Auditoría de Stone Tech Unity State

Gabriel Torres

Facultad de Informática, Instituto Universitario Mario Briceño Iragorry

I53: Auditoría de Sistemas

Ingeniera Kerly Hernández

05 de agosto de 2022

Índice

Introducción

Los imparables avances de la tecnología en el mundo actual crean un amplio abanico de peligros y problemas para la seguridad de la información y el funcionamiento de un servicio, afectando empresas, organizaciones e individuos particulares. Con el fin de poder anticiparse a estas amenazas y detectar fallos antes que ellas, nace la auditoría de sistemas que analiza el sistema en busca de posibles vulnerabilidades que puedan comprometer el sistema o procesos innecesarios que entorpezcan el funcionamiento el software.

Normalmente, los entes que más hacen uso de las auditorías informáticas son las empresas, pues las mantiene a la par del mundo actual proveyendo información valiosa sobre las fallas en el sistema y ayuda a resolver cualquier incidencia que se presente, todo ello a través del uso de informes de auditoría, planes de auditoría y controles internos. Con el fin de demostrar cómo luce tal documentación, se realizará la misma basándose en una compañía que perdió llaves del registro imposibilitando la gestión de los usuarios en su software.

Planeación

Al ejecutar cualquier tipo de acciones con el fin de obtener algo a cambio, es necesario llevar a cabo una planeación que pavimente el camino por el que se transitará para conseguir este fin. Por tanto, primero se han de definir los objetivos de la auditoría, la metodología a usar, la metodología de auditoría de la aplicación y el plan de auditoría.

Objetivos

Objetivo General

Auditar el sistema y hallar la razón que dificulta la gestión de los usuarios.

Objetivos específicos

- Hallar el error que causa el problema en el sistema.
- Dar recomendaciones sobre la solución del problema.
- Informar de las vulnerabilidades halladas.

Metodología

En el mundo empresarial, la realidad que las compañías experimentan suele ser dinámica, abarcando problemas imprevistos. Por ende, para hacer frente a cualquier incidente imprevisto, las metodologías ágiles surgen como los marcos más óptimos para manejar la auditoría de estas situaciones por su flexibilidad y adaptabilidad. En este orden de ideas, el incidente que imposibilita la gestión de los usuarios, será auditado aplicando la metodología SCRUM.

SCRUM es un marco de trabajo basado en los principios de las metodologías agiles, cuyo flujo de trabajo se realiza en un periodo llamado sprint que consta de 4 pasos para sacarle el mayor provecho al mismo. El primer paso es la planificación del sprint, en el que se definen las tareas que podrían ser realizadas durante el sprint; el segundo paso se llama scrum diario que, en síntesis, es una reunión breve para informar sobre cualquier inconveniente e informar sobre los

avances realizados; el tercer paso es la revisión del sprint en el cual se presentan los trabajos culminados y por último, el cuarto paso llamado retrospectiva del sprint, recoge las impresiones de los miembros del equipo sobre el sprint finalizado para mejorar el siguiente.

Metodología de auditoría de la aplicación

Programa de revisión

1. Obtener toda la información relacionada a la incidencia que exigió la auditoría.
2. Determinar el objetivo y el alcance de la auditoría.
3. Obtener información detallada sobre el funcionamiento del sistema. Se realiza con entrevistas y cuestionarios al personal implicado en el sistema, el análisis de la documentación y de todos los aspectos del sistema.
4. Identificación de los posibles puntos críticos del sistema relacionados a la incidencia apoyándose en la información obtenida sobre el mismo.
5. Creación de los procedimientos que serán usados en la auditoría para probar los puntos críticos.
6. Ejecución de pruebas en los puntos críticos haciendo uso de los procedimientos creados.
7. Entrega del informe de auditoría con los respectivos hallazgos.

Plan de auditoría

Fecha	04/08/2022
Objetivo	Hallar la razón de la incidencia en el sistema.
Alcance	Se ejecutará la auditoría en el área IT evaluando el software que gestiona los usuarios y el sistema donde se encuentra alojado el mismo.
Criterios	ISO 9001. Sistemas de gestión de la calidad.
Equipo auditor	Gabriel Alejandro Torres Mendoza. Auditor jefe.

Fecha de ejecución de la auditoría	04/08/2022
Reunión de apertura	04/08/2022 a las 9:55 PM
Reunión de Cierre	04/08/2022 a las 11:30 PM

Actividad	**Área a auditar**	**Auditor**	**Fecha**	**Hora**
Reunión de apertura		Auditor jefe	04/08/2022	9:55 – 10 PM
Análisis del sistema	Departamento de informática	Auditor jefe	04/08/2022	10 – 10:30 PM
Determinación de puntos críticos	Departamento de informática	Auditor jefe	04/08/2022	10:30 – 11 PM
Ejecución de pruebas en los puntos críticos	Departamento de informática	Auditor jefe	04/08/2022	11 - 11:30 PM
Reunión de Cierre			04/08/2022	11:30 – 11:59 PM

Control interno

Con el fin de facilitar la realización de la auditoría, se recurren a acciones manuales y/o automáticas cuyo fin es prevenir y corregir errores o irregularidades en el sistema, las cuales reciben el nombre de control interno.

Controles de preparación de datos

- Crear un manual de usuario para que los usuarios realizan los procedimientos adecuados dentro del sistema.

- Chequear que los usuarios reciban la inducción necesaria para usar la terminal.
- Revisar los procedimientos para solventar cualquier incidencia
- Determinar la cantidad total de usuarios de control por la terminal.
- Comprobar que la cantidad de usuarios de control por terminal sean igual de entrada que de salida.
- Comprobar la existencia de un respaldo apropiado para cualquier incidencia.

Controles de entrada a la aplicación

- Revisar los logs del sistema para determinar si existe algún intruso o un fallo.
- Comprobar si los usuarios revisan las tablas internas del sistema regularmente.
- Revisar los procedimientos para corregir errores.
- Registrar los datos de elementos críticos en el sistema.
- Revisar los procedimientos de validación internos del sistema.

Controles de salida a la aplicación

- Determinar si los informes listados son evaluados apropiadamente para hallar errores evidentes.
- Asegurarse de que los informes que ya no sean aplicables, sean destruidos totalmente.
- Asegurarse de revisar los informes pasados que tengan incidencias similares a la actual.
- Verificar que los periodos de retención de informes existan y se sigan rigurosamente.
- Verificar que se identifican los informes siguiendo los parámetros apropiados.

Seguridad en aspectos físicos y en aspectos técnicos de la aplicación

- Asegurarse de concientizar al personal del uso adecuado de los sistemas.
- Crear planes de contingencia ante cualquier incidencia.

- Usar dispositivos que monitoreen el sistema y la empresa con el fin de detectar cualquier irregularidad.
- El acceso al sistema interno debe estar protegido por varias capas de validación.
- Crear normas que regulen el acceso a los recursos informáticos.
- Crear un grupo encargado de la seguridad de la información.

Controles generales organizativos

● Plan estratégico de información

- Usa softwares que monitorizan constantemente las entradas y salidas de los usuarios en el sistema.
- Usa sistemas que realizan respaldos constantes de la información del sistema interno.

● Plan informático

- Constante mejoramiento de la integridad del sistema.
- Crear una documentación detallada del sistema.

● Plan general de seguridad

- Tener personal calificado y de confianza usando el sistema.
- Mantener un respaldo de toda la información del sistema.
- Poseer varias capas de seguridad para evitar infiltrados.
- Chequeos constantes del sistema para hallar vulnerabilidades.

● Plan de emergencia ante desastres que garanticen la disponibilidad de todos los sistemas informáticos ante eventos.

- Recurrir al equipo de gestión de incidencias.

- Mantener toda la documentación sobre los problemas ocurridos con el fin de consultarla en el futuro.

Talento humano de la aplicación

Gabriel Torres, auditor de sistemas.

Informe de hallazgos

Organización: Stone Tech Unity State	
Auditor: Gabriel Torres	**Docente evaluadora:** Kerly Hernández
Ciudad: Valera, estado Trujillo	**Fecha emisión del informe:** agosto 4, 2022

Descripción de auditoría

Alcance	Aplica al software encargado de gestionar los usuarios y el sistema en el que se encuentra alojado.		
Objetivo	Hallar la razón de la incidencia que no permite gestionar los usuarios en la plataforma.		
Documentos de referencia	Normas ISO 9001-2015 y procedimientos aplicables.		
Criterios de auditoría	No conformidad y acción correctiva establecidos dentro de la norma ISO 9001-2015		
Tipos de auditoría	Auditoría interna		
Fecha de ejecución	Jueves, 04 de agosto de 2022	Plan de auditoría anexo	
Reunión de apertura	Jueves, 04 de agosto de 2022		
Reunión de cierre	Jueves, 04 de agosto de 2022		
Entrega del informe	Jueves, 04 de agosto de 2022		
Equipo auditor	Torres, Gabriel		
Auditor líder	Torres, Gabriel	**Email**	Gabrieltorres2014@gmail.com

Conclusiones del equipo auditor

Principales anotaciones
• La reunión de apertura se realizó con urgencia el mismo día de la auditoría y duró 5 minutos. Esto debido a que hallar la razón al problema de gestionar usuarios en el sistema es de suma importancia. • La auditoría interna se realizó el día jueves 04 de agosto del 2022 y su duración fue de 2 horas y 4 minutos. • La reunión de cierre y la entrega del informe, al igual que la de apertura, fue realizada el mismo día. Presentando en el informe los hallazgos respectivos a la incidencia y mejoras que se pueden llevar a cabo.
Hallazgos
Observaciones
Durante la realización de la auditoría, es posible observar que el acceso al editor de registros de la máquina no tiene ninguna capa de seguridad, facilitando que cualquier usuario haga lo que desee dentro de la máquina. Además, la compañía tiene personal que no es de confianza, puesto que un usuario con acceso, borró accidental o intencionalmente una registry key que permite gestionar los usuarios en el sistema. Se asume que fue un usuario dentro de la compañía con acceso al sistema, debido a que no se detectó ningún software malicioso.
Fortalezas
• Personal dispuesto a colaborar en los procesos necesarios para solucionar cualquier incidente en el sistema. • Se cuenta con un personal altamente capacitado que comprende a detalle el funcionamiento del software. • El tiempo de respuesta ante la incidencia fue óptimo.
Oportunidades de mejora
• Implementar medidas de seguridad más robustas al sistema. • Mejorar el proceso de selección de personal con el fin de que no perjudique a la compañía intencionalmente.

• Concientizar al personal sobre el uso del sistema.
Conclusiones
La realización de la auditoría fue exitosa. El incidente que convocó a la auditoría logró ser analizado exitosamente con rapidez, además, se logró encontrar vulnerabilidades en el sistema que aloja al software y en la estructura del personal de la compañía, lo cual servirá para implementar mejoras que aumenten la seguridad.

Distribución del informe de auditoría

El presente informe será distribuido a la profesora Kerly Hernández de Auditoría de Sistemas para su verificación.

Evidencias fotográficas

Figura 1

Captura de pantalla del visor de eventos de Windows advirtiendo la eliminación de una llave del registro.

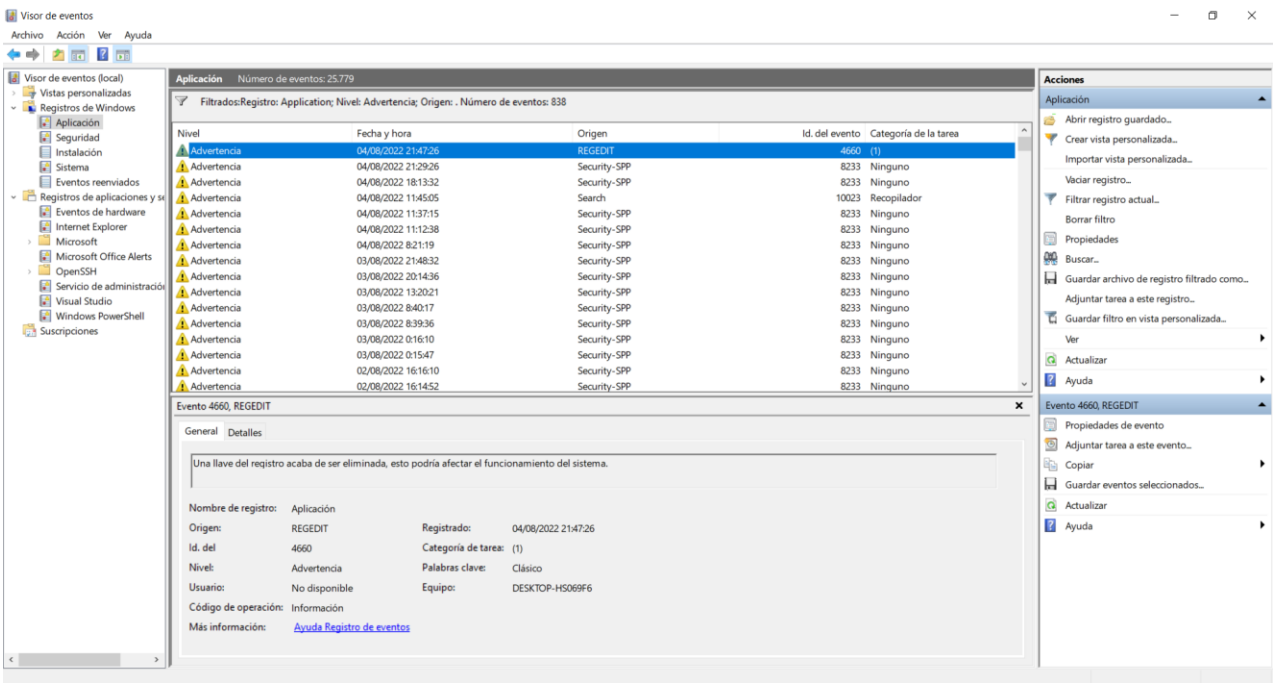


Figura 2

Captura de pantalla accediendo al editor de registro.

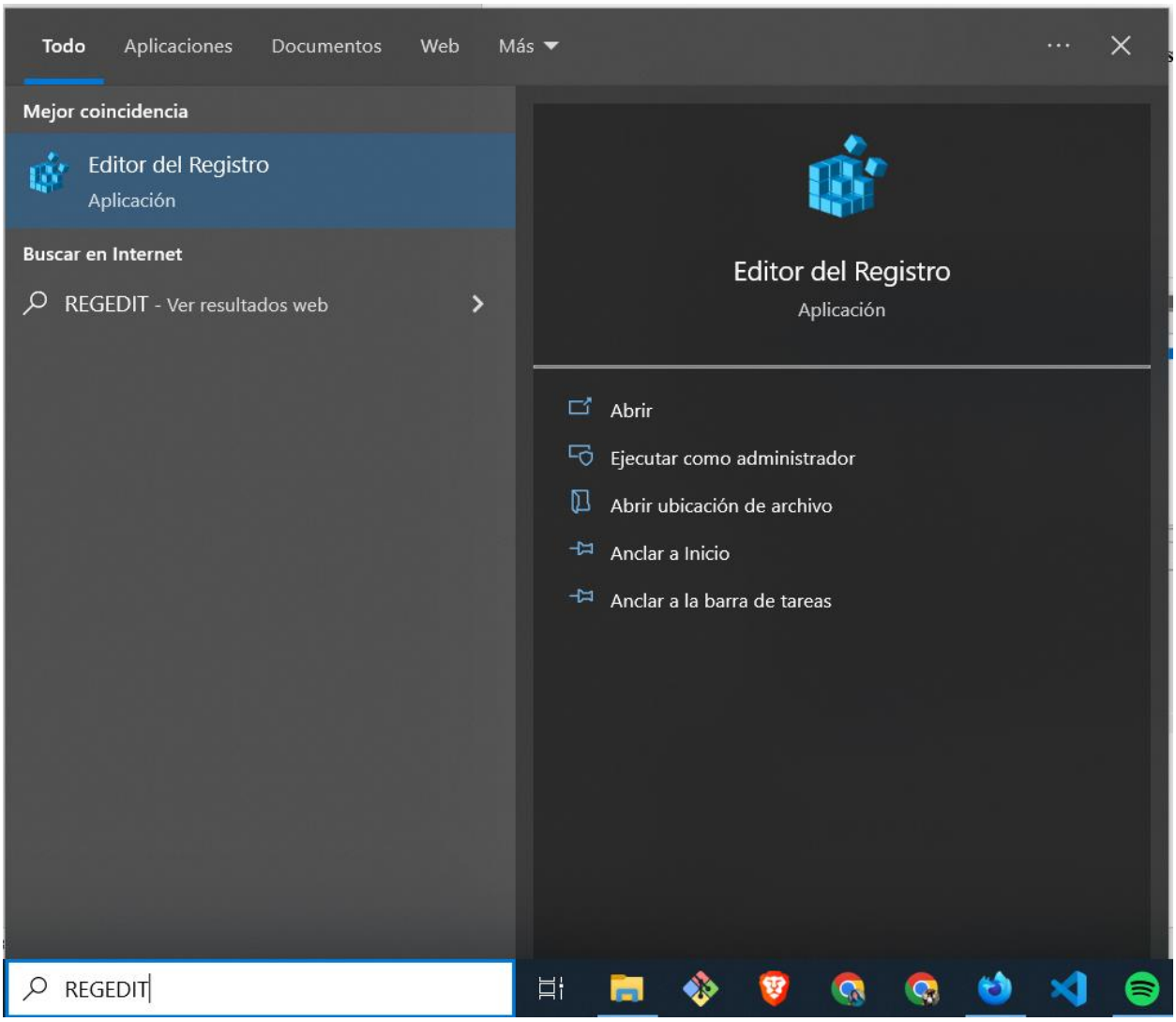


Figura 3

Captura dentro del editor del registro, en el registro del sistema de Stone Tech Unity State

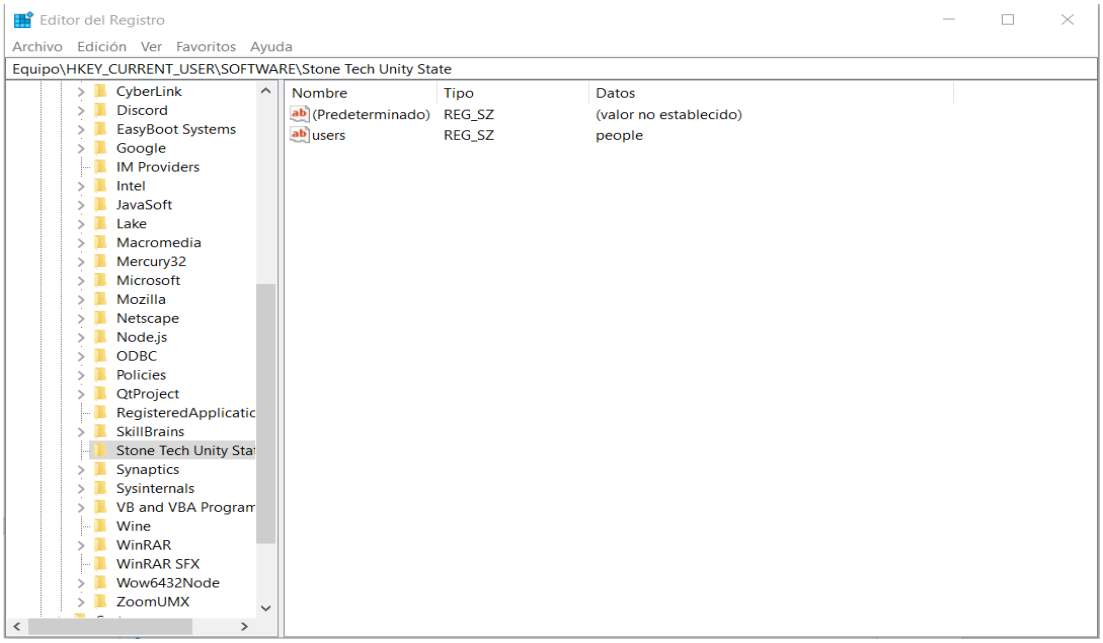


Figura 4

Captura creando una registry key de Stone Tech Unity State.

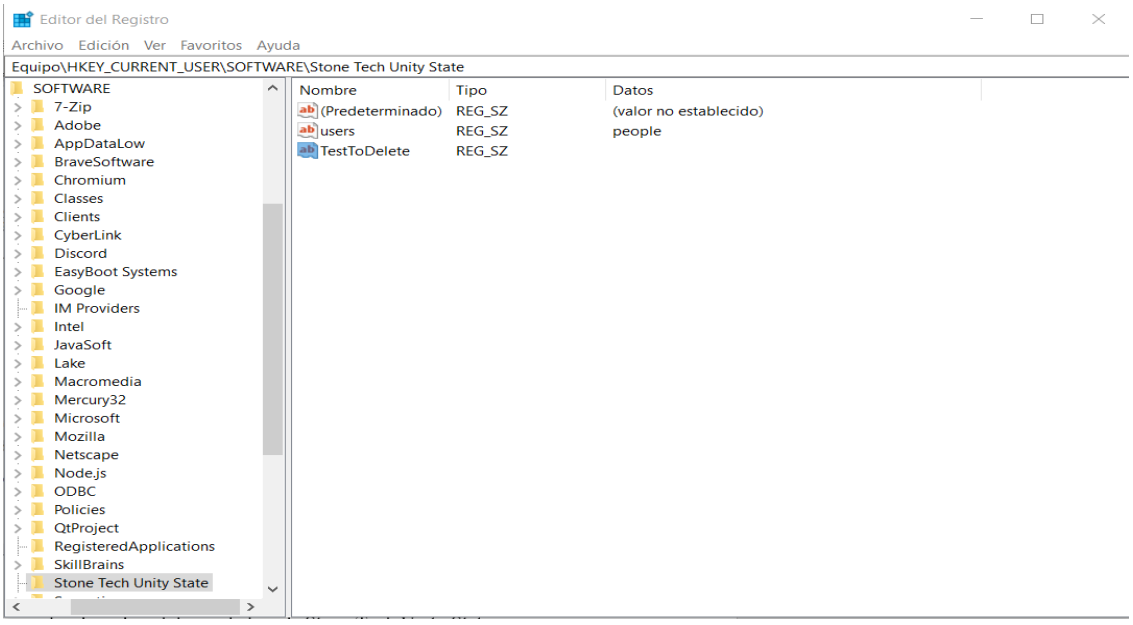


Figura 5

Captura borrando la registry key falsa sin ningún problema desde la máquina.

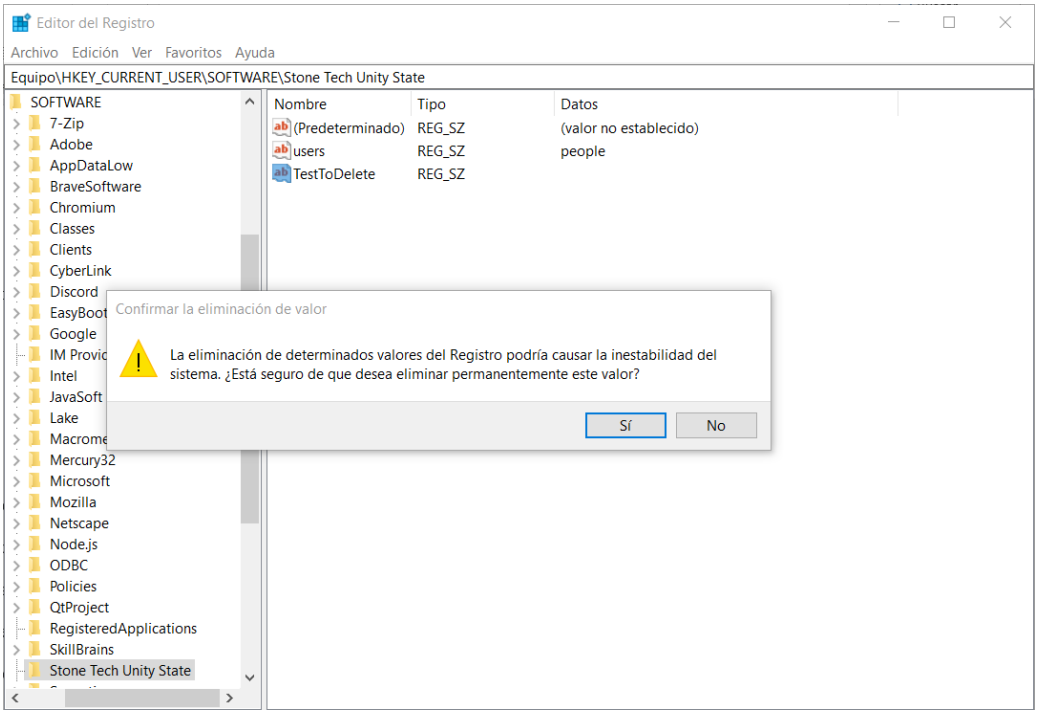
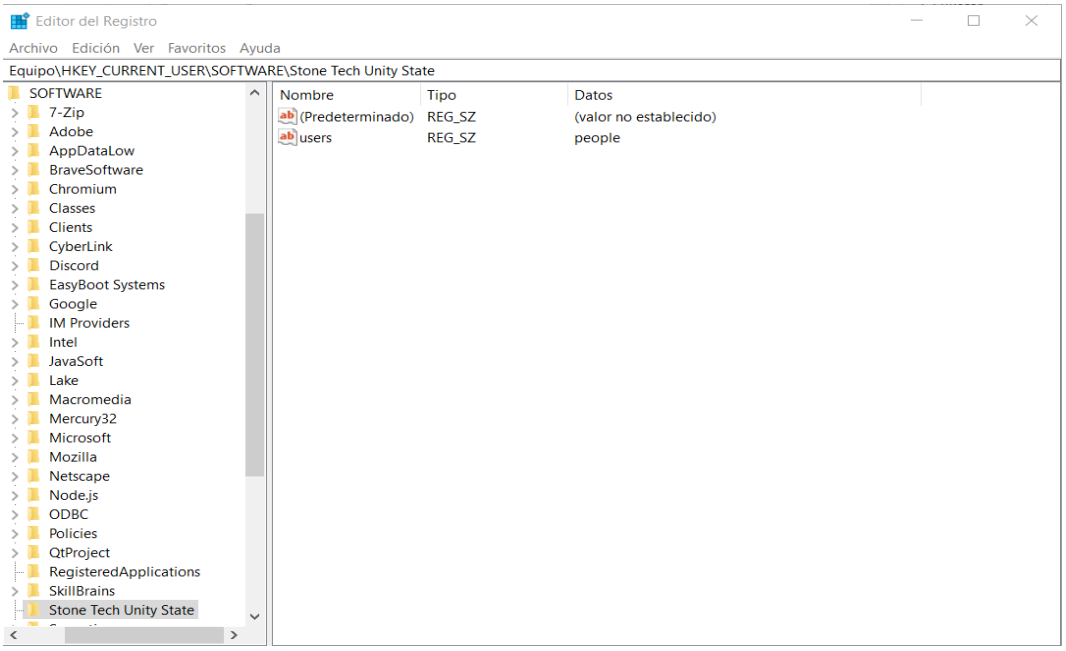


Figura 7

Captura del registro luego de haber borrado la registry key falsa sin dificultad.



Conclusión

Los elementos documentales que componen una auditoría de sistemas quedan lo suficientemente claros en el ejemplo expuesto de la compañía Stone Tech Unity State, aunque el problema fue relativamente fácil y el informe corto, en la realidad suelen ser más extensos, puesto que los problemas son más o más complejos. Por tanto, debido a lo extensa que puede ser la documentación, lo ideal como futuros posibles auditores es seguir aprendiendo sobre la auditoría de sistemas con el fin de facilitar mucho más el trabajo de los desarrolladores, aumentar las ganancias de la empresa y reducir los problemas que puedan afectar a la compañía y, por ende, a nosotros.