UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN

FRANCISCO XAVIER DE CHUQUISACA

FACULTAD DE TECNOLOGÍA

SIS (316)



TÍTULO DEL PROYECTO:

Ejercicio de un Proceso de Auditoría

ESTUDIANTES:

Tumiri Huanca Alex

Flores Torres Luis David

Vargas Lastra David

DOCENTE: Ing. Angel Hilmar Baspineiro Valverde

MATERIA: SIS (316)

**Sucre-Bolivia**

**Escenario o Caso de Estudio .-**

En nuestro anterior trabajo se realizó el estudio y auditoría de la redes de internet de hogar y las posibles amenazas como por ejemplo :

* **Wifiphisher (R1)**
* **MITM Wifi (R2)**
* **Secuestro de sesión (R3)**
* **Ataque de Queensland (R4)**
* **Espionaje (R5)**
* **Sniffing (R6)**
* **Spoofing (R7)**
* **Rogue APs (R8)**
* **Ataque de SSID falsos (R9)**
* **Denegación de servicio DOS (R10)**

Uno de los activos amenazados sería nuestra información personal, nuestra red, nuestro ancho de banda para ser específicos, el dinero invertido para tener el servicio y que el o los atacantes se beneficien de este servicio sin autorización alguna.

**Entendimiento de los riesgos relacionados y de las medidas relevantes de control.**

Matriz de Riesgos Resultante :

| IMPACTO DE PROBABILIDAD | DESPRECIABLE(1) | MARGINAL(3) | PROMEDIO(5) | CRÍTICO(7) | CATASTRÓFICO(10) |
| --- | --- | --- | --- | --- | --- |
| MUY ALTO(10) |  |  |  | R8 | R1, |
| ALTO(7) |  |  |  |  |  |
| NOMINAL(5) |  |  | R2, R6, R7 |  |  |
| BAJO(3) |  | R3, R9 |  |  |  |
| MUY BAJO(1) | R4, R10 |  | R5 |  |  |

Priorización de los Riesgos revisados :

| Amenaza | Probabilidad (P)  (1-10) | Justificación  consensuada de P | Impacto (I)  (1 a 10) | Justificación  Consensuada de I | Impacto Total  IT |
| --- | --- | --- | --- | --- | --- |
| R1 | 2 | Es una amenaza poco probable | 5 | Es una amenaza con riesgo medio | 10 |
| R2 | 1 | Es una amenaza poco probable | 6 | Es una amenaza con riesgo medio bajo | 6 |
| R3 | 4 | Es un ataque probablemente medio | 7 | Es una amenaza con riesgo medio alto | 28 |
| R4 | 7 | Es una amenaza comun | 5 | Es una amenaza con riesgo medio | 35 |
| R5 | 1 | Es una amenaza poco probable | 5 | Es una amenaza con riesgo medio | 5 |
| R6 | 6 | Es un ataque comun | 3 | Es una amenaza con riesgo bajo | 18 |
| R7 | 4 | Es una amenaza poco probable | 5 | Es una amenaza con riesgo medio | 20 |
| R8 | 4 | Es una amenaza poco probable | 8 | Es una amenaza con riesgo alto | 32 |
| R9 | 9 | Es una amenaza probablemente alta | 3 | Es una amenaza con riesgo bajo | 27 |
| R10 | 2 | Es una amenaza poco probable | 9 | Es una amenaza con riesgo alto | 18 |

**Objetivos de control asociados a cada riesgo (que efecto del control quiero obtener)**

| Amenaza | Control que se quiere obtener |
| --- | --- |
| R1 | Seguridad de que accedemos a la red wi fi correcta |
| R2 | Evitar el espionaje de nuestra información |
| R3 | Evitar el robo de nuestra información de nuestra sesión |
| R4 | Proteger y tener una conexión estable y segura a nuestra red |
| R5 | Seguridad de nuestra red física y router |
| R6 | Evitar la monitorización de nuestra red |
| R7 | Evitar la suplantación de identidad |
| R8 | Evitar los puntos de acceso no autorizados a nuestra red |
| R9 | Evitar la falsificación de puntos de accesos conocidos |
| R10 | Tener conexión 24/7 a nuestra red cuando se necesita |

**Medidas de Control a evaluar.(controles preventivos y correctivos identificados)**

| Amemanza | Controles Preventivos | Controles Correctivos |
| --- | --- | --- |
| R1 | Revisar que nuestra conexión wi fi sea legítima | Eliminar todos los puntos de accesos ilegítimos y proteger los legítimos |
| R2 | Cifrar nuestro mensaje e información en nuestra comunicación | Cambiar y proteger nuestra canal de comunicación de forma recurrente |
| R3 | No acceder a páginas web no seguras | Realizar periódicamente un análisis de virus y de malware a nuestro equipo |
| R4 | Evitar las peticiones constantes que sobrecarguen nuestra red | Reiniciar y restablecer la configuración por defecto de nuestro Router |
| R5 | Tener un ambiente seguro para nuestra red | Cambiar la localización de nuestros puntos de acceso |
| R6 | Revisar que nuestra red no sea monitorizada | Eliminar a los usuarios desconocidos de la red |
| R7 | Revisar los parámetros de nuestra red que permanezcan seguros | Restablecer la configuración de parámetros de nuestra red por defecto |
| R8 | Denegar puntos de acceso no autorizados | Eliminar puntos de acceso no autorizado y proteger nuestra red |
| R9 | Proteger con una autenticación segura | Realizar un diagnóstico periódicamente de nuestros puntos de acceso |
| R10 | Proteger el acceso a nuestra red | Expulsar a los usuarios no deseados |

**Pruebas de Auditoría**

La evaluación de la conveniencia de los controles establecidos o existentes

**Elección de herramientas de auditoría :**

Las **herramientas** son el conjunto de elementos que permiten llevar a cabo las acciones definidas en las técnicas. Las herramientas utilizadas son: cuestionarios, entrevistas, checklist, trazas y software de interrogación.

**Entrevista .-** en la que llega a obtener información más específica que la obtenida mediante cuestionarios, utilizando el método del interrogatorio, con preguntas variadas y sencillas, pero que han sido convenientemente elaboradas.

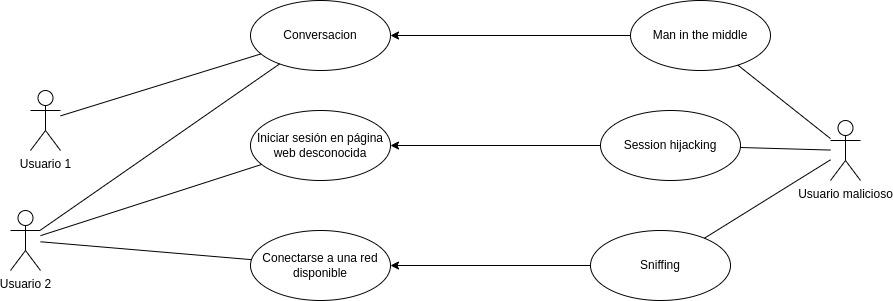
**Checklist .-** conjunto de preguntas respondidas en la mayoría de las veces oralmente, destinados principalmente a personal técnico. Por estos motivos deben ser realizadas en un orden determinado, muy sistematizadas, coherentes y clasificadas por materias, permitiendo que el auditado responda claramente.

**Pruebas de Cumplimiento:**

Son las que tienen como propósito comprobar los riesgos internos y externos y la efectividad de los sistemas de control o denominadas según las normas internacionales NIA 400 (evaluación del riesgo y Control Interno) como “pruebas de control” para identificar los riesgos incluidos en las transacciones, como sus características o atributos que indican la efectividad o desviación de ellos.

**Pruebas Sustantivas:**

Las pruebas sustantivas consisten en comprobaciones diseñadas para obtener evidencia de la validez y propiedad de las transacciones y saldos que van formando los estados financieros de una organización; incluyen comprobaciones de detalles, como las aplicaciones de muestreo o pruebas selectivas, y procedimientos analíticos, diseñados para detectar errores e irregularidades en la información financiera y sus acumulaciones, dichas pruebas son básicas para determinar la opinión final a los estados financieros. Es decir, que se tiene como pruebas sustantivas, los procedimientos de auditoría dirigidos o examinados a obtener evidencia de validez y corrección del manejo contable de las transacciones y los estados financieros y detección de errores o irregularidades en ellos.



* Aspectos Positivos

Controles que funcionan bien y no requieren mejora.

R1,R2,R3,R4,R9,R8. Son los controles que funcionan correctamente y no se encuentran fallas, por el establecimiento de éstas.

* Recomendaciones

Un resumen de las mejoras que deben aplicarse a los controles insuficientes o inexistentes para lograr que los riesgos queden en la Zona Verde de la Matriz e Riesgos.

R5,R7,R10,R6. Es posible el fallo de éstas por el ingenio del intruso, pueden ser vulnerados de formas que no hayamos planificado, lo cuál tenemos que replantear los controles para que no sucedan éstas amenazas.