Política de gestión de contraseñas para usuarios finales

Password management policy for end-users

Ana María López Echeverry, Paula Andrea Villa Sánchez
Facultad de Ingenierías, Universidad Tecnológica de Pereira, Pereira, Colombia
Correo-e: anamayi@utp.edu.co, pavaji@utp.edu.co

***Resumen*— Este artículo contiene el ciclo de vida de una contraseña, que va desde la generación hasta su tiempo de expiración. Adicionalmente, se presenta una política de gestión de contraseñas que contiene las pautas necesarias para generar e implementar claves seguras para el usuario final manteniendo su usabilidad, con el objetivo de mejorar la seguridad de los sistemas de información y capacitar a estos usuarios en cuanto a la protección de los datos de la organización.**

***Palabras clave*— Clave, contraseña, ciclo de vida de las contraseñas, política de gestión de contraseñas, usuario final.**

***Abstract*— This article contains the life cycle of a password that begins since the generation until its expiration time. Additionally, It is presented a password management policy which contains the necessary guidelines to generate and implement the use of safe passwords for the end-user maintaining its usability, with the objective of improve the security of the information systems and train these users with topics related to the data protection of the organization.**

***Key Word* — cycle life of a password, End-user, password, password management policy.**

I. INTRODUCCIÓN

Los métodos de autenticación se dividen en tres grandes categorías en función de lo que utilizan para la verificación de identidad, las cuales son: (a) algo que el usuario sabe (contraseña), (b) algo que éste posee (tarjeta inteligente), y (c) una característica física del usuario. Esta última categoría se conoce con el nombre de autenticación biométrica [1], pero aun así, las contraseñas siguen siendo el método más empleado[1] [2].

Así como la biometría cuenta con varios tipos de validación como las huellas dactilares, el iris, la voz, entre otros, en las contraseñas también es posible encontrar diferentes tipos, por ejemplo las claves simétricas y asimétricas, claves de un solo uso, clave estructural, clave maestra, clave primaria, entre otras [3], y estas a su vez, cuentan con métodos de protección como hash, md5, DES, RSA, etc [4]. Estos algoritmos sirven para generar contraseñas seguras, pero que en cierta medida son utilizadas por usuarios que poseen un nivel de conocimiento técnico menor que los usuarios especializados, que usualmente son usuarios sofisticados, programadores de aplicaciones y administradores de bases de datos [5].

Se recomienda que los usuarios finales tengan políticas diferentes ya que son usuarios normales con una formación tecnológica diferente y representan el eslabón más débil de la cadena de seguridad [6]

II. CICLO DE VIDA DE LAS CONTRASEÑAS

El ciclo de vida de las contraseñas como se define en la figura 1, consta de una serie de etapas que van desde la generación hasta la terminación de la clave.

El problema que se presenta es que a pesar de que actualmente se cuenta con herramientas para la generación de contraseñas como "Random Password Generator"[7] o el Analyzer and Modifier for Passwords (AMP)[2][8] que ayudan al usuario a generar contraseñas robustas manteniendo la usabilidad, y herramientas que generan claves aleatorias [9] o pseudoaleatorias [10], se siguen teniendo dificultades con el manejo de las mismas por parte del usuario final. Sin embargo, existe otra mirada como se observa en varias publicaciones de revistas científicas tipo A como la IEEE y ACM según estudios como [8][11][12][13][14][15], centrados en la generación de contraseñas no a partir de programas ya que esto conlleva a tener problemas de seguridad por parte de los usuarios, sino a establecer el uso de políticas que permitan la generación de claves seguras y con un alto grado de usabilidad por parte de quien las va a utilizar.

[1] FRAGKOS, Grigorio, TRYFONAS, Theodore, A Cognitive Model for the Forensic Recovery of End-User Passwords , IEEE Xplore digital library, p. 1, Agosto 2007.

[2] HOUSHMAND, Shiva, AGGARWAL, Sudhir, Building better passwords using probabilistic techniques, ACM digital library, p. 5, Diciembre 2012

Fecha de Recepción: 09 de septiembre de 2014
Fecha de Aceptación: 10 de febrero de 2016

En este orden de ideas, se definirá una política para la gestión de contraseñas tomando como base diferentes trabajos e investigaciones que se han realizado.

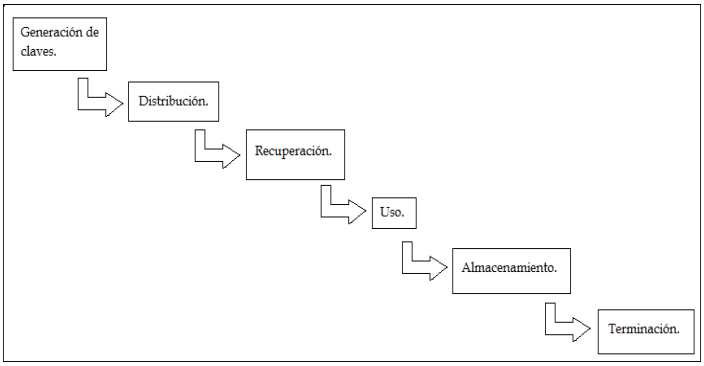

Figura 1: Ciclo de vida de las contraseñas

Generación de contraseñas.

El primer paso para comenzar a generar una contraseña segura, es saber que esta debe contener una mezcla de símbolos (letras mayúsculas, minúsculas, números, caracteres especiales), sin ningún tipo de secuencia o coherencia, es decir, no generar claves tipo "Luis123" o con nombres de series de televisión como "lossimpsons1" ya que existen herramientas que utilizan diccionarios de palabras que hacen que estas claves sean vulnerables.

Uno de los métodos de generación de claves seguras es el uso de mnemotecnias a partir de frases[3][12][16], por ejemplo:
"Es mejor un pájaro en mano que cien volando", se toman las iniciales de cada palabra para formar un acrónimo, que daría como resultado algo así "emupemqcv", luego se cambian algunas letras por números, para este caso la letra "e" por un "3" y la "c" por una "@" y se obtiene la siguiente palabra "3mup3mq@v", finalmente para agregar un grado más de complejidad se cambiaran algunas de las letras por mayúsculas, se toma la letra "m" para obtener finalmente "3Mup3Mq@v" una clave robusta que difícilmente se encontrará en un diccionario y que a pesar de que alguien más esté utilizando la misma frase, esta es una contraseña personalizada y que seguramente nadie más sabrá que cambios se realizaron.

Otras de las recomendaciones para la generación de contraseñas seguras son [17]:

- Cambiarlas con regularidad
- Utilizar signos de puntuación si el sistema lo permite.
- Elegir palabras sin sentido pero que sean pronunciables.
- Evitar utilizar información personal en la contraseña, ya que alguien que lo conozca puede vulnerarla

Distribución.

Existen algunas técnicas de distribución de claves como [18]:

- Distribución manual

El envío de la clave no es por la línea de comunicación por la cual se mandan los mensajes cifrados, sino que se utilizan otros métodos, por ejemplo:

- ✓ carta certificada + vía telefónica + fax.
- ✓ Utilizando un inyector de claves

- Distribución basada en centro

Las dos entidades interesadas en intercambiar datos tienen una conexión cifrada con una tercera entidad de confianza, esta tercera entidad es la encargada de entregar la clave a través de los enlaces cifrados a las otras dos entidades.

- Distribución basada en certificado

Es posible diferenciar dos técnicas para la distribución basada en certificado:

1. Transferencia de claves: El emisor genera localmente una clave y la cifra con un algoritmo asimétrico utilizando la llave pública del receptor, con el objetivo de que solo éste pueda recuperarla y así protegerla durante su transmisión.

2. Intercambio de claves o acuerdo de claves: la clave es generada por las dos entidades involucradas en la comunicación.

Recuperación.

Cuando un usuario olvida su contraseña, generalmente hay dos opciones, obtener acceso a la antigua clave "password recovery" o establecer una nueva "password reset". El "password reset" también se usa cuando una cuenta nueva es creada, para asignar una clave inicial, en todo caso si no hay razón para descartarla, debe haber alguna manera definida en las políticas de gestión de claves que dé en detalle y bajo qué condiciones una clave puede ser recuperada [19].

Pero se debe tener especial atención sobre el "password recovery" y el "password reset" ya que si no se verifica con veracidad la autenticidad del usuario, un atacante podría obtener acceso a esa contraseña, así que se deben establecer fuertes políticas para asegurarse de ello (fecha de nacimiento, número de identificación, código laboral, etc.) [4][20]

[3] FORGET, Alain, CHIASSON, Sonia, BIDDLE, Robert, Helping Users Create Better Passwords: Is this the right approach?, ACM digital library, p. 1, Julio 2007

[4] SCARFONE, Karen, SOUPPAYA, Murugiah, Guide to Enterprise Password Management (Draft), National Institute of Standards and Technology (NIST), p. 24-25, Abril 2009

Uso.

El estudio realizado en [13] define que el uso de las claves debe estar establecido en las políticas de seguridad y da el ejemplo de la Universidad de Brown, donde se establece que es posible enviar la contraseña por e-mail únicamente con permiso administrativo, como también define que estas deben ser encriptadas para ser transmitidas; sin embargo, en otras instituciones está restringido compartir la clave. Lo anterior permite entonces resaltar que es necesario establecer dentro de la política de gestión de claves de usuario final, todas las consideraciones de manejo de las mismas, con una definición clara de que se puede hacer y que se encuentra restringido en condiciones específicas de manejo de una clave particular.

Almacenamiento.

Las claves son guardadas en el sistema para validar la autenticidad del usuario y por esta razón, estas deben estar almacenadas de forma segura para que ninguna persona pueda acceder fácilmente de manera lógica o física y afectar la estabilidad del negocio, estas contraseñas deben estar protegidas con controles de seguridad, como por ejemplo [20]:

- Encriptar los archivos que contienen las contraseñas[5] [13].
- Usar las funciones de control de acceso al sistema operativo para restringir el acceso a los archivos que contienen las claves.
- Almacenar los hashes criptográficos[6] para contraseñas de un solo sentido, en vez de almacenar las claves mismas.

Los controles de seguridad apropiados para una situación particular, dependen de varios factores, tales como las capacidades de seguridad del host, las amenazas en contra del host, y los requerimientos de autenticación[7].

Terminación.

Es la última etapa en el ciclo de vida de una contraseña, cuando esta ya no es útil y debe ser cambiada, una clave nunca debería usarse por tiempo indefinido. Esta debe tener una fecha de caducidad, por las siguientes razones [21]:

- Cuanto más tiempo se usa una clave, aumenta la probabilidad de que se comprometa (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).
- Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, ya que toda la información protegida con esa clave queda al descubierto.
- Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar descifrarla.

Al igual que en las etapas anteriores, esta debe ser tratada en las políticas de seguridad. Pero estas claves solo deben ser eliminadas por 2 razones, "Expiración" o" Revocación". En las políticas se seguridad de contraseñas, debe existir un tiempo de vida útil de una clave, cuando este tiempo ha llegado a su límite de vigencia, se dice que una contraseña "Expira", pero cuando un administrador determina que una contraseña se encuentra comprometida, este la puede "Revocar" [8][13]

Las organizaciones comúnmente destruyen datos innecesarios, especialmente datos sensibles que pueden estar bajo los requisitos de cumplimiento normativo y las contraseñas hacen parte de estos datos, Securosis[9] brinda una serie de controles para la destrucción de esta información:

- Crypto-Shredding, es la destrucción de todas las claves encriptadas para los datos.
- Borrado seguro
  Limpieza del espacio libre del disco duro y destrucción física.
  Esta opción está solamente disponible cuando se tiene un bajo nivel de acceso administrativo a los medios de almacenamiento físico. Esto incluye hardware o software diseñado para destruir los datos en los discos duros y otros medios, o la destrucción física de los drivers.
- Destrucción física se tiene lo siguiente:
- ✓ Desmagnetización: Uso de Fuertes imanes para codificar los medios magnéticos, como discos duros y cintas de copia de seguridad.

[5] SHAY, Richard J., BHARGAV-SPANTZEL, Abhilasha, BERTINO, Elisa, Password Policy Simulation and Analysis, ACM digital library, p .2, Noviembre 2007

[6] Un hash criptográfico, es un algoritmo de encriptación de un solo sentido que sirve para proteger las contraseñas.

[7] SCARFONE, Karen, SOUPPAYA, Murugiah, Guide to Enterprise Password Management (Draft), National Institute of Standards and Technology (NIST), p. 14, Abril 2009

[8] SHAY, Richard J., BHARGAV-SPANTZEL, Abhilasha, BERTINO, Elisa, Password Policy Simulation and Analysis, ACM digital library, p .2, Noviembre 2007

[9] Securosis es la firma líder independiente en el mundo en asesoría e investigación en seguridad

- ✓ Destrucción física: Completar la destrucción física de los dispositivos de almacenamiento, centrándose en la trituración de los medios magnéticos actuales (discos o cintas).

- Descubrir contenido.
  Cuando los datos sensibles verdaderamente alcanzan el fin de su ciclo de vida, se debe asegurar que la información destruida, es realmente destruida. Use herramientas para descubrir contenido como ayuda para asegurarse que no existen copias o versiones de la información que se mantengan accesibles en la empresa [22].

III. POLÍTICA SUGERIDA PARA LA GENERACIÓN DE CONTRASEÑAS

Generación de contraseñas.

Para garantizar la seguridad de una contraseña se podría crear una clave con una letra mayúscula, un número entre 6 y 43 divisible por 7, y que incluya por lo menos un diptongo, pero no tendría la usabilidad necesaria para un usuario normal, por tal motivo, se deben realizar contraseñas con características especiales para que sean más fáciles de emplear por un usuario final.

A partir del uso del método de la mnemotecnia, se selecciona una frase con la que se sienta cómodo, y se realiza el tratamiento para la generación de las contraseñas como se mencionó anteriormente, pero adicional a ello, debe tener las siguientes características:

- No se pueden repetir las últimas 6 contraseñas utilizadas.
- La longitud de la contraseña debe ser máximo 15 caracteres y mínimo 8
- **Sintaxis**
  - ✓ La contraseña debe contener caracteres de la [a-z]
  - ✓ La contraseña debe contener caracteres de la [A-Z]
  - ✓ La contraseña debe contener números del [10-99]
  - ✓ La contraseña debe contener caracteres no alfanuméricos [# $ & %]
    - Ejemplo de contraseña: 33MupMq@v$
  - ✓ No debe derivarse de algún tipo de información personal como la dirección o la cédula.
  - ✓ No debe generarse de ninguna palabra de diccionario.
  - ✓ No debe generarse del nombre de algún pariente
- Se debe cambiar la contraseña cada 120 días OBLIGATORIAMENTE y debe aparecer un aviso 30 días antes de que caduque para que el usuario tenga tiempo de realizar el cambio.
- Si la contraseña no es cambiada en el tiempo estipulado, el administrador generará una nueva.
- Una vez seleccionada una contraseña se debe emplear el uso de aplicaciones como las mencionadas durante el desarrollo de este documento, para corroborar la seguridad de las mismas.

Distribución de claves

La distribución de claves es de gran importancia ya que en ese proceso pueden haber problemas de seguridad, en especial cuando estas viajan por redes externas a la organización para proveer autenticación entre hosts, pero a pesar de que los datos que viajen por esta infraestructura pueden tener las medidas necesarias de protección lógica, pueden haber problemas físicos como: filtrado de información, sniffing, un hombre en el medio, o si son por redes inalámbricas alguien con una antena de gran potencia podría estar recepcionando esta información, estos son problemas que surgen a nivel organizacional, pero la pregunta que surge es ¿Qué consideraciones debe tener en cuenta un usuario a la hora de recibir su contraseña, y como entregárselas de manera confiable sin que se pierda la confidencialidad?

1. Envío de contraseñas por correo electrónico, al que se responderá una vez recibida con la firma digital[10].

2. A través de una línea telefónica, se debe tener en cuenta que la línea sea segura y nadie más pueda estar escuchando esta conversación, se solicitará al usuario devolver la llamada para confirmar algunos datos para dar veracidad de la autenticidad de que es el legítimo dueño de la cuenta para asignarle la contraseña.

Una vez recibida la contraseña, hay factores que se deben tener en cuenta como:

[10] Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

1. Estar atento al entorno
   Si bien se considera al factor humano como el eslabón más débil en la cadena de seguridad, la causa de estas fallas, es debido a problemas de distracción. Cuando se reciba la contraseña, se debe tener especial atención a quien está alrededor, quien mira, quien está demasiado interesado en ayudar, etc.

2. No dejar el correo abierto
   Esto puede sonar obvio, pero en un descuido alguien podría ver su correo y darse cuenta de su contraseña.

Estas son recomendaciones simples pero que, si bien no se toman en cuenta, pueden convertirse en riesgos y volverse en grandes vulnerabilidades para la seguridad de la compañía.

Recuperación

Proteger la confidencialidad de una cuenta a la hora de recuperar una contraseña es muy importante ya que se deben generar mecanismos que garanticen la autenticidad del usuario como:

- Verificar vía electrónica que el cambio o recuperación de contraseña si es solicitado por el dueño de la cuenta y de igual manera responder con firma digital.

- Generar preguntas para recuperar contraseñas con un elevado grado de complejidad y que puedan ser formuladas por el mismo usuario, por ejemplo ¿Cuándo le propuso matrimonio a su actual pareja? O ¿Qué tic tiene su madre cuando se enoja?, preguntas que solamente el dueño de la cuenta pueda saberlas o que alguien con demasiada confianza pero que no sea parte de la organización sepa, y no generar preguntas del tipo ¿Nombre de la madre? O ¿Cuál es su comida favorita? Ya que estas son preguntas bastantes obvias y cualquier persona que tenga un ligero conocimiento del usuario podría responder

Uso

El uso de las contraseñas debe ser de carácter confidencial y personal, lo cual ayudará a prevenir malos entendidos y futuros inconvenientes.

A continuación se presentan unas consideraciones a tener en cuenta propuestas por el SANS Institute[11] [23]:

- No revelar su contraseña ni a sus familiares más cercanos.

- No use la misma contraseña que utiliza en la organización en otras cuentas como Gmail, Outlook, Yahoo, entre otras.

- No darle conocimiento de su contraseña a compañeros en caso de que realice un viaje.

- No revelar su contraseña a alguna entidad, a sus jefes o colaboradores, salvo que sea para realizar auditorías.

- No revelar la contraseña por teléfono.

- No hable de las contraseñas en frente de otros.

- No escriba contraseñas en formularios, por más confiables que estos le parezcan.

Almacenamiento

Una vez la contraseña es creada y entregada, esta debe ser memorizada o en su defecto almacenada, pero para ser almacenada se deben tener ciertos cuidados. Los que se presentan a continuación también son proporcionados por el SANS Institute:

- No revelar la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.

- En caso de ser autorizado por la administración para enviar la contraseña por correo electrónico, esta debe ser encriptada y nunca ser enviada en texto plano.

- Nunca escribir la contraseña en papel y guardarla. Tampoco almacenar contraseñas en ficheros de ordenador sin cifrar o desprovisto de algún mecanismo de seguridad.

- No utilizar la característica de "Recordar Contraseña" existente en algunas aplicaciones (Firefox, Internet Explorer, google chrome).

Terminación

Al terminar el ciclo de vida útil de una contraseña, los usuarios deben:

- Cambiar su contraseña por una nueva.

- Borrar la contraseña de todo sitio donde este almacenada (USB, correo, computador, etc)

RECOMENDACIONES

Se deben realizar capacitaciones constantes con los usuarios finales para concientizarlos de la importancia de la seguridad

[11] SANS es la fuente más grande y confiable de formación en seguridad del mundo.

de la información y de esta manera prevenir riesgos en la organización.

Las vulnerabilidades presentadas en las organizaciones en cuanto al manejo de las contraseñas no son causadas únicamente por la generación de estas, sino también por los malos manejos que realizan los usuarios de ellas.

Se deben generan políticas que garanticen el cumplimiento de estas normas y que no sean solamente recomendaciones y uso de buenas prácticas.

Existen muchas herramientas para la generación de contraseñas seguras pero que pueden ser de difícil aprendizaje para el usuario, sin embargo, también hay herramientas que permiten corroborar la fortaleza de una contraseña una vez ha sido creada con las políticas acá presentadas.

REFERENCIAS

[1] http://www.rediris.es/cert/doc/unixsec/node14.html (Visitado el 12 de Agosto de 2012)

[2] FRAGKOS, Grigorio, TRYFONAS, Theodore, A Cognitive Model for the Forensic Recovery of End-User Passwords , IEEE Xplore digital library, Digital Forensics and Incident Analysis, 2007, p. 1, (Visitado el 12 de Agosto de 2013)

[3] http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestion-de-claves/32-tipos-de-claves (Visitado el 13 de Agosto de 2013)

[4] http://www.ecured.cu/index.php/Algoritmo_criptogr%C3%A1fico (Visitado el 12 de Agosto de 2013)

[5] http://uvfdatabases.wordpress.com/2009/02/07/tipos-de-usuarios-de-la-base-de-datos (Visitado el 12 de Agosto de 2013)

[6] http://revistaitnow.com/2013/05/seguridad/el-eslabon-mas-debil-de-la-cadena-en-seguridad-es-el-usuario (Visitado el 12 de Agosto de 2013)

[7] FRENZ, Christopher M, Improving Organizational Password Policy Compliance via Open Source Tools, 2011 IEEE World Congress on Services (SERVICES), p.1 (Visitado el 1 de Agosto de 2013)

[8] HOUSHMAND, Shiva, AGGARWAL, Sudhir, Building better passwords using probabilistic techniques, ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference 2012 (Visitado el 1 de Agosto de 2013)

[9] INTECO, instituto nacional de tecnologías, gestion_de_contrasenas, p. 9-14 (Visitado el 1 de agosto de 2013)

[10] http://www.segu-info.com.ar/proyectos/p1_algoritmos-basicos.htm (Visitado el 12 de Agosto de 2013)

[11] BLOCKI, Jeremiah, KOMANDURI, Saranga, PROCACCIA, Ariel D, SHEFFET, Or, Optimizing Password Composition Policies, EC '13 Proceedings of the fourteenth ACM conference on Electronic commerce 2013 (Visitado el 1 de Agosto de 2013)

[12] FORGET, Alain, CHIASSON, Sonia, BIDDLE, Robert, Helping Users Create Better Passwords: Is this the right approach?, SOUPS '07 Proceedings of the 3rd symposium on Usable privacy and security 2007 (Visitado el 1 de Agosto de 2013)

[13] SHAY, Richard J., BHARGAV-SPANTZEL, Abhilasha, BERTINO, Elisa, Password Policy Simulation and Analysis, DIM '07 Proceedings of the 2007 ACM workshop on Digital identity management (Visitado el 1 de Agosto de 2013)

[14] VILLARUBIA, Carlos, FERNÁNDEZ-MEDINA, Eduardo, PIATTINI, Mario, Quality of Password Management Policy, Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on Availability, Reliability and Security. (Visitado el 1 de Agosto de 2013)

[15] KOMANDURI, Saranga, SHAY, Richard, GAGE KELLEY, Patrick, MAZUREK, Michelle L., BAUER, Lujo, CHRISTIN, FAITH CRANOR, Lorrie, EGELMAN, Serge, Of Passwords and People: Measuring the Effect of Password-Composition Policies, CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2011 (Visitado el 6 de Agosto de 2013)

[16] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html (Visitado el 2 de agosto de 2013)

[17] INTECO, instituto nacional de tecnologías, politica_contrasenas, p. 4-5 (Visitado el 1 de agosto de 2013)

[18] http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestion-de-claves/33-generadores-y-distribucion-de-claves/333-distribucion-de-claves
(Visitado el 5 de agosto de 2013)

[19] http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestion-de-claves/31-politicas-de-gestion-de-claves?showall=&start=1
(Visitado el 5 de agosto de 2013)

[20] SCARFONE, Karen, SOUPPAYA, Murugiah, Guide to Enterprise Password Management (Draft), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930 April 2009, p. 24-25 (Visitado el 5 de agosto de 2013)

[21] http://www.iec.csic.es/criptonomicon/seguridad/claves.html (Visitado el 8 de agosto de 2013)

[22] https://securosis.com/tag/information-centric+security (Visitado el 8 de agosto de 2013)

[23] SANS Institute, Password Policy - http://www.sans.org/security-resources/policies/Password_Policy.pdf, p. 2 (Visitado el 14 de Agosto de 2013)