

# LAS PEORES PRÁCTICAS EN CONTRASEÑAS

Basado en Artículo de Imperva “Las Peores Prácticas en Contraseñas : Latinoamérica”

Diego Samuel Espitia Montenegro <dsepitia@gmail.com>

Agosto de 2010

## Resumen

*Debido a una vulnerabilidad detectada y explotada por un criminal electrónico que uso la SQL injection sobre el sitio rockyou.com, se lograron extraer 32 millones de contraseñas, brindando un volumen de información que nunca antes se había tenido y que permite un análisis detallado sobre las características que los usuarios más usan en las contraseñas, en Latinoamérica.*

Teniendo en cuenta que nunca se había tenido tal cantidad de contraseñas del mundo real, fue una oportunidad que el Centro de Defensa de Aplicaciones (ADC) de la empresa Imperva no pudo dejar pasar y aprovechó para realizar un análisis a profundidad de las características que los usuarios usan para crear sus contraseñas, que son en algunos casos el único medio de protección para salvaguardar datos muy privados.

Usando como muestra las contraseñas que se encontraron en español y las combinaciones alfanuméricas usadas en todo el mundo, se tiene una base de 1.830.196 contraseñas que se pueden catalogar como hispanoparlantes y son la base sobre la cual se realizó el estudio.

Los datos encontrados no son nada favorables para los usuarios desde el punto de vista de la seguridad, ya que las características de las contraseñas analizadas no provee un buen grado de seguridad en contra de piratas informáticos, que con unos conocimientos no muy altos puedan acceder a la información que estas protegen. Esto se puede deducir a partir de un análisis de lo encontrado, donde la mayoría de las contraseñas son muy cortas y de contenidos muy simples, permitiendo que con un ataque

sencillo se encuentren las contraseñas del usuario.

Los principales problemas que se han detectado es el mal uso de las contraseñas por parte de los usuarios, ya que no tienen en cuenta que en la actualidad son la puerta de acceso a la mayoría de los servicios informáticos que ellos usan, tales como correo electrónico, sistemas operativos, mensajería instantánea, redes sociales y demás.

Este mal uso hace que para los criminales informáticos sea de gran utilidad obtener la mayor cantidad de contraseñas de todo este tipo de sistemas, basándonos en un estudio realizado por los laboratorios de ESET<sup>1</sup> en latinoamericana se encontró que el 15% de los usuarios nunca modifica su contraseña y más del 60% de los consultados cambia la contraseña menos de una vez al año (Figura1)

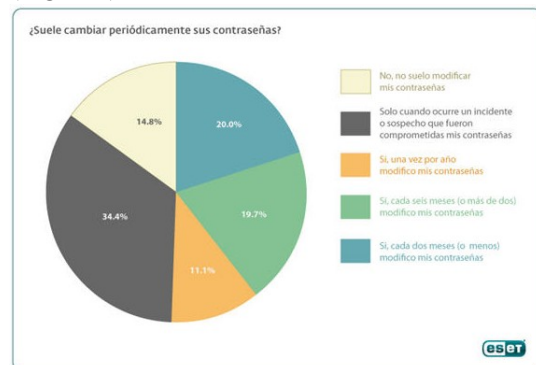


Figura 1. Cambia usted periódicamente sus contraseñas

Teniendo en cuenta esta información de ESET y los datos entregados en el informe de Imperva, podemos ver cómo este comportamiento no ha variado en muchos años, lo que ha sido demostrado en múltiples estudios de Unix, de tech herald, hotmail, entre otros

Este comportamiento es inducido por una mala gestión por parte de la mayoría de

<sup>1</sup> <http://blogs.eset-la.com/laboratorio/2010/08/18/cuidan-los-usuarios-sus-contrasenas/>

administradores, pues no se aplican los controles y restricciones que las nuevas tecnologías permiten para el control de contraseñas, tales como políticas de contraseñas seguras, caducidad de las contraseñas, detección activa de ataques a contraseñas, entre otras que analizaremos más adelante.

Esta permisividad de los administradores permite que los usuarios usen contraseñas simples por facilidad y desconocimiento de los riesgos que implica, no sólo para sus datos personales sino para las organizaciones a las que pertenecen.

### ***Análisis de las Contraseñas en Español***

Revisando los resultados del análisis sobre las contraseñas en español se pueden evidenciar y catalogar las características de su composición en unas categorías muy específicas, donde la más predominante es el uso de nombres ocupando el 48% de las preferencias de los usuarios, con una leve tendencia en preferir los nombres femeninos a los nombres masculinos.

Esta tendencia es muy típica en países latinoamericanos donde los principales consumidores de servicios de informáticos son los hombres y para este tipo de usuarios es más sencillo recordar datos como el nombre de su madre, esposa o hija, o en su defecto la forma cariñosa en que llama a alguna de estas mujeres, generando la preferencia de nombres femeninos en las contraseñas.

Las categorías principales en las que se pueden caracterizar las contraseñas usadas en el 1'8 millones de contraseñas encontradas en español son las siguientes

- Nombre de Personas (48%)
- Secuencias de Teclado (23%)
- Cosas Favoritas (17%)
- Términos Cariñosos (8%)
- Términos Computacionales (2%)
- Términos Religiosos (2%)

Como se puede apreciar de forma gráfica en la Figura 2, mostrada a continuación



***Figura 2. Categorías de contraseñas Latinoamericanas***

En las secuencias del teclado se mantiene la tendencia mundial de uso de solo números en las contraseñas siendo la más usada “123456” y el “abc123” que son las más comunes en cualquier idioma.

Siguiendo con las características propias de los países latinoamericanos, una de las cosas favoritas más usadas como contraseñas son los nombres de los equipos de fútbol, tales como América, Arsenal, Barcelona, entre otros. Las otras cosas favoritas más usadas son superhéroes y marcas de productos.

En la cuarta categoría se encuentran los términos cariñosos donde se mantiene la tendencia del género femenino y le siguen las palabras de amor compuestas, tales como teamo, tequiero, y miamor.

Las últimas categorías son términos de informática y términos religiosos, donde se refleja el uso de los términos más comunes de cada una de éstas tales como contraseña, hotmail, jesus, angel, entre otros. De esta manera se puede ver cómo las culturas y creencias de los pueblos latinoamericanos son bien definidas y muy arraigadas en las personas.

### ***Comparación con las Recomendaciones***

Ya tomando el total de 32 millones de contraseñas el Centro de Defensa de las Aplicaciones (ADC) usó los parámetros de seguridad entregados por la NASA en la sección 8 de la comunicación técnica SP800-

47<sup>2</sup> de Noviembre de 2007, donde se marcan cuatro características que como mínimo todas las contraseñas deben cumplir.

La primera recomendación indica que la longitud mínima de la contraseña es de 8 caracteres, lo cual sólo lo cumple el 49.8% de las contraseñas analizadas en el estudio. Ésto comprueba que restricciones como la de rockyou.com de un mínimo de 5 caracteres en la contraseña permite que los usuarios cometan errores que ponen en riesgo la seguridad de sus datos.

La segunda recomendación indica cómo debe ser la composición de la contraseña, la cual debe tener letras mayúsculas, minúsculas, números y caracteres especiales. El análisis sobre esta recomendación entregó datos alarmantes, demostrando que casi en la totalidad de las contraseñas usan un conjunto bastante limitados de combinaciones entre los tipos de caracteres, con un 41.69% que solo usa letras minúsculas y solo el 3.81% usan caracteres especiales.

La tercera recomendación indica que el contenido de las contraseñas no se debe encontrar directamente en ningún diccionario, ni ser una palabra común, ni incluir fragmentos de éstas o datos personales del usuario, más del 20% de las contraseñas utilizadas no cumplían esta recomendación.

La cuarta recomendación de la NASA no pudo ser analizada en este estudio pues indica que la frecuencia con la que se debe modificar la contraseña es de mínimo cada 90 días. Pero en la figura 1 se muestra, gracias al análisis realizado por ESET, que ésta no se cumple en Latinoamérica.

Estas comparaciones muestran un crítico panorama sobre el cumplimiento de las buenas prácticas recomendadas por la industria, demostrando la falta de conocimiento por parte de los usuarios y la falta de control por parte de los administradores.

En el análisis realizado por el Centro de Defensa de las Aplicaciones usaron una lista de las 5000 contraseñas mas usuales en las listas de ataque por diccionario usadas por los piratas informáticos para hacer una laboratorio de un ataque simulado contra estos 32 millones de contraseñas, descubriendo que con solo esta lista de 5000 se habrían comprometido la seguridad del 20% de las cuentas y en menos de 17 minutos se tendría el control de 1000 cuentas.

En la figura 3 se ve cual es el porcentaje de cuentas comprometidas contra el número de contraseñas probadas, y se puede apreciar la efectividad del ataque es exponencial, donde una vez se va aumentando la cantidad de contraseñas probadas va disminuyendo el número de cuentas comprometidas y donde en el primer tercio de la muestra se compromete la mayor cantidad.

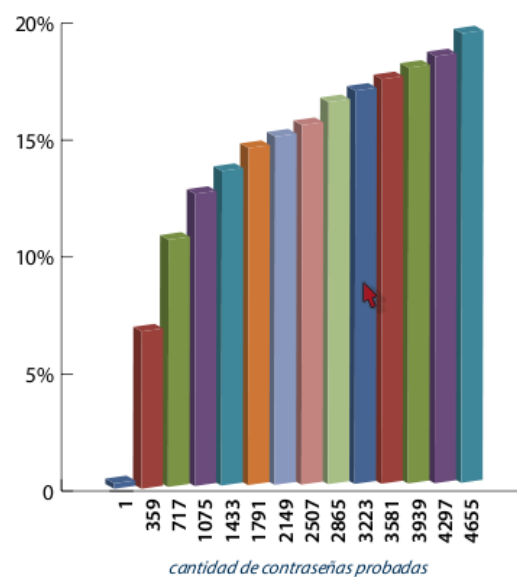


Figura 3. Resultados de ataque por diccionario

## Conclusiones

Los administradores de los diferentes sistemas deben hacer cumplir las políticas de contraseñas seguras, evitando que los usuarios tengan la capacidad de decidir características que no cumplan con las buenas prácticas establecidas por la industria.

2 [http://www.nisn.nasa.gov/DOCUMENTS1/ONet\\_Security\\_Policy.pdf](http://www.nisn.nasa.gov/DOCUMENTS1/ONet_Security_Policy.pdf)

Por medio de los avances en la tecnologías de seguridad, existen diversas herramientas que, complementadas con una correcta concienciación y educación a los usuarios permiten incrementar la confiabilidad de las contraseñas, no solo en su composición sino en su uso y transmisión.

Los usuarios deben ser conscientes de los riesgos que se generan para sus datos personales y para las organizaciones a las que pertenecen, cuando el único sistema que puede proteger sus datos de intrusiones no permitidas es débil y no cumple con unos niveles mínimos de seguridad.

El no cumplimiento de los parámetros de seguridad de las contraseñas en su composición y transmisión, facilita a los piratas informáticos comprometer un número muy alto de cuentas con unos ataques relativamente sencillos.