Actas de la IX Reunión Española sobre Criptología y Seguridad de la Información

Casa de Convalescència, Hospital de la Santa Creu i Sant Pau

7, 8 y 9 de septiembre del 2006, Barcelona

Departament d'Enginyeria de la Informació i les Comunicacions,
Universitat Autònoma de Barcelona
Estudis d'Informàtica, Multimèdia i Telecomunicacions,
Universitat Oberta de Catalunya

Editores
Joan Borrell Viader
Jordi Herrera Joancomartí

Editores: Joan Borrell Viader y Jordi Herrera Joancomartí.

Primera edición: julio 2006.
ISBN: 84-9788-502-3

Prólogo

Esta publicación recoge las actas de la Reunión Española sobre Criptología y Seguridad de la Información (RECSI), celebrada los días 7, 8 y 9 de septiembre del 2006 en Barcelona.

La RECSI llega en el año 2006 a su novena edición, organizada de forma conjunta por el Departamento de Ingeniería de la Información y de las Comunicaciones de la Universidad Autònoma de Barcelona y el Departamento de Informática y Multimedia de la Universidad Oberta de Catalunya. Esta IX RECSI quiere seguir siendo el lugar de encuentro y el foro en el que los criptólogos y, en general, todos aquellos que trabajan en el campo de la Seguridad de la Información expongan sus hallazgos y debatan sus ideas. Se trata de un congreso bienal que se celebra en universidades y centros de investigación de España. Las ediciones anteriores se llevaron a cabo en Palma de Mallorca (U. Illes Balears), Madrid (CSIC), Barcelona (U. Politècnica de Catalunya), Valladolid (U. de Valladolid), Torremolinos (U. de Málaga), Santa Cruz de Tenerife (U. de La Laguna), Oviedo (U. de Oviedo) y Leganés (U. Carlos III).

La expansión de Internet, el incremento exponencial del volumen de datos automatizados que se maneja, la creciente inquietud por la protección de la intimidad y, en general, la entrada en la era de la información hace que la seguridad de ésta se configure como un campo de singular importancia, y por ello concentre un especial interés por parte de las empresas, las administraciones, los profesionales y más ampliamente, la sociedad entera. Por otro lado, la Criptología, en su doble vertiente de diseño de algoritmos criptográficos y de análisis de sus posibles debilidades, se ha convertido en la disciplina vertebral de la seguridad, habiendo abandonado los círculos impenetrables en los que se desplegaba históricamente, para ser tratada en universidades, centros de investigación, empresas y organismos de todo tipo interesados en proteger las informaciones que manejan.

Conscientes de lo anterior, en la IX RECSI se tratan y profundizan los aspectos de estas materias que más despiertan la atención en estos días, así como otros, aún en investigación, pero que están llamados a ser de capital importancia en los sistemas y mecanismos de seguridad en un inmediato futuro. A lo largo de las tres jornadas que conforman la Reunión se presentan 63 comunicaciones en 18 sesiones paralelas. Queremos agradecer desde estas líneas el trabajo realizado por el Comité Científico y los revisores en el proceso de revisión.

La IX RECSI, buscando mantener un elevado nivel académico y también un adecuado nivel de contacto de la comunidad investigadora con las empresas y la sociedad, incluye también:

- Tres conferencias magistrales a cargo de investigadores de reconocido prestigio en el ámbito de la Criptología y la Seguridad de la Información, el Dr. Moni Naor, del Weizmann Institute of Science (Israel), el Dr. Frédéric Cuppens de la Escuela Normal Superior de Telecomunicaciones de Bretaña

(Francia) y el Dr. Gene Tsudik de la Universidad de California en Irvine (USA).

- Dos presentaciones de empresas, Safelayer Secure Communications, compañía líder en el mercado de seguridad y confianza para las TIC, desarrollando tecnología de identificación electrónica, firma electrónica y protección de datos basada en Infraestructura de Clave Pública (PKI), y Scytl Secure Electronic Voting, compañía líder en el desarrollo de plataformas de votación electrónica seguras y confiables, aplicables desde procesos electorales clásicos a juntas generales de accionistas.
- La presentación de la Unidad Central de Informática Forense de la Policía de la Generalitat de Catalunya - Mossos d'Esquadra.

Manifestar también nuestro agradecimiento por la ayuda financiera y de difusión recibida de los distintos patrocinadores, cuya relación aparece en la página de agradecimientos de estas actas.

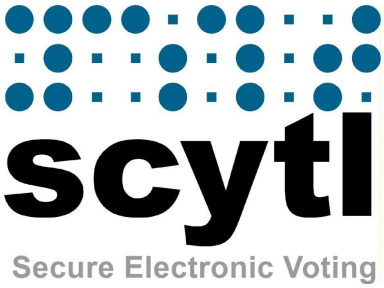
No quisieramos finalizar este prólogo sin recordar a nuestro amigo Andreu Riera Jorba, participante en varias Reuniones, tristemente fallecido en accidente de coche el 11 de marzo de 2006. Andreu, doctor por la UAB, era conocido tanto por su valiosa aportación en el campo de la criptografía aplicada al voto electrónico, como por su espíritu emprendedor que le llevó a fundar Scytl Secure Electronic Voting, empresa de la cual era Consejero Delegado.

Septiembre 2006

Joan Borrell Viader
Jordi Herrera Joancomartí

Agradecimientos

Los organizadores de la RECSI quieren agradecer a los patrocinadores de la Reunión su apoyo logístico y económico.



Organización

La IX RECSI ha sido organizada conjuntamente por el Departament d'Enginyeria de la Informació i les Comunicacions de la Universitat Autònoma de Barcelona y los Estudis d'Informàtica, Multimèdia i Telecomunicacions de la Universitat Oberta de Catalunya.

Comité ejecutivo

Joan Borrell Viader
Jordi Herrera Joancomartí
Josep Rifà Coma

Comité científico

Abascal Fuentes, Policarpo (U. de Oviedo)
Arranz Chacón, Maria Luisa (Alcatel)
Areitio Bertolín, Javier (U. de Deusto)
Borrell Viader, Joan (U.Autònoma de Barcelona)
Caballero Gil, Pino (U. de La Laguna)
Dávila Muro, Jorge (U. Politécnica de Madrid)
Domingo-Ferrer, Josep (U. Rovira i Virgili)
Fernández-Medina Patón, Eduardo (U. de Castilla La Mancha)
Ferrer Gomila, Josep Lluis (U. de les Illes Balears)
Fúster Sabater, Amparo (CSIC)
Gómez Skarmeta, Antonio (U. de Múrcia)
González Jiménez, Santos (U. de Oviedo)
Guía Martínez, Dolores de la (CSIC)
Gutiérrez Gutiérrez, Jaime (U. de Cantabria)
Herrera Joancomartí, Jordi (U. Oberta de Catalunya)
Huguet Rotger, Llorenç (U. de les Illes Balears)
López Muñoz, Javier (U. de Málaga)
Martín del Rey, Angel (U. de Salamanca)
Mañas Argemí, José Antonio (U. Politécnica de Madrid)
Miret Biosca, Josep Maria (U. de Lleida)
Padró Laimon, Carles (U. Politècnica de Catalunya)
Peinado Domínguez, Alberto (U. de Málaga)
Ramió Aguirre, Jorge (U. Politécnica de Madrid)
Ramos Álvarez, Benjamín (U. Carlos III de Madrid)
Ribagorda Garnacho, Arturo (U. Carlos III de Madrid)
Rifà Coma, Josep (U. Autónoma de Barcelona)
Robles Martínez, Sergi (U. Autónoma de Barcelona)

Salazar Riaño, Jose Luís (U. de Zaragoza)
Sempere Luna, José Maria (U. Politécnica de Valencia)
Soriano Ibáñez, Miquel (U. Politècnica de Catalunya)
Rifà Coma, Josep (U. Autònoma de Barcelona)
Tena Ayuso, Juan (U. de Valladolid)
Villar Santos, Jorge (U. Politècnica de Catalunya)

Comité Organizador

Joan Arnedo (Universitat Oberta de Catalunya)
Carles Garrigues (Universitat Autònoma de Barcelona)
David Megías (Universitat Oberta de Catalunya)
Alvaro Moratalla (Universitat Autònoma de Barcelona)
Guillermo Navarro (Universitat Autònoma de Barcelona)
Josep Prieto (Universitat Oberta de Catalunya)
Segi Robles (Universitat Autònoma de Barcelona)
Jordi Serra (Universitat Oberta de Catalunya)
Pere Urbón (Universitat Autònoma de Barcelona)

Revisores

Guillermo Azuara Guillén
Óscar Cánovas Reverte
Jordi Castellà Roca
Sergio Castillo Pérez
Vanesa Daza Fernández
Oscar Esparza Martín
Juan M. Estévez Tapiador
Joaquín García Alfaro
Félix J. García Clemente
Maria Isabel González Vasco
Julio César Hernández Castro
Gabriel López Millán
Consuelo Martínez López
Antoni Martínez Ballesté
Gregorio Martinez Perez
José Luis Muñoz-Tapia
Josep Pegueroles
Joan Josep Piles Contreras
Helena Rifà Pous
Francesc Sebé Feixas
Agusti Solanas Gómez

Índice general

Sesión C1

Sesión S1

Sesión C2

Sesión S2

Sesión C3

Sesión S3

Sesión C4

Sesión S4

Sesión C5

Sesión S5

Sesión S6

Sesión S7

Sesión C6

Sesión S8

Sesión S12

Utilización de métricas para la gestión de sistemas de autenticación basados en contraseñas

Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini

Grupo de Investigación Alarcos,
Departamento de Tecnologías y Sistemas de Información
Centro Mixto de Investigación y Desarrollo de Software UCLM-Soluziona
Universidad Castilla-La Mancha
Paseo de la Universidad 4 - 13071, Ciudad Real, España.
{Carlos.Villarrubia, Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen La necesidad de gestionar la seguridad informática de una institución implica una fase de evaluación y el método más común para realizar esta evaluación consiste en la utilización de un conjunto de métricas. Como cualquier sistema de información necesita de un mecanismo de autenticación siendo el más utilizado aquellos basados en contraseñas, en este artículo se propone un conjunto de métricas de política de contraseñas basado en los factores más relevantes de este mecanismo de autenticación. Junto a las métricas se propone un indicador de nivel de seguridad que se deriva de estas métricas y que permite tener una visión global de la calidad de la política de gestión de contraseñas utilizada. Para ilustrar el método de obtención de las métricas y del indicador de nivel de seguridad se utiliza un ejemplo completo de cálculo de las métricas propuestas. Finalmente, se indica los trabajos futuros a realizar en este ámbito para comprobar la validez y utilidad de estas métricas.

Palabras clave: gestión de la seguridad, aseguramiento, métricas, contraseñas.

1. Introducción

La información y sus procesos de soporte, junto con los sistemas y redes son recursos importantes para cualquier organización. Estos recursos están sometidos continuamente a riesgos e inseguridades provenientes de una gran variedad de fuentes, donde se incluyen amenazas basadas en código malicioso, errores de programación, errores de las personas, sabotajes o incendios. Esta preocupación ha impulsado a muchas organizaciones e investigadores a proponer distintas métricas para evaluar la seguridad de sus sistemas de información. En general, existe un consenso en afirmar que la elección de estas métricas depende de las necesidades concretas de seguridad de cada organización. La mayoría de las propuestas realizadas proponen metodologías para la elección de estas métricas [1,4,15,16,17,19,22,24,26,27,28]. Incluso en algunos casos, se sugiere la necesidad de desarrollo de metodologías específicas para cada organización [7].

En cualquiera de las propuestas, la necesidad es cuantificar los distintos aspectos de la seguridad para poder comprender, controlar y mejorar la confianza en el sistema de información.
Si una organización no usa métricas de seguridad para su toma de decisiones, las elecciones estarán motivadas por aspectos subjetivos, presiones externas e inclusive motivaciones puramente comerciales.
Con objeto de sistematizar todas estas propuestas, se han desarrollado esquemas de clasificación de métricas de seguridad [29] donde se han incluido las métricas propuestas en la literatura existente. En este estudio, se concluye que la mayoría de las métricas propuestas son de tipo general. Esta clase de métricas sólo miden acciones genéricas relativas a la seguridad, y en una forma indirecta, los objetivos específicos como confidencialidad, integridad y disponibilidad.

Sistemas de autenticación

En el caso de la seguridad de un sistema de información se tiene como objetivos generales la mejora continua de la disponibilidad, confidencialidad, integridad y autenticación del sistema. En la utilización de un sistema de autenticación se requiere la integración de múltiples elementos; dependiendo de la técnicas utilizadas, es necesario usar criptografía, medicina, psicología, análisis de sistemas y diseño de protocolos. Todos los sistemas de autenticación están diseñados para asegurar la identidad de un participante a otro participante, y requiere que el primero demuestre su identidad en base a alguna información (prueba de conocimiento, prueba de posesión y prueba biológica). Esta prueba de autenticación puede ser una palabra o contraseña como es utilizado en la mayoría de sistemas operativos y aplicaciones (prueba de conocimiento), una tarjeta criptográfica (prueba de posesión) o alguna característica biológica de la persona a autenticar y que es medida a través de un dispositivo biométrico (prueba biológica).
La utilización de un mecanismo basado en contraseñas ha sido históricamente el método más utilizado. La importancia de este mecanismo de autenticación ha llevado a la elaboración de normas y recomendaciones de múltiples niveles [11, 12 ,13, 14, 20, 21]. Su facilidad para la integración en todos los sistemas y su bajo coste han motivado esta aceptación [18]. Sus deficiencias han sido estudiadas de forma extensa y se han propuesto medidas para limitar estas desventajas [2, 9, 23]. En algunos diseños, los principales inconvenientes están ligados a la necesaria confianza en los usuarios en el tratamiento de las contraseñas. En otros casos, están motivados por diseños que presuponían un entorno seguro (por ejemplo, redes cerradas) y que han sido utilizados en otros entornos (por ejemplo, Internet) [10].
Toda esta problemática debería indicar que las contraseñas es un mecanismo a reemplazar pero la aceptación de los usuarios en su uso, su bajo coste unido a la complejidad y los costes de las alternativas garantizan su permanencia a corto y medio plazo.
En este artículo, se proponen métricas e indicadores relativos a la política de gestión de contraseñas debido a esta falta de propuestas específicas en áreas de especial relevancia en la seguridad de los sistemas de información.
En la sección 2, se proponen las métricas de política de gestión de contraseñas, justificando su necesidad y clasificando el conjunto propuesto en función de varios

criterios. En la sección 3, se propone una clasificación en niveles de las políticas de gestión de contraseñas que permite a las organizaciones conocer su situación actual, proponer de forma dirigida las mejoras relevantes y relacionar comparaciones entre diferentes instituciones para conocer las mejores prácticas. Finalmente, se exponen algunas conclusiones obtenidas y una propuesta de trabajo futuro en este ámbito.

2. Propuesta de métricas de gestión de contraseñas

La metodología utilizada para derivar las métricas de gestión de contraseñas ha consistido en una modelización de todos los factores que intervienen en la gestión de contraseñas. A tal efecto, se ha recopilado de la literatura existente estos factores [2,3,9,13,18,20,21]. Las métricas propuestas no intentan cubrir toda la problemática sino capturar la más representativa. En esta hipótesis, no se incluye la utilización de contraseñas para la autenticación entre procesos o equipos, estando sólo contemplada la participación de una persona como entidad a ser autenticada. Tampoco se incluyen los sistemas de autenticación multifactor aunque uno de los mecanismos de autenticación sea una contraseña.

La definición de estas métricas se realizará de la siguiente forma:

- *Nombre*: Título representativo de la métrica.
- *Descripción de la métrica*: Generalmente, particulariza el nombre de la métrica indicando el método de cálculo de los valores.
- *Fase del ciclo de vida*: Para una mejor comprensión y análisis de las métricas, se clasifica las métricas en función de su papel dentro del ciclo de vida de las contraseñas. Las fases definidas son:
  - General: Engloba las métricas con una difícil clasificación en otra fase.
  - Alta: Se incluyen todas las métricas relacionadas con la asignación de identificadores y contraseñas iniciales a los usuarios.
  - Almacenamiento: Contempla la problemática del almacenamiento de las contraseñas por el sistema de autenticación.
  - Transmisión: Incluye las métricas relacionadas con los protocolos de autenticación utilizados por el usuario o la comunicación al usuario de la contraseña por parte del sistema de autenticación.
  - Utilización: Agrupa las métricas que miden la forma de utilización de la contraseña por parte del usuario.
  - Renovación: Fase con las métricas relativas a la modificación de contraseña.
- *Escala*: Conjunto de valores que puede tener las medidas asociadas a esta métrica.
- *Multivaluado*: Algunas de las métricas propuestas son susceptibles de tener varios medidas simultáneas. Con este atributo se indica si la métrica puede tener o no varias medidas simultáneas.

Los nombres, descripción de la métrica, fase del ciclo de vida y el carácter multivaluado de las métricas propuestas figuran en la tabla 1.

Nombre	Descripción	Fase	Mult.
Formación de usuarios	Tipo de formación recibida por los usuarios para el tratamiento o selección, si procede, de las contraseñas.	General	Si
Contraseña de grupos	Existencia de contraseñas utilizadas por un grupo de usuarios o de contraseñas necesarias para acceder a recursos que no tienen un mecanismo de control de acceso separado del mecanismo de autenticación.	General	No
Registro de acciones	Tipo de registro utilizada por el sistema de información para monitorizar las acciones relacionadas con la gestión de contraseñas.	General	Si
Tamaño del alfabeto	Nº de caracteres del alfabeto utilizado para la formación de contraseñas validas en el sistema.	Alta	No
Nº de clases distintas exigidas	Nº de clases, en las cuales, está dividido el alfabeto y que son exigidas a la fuente de selección para determinar una contraseña valida.	Alta	No
Longitud mínima	Nº de caracteres mínimos que se exige a una contraseña valida.	Alta	No
Fuente de selección	Conjunto de agentes que se pueden utilizar para elegir una contraseña.	Alta	No
Restricción en la selección	Conjunto de restricciones que impiden a la fuente de selección utilizar una contraseña con facilidad de averiguación por parte de terceros.	Alta	Si
Clase de identificador de usuario	Tipo de identificador de usuario usado por el sistema de información.	Alta	No
Usuarios predefinidos	Tratamiento recibido a los usuarios predefinidos por el sistema de información.	Alta	Si
Clase de almacenamiento	Forma de almacenamiento de las contraseñas en el sistema de autenticación.	Almacena-miento	Si
Comunicación inicial	Método de comunicación de la contraseña inicial o en una reasignación por parte del sistema de autenticación al usuario.	Transmisión	Si
Transmisión en redes	Mecanismo de transmisión utilizado por el protocolo de autenticación sobre la base de sus características de confidencialidad e integridad de la contraseña.	Transmisión	No
Visualización en la entrada	Método utilizado por el sistema para la visualización de la contraseña cuando es solicitada al usuario.	Utilización	No
Nº máximo de intentos erróneos	Nº máximo de intentos fallidos antes que el sistema de autenticación realice una operación de defensa por el riesgo de usurpación de identidad por parte de un tercero.	Utilización	No
Información sobre uso	Grupo de mecanismos utilizados por el sistema de autenticación para informar al usuario sobre las autenticaciones realizadas en el pasado.	Utilización	No
Período de autenticación	Tiempo máximo, tras el cual, el control de acceso solicita una reautenticación al usuario.	Utilización	No
Bloqueo por baja de usuario	Procedimientos utilizados para garantizar que usuarios legítimos en un tiempo pasado no pueda seguir accediendo al sistema.	Renovación	No
Tiempo de vida mínimo	Tiempo de vida mínimo de una contraseña valida.	Renovación	No
Tiempo de vida máximo	Tiempo de vida máximo de una contraseña valida. Transcurrido este tiempo se fuerza al usuario a cambiar de contraseña.	Renovación	No
Longitud del historial	Nº de contraseñas validas utilizados en el pasado por el usuario y que el sistema no permite reutilizar.	Renovación	No
Reasignación de contraseñas	Procedimiento utilizado reactivar la credencial de un usuario que no recuerda la contraseña.	Renovación	No

Tabla 1. Métricas de política de gestión de contraseñas.

El atributo de la escala se define en el siguiente apartado por su estrecha relación con el indicador de nivel de seguridad.

3. Indicador de nivel de seguridad en la gestión de contraseñas

La definición de un conjunto de métricas no es suficiente para que una organización pueda utilizarlas para gestionar los cambios necesarios en el ámbito de esas métricas. Es necesario tener información sobre su forma de utilización y la repercusión de los valores de las métricas en la gestión del sistema.

Con este objetivo, se propone una serie de valores preestablecidos para cada métrica que facilita su utilización. Salvo alguna excepción, estos valores están ordenados en una jerarquía, empezando por un valor mínimo hasta un valor máximo, pasando en la mayoría de métricas por valores intermedios. A medida que una institución tiene un valor superior en cada métrica tendrá una mayor confianza en su sistema de autenticación.

La mejora del sistema de autenticación implica que todos los factores de autenticación utilizados mejoran de forma homogénea. Teniendo este principio como objetivo, se propone un indicador de calidad de política de gestión de contraseñas basado en cinco niveles que tiene en cuenta todos los factores. Esta propuesta está basada en la utilidad demostrada en los modelos de madurez y en los programas de gestión de métricas [5, 6, 8, 25, 26].

Estos niveles están estructurados desde un nivel mínimo (nivel 1) a un nivel máximo (nivel 5). Como se indica en la tabla 2, en cada nivel se definen los valores requeridos en cada métrica. En alguna de estas métricas, además se define un valor recomendado para cada nivel. Estas recomendaciones tiene por objeto dotar de flexibilidad al indicador, permitiendo definir los valores requeridos a la medida más baja posible en cada nivel. Por último, el valor '+' indica que el valor de esa métrica en ese nivel está superado pues tiene un valor mayor que el exigido o recomendado para ese nivel.

Formación de usuarios (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Ninguna	Oblig.[1]				
Información en el alta de usuario	Rec.[2]	Oblig.	Oblig.	Oblig.	Oblig.
Curso obligatorio	Rec.	Rec.	Rec.	Oblig.	Oblig.
Curso periódico	+[3]	+	+	Rec.	Oblig.
Contraseña de grupo	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Existencia de contraseñas de grupos o de acceso a recursos	Oblig.				
Existencia única de grupo de administradores	+	Oblig.	Oblig.		
No existen contraseñas de grupos	+	+	Rec.	Oblig.	Oblig.
Registro de acciones (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Ninguno	Oblig.				
Registro de altas	+	Oblig.	Oblig.	Oblig.	Oblig.
Registro de renovaciones y bajas	+	Rec.	Oblig.	Oblig.	Oblig.
Registro de bloqueos y reasignaciones	+	Rec.	Rec.	Oblig.	Oblig.
Tamaño de alfabeto	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**

[1] Oblig. Valor obligatorio
[2] Rec.: Valor recomendado
[3] +: Valor superado en el nivel indicado

Hasta diez caracteres	Oblig.				
Entre once y veinticinco caracteres	+	Oblig.			
Entre veintiséis y cincuenta caracteres	+	Rec.	Oblig.		
Entre cincuenta y un caracteres y setenta y cinco caracteres	+	+	Rec.	Oblig.	
Más de setenta y cinco caracteres	+	+	Rec.	Rec.	Oblig.
Nº de clases distintas exigidas	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Una	Oblig.				
Dos	+	Oblig.			
Tres	+	+	Oblig.	Oblig.	
Cuatro o más	+	+	+	Rec.	Oblig.
Longitud mínima	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Menor o igual a cuatro caracteres	Oblig.				
Entre cinco y ocho caracteres	+	Oblig.			
Entre nueve y doce caracteres	+	+	Oblig.		
Entre trece y dieciséis caracteres	+	+	+	Oblig.	
Mayor a dieciséis caracteres	+	+	+	+	Oblig.
Fuente de selección	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Usuario	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Sistema	+	+	+	Rec.	Rec.
Restricción en la selección (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Ninguna					
Información de usuario	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Combinaciones de teclas	+	Rec.	Rec.	Oblig.	Oblig.
Contraseña en diccionario	+	+	Rec.	Oblig.	Oblig.
Variaciones de las anteriores	+	+	+	Rec.	Oblig.
Clase de identificador de usuario	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Identificador público	Oblig.	Oblig.	Oblig.		
Identificador semipúblico	+	+	Rec.	Oblig.	
Identificador privado	+	+	+	Rec.	Oblig.
Usuarios predefinidos (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Ningún cambio					
Cambio de contraseña	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Cambio de identificador	+	+	Rec.	Oblig.	Oblig.
Clase de almacenamiento (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Almacenamiento en claro					
Almacenamiento irreversible	Oblig.	Oblig.	Rec.	Rec.	Rec.
Almacenamiento cifrado	+	+	Oblig.	Oblig.	Oblig.
Comunicación inicial (Multivaluado)	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Transmisión no segura	Oblig.				
Transmisión con cambio obligatorio de contraseña	+	Oblig.	Oblig.	Rec.	Rec.
Transmisión segura	+	+	Rec.	Oblig.	Oblig.
Transmisión en redes	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Transmisión en claro					
Utilización de un protocolo de desafío-respuesta	Oblig.	Oblig.	Oblig.		
Transmisión cifrada	+	+	Rec.	Oblig.	Oblig.
Visualización en la entrada	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Visualización en claro					
Visualización del nº de caracteres	Oblig.	Oblig.	Oblig.		
Ninguna visualización	+	+	Rec.	Oblig.	Oblig.
Nº máximo de intentos de autenticación erróneos	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Sin límite	Oblig.				
Menor o igual a cincuenta intentos	Rec.	Oblig.			
Menor o igual diez intentos	+	Rec.	Oblig.	Oblig.	
Menor o igual de tres intentos	+	+	+	Rec.	Oblig.
Información sobre uso	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**

Ninguna información	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Información sobre el último uso	+	+	Rec.	Rec.	Rec.
Período de autenticación	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Sesión de trabajo	Oblig.	Oblig.			
Máximo de quince minutos de inactividad	+	+	Oblig.	Oblig.	
Máximo de cinco minutos de inactividad	+	+	+	Rec.	Oblig.
Bloqueo por baja de usuario	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Sin método establecido	Oblig.				
Eliminación periódica (período máximo de seis meses)	Rec.	Oblig.	Oblig.		
Límite de tiempo establecido en el alta	+	+	Rec.	Oblig.	Oblig.
Tiempo de vida mínimo	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
No existe tiempo de vida mínimo	Oblig.	Oblig.	Oblig.	Oblig.	
Existe tiempo de vida mínimo (igual o superior a 1 día)	+	+	Rec.	Rec.	Oblig.
Tiempo de vida máximo	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Mayor a doce meses	Oblig.				
Menor o igual de doce meses	+	Oblig.			
Menor o igual a seis meses	+	+	Oblig.	Oblig.	
Menor o igual a tres meses	+	+	+	Rec.	Oblig.
Longitud del historial	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Uno	Oblig.				
Menor o igual a tres	+	Oblig.			
Menor o igual de diez	+	+	Oblig.		
Menor o igual a veinticinco	+	+	+	Oblig.	
Mayor de veinticinco	+	+	+	+	Oblig.
Reasignación de contraseñas	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Se reasigna la contraseña anterior	Oblig.				
Se asigna una nueva contraseña	Rec.	Oblig.	Oblig.	Oblig.	Oblig.

Tabla 2. Valores de cada métrica y el nivel asociado.

El cálculo del valor del indicador de nivel de seguridad en la gestión de contraseñas requiere que se tengan como mínimo los valores de las métricas con el requisito de obligatorio, superado o recomendado. Es necesario destacar que aunque el nº de métricas es veintidós, los valores obtenidos pueden ser mayores debido a que varias métricas pueden tener varios valores simultáneamente (por ejemplo, formación de usuarios). El número mínimo de valores para alcanzar el correspondiente nivel está indicado en la tabla 3.

Nivel	**Nº mínimo**
1	22
2	22
3	23
4	28
5	30

Tabla 3. Nº de valores por nivel

Aplicación de las métricas

En este apartado se detalla un caso concreto de aplicación de estas métricas. El sistema de información utilizado tiene las siguientes características: se informa al

nuevo usuario de la política de gestión de contraseñas y en el plazo máximo de un mes recibe una sesión de formación donde se incluyen aspectos de seguridad informática. La elección de las contraseñas la realiza el usuario con las siguientes restricciones: 8 caracteres mínimos elegidos de un alfabeto con discriminación entre mayúsculas y minúsculas y con una mezcla de dígitos. En la comunicación de la contraseña inicial al usuario se obliga a este a un cambio de contraseñas y estas se almacenan cifradas y utilizando una función de dispersión para ser irreversibles. Estas características junto con otras que se deducen de la tabla 4 nos permiten obtener los siguientes valores para las métricas propuestas.

Métrica: Valor del sistema	**Nivel 1**	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
Formación de usuarios: Información en el alta de usuario	Rec.	Oblig.	Oblig.	Oblig.	Oblig.
Formación de usuarios: Curso obligatorio	Rec.	Rec.	Rec.	Oblig.	Oblig.
Contraseña de grupos: Existencia única de grupo de administradores	+	Oblig.	Oblig.		
Registro de acciones: Registro de altas	+	Oblig.	Oblig.	Oblig.	Oblig.
Tamaño de alfabeto: Más de setenta y cinco caracteres	+	+	Rec.	Rec.	Oblig.
Nº de clases distintas exigidas: Dos	+	Oblig.			
Longitud mínima: Entre cinco y ocho caracteres	+	Oblig.			
Fuente de selección: Usuario	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Restricción en la selección: Información de usuario	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Clase de identificador de usuario: Identificador público	Oblig.	Oblig.	Oblig.		
Usuarios predefinidos: Cambio de contraseña	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Clase de almacenamiento: Almacenamiento irreversible	Oblig.	Oblig.	Rec.	Rec.	Rec.
Clase de almacenamiento: Almacenamiento cifrado	+	+	Oblig.	Oblig.	Oblig.
Comunicación inicial: Transmisión con cambio obligatorio de contraseña	+	Oblig.	Oblig.	Rec.	Rec.
Transmisión en redes: Transmisión cifrada	+	+	Rec.	Oblig.	Oblig.
Visualización en la entrada: Visualización del nº de caracteres	Oblig.	Oblig.	Oblig.		
Nº máximo de intentos de autenticación erróneos: Menor o igual diez intentos	+	Rec.	Oblig.	Oblig.	
Información sobre uso: Ninguna información	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Período de autenticación: Sesión de trabajo	Oblig.	Oblig.			
Bloqueo por baja de usuario: Eliminación periódica (período máximo de seis meses)	Rec.	Oblig.	Oblig.	Oblig.	Oblig.
Tiempo de vida mínimo: No existe tiempo de vida mínimo	Oblig.	Oblig.	Oblig.	Oblig.	
Tiempo de vida máximo: Menor o igual de doce meses	+	Oblig.			
Longitud del historial: Menor o igual de diez	+	+	Oblig.		
Reasignación de contraseñas: Se asigna una nueva contraseña	Rec.	Oblig.	Oblig.	Oblig.	Oblig.

Tabla 4. Valores de cada métrica en el supuesto.

Con estas medidas se obtiene la tabla 5 con un resumen por nivel y por el carácter obligatorio, recomendado o superado de cada métrica.

Totales	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Valores obligatorios	9	18	16	13	12
Valores recomendados	4	2	4	3	2
Valores superados	11	4			
Total de valores	24	24	20	16	13

Tabla 5. Suma de valores por tipo y nivel.

De la tabla 4 se obtiene que la política de gestión de contraseñas utilizada tiene los niveles 1 y 2 pues tiene todos los valores requeridos. En cambio, para obtener el nivel 3 tiene que mejorar en cuatro métricas: nº de clases distintas exigidas, longitud mínima, período de autenticación y tiempo de vida máximo. Y por último, para alcanzar el nivel 4 necesita mejorar en ocho métricas y para el nivel 5 en diez métricas.

4. Conclusiones y trabajo futuro

En este trabajo, se propone un conjunto de métricas y un indicador de nivel de seguridad en la política de gestión de contraseñas que cumplen el objetivo de evaluar el proceso de autenticación a través de contraseñas.

Se proponen veintidós métricas agrupadas en seis áreas que abarcan el ciclo completo de gestión de contraseñas. Estas métricas tienen un conjunto limitado de valores que simplifica el proceso de obtención de medidas y la utilización de estas métricas para la toma de decisiones.

Como método de valoración global de la política de gestión de contraseñas, se propone un indicador de calidad cuyo rango de valores es una escala de cinco niveles. Este indicador permite de una forma sencilla y comprensible comunicar a todos los actores involucrados en la seguridad de la organización la calidad alcanzada en un sistema de información.

Se incluye como ejemplo de aplicación, un supuesto donde se obtiene el nivel de cada métrica junto con el indicador de nivel de seguridad de todo el conjunto de métricas. En este supuesto se pone de manifiesto la sencillez en la orientación a los responsables para dirigir sus actuaciones futuras.

Esta propuesta está enmarcada dentro de un proyecto mayor de definición de métricas que contempla todos los ámbitos generales de la seguridad. No obstante, en este ámbito de la identificación y autenticación es necesario extender estas métricas a la explotación del sistema de información para completar el sistema de gestión de contraseñas.

Asimismo, la mayoría de las organizaciones tienen una diversidad de sistemas de información con requisitos y mecanismos de autenticación diferentes. Para obtener una visión de conjunto, a través de un conjunto de métricas, es necesario combinar toda esta información de una forma coherente y útil para los directivos y técnicos de la institución.

En este aspecto, se debe completar las métricas propuestas con otras que tengan en cuenta estas circunstancias.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS, parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) y RETISTIC (TIC2002-12487-E) concedidos por la "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

Referencias

1. ACSA, editor. Proceedings of the Workshop on Information Security System Scoring and Ranking, Williamsburg, Virginia, may 2001.
2. A. Adams, M. A. Sasse, y P. Lunt. Making passwords secure and usable. En Proceedings of Human Computer Interaction, Bristol, England, aug 1997.
3. M. Bishop. Comparing authetication techniques. En Proceedings of the Third Workshop con Computer Incident Handling, pp. 1–10, aug 1991.
4. P. Bouvier y R. Longeon. Le tableau de bord de la sécurité du système d'information. Sécurité Informatique, jun 2003.
5. Carnegie Mellon University, Pittsburgh, Pennsylvania. SSE-CMM Model Description Document, 3.0 edition, jun 2003.
6. D. A. Chapin y S. Akridge. How can security be measured? Information Systems Control Journal, 2:43–47, 2005.
7. C. Colado y A. Franco. Métricas de seguridad: una visión actualizada. SIC. Seguridad en Informática y Comunicaciones, 57:64–66, nov 2003.
8. Departament of the Air Force. AFI33-205. Information Protection Metrics and Measurements Program, aug 1997.
9. A. Halderman, B. Waters, y E. W. Felten. A convenient method for securely managing passwords. En Proceedings of the 14th International World Wide Web Conference, pp. 471–479, Chiba, Japan, may 2005.
10. ISO. ISO 7498-2. Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989.
11. ISO/IEC. ISO/IEC TR 13335-1. Guidelines for the Management of IT Security. Part I: Concepts and Models of IT Security, 1996.
12. ISO/IEC. ISO/IEC 15408. Evaluation Criteria for IT Security, dec 1999.
13. ISO/IEC. ISO/IEC 17799. Code of Practice for Information Security Management, 2000.
14. G. King. Best security practices: An overview. En Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, oct 2000. NIST.
15. J. M. Marcelo. Seguridad de las Tecnologías de la Información, capítulo Identificación y Evaluación de Entidades en un Método AGR, pp. 69–103. AENOR, 2003.
16. W. L. McKnight. What is information assurance? CrossTalk. The Journal of Defense Software Engineering, pp. 4–6, jul 2002.
17. R. T. Mercuri. Analyzing security costs. Communications of the ACM, 46(6):15–18, jun 2003.
18. R. Morris y K. Thompson. Password security: A case history. CACM, 22(11):594–597, 1979.
19. F.Nielsen. Approaches of security metrics. Technical report, NIST-CSSPAB, jun 2000.
20. NIST. FIPS-112: Password Usage, may 1985.
21. NIST. FIPS-181: Automated Password Generator, oct 1993.
22. S. C. Payne. A guide to security metrics. Technical report, SANS Institute, jul 2001.
23. B. Pinkas y T. Sander. Securing passwords against dictionary attacks. En Proceedings of the ACM Computer and Security Conference (CSC' 02), pp. 161–170, nov 2002.

24. G. Schuedel y B. Wood. Adversary work factor as a metric for information assurance. En Procedings of the New Security Paradigm Workshop, pp. 23–30, Ballycotton, Ireland, sep 2000.
25. M. Swanson. Security self-assessment guide for information technology systems. Technical Report NIST 800-26, National Institute of Standards and Technology, nov 2001.
26. M. Swanson, N. Bartol, J. Sabato, . J. Hash, y L. Graffo. Security metrics guide for information technology systems. Technical Report NIST 800-55, National Institute of Standards and Technology, jul 2003.
27. R. B. Vaughn, Jr., R. Henning, y A. Siraj. Information assurance measures and metrics – state of practice and proposed taxonomy. En Proceedings of the 36th Hawaii International Conference on Systems Sciences, 2003.
28. R. B. Vaughn, Jr., A. Siraj, y D. A. Dampier. Information security system rating and ranking. CrossTalk. The Journal of Defense Software Engineering, pp. 30–32, may 2002.
29. C. Villarrubia, E. Fernández-Medina, y M. Piattini. Hacia una clasificación de métricas de seguridad. En VIII Reunión Española sobre Criptología y Seguridad de la Información, pp. 363–371, sep 2004.