NORMA DE SEGURIDAD PARA AUTENTICACIÓN EN LOS SISTEMAS INFORMATICOS DE LA AUTORIDAD DEL CANAL DE PANAMA (IMXI-NO-04-005 / Rev. 05.01.05)

1. INTRODUCCIÓN

Este documento define los parámetros a seguir para la implementación de mecanismos de autenticación en los sistemas informáticos de la Autoridad del Canal de Panamá (ACP). Esto incluye tanto a sistemas desarrollados internamente como aquellos que son adquiridos por medio de fabricantes o representantes de los mismos. Por consiguiente, este documento está dirigido a personal encargado por el desarrollo o administración de los sistemas informáticos en la ACP.

La autenticación es una de las funciones más importantes a implementar para desarrollar un esquema de seguridad adecuado a las necesidades y riesgos presentes en los sistemas informáticos de la ACP. Es vital que todas aquellas personas involucradas en el diseño, implementación o administración de un sistema informático cumplan con los criterios definidos en esta norma.

La norma de seguridad para autenticación define que todo usuario que acceda algún sistema informático de la ACP lo hará con una cuenta individual, no compartida, con un mecanismo protegido que lo autentique y que este proceso se realice antes de que pueda ejecutar cualquier otra acción en el sistema. Todo sistema debe proteger los datos de autenticación de forma que no puedan ser accedidos por un usuario no autorizado.

Este documento es de carácter obligatorio y alcance corporativo. Excepciones a la norma deben ser evaluadas por la Oficina de Seguridad de Sistemas de Informática (IMXI) y aprobadas por el Director del Departamento de Informática y Tecnología (IM). Las excepciones son de tipo temporal por lo que los responsables de los sistemas deberán tomar las medidas necesarias para corregir estas excepciones.

Esta norma forma parte de las responsabilidades asignadas por el Administrador de la ACP a IM de acuerdo a la Directriz AD-2004-nn sobre el uso de contraseñas en los sistemas informáticos de la ACP.

2. ALCANCE

Esta norma aplica a todos los sistemas informáticos de la ACP, tanto aquellos adquiridos por medio de terceros como los que son desarrollados o utilizados por personal de la Autoridad.

3. DEFINICIONES

3.1 Autenticación: proceso de vincular una identidad a un sujeto en un sistema informático. El sujeto debe proveer información al sistema que le permita confirmar su identidad.

3.2 Carácter: miembro de un conjunto de elementos utilizado para la organización, control y representación de datos. Signo de escritura o de imprenta. Ejemplos son las letras, mayúsculas y minúsculas, números y otros símbolos utilizados en la escritura e imprenta como la arroba (@), porcentaje (%), interrogación (¿?), exclamación (¡!), el punto (.) y la suma (+). A estos últimos símbolos también se les conoce como caracteres especiales.

3.3 Contraseña: Información asociada a un sujeto que confirma su identidad. Ejemplo de un mecanismo de autenticación basado en algo que conoce quien desea o debe autenticarse.

3.4 Cuenta de usuario: nombre asignado a una entidad, por ejemplo persona, para acceder un sistema informático. Usualmente es utilizado con algún mecanismo de autenticación en sistemas múlti-usuarios.

3.5 Frase secreta: versión más larga de una contraseña. Una frase secreta está típicamente compuesta de varias palabras y puede incluir espacios o cualquier otro caracter especial.

3.6 Sistema informático: arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas. Esto incluye, pero no se limita a estaciones de trabajo, periféricos, servidores, aplicaciones, bases de datos, equipo de comunicaciones, redes, equipos industriales o cualquier combinación de ellos que se pueda realizar.

4. NORMA

4.1 Autenticación

4.1.1 Todo sistema o aplicación informática que lo permita, deberá desplegar una notificación o mensaje previo a la autenticación del usuario. Este mensaje contendrá el siguiente texto:

4.1.1.1 Este sistema sólo debe ser utilizado por personal autorizado por la Autoridad del Canal de Panamá (ACP). Toda la actividad en el sistema podrá ser registrada y cualquier violación a las directrices, normas y procedimientos de la ACP podrá producir acciones disciplinarias, civiles o penales por parte de la ACP o de las autoridades competentes de la República de Panamá.

4.1.2 Todo sistema informático debe estar configurado para no ofrecer acceso antes que un usuario se haya autenticado exitosamente. Adicionalmente, el sistema sólo podrá enviar información que le permita al usuario identificarlo, antes de que este último se

autentique. Información que no se podrá enviar antes de la autenticación incluye el nombre del departamento o personal que administra el recurso, nombre o versión del sistema operativo o aplicación utilizada, parches aplicados o configuración de red.

4.1.3 Todo sistema debe limitar el número de intentos de autenticación entre un mínimo de tres (3) intentos y máximo de cinco (5). Si se alcanza el máximo de intentos configurados, la cuenta utilizada será bloqueada automáticamente por un periodo de quince (15) minutos como mínimo.

4.1.4 Todo sistema informático deberá suspender una sesión luego de quince (15) minutos de inactividad. El re-establecimiento de la sesión requerirá que el usuario se autentique nuevamente.

4.1.5 El acceso inicial a los sistemas sólo se realizará por medio de cuentas individuales que demuestren claramente la identidad del usuario. Se podrán utilizar cuentas administrativas compartidas sólo luego de que el usuario se autentique inequívocamente. Un ejemplo de tales cuentas administrativas es el caso de la cuenta 'root' en los sistemas Unix.

4.1.6 Todo colaborador de la ACP que realice operaciones administrativas en los sistemas informáticos y requiera una cuenta regular en estos sistemas, deberá utilizar una cuenta regular distinta a su cuenta administrativa para realizar estas actividades.

4.1.7 Cada usuario es responsable por el uso que se le da a la cuenta asignada.

4.1.8 Deberá existir una cuenta por cada usuario del sistema. El caso de cuentas compartidas entre varios usuarios sólo podrá ser autorizado por el Director de Informática y Tecnología.

4.1.9 Las cuentas otorgadas a usuarios que no son empleados de la ACP deberán contar con una fecha de expiración antes de ser habilitadas.

4.1.10 La información utilizada para autenticación, almacenada y transmitida por la red informática deberá ser cifrada y sólo con mecanismos de criptografía fuerte. Criptografía fuerte se refiere a la utilización de métodos difíciles de abatir según las mejores prácticas públicamente conocidas.

4.1.11 La información que utiliza un usuario para autenticarse puede provenir de las siguientes fuentes: (a) lo que el usuario sabe como por ejemplo una contraseña, (b) lo que el usuario tiene como por ejemplo una tarjeta, "token" o credencial, (c) lo que el usuario es como por ejemplo las características de la retina o huellas dactilares, y (d) donde el usuario está como por ejemplo si se encuentra en su oficina. Las secciones 4.2, 4.3 y 4.4 definen requisitos adicionales para cada uno de estos casos.

4.2 Contraseñas

Las contraseñas son el principal mecanismo de autenticación utilizado en la ACP. Una contraseña puede ser la causa de que todo un sistema corporativo sea comprometido. Por esta razón, todo usuario regular y administrativo debe implementar al menos las medidas definidas en esta sección para los sistemas que utilicen contraseñas como mecanismo de autenticación.

Las cuentas de usuarios administrativos son las utilizadas para la administración del sistema informático, servidor o de la aplicación en cuestión. Las cuentas regulares son las utilizadas por los usuarios regulares del sistema para una función específica designada.

4.2.1 Cada usuario de la red informática de la ACP es responsable de proteger su contraseña y de no compartirla.

4.2.2 Las contraseñas deben estar compuestas de al menos un carácter especial y dos de los siguientes tres grupos: mayúsculas, minúsculas y números. Se prohíbe el uso de contraseñas en blanco.

4.2.3 Las cuentas de usuarios regulares deberán tener una longitud mínima de ocho (8) caracteres y las cuentas administrativas una longitud mínima de diez (10) caracteres.

4.2.4 En los sistemas que lo permitan, se recomienda utilizar frases secretas en lugar de contraseñas. Todas las reglas definidas en esta norma y que aplican para una contraseña también aplican para una frase secreta.

4.2.5 Las cuentas de usuarios regulares deben cambiar sus contraseñas al menos cada noventa (90) días y las de usuarios administrativos deben cambiar las contraseñas al menos cada sesenta (60) días. En aquellos sistemas que sólo se pueda definir un periodo de validez para las contraseñas, se seleccionará noventa días.

4.2.6 Los usuarios no deberán almacenar las contraseñas en archivos o documentos que puedan ser accedidos por personas no autorizadas y que no hayan sido cifrados.

4.2.7 Se prohíbe el uso de la función de almacenar o recordar contraseñas que puedan tener las aplicaciones utilizadas por el usuario.

4.2.8 Al crear una cuenta de usuario, la contraseña sólo podrá ser transmitidas por medios no públicos como teléfono, fax o en persona. No debe ser transmitida por medio de la red informática, especialmente correo electrónico, a menos que sea enviada de forma cifrada. El usuario deberá cambiar la contraseña inmediatamente entre al sistema luego de recibir la contraseña por parte del administrador.

4.2.9 Los siguientes criterios aplican específicamente a los mecanismos de autenticación implementados en sistemas operativos Microsoft Windows. Esto aplica para servidores y estaciones de trabajo que pertenezcan al dominio corporativo

PANCANAL, algún otro dominio departamental o que no formen parte de ningún dominio:

4.2.9.1 Configurar el "Account Policies" de acuerdo a los criterios establecidos en esta norma, tanto el "Password Policy" como el "Account Lockout Policy". Las contraseñas no deberán ser almacenadas utilizando el algoritmo de cifrado reversible que permiten los sistemas.

4.2.9.2 Dentro de las opciones de seguridad del "Local Policies" se deberán configurar los siguientes parámetros:

- Additional Restrictions for Anonymous Connections: "Do Not Allow Enumeratin of SAM Accounts and Zares"
- Digital Sign Client Communication: "When Posible" (al menos) o "Always"
- Digital Sign Server Communication: "When Posible" (al menos) o "Always"
- LAN Manager Authentication Level: "Send NTLMv2 response only" (al menos) o "Send NTLMv2 Response Only\Refuse LM & NTLM
- Prevent System Maintenance of Computer Account Password: "Disabled"
- Prompt User to Change Password Before Expiration: 14 days
- Send Unencrypted Password to Connect to Third-Party SMB Servers: "Disabled"

4.2.10 Los siguientes criterios aplican específicamente a los mecanismos de autenticación implementados en sistemas operativos Sun Solaris versiones 2.6, 8 y 9:

4.2.10.1 Remover las cuentas del sistema que no sean necesarias. Para remover estas cuentas, es necesario hacer lo siguiente:

```
for user in smtp listen nobody4 ; do
/usr/bin/passmgmt -d $user
done
```

4.2.10.2 Asignar el grupo del usuario 'root' al número 0 para prevenir que este usuario comparta un grupo con usuarios sin privilegios.
Para cambiar el grupo de 'root' a 0, se debe ejecutar el siguiente comando desde una consola (shell):

```
/usr/bin/passmgmt -m -g 0 root
```

4.2.10.3 Configurar el servicio Solstice AdminSuite (sadmind) para que utilice el tipo de autenticación a STRONG, si el servicio requiere ser utilizado. Por defecto, este servicio no es necesario.

Para asignar el mecanismo de autenticación del servicio sadmind a STRONG se debe editar el archivo /etc/inetd.conf y añadir la opcion -S 2 a la línea de sadmind:

```
100232/10   tli   rpc/udp wait root /usr/sbin/\
sadmind
sadmind -S 2
```

4.2.11 Los siguientes criterios aplican específicamente a los mecanismos de autenticación implementados en base de datos:

4.2.11.1 Las cuentas de usuario y contraseñas deben ser almacenadas en un archivo independiente del programa o aplicación.

4.2.11.2 Los credenciales pueden ser almacenados en el mismo servidor donde reside la base de datos o de forma separada en un servidor de autenticación. En el último caso, deberá utilizarse un algún servidor de autenticación existente en la red de la ACP como Microsoft Active Directory, RADIUS o LDAP (Lightweight Directory Access Protocol).

4.3 Sistemas Biométricos

4.3.1 Cumplir con la norma FIPS 140-2 de Requisitos de Seguridad para Módulos Criptográficos, nivel 2 o superior. En casos previamente aprobados por IM se podrá adquirir productos bajo la norma FIPS 140-1.

4.3.2 Uso de algoritmos simétricos, al menos 3DES (Triple Data Encryption Standard) y de ser posible AES (Advanced Encryption Standard). Para 3DES se permite el uso de dos o tres llaves de 56 bits cada una. Para AES la longitud de la llave es de 128 bits o superior.

4.3.3 Datos biométricos deben permanecer cifrados mientras sean almacenados.

4.3.4 Permisos de las carpetas o directorios de la aplicación biométrica. Acceso solo debe ser permitido a los procesos del sistema biométrico.

4.3.5 La razón de aceptación falsa (FAR, false acceptance rate) debe ser de 1 en 100,000 o menor.

4.3.6 La razón de rechazo falso (FRR, false rejection rate) debe ser de 5 en 100 o menor.

4.3.7 Cualquier sistema de biometría utilizado en la ACP no debe ser el único mecanismo de control de acceso a un sistema. El sistema biométrico debe ser parte de una solución de autenticación de al menos dos factores.

4.3.8 Planes de contingencia para cuando el sistema biométrico no esté disponible. Esto debe incluir los procedimientos y requisitos para operar el sistema de autenticación sin el sistema biométrico.

4.4 Dispositivo de autenticación: "Tokens" y Tarjetas Inteligentes

4.4.1 Cumplir con la norma FIPS 140-2 de Requisitos de Seguridad para Módulos Criptográficos, nivel 2 o superior. En casos previamente aprobados por IM se podrá adquirir productos bajo la norma FIPS 140-1.

4.4.2 En los casos de uso de tarjetas inteligentes, estas deberán cumplir con la norma ISO 7816-3 y 4.

4.4.3 El controlador criptográfico debe permitir al menos del uso de los siguientes algoritmos de cifrado simétrico: 3DES (Triple Data Encryption Standard) y de ser posible AES (Advanced Encryption Standard). Para 3DES se permite el uso de dos o tres llaves de 56 bits cada una. Para AES la longitud de la llave es de 128 bits o superior.

4.4.4 El controlador criptográfico debe permitir al menos del uso de los siguientes algoritmos de cifrado asimétrico: RSA (como se especifica en norma ANSI X9.31) y DSA (Digital Signature Algorithm).

4.4.5 El controlador criptográfico debe permitir al menos del uso de las siguientes funciones de compendio: MD5 (de acuerdo al documento RFC1321) y SHA-1 (de acuerdo a la norma FIPS PUB 180-1).

4.4.6 El token debe permitir la implementación de al menos las siguientes normas de interfase: PKCS#11 (según la norma de los Laboratorios RSA) y PC/SC (según el grupo de trabajo Personal Computer/SmartCard).

4.5 Administración

4.5.1. La asignación inicial o cambio de contraseña de las cuentas de usuario sólo podrá ser realizada por los administradores o personal designado para dichas tareas. Tal es el caso de: el Centro de Ayuda Técnica (IMCH), IMXI, los administradores de redes de área local, coordinadores de automatización de oficina departamentales u otros grupos que sean responsables del control de acceso de sistemas informáticos o aplicaciones en la ACP.

4.5.2. Los dueños de los sistemas informáticos, previa aprobación del Departamento de Informática y Tecnología, designarán a los administradores de los sistemas.

4.5.3. Los administradores o responsables del control de acceso, deberán elaborar e implementar los procedimientos que regulen la administración de las contraseñas en los sistemas informáticos bajo su responsabilidad. Estos procedimientos deberán incluir en detalle, el proceso de solicitud, los requisitos, acciones a realizar, responsabilidades, coordinación y cualquier otro aspecto relativo a la administración de las contraseñas.

4.5.4. Inhabilitación de cuentas. Las cuentas podrán ser inhabilitadas y/ reactivadas solamente por los administradores asignados de los sistemas.

4.5.4.1. Cuentas de usuarios que no laboran en ACP. La Oficina de Seguridad de Sistemas de Informática generará mensualmente, el Informe de Terminaciones, el cual contendrá un listado de colaboradores que han dejado de laborar recientemente en la ACP. Este informe será obtenido del sistema de recursos humanos y se distribuirá a los administradores responsables de los sistemas informáticos. Los administradores deberán inhabilitar (eliminar, remover, desactivar) las cuentas de los colaboradores que se encuentren listadas en dicho informe, en un lapso no mayor a 15 días, y guardarán las acciones realizadas para futuras auditorías o referencia.

4.5.4.2. Cuentas de usuarios regulares. Se deberán desactivar aquellas cuentas que no presentan actividad o de usuarios que se ausentarán por un periodo de 90 días o más. En el caso de usuarios con ausencias de 90 días o más, las oficiales administrativas informarán de dicha ausencia a los administradores respectivos para gestionar la inhabilitación de los accesos. Los usuarios que soliciten la inhabilitación voluntaria de sus cuentas por cualquier motivo, deberán contar con la aprobación de su supervisor. La reactivación de las cuentas se realizará una vez el usuario retorne a sus funciones o posición.

4.5.4.3. Cuentas de usuarios con funciones administrativas. Las cuentas de usuarios administrativos deberán ser inhabilitadas en el caso de ausencia en su puesto por 7 días o más, y se reactivarán una vez retorne a su puesto.

4.5.5. La ausencia permanente de un colaborador con funciones administrativas en al menos un servidor informático, requerirá el cambio de todas las contraseñas de cuentas administrativas a las que tenía acceso el administrador.

4.6 Seguridad Física

La seguridad física es un factor importante para garantizar que los recursos informáticos sean protegidos contra alteraciones no autorizadas, robo, fuego, inundaciones y fallas eléctricas. Los servidores y estaciones de trabajo que almacenen información utilizada para autenticar a los usuarios deben ser protegidos contra estos riesgos.

4.6.1 Los sistemas informáticos utilizados para operaciones corporativas deberán residir en el Centro de Datos de la ACP o en instalaciones con seguridad física similar.

4.6.2 Los sistemas informáticos utilizados para operaciones departamentales deberán tomar las siguientes medidas:

4.6.2.1 Colocar el o los servidores en una habitación o mueble que requiera el uso de llave y bajo el acceso controlado de los administradores del servidor. De ser posible el

acceso puede ser controlado por medios electrónicos. El techo, piso y ventanas que posea la habitación no debe permitir el acceso no controlado.

4.6.2.2 Igual medida de protección física debe ser aplicado a las unidades y cintas de respaldo. Se debe coordinar el almacenamiento de los respaldos en otra área distinta a la ubicación de los servidores. De ser posible, el área de almacenamiento de los respaldos debe ser a prueba de desastres como incendios e inundaciones.

4.7 Desarrollo de Aplicaciones

4.7.1 Las aplicaciones desarrolladas por la ACP deberán contener las siguientes capacidades o funciones:

4.7.1.1 Permitir la autenticación de usuarios individuales, no por grupos.

4.7.1.2 No se debe almacenar contraseñas sin cifrar o utilizando un algoritmo que sea fácilmente reversible sin el conocimiento de un secreto.

4.7.1.3 Proveer un mecanismo de administración de roles, de forma que un usuario pueda reemplazar a otro usuario y realizar su trabajo sin necesidad de conocer la contraseña del otro.

4.7.1.4 En los casos que sea posible, utilizar algún servidor de autenticación existente en la red de la ACP como Microsoft Active Directory, RADIUS o LDAP (Lightweight Directory Access Protocol).

4.7.2 El equipo de desarrollo deberá informar a IMXI sobre el diseño de una nueva aplicación para que esta oficina realice una evaluación del mecanismo de autenticación a utilizar y formule recomendaciones del mismo. El equipo de desarrollo deberá realizar esta gestión lo antes posible, preferiblemente en la fase de diseño de la aplicación.

4.8 Excepciones

4.8.1 Toda excepción a la norma debe ser notificada por escrito a la Oficina de Seguridad de Sistemas de Informática antes de que el mecanismo de autenticación sea implementado en un sistema informático de la ACP. Se utilizará el formulario IMXI-FO-04-032 para estos casos. En caso de sistemas existentes que no puedan cumplir con la norma, IMXI deberá hacer las recomendaciones necesarias para que sean incluidas en la siguiente actualización del sistema. Las correcciones se deberán realizar en un lapso no mayor de dos (2) años.

4.8.2 Las excepciones a esta norma serán aprobadas por el Director del Departamento de Informática y Tecnología.

4.9 Cumplimiento

4.9.1 IMXI deberá certificar cada sistema, creando un reporte por cada sistema de autenticación en un sistema informático

4.9.2 Definir los requisitos y documentación necesaria
4.9.3 IMXI realizará auditorías de cumplimiento de esta norma sobre los sistemas críticos de la ACP, cada doce (12) meses.
4.9.4 IMXI realizará revisiones sobre la fortaleza de las contraseñas utilizadas por los usuarios de un sistema informático, de forma periódica o aleatoria.
4.9.5 Se realizarán revisiones anuales de las cuentas habilitadas y los accesos autorizados en los sistemas críticos. La responsabilidad de realizar la revisión y presentar el reporte al Director de Informática será del Oficial de Seguridad.

5. RESPONSABILIDADES

5.1 La Oficina de Seguridad de Sistemas de Informática es responsable de:
5.1.1 Recomendar las actualizaciones necesarias de este documento al Director de Informática y Tecnología para su aprobación,
5.1.2 Incluir esta norma y todos los esfuerzos que se realizan para fortalecer los sistemas de autenticación de la ACP en el programa de educación en seguridad informática corporativa que dirige,
5.1.3 Realizar las auditorías y revisiones de seguridad que se detallan en este documento,
5.1.4 Presentar en un lapso no mayor de treinta (30) días los comentarios sobre las propuestas de autenticación que presente la División de Ingeniería de Software (IMS),
5.1.5 Hacer las recomendaciones necesarias a los sistemas existentes para que cumplan con esta norma durante la próxima actualización que se le haga a cada sistema,
5.1.6 Presentar al Director de Informática y Tecnología las excepciones que puedan surgir en los sistemas informáticos de la ACP para su aprobación y,
5.1.7 Realizar cambios de contraseñas en los sistemas bajo su responsabilidad.

5.2 El Centro de Ayuda Técnica es responsable de:
5.2.1 Realizar cambios de contraseñas en los sistemas bajo su responsabilidad y,
5.2.2 Apoyar a los usuarios en el cambio y selección de contraseñas que cumplan con los criterios de esta norma.

5.3 Los administradores de red y de sistemas son responsables de:
5.3.1 Implementar los parámetros y criterios definidos en esta norma en los sistemas informáticos que administran,
5.3.2 Realizar cambios de contraseñas en los sistemas bajo su responsabilidad y,
5.3.3 Apoyar a los usuarios en el cambio y selección de contraseñas que cumplan con los criterios de esta norma.

5.4 La División de Ingeniería de Sistemas (IMS) y demás desarrolladores de aplicaciones departamentales son responsables de:

5.4.1 Presentar un esquema del mecanismo de autenticación a utilizar en los sistemas informáticos a desarrollar por esta división, a IMXI antes de su implementación y,

5.4.2 Implementar las medidas de autenticación definidas en este documento.

6. FECHA DE EXPIRACION: Ninguna

Francisco Loaiza
Director de Informática y Tecnología

7. REFERENCIAS

American National Standards Institute. (1998). ANSI X9-31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).

International Standard Organization. (1993) ISO/IEC 10646-1: Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane.

International Standard Organization. (1998) ISO/IEC 7816-3 Smart Card Standard - Part 3: Electronic Signals and Transmission Protocols.

International Standard Organization. (1995). ISO/IEC 7816-4 Smart Card Standard - Part 4: Interindustry Commands for Interchange.

National Institute of Standards and Technologies. (2002). FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Documento accedido Diciembre 15, 2004, del sitio del NIST: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

National Institute of Standards and Technologies. (1995). FIPS PUB 180-1, Secure Hash Standard. Documento accedido Diciembre 15, 2004, del sitio del NIST: http://www.itl.nist.gov/fipspubs/fip180-1.htm

National Institute of Standards and Technologies. (2001). FIPS PUB 197, Advanced Encryption Standard. Documento accedido Diciembre 15, 2004, del sitio del NIST: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Personal Computer/SmartCard (PC/SC) Workgroup. (2004). PC/SC Workgroup Specifications 2.0. Documentos accedidos Diciembre 15, 2004, del sitio de PC/SC: http://www.pcscworkgroup.com/specifications/specdownload.php

Rivest, R. (1992). RFC 1321: The MD5 Message-Digest Algorithm. Documento accedido Diciembre 15, 2004, del sitio de IETF: ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt

RSA Laboratories. (2004). PKCS#11: Cryptographic Token Interface Standard. Versión 2.20. Documento accedido Diciembre 15, 2004, del sitio de RSA: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf

8. HISTORIAL

Revisión	Autor(es)	Descripción
04.12.17	GMHoward/CMead	Documento original
04.12.23	GMHoward	Incluye comentarios de AAMock
05.01.05	GMHoward	Incluye comentarios de CIO

9. APÉNDICE A

REGISTRO DE MECANISMO DE AUTENTICACIÓN EN SISTEMAS INFORMATICOS DE LA AUTORIDAD DEL CANAL DE PANAMA
(IMXI-FO-04-032 / Rev.04.12.16)

SECCION 1: DESCRIPCIÓN DEL SISTEMA/PROYECTO	
Sistema Operativo (incluir versión)	
Aplicación(es) (incluir versión, indicar los componentes si ha sido desarrollada por o para ACP)	
Líder Funcional por ACP del Proyecto	
Líder Técnico por ACP del Proyecto	
Unidad de ACP que administrará cuentas de usuarios	

SECCION 2: PARÁMETROS GENERALES DE AUTENTICACION			
PARAMETRO	CUMPLE?		DETALLE
	SI	NO	
Sistema despliega notificación previo a la autenticación de usuario (4.1.1.1)			
Limita el número de intentos de autenticación (4.1.3)			Cantidad máxima de intentos: _____
Suspende la sesión luego de un período de inactividad (4.1.4)			Periodo de inactividad: ___ minutos
Permite el uso de cuentas al nivel de usuarios, no grupos (4.1.5)			
Permite uso de cuentas con roles administrativos (4.1.6)			

SECCION 2: PARÁMETROS GENERALES DE AUTENTICACION			
PARAMETRO	CUMPLE?		DETALLE
	SI	NO	
Datos de autenticación son almacenados utilizando criptografía fuerte (4.1.10)			Algoritmo de cifrado utilizado:

SECCION 3: SISTEMAS DE AUTENTICACIÓN SELECCIONADOS (Colocar una cruz a cada sistema a utilizar, puede seleccionar más de uno)			
Contraseñas		Otro (detallar)	
Tarjetas Inteligentes o "Tokens"			
Biométrico			

SECCION 3a: SISTEMA POR CONTRASEÑAS			
PARAMETRO	CUMPLE?		DETALLE
	SI	NO	
Sistema permite contraseñas con mayúsculas, minúsculas, números y caracteres especiales			
Permite contraseñas de al menos ocho caracteres			Longitud máxima de una contraseña: _____ caracteres
Permite uso de frases secretas			
Permite cambios periódicos de contraseñas de forma manual y automática			
No permite almacenar contraseñas en el cliente			

SECCION 3b: SISTEMA POR TARJETAS INTELIGENTES O TOKENS	
DESCRIPCIÓN (incluir marca y modelo si aplica)	

SECCION 3b: SISTEMA POR TARJETAS INTELIGENTES O TOKENS			
PARAMETRO	CUMPLE?		DETALLE
	SI	NO	
Cumple con la norma FIPS 140-1/2 nivel 2 o superior			
Cumple con la norma ISO 7816-3 y 4			
Permite el uso de algoritmos públicos de cifrado simétrico			Algoritmos que se pueden implementar:
Permite el uso de algoritmos públicos de cifrado asimétrico			Algoritmos que se pueden implementar:
Permite el uso de funciones de compendio públicas			Algoritmos que se pueden implementar:
Cumple con la norma de interfases PKCS#11 y PC/SC			

SECCION 3c: SISTEMA BIOMETRICO			
DESCRIPCIÓN (incluir marca y modelo si aplica)			
PARAMETRO	CUMPLE?		DETALLE
	SI	NO	
Cumple con la norma FIPS 140-1/2			
Permite el uso de algoritmos públicos de cifrado simétrico			Algoritmos que se pueden implementar:
Razón de Aceptación Falsa es igual o menor a 1 en 100,000			
Razón de rechazo falso es igual o menor a 5 en 100			

SECCION 3c: SISTEMA BIOMETRICO			
Es utilizado con otro mecanismo de autenticación			Mecanismo adicional de autenticación:
Posee plan de contigencia para cuando sistema biométrico falle			

Información adicional (si desea detallar algo o explicar alguna excepción)

_____

_____

_____

_____

_____

_____

Nombre del Solicitante: _____

Unidad Administrativa: _____

Fecha: _____ Firma: _____

Enviar o entrega a la Oficina de Seguridad de Sistemas de Informática.
Teléfono 272-4630, Correo electrónico: imxi@pancanal.com

Original: IMXI Copia 1: IM Copia 2: Autor

10. APÉNDICE B

Ejemplo de un Archivo de Configuración /etc/default/su

```
#ident  "@(#)su.dfl     1.6   93/08/14 SMI"     /*SVr4.0 1.2      */

# SULOG determines the location of the file used to log all su attempts
#
SULOG=/var/adm/sulog

# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
CONSOLE=/dev/console

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
SUPATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/local/sbin:/usr/local/bin

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all su attempts.  LOG_NOTICE messages are generated for su's to
# root, LOG_INFO messages are generated for su's to other users, and
# LOG_CRIT messages are generated for failed su attempts.
#
SYSLOG=YES
```