibe una clasificación crítica o alta, se debe seguir con los siguientes pasos:			
Contactar representante local (opcional)	4.1.2		
Bajar parche(s) del sitio del fabricante	4.2.1		
Verificar integridad del archivo	4.2.1		
Instalación de prueba del parche	4.2.2		
Redactar alerta	4.2.3		
Publicación de alerta	4.2.4		
Correo electrónico			
Infored.acp			
Verificación de la instalación	4.2.5		
Número de sistemas			
Parchados		Porcentaje de Sistemas parchados	
Afectados			

Original: IMXI Copia 1: Autor Copia 2: Carpeta de administración de parches

6. REFERENCIAS

[CERT] CERT/CC Statistics 1998-2003. Disponible en http://www.cert.org/stats/cert_stats.html. Ultimo acceso: Julio 7, 2004.

[CVA] SANS Critical Vulnerability Analysis Archive. Disponible en http://www.sans.org/newsletters/cva/ Ultimo acceso: Julio 2, 2004.

[CVE] Common Vulnerabilities and Exposures Dictionary. Disponible en http://cve.mitre.org Ultimo acceso: Julio 6, 2004.

[DAVIS] N. Davis and J. Mullaney, The Team Software Process in Practice: A Summary of Recent Results, tech. Report CMU/SEI-2003-TR-014, Software Engineering Institute, Carnegie Mellon University, Sept. 2003.

[ICAT] National Institute of Standards and Technology ICAT Metabase. Disponible en http://icat.nist.gov/. Ultimo acceso: Julio 7, 2004.

[INFOSEC] P. Lindstrom. A Patch In Time. Information Security Magazine. February 2004.

[ISO01] ISO/IEC 17799:2000 Information technology - Code of practice for information security management. March 2000.

[NIST01] National Institute of Standards and Technology. Special Publication 800-30: Risk Management Guide for Information Technology Systems. October 2001.

[NIST02] National Institute of Standards and Technology. Special Publication 800-40: Procedures for Handling Security Patches. August 2002.

7. HISTORIAL

Revisión	Autor(es)	Descripción
04.07.19	GMHoward	Borrador con revisión de IMXI