



Trabajo de fin de carrera titulado

**“ANÁLISIS DE VULNERABILIDADES PARA LA
INFRAESTRUCTURA DE RED DE LA BOLSA DE VALORES DE
QUITO, APLICANDO UNA METODOLOGÍA DE ETHICAL
HACKING”**

Realizado por:

CALERO SUNTASIG HENRY DANIEL

Director de Proyecto:

MGS. LUIS FABIÁN HURTADO VARGAS

Como requisito para la obtención del título de: **MÁSTER EN
TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN
SEGURIDAD DE REDES Y COMUNICACIÓN**

Quito, mayo de 2020

DECLARACIÓN JURAMENTADA

Yo, HENRY DANIEL CALERO SUNTASIG, con cédula de identidad # 1716997828, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría que no ha sido previamente presentado por ningún grado a calificación profesional y, que se ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

Henry Daniel Calero Suntasig
C.C.: 1716997828

DECLARATORIA

El presente trabajo de investigación titulado:

**“ANÁLISIS DE VULNERABILIDADES PARA LA INFRAESTRUCTURA DE RED
DE LA BOLSA DE VALORES DE QUITO, APLICANDO UNA METODOLOGÍA
DE ETHICAL HACKING”**

Realizado por:

CALERO SUNTASIG HENRY DANIEL

Como requisito para la Obtención del Título de:

**MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN
SEGURIDAD DE REDES Y COMUNICACIÓN**

Ha sido dirigido por el profesor

ING. LUIS FABIÁN HURTADO VARGAS, MGS.

Quien considera que constituye un trabajo original de su autor

Ing. Luis Fabián Hurtado Vargas, MGS.

DIRECTOR

PROFESORES INFORMANTES

Después de revisar el trabajo presentado. Lo ha calificado como apto para su defensa oral ante el tribunal examinador.

Ing. Diego Fernando Riofrío Luzcando, PhD

Ing. Joe Carrión Jumbo, PhD

AGRADECIMIENTO

A la Universidad Internacional SEK por aportarme con todo sus conocimientos prácticos y teóricos.

Al Ing. Fabián Hurtado por la dirección del presente proyecto

A la Bolsa de Valores de Quito por brindarme las facilidades para culminar este proyecto.

DEDICATORIA

El presente trabajo va dedicado:

A Dios, a mi esposa Paola, a mi pequeño que está por venir a nuestras vidas, quienes son los pilares en mi vida y son fuente de inspiración para ser cada día mejor.

RESUMEN

La Bolsa de Valores de Quito (BVQ) tenía la necesidad de realizar un escaneo de vulnerabilidades sobre la seguridad informática de su red de datos. En esta propuesta se revisa la situación actual de la BVQ antes de la intervención sobre el análisis de vulnerabilidades, además se realiza un repaso conceptual que brinda un soporte teórico al trabajo.

Para el desarrollo del presente proyecto se utilizó el tipo de estudio exploratorio porque al realizar el escaneo de vulnerabilidades fue examinada la red de datos de la BVQ determinando así los huecos de seguridad, a través del método inductivo – deductivo se recolectó información pública, la misma que proporcionó algunas posibles razones de las supuestas vulnerabilidades localizadas.

Para este estudio se analizaron dos metodologías de ethical hacking, las cuales permitieron seleccionar la que más se adapta a la realidad de la BVQ, la metodología seleccionada fue OSSTMMv3 ya que es una metodología completa, además muestra los criterios que se deben considerar para auditar o evaluar las vulnerabilidades dentro de una organización; no establece ningún objetivo de análisis, pero indica las directrices para la selección más adecuada del objetivo a ser analizado, para la evaluación de riesgos la metodología utiliza RAVS.

Para el análisis de vulnerabilidades se utilizaron los canales sugeridos por la metodología OSSTMMv3 estos son: físico, humano, inalámbrico, telecomunicaciones y red de datos, la metodología indica que se debe comprobar, verificar y contabilizar en cada uno de los canales de acuerdo con el objetivo seleccionado, así también se utilizó herramientas de software libre como Kali Linux para el escaneo interno y externo de la red de datos de la BVQ.

Al final del documento se presentan los resultados obtenidos luego del escaneo de vulnerabilidades, como también una matriz de riesgos que permitió el análisis de la probabilidad y el impacto de cada una de las vulnerabilidades detectadas dentro de los canales de la metodología.

Palabras clave: Seguridad informática, Ethical Hacking y Metodología OSSTMMv3.

ABSTRACT

The Quito Stock Exchange (BVQ) needed to perform a vulnerability scan on the computer security of its data network. In this proposal, the current situation of the BVQ is reviewed before the intervention on vulnerability analysis, and a conceptual review is also carried out that provides theoretical support for the work.

For the development of this project, the exploratory study type was used because when carrying out the vulnerability scan, the BVQ data network was examined, thus determining the security gaps, through the inductive-deductive method, public information was collected, the same which provided some possible reasons for the alleged localized vulnerabilities.

For this study, two ethical hacking methodologies were analyzed, which allowed selecting the one that best suits the reality of the BVQ, the selected methodology was OSSTMMv3 since it is a complete methodology, it also shows the criteria that must be considered to audit or assess vulnerabilities within an organization; It does not establish any analysis objective, but indicates the guidelines for the most appropriate selection of the objective to be analyzed. For risk assessment, the methodology uses RAVS.

For the vulnerability analysis the channels suggested by the OSSTMMv3 methodology were used, these are: physical, human, wireless, telecommunications and data network, the methodology indicates that it must be verified, verified and accounted for in each of the channels according to the selected objective, so free software tools such as Kali Linux were used for internal and external scanning of the BVQ data network.

At the end of the document, the results obtained after the vulnerability scan are presented, as well as a risk matrix that allowed the analysis of the probability and impact of each of the vulnerabilities detected within the channels of the methodology.

Keywords: Computer security, Ethical Hacking and OSSTMMv3 Methodology.

ÍNDICE GENERAL DE CONTENIDOS

1. CAPÍTULO I	1
INTRODUCCIÓN.....	1
1.1. PROBLEMA DE INVESTIGACIÓN.....	1
1.1.1. Planteamiento del problema	1
1.1.1.1. Diagnóstico	2
1.1.1.2. Pronóstico	2
1.1.1.3. Control del pronóstico	3
1.1.2. Formulación del problema	3
1.1.3. Objetivo General	3
1.1.4. Objetivos Específicos.....	3
1.1.5. Justificación.....	4
2. CAPÍTULO II	5
MARCO TEÓRICO.....	5
2.1. Seguridad de la Información	5
2.1.1. Confidencialidad.....	5
2.1.2. Integridad	6
2.1.3. Disponibilidad.....	7
2.1.4. Riesgos de Seguridad de la Información.....	7
2.1.5. Vulnerabilidad.....	8
2.1.6. Amenaza.....	8
2.1.7. Probabilidad	8
2.1.8. Impacto.....	8
2.2. Ethical Hacking	8
2.2.1. Hacker.....	8
2.2.2. Tipos de Ataque	9
2.2.3. Modalidades de ataque	10
2.2.4. Modalidades de pruebas	10
2.2.5. Tipos de pruebas de penetración.....	11
2.3. Metodologías de ethical hacking.....	11
2.3.1. Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM	12
2.3.2. Sistema de puntuación de vulnerabilidad común (CVSS)	14
2.3.3. Análisis comparativo de las metodologías analizadas	16
2.4. Herramientas de análisis de vulnerabilidades	19
2.4.1. Tráfico de red.....	19
2.4.1.1. Verificación de puertos.....	22
2.4.1.2. Captura de contraseñas	24

2.5.	Legislación Ecuatoriana que regula delitos informáticos	26
2.6.	Valores Evaluados de Riesgo (RAV) métrica operacional	27
2.6.1.	Seguridad Operacional (Porosidad).....	28
2.6.2.	Controles verdaderos (TC)	28
2.6.3.	Limitaciones	29
2.6.4.	Exposición	29
2.6.5.	Vulnerabilidad	29
2.6.6.	Debilidad.....	29
2.6.7.	Preocupación.....	29
2.6.8.	Anomalía.....	30
3.	CAPÍTULO III.....	31
	ANÁLISIS DE VULNERABILIDADES.....	31
3.1.	Aplicación OSSTMM sobre la infraestructura de red de la Bolsa de Valores de Quito.....	31
3.1.1.	Fase de inducción	31
3.1.2.	Fase de interacción	31
3.1.3.	Fase de indagación	32
3.1.4.	Fase de intervención.....	32
3.2.	Pruebas de seguridad humana Bolsa de Valores de Quito (BVQ).....	32
3.2.1.	Seguridad operacional	32
3.2.1.1.	Visibilidad (PV).....	32
3.2.1.2.	Acceso (PA).....	33
3.2.1.3.	Confianza (PT).....	34
3.2.2.	Controles	35
3.2.2.1.	Autenticación (LCAu)	35
3.2.2.2.	Indemnización (LCId)	35
3.2.2.3.	Resiliencia (LCRe)	36
3.2.2.4.	Subyugación (LCSu)	36
3.2.2.5.	Continuidad (LCCT).....	37
3.2.2.6.	No repudio LCNR.....	37
3.2.2.7.	Confidencialidad (LCCf).....	38
3.2.2.8.	Privacidad (LCPr).....	38
3.2.2.9.	Integridad (LCIt).....	38
3.2.2.10.	Alarma (LCAI).....	39
3.2.3.	Limitaciones	40
3.2.3.1.	Exposición (LE).....	40
3.2.3.2.	Vulnerabilidad (LV)	40
3.2.3.3.	Debilidad (Lw).....	40

3.2.3.4. Preocupación (Lc).....	41
3.2.3.5. Anomalía (LA).....	42
3.3. Pruebas de seguridad física Bolsa de Valores de Quito (BVQ).....	45
3.3.1. Seguridad operacional.....	45
3.3.1.1. Visibilidad (PV).....	45
3.3.1.2. Acceso (PA).....	46
3.3.1.3. Confianza (PT).....	47
3.3.2. Controles	47
3.3.2.1. Autenticación (LCAu)	47
3.3.2.2. Indemnización (LCId)	48
3.3.2.3. Resiliencia (LCRe)	48
3.3.2.4. Subyugación (LCSu)	49
3.3.2.5. Continuidad LCCt.....	49
3.3.2.6. No Repudio (LCNR).....	50
3.3.2.7. Confidencialidad (LCCf).....	50
3.3.2.8. Privacidad (LCPr).....	51
3.3.2.9. Integridad (LCIt).....	51
3.3.2.10. Alarma (LCAI).....	52
3.3.3. Limitaciones	52
3.3.3.1. Exposición (LE).....	52
3.3.3.2. Vulnerabilidad (LV)	52
3.3.3.3. Debilidad (Lw).....	53
3.3.3.4. Preocupación (Lc).....	53
3.3.3.5. Anomalía (LA).....	54
3.4. Pruebas de seguridad Inalámbrica Bolsa de Valores de Quito (BVQ)	57
3.4.1. Seguridad operacional.....	57
3.4.1.1. Visibilidad (PV).....	57
3.4.1.2. Acceso (PA).....	58
3.4.1.3. Confianza (PT).....	59
3.4.2. Controles	59
3.4.2.1. Autenticación (LCAu)	59
3.4.2.2. Indemnización (LCId)	60
3.4.2.3. Resiliencia (LCRe)	60
3.4.2.4. Subyugación LCSu	61
3.4.2.5. Continuidad (LCCt).....	61
3.4.2.6. No Repudio (LCNR).....	61
3.4.2.7. Confidencialidad LCCf.....	62

3.4.2.8. Privacidad LCPr.....	62
3.4.2.9. Integridad LCIt	63
3.4.2.10. Alarma (LCAI).....	63
3.4.3. Limitaciones	63
3.4.3.1. Exposición (LE).....	64
3.4.3.2. Vulnerabilidad (LV)	64
3.4.3.3. Debilidad (LW).....	64
3.4.3.4. Preocupación (LC).....	65
3.4.3.5. Anomalía (LA).....	65
3.5. Evaluación de seguridad de Telecomunicaciones Bolsa de Valores de Quito (BVQ)	68
3.5.1. Seguridad operacional	68
3.5.1.1. Visibilidad (PV).....	68
3.5.1.2. Acceso (PA).....	69
3.5.1.3. Confianza (PT).....	70
3.5.2. Controles	70
3.5.2.1. Autenticación (LCAu)	70
3.5.2.2. Indemnización (LCId)	71
3.5.2.3. Resiliencia (LCRe)	71
3.5.2.4. Subyugación (LCSu)	72
3.5.2.5. Continuidad LCCt.....	72
3.5.2.6. No Repudio (LCNR).....	73
3.5.2.7. Confidencialidad (LCCf).....	73
3.5.2.8. Privacidad (LCPr).....	74
3.5.2.9. Alarma (LCAI).....	75
3.5.3. Limitaciones	75
3.5.3.1. Exposición (LE).....	75
3.5.3.2. Vulnerabilidad (LV)	75
3.5.3.3. Debilidad (Lw).....	76
3.5.3.4. Preocupación (LC).....	76
3.5.3.5. Anomalía (LA).....	77
3.6. Evaluación de la seguridad de Redes de Datos Bolsa de Valores de Quito (BVQ)	79
3.6.1. Seguridad operacional	80
3.6.1.1. Visibilidad (PV).....	80
3.6.1.2. Acceso (PA).....	81
3.6.1.3. Confianza (PT).....	81

3.6.2. Controles	82
3.6.2.1. Autenticación (LCAu)	82
3.6.2.2. Indemnización (LCId)	83
3.6.2.3. Resiliencia LCRE	83
3.6.2.4. Subyugación (LCSu)	84
3.6.2.5. Continuidad (LCCt)	84
3.6.2.6. No Repudio (LCNR).....	84
3.6.2.7. Confidencialidad (LCCf)	85
3.6.2.8. Privacidad (LCPr).....	86
3.6.2.9. Integridad (LCIt).....	86
3.6.2.10. Alarma (LCAI).....	86
3.6.3. Limitaciones	87
3.6.3.1. Exposición (LE).....	87
3.6.3.2. Vulnerabilidad (LV)	87
3.6.3.3. Debilidad (LW).....	87
3.6.3.4. Preocupación (LC).....	88
3.6.3.5. Anomalías (LA)	88
3.7. Interpretación de resultados	91
4. CAPÍTULO IV.....	119
CONCLUSIONES Y RECOMENDACIONES	119
Bibliografía	121
Anexos	124
Anexo 1.- Encuesta Pruebas de Seguridad Humana, Física e Inalámbrica BVQ.....	124
Anexo 2.- Resultados de la encuesta de Pruebas de Seguridad Humana, Física e Inalámbrica BVQ.....	129
Anexo 3.- Resultados de la encuesta realizada al Analista de Desarrollo TI / Analista de Soporte TI	136
Anexo 4.- Resultados de la encuesta realizada al Analista Senior de Infraestructura	138
Anexo 5.- Recolección de datos e interpretación de resultados de la consola de WIFI de la BVQ.....	141
Anexo 6.- Herramientas de Kali Linux utilizadas para este proyecto.	146
Anexo 7.- Convenio BVQ.....	162

ÍNDICE DE FIGURAS

Figura 1. Pilares de la seguridad de la información.....	5
Figura 2. Tipos de test OSSTMM v3.....	13
Figura 3. Metodología OSSTMM.....	14
Figura 4. Grupo de métricas CVSS.....	15
Figura 5. Métricas y Ecuaciones CVSS.....	16
Figura 6. Interfaz gráfica de Wireshark..	20
Figura 7. TCPDUMP línea de comandos..	21
Figura 8. Interfaz gráfica de resultados SNORT..	21
Figura 9. NMAP interfaz de línea de comandos.....	22
Figura 10. NESSUS Interfaz gráfica de resultados.....	23
Figura 11. NETCAT consola de línea de comandos.....	23
Figura 12. KISMET consola de monitoreo.....	24
Figura 13. AIRCRACK-NG Consola..	25
Figura 14. ASLEAP Consola de línea de comandos..	26
Figura 15. Cálculo de la seguridad..	28
Figura 16. Cálculo Seguridad Operacional (Porosidad)..	28
Figura 17. Cálculo Controles Verdaderos (TC).....	28
Figura 18. Cálculo de Control Ausentes de Autenticación.....	28
Figura 19. Cálculo de Controles Ausentes (MC).....	28
Figura 20. Cálculo de la debilidad (Lw)..	29
Figura 21. Cálculo de la Preocupación..	29
Figura 22. Búsqueda de funcionarios en LinkedIn..	34
Figura 23. Búsqueda de funcionarios en WebMii..	34
Figura 24. Calculadora RAVS – Seguridad Canal Humano.....	44
Figura 25. Calculadora RAVS – Seguridad Canal Físico.....	56
Figura 26. Calculadora RAVS – Seguridad Canal Inalámbrico..	67
Figura 27. Calculadora RAVS – Seguridad Canal Telecomunicaciones.....	78
Figura 28. Calculadora RAVS – Seguridad Canal Red de Datos..	90
Figura 29. Análisis de la probabilidad y el impacto.	116
Figura 30. Análisis de la probabilidad y el impacto.	117
Figura 31. Análisis de la probabilidad y el impacto.	118

ÍNDICE DE TABLAS

<i>Tabla 1 Diagnóstico, síntomas y causas detectadas.....</i>	<i>2</i>
<i>Tabla 2 Área de trabajo OSSTMM v3 Fuente Ávila (2018).....</i>	<i>12</i>
<i>Tabla 3 Cuadro comparativo de metodologías de análisis de vulnerabilidades.....</i>	<i>19</i>
<i>Tabla 4 Estructura métrica operacional RAV.....</i>	<i>27</i>
<i>Tabla 5 Visibilidad canal Humano.....</i>	<i>33</i>
<i>Tabla 6 Acceso Canal Humano.....</i>	<i>33</i>
<i>Tabla 7 Confianza Canal Humano.....</i>	<i>34</i>
<i>Tabla 8 Autenticación Canal Humano.....</i>	<i>35</i>
<i>Tabla 9 Indemnización Canal Humano.....</i>	<i>36</i>
<i>Tabla 10 Resiliencia Canal Humano.....</i>	<i>36</i>
<i>Tabla 11 Subyugación Canal Humano.....</i>	<i>36</i>
<i>Tabla 12 Continuidad Canal Humano.....</i>	<i>37</i>
<i>Tabla 13 No Repudio Canal Humano.....</i>	<i>37</i>
<i>Tabla 14 Confidencialidad Canal Humano.....</i>	<i>38</i>
<i>Tabla 15 Privacidad Canal Humano.....</i>	<i>38</i>
<i>Tabla 16 Integridad Canal Humano.....</i>	<i>39</i>
<i>Tabla 17 Alarma Canal Humano.....</i>	<i>39</i>
<i>Tabla 18 Exposición Canal Humano.....</i>	<i>40</i>
<i>Tabla 19 Vulnerabilidad Canal Humano.....</i>	<i>40</i>
<i>Tabla 20 Debilidad Canal Humano.....</i>	<i>41</i>
<i>Tabla 21 Preocupación Canal humano.....</i>	<i>41</i>
<i>Tabla 22 Anomalía Canal Humano.....</i>	<i>42</i>
<i>Tabla 23 Datos Canal Humano RAV.....</i>	<i>42</i>
<i>Tabla 24 Visibilidad Canal Físico.....</i>	<i>46</i>
<i>Tabla 25 Acceso Canal Físico.....</i>	<i>46</i>
<i>Tabla 26 Confianza Canal Físico.....</i>	<i>47</i>
<i>Tabla 27 Autenticación Canal Físico.....</i>	<i>47</i>
<i>Tabla 28 Indemnización Canal Físico.....</i>	<i>48</i>
<i>Tabla 29 Resiliencia Canal Físico.....</i>	<i>49</i>
<i>Tabla 30 Subyugación Control Físico.....</i>	<i>49</i>
<i>Tabla 31 Continuidad canal Físico.....</i>	<i>50</i>
<i>Tabla 32 No Repudio Canal Físico.....</i>	<i>50</i>

<i>Tabla 33 Confidencialidad Canal Físico.....</i>	<i>50</i>
<i>Tabla 34 Privacidad Canal Físico.....</i>	<i>51</i>
<i>Tabla 35 Integridad Canal Físico.....</i>	<i>52</i>
<i>Tabla 36 Alarma Control Físico.....</i>	<i>52</i>
<i>Tabla 37 Exposición Canal Físico.....</i>	<i>52</i>
<i>Tabla 38 Vulnerabilidad Canal Físico</i>	<i>53</i>
<i>Tabla 39 Debilidad Canal Físico</i>	<i>53</i>
<i>Tabla 40 Preocupación Canal Humano</i>	<i>53</i>
<i>Tabla 41 Anomalía Canal Físico.....</i>	<i>54</i>
<i>Tabla 42 Datos Canal Físico RAV.....</i>	<i>54</i>
<i>Tabla 43 Visibilidad Canal Inalámbrico</i>	<i>57</i>
<i>Tabla 44 Acceso Canal Inalámbrico</i>	<i>58</i>
<i>Tabla 45 Confianza Canal Inalámbrico</i>	<i>59</i>
<i>Tabla 46 Autenticación Canal Inalámbrico</i>	<i>60</i>
<i>Tabla 47 Indemnización Canal Inalámbrico</i>	<i>60</i>
<i>Tabla 48 Resiliencia Canal Inalámbrico.....</i>	<i>60</i>
<i>Tabla 49 Subyugación Canal Inalámbrico.....</i>	<i>61</i>
<i>Tabla 50 Continuidad Canal Inalámbrico.....</i>	<i>61</i>
<i>Tabla 51 No Repudio Canal Inalámbrico.....</i>	<i>62</i>
<i>Tabla 52 Confidencialidad Canal Inalámbrico.....</i>	<i>62</i>
<i>Tabla 53 Privacidad Canal Inalámbrico.....</i>	<i>62</i>
<i>Tabla 54 Integridad Canal Inalámbrico.....</i>	<i>63</i>
<i>Tabla 55 Alarma Canal Inalámbrico.....</i>	<i>63</i>
<i>Tabla 56 Exposición Canal Inalámbrico.....</i>	<i>64</i>
<i>Tabla 57 Vulnerabilidad Canal Inalámbrico</i>	<i>64</i>
<i>Tabla 58 Debilidad Canal Inalámbrico.....</i>	<i>64</i>
<i>Tabla 59 Preocupación Canal Inalámbrico</i>	<i>65</i>
<i>Tabla 60 Anomalía Canal inalámbrico</i>	<i>65</i>
<i>Tabla 61 Datos Canal Inalámbrico RAV.....</i>	<i>66</i>
<i>Tabla 62 Visibilidad Canal Telecomunicaciones</i>	<i>69</i>
<i>Tabla 63 Visibilidad Canal Telecomunicaciones</i>	<i>70</i>
<i>Tabla 64 Confianza Canal Telecomunicaciones</i>	<i>70</i>
<i>Tabla 65 Autenticación Canal Telecomunicaciones.....</i>	<i>71</i>
<i>Tabla 66 Indemnización Canal Telecomunicaciones</i>	<i>71</i>

<i>Tabla 67 Resiliencia Canal Telecomunicaciones</i>	<i>72</i>
<i>Tabla 68 Subyugación Canal Telecomunicaciones</i>	<i>72</i>
<i>Tabla 69 Continuidad Canal de Telecomunicaciones</i>	<i>73</i>
<i>Tabla 70 No Repudio Canal Telecomunicaciones.....</i>	<i>73</i>
<i>Tabla 71 Confidencialidad Canal Telecomunicaciones</i>	<i>74</i>
<i>Tabla 72 Privacidad Canal Telecomunicaciones</i>	<i>74</i>
<i>Tabla 73 Privacidad Canal Telecomunicaciones</i>	<i>74</i>
<i>Tabla 74 Alarma Canal Telecomunicaciones.....</i>	<i>75</i>
<i>Tabla 75 Debilidad Canal Telecomunicaciones.....</i>	<i>76</i>
<i>Tabla 76 Preocupación Canal Telecomunicaciones</i>	<i>76</i>
<i>Tabla 77 Anomalía Canal Telecomunicaciones</i>	<i>77</i>
<i>Tabla 78 Datos Canal Telecomunicaciones RAV.....</i>	<i>77</i>
<i>Tabla 79 Visibilidad Canal Redes de Datos</i>	<i>80</i>
<i>Tabla 80 Acceso Canal Redes de Datos</i>	<i>81</i>
<i>Tabla 81 Acceso Canal Redes de Datos</i>	<i>82</i>
<i>Tabla 82 Indemnización Canal Redes de Datos</i>	<i>83</i>
<i>Tabla 83 Resiliencia Canal Redes de Datos.....</i>	<i>83</i>
<i>Tabla 84 Subyugación Canal Redes de Datos.....</i>	<i>84</i>
<i>Tabla 85 Continuidad Canal Redes de Datos.....</i>	<i>84</i>
<i>Tabla 86 No Repudio Canal Redes de Datos.....</i>	<i>85</i>
<i>Tabla 87 Confidencialidad Canal Redes de Datos.....</i>	<i>85</i>
<i>Tabla 88 Privacidad Canal Redes de Datos.....</i>	<i>86</i>
<i>Tabla 89 Privacidad Canal Redes de Datos.....</i>	<i>86</i>
<i>Tabla 90 Alarma Canal Redes de Datos.....</i>	<i>87</i>
<i>Tabla 91 Vulnerabilidad Canal Redes de Datos</i>	<i>87</i>
<i>Tabla 92 Debilidad Canal Redes de Datos.....</i>	<i>87</i>
<i>Tabla 93 Preocupación Canal Redes de Datos</i>	<i>88</i>
<i>Tabla 94 Anomalía Redes de Datos.....</i>	<i>88</i>
<i>Tabla 95 Datos Canal Red de Datos RAV.....</i>	<i>89</i>
<i>Tabla 96 Resultados obtenidos de la seguridad actual de la BVQ.....</i>	<i>91</i>
<i>Tabla 97 Resultados obtenidos de riesgo actual de la BVQ.....</i>	<i>91</i>
<i>Tabla 98 Escala de Likert medición de Riesgo.....</i>	<i>91</i>
<i>Tabla 99 Resultados de riesgos actuales de la BVQ utilizando escala de Likert.....</i>	<i>92</i>

CAPÍTULO I

INTRODUCCIÓN

1.1. PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del problema

En la actualidad la gran mayoría de instituciones financieras se encuentran expuestas a diferentes delitos cibernéticos poniendo en peligro la información que genera a diario, para garantizar que este activo sea utilizable debe cumplir los tres principios básicos de la seguridad de la información que son confidencialidad, integridad y disponibilidad.

Estos delitos cibernéticos pueden presentarse desde el interior de las empresas como también desde exterior, para realizar este tipo de delitos existen varias técnicas tales como ataque DoS, ping flood, escaneo de puertos, ARP spoofing, ACK flood, ataque Man-In-The-Middle, ingeniería social, entre otros. Los delincuentes al detectar este tipo de vulnerabilidades las explotan para beneficio propio.

Esto evidencia que tan protegida se encuentra una red de datos y que tan segura es la infraestructura de una empresa, el ethical hacking realiza una búsqueda de vulnerabilidades para detectar huecos de seguridad.

Por otra parte, en el año 2016 la Corporación Civil Bolsa de Valores de Quito se convirtió a Bolsa de Valores de Quito Sociedad Anónima (BVQ), en este mismo año la BVQ para mejorar sus servicios contrató a KPMG para que realice una auditoría externa en las áreas financiera y tecnológica, ya que estas son áreas críticas del giro del negocio de la BVQ y dentro de su informe final del año 2016 y 2017 Rivas (2017) afirmó que:

Ethical Hacking

No se han realizado pruebas de análisis de vulnerabilidades y escaneo de puertos sobre la red de la Institución, para detectar deficiencias de seguridad que puedan afectar al normal desempeño de las aplicaciones e infraestructura de red.

La situación indicada representa un riesgo de seguridad para la información e infraestructura tecnológica de la Institución. Ya que no se han identificado las vulnerabilidades que de ser explotadas podrían afectar las operaciones diarias. (p. 10)

Con estos antecedentes, la Bolsa de Valores de Quito tiene como prioridad realizar un análisis de vulnerabilidades utilizando una metodología de Ethical Hacking, al realizar este trabajo se obtendrá una fotografía de la red donde se observa las diferentes vulnerabilidades de nivel lógico o físico, al conocer estas vulnerabilidades se deben planificar acciones preventivas y correctivas ante ataques de personal ajenas a la empresa.

1.1.1.1. Diagnóstico

A continuación, se presenta la tabla de síntomas y causas detectadas.

Síntomas	Causas
Observación por dos años seguidos de KPMG firma auditora externa para la realización de un análisis de vulnerabilidades.	Desconocimiento de los huecos de seguridad que pueden existir dentro de la infraestructura de red de la BVQ y pueden ser aprovechados por los atacantes.

Tabla 1 Diagnóstico, síntomas y causas detectadas. Fuente: Henry Daniel Calero Suntasig

El departamento de Tecnología de la BVQ al desconocer los huecos de seguridad que tiene la infraestructura de red puede estar expuesto a varias amenazas que comprometen la confidencialidad, integridad y disponibilidad de la información que se genera dentro de la institución, causando la indisponibilidad de los servicios que provee a sus clientes, mala reputación institucional e incluso multas o pérdidas económicas.

1.1.1.2. Pronóstico

Al no analizar las vulnerabilidades en la infraestructura de red de la Bolsa de Valores de Quito utilizando una metodología de ethical hacking, el encargado de la red institucional no conocería las vulnerabilidades a la que está expuesta la red, provocando en un futuro posibles ataques malintencionados que provoquen interrupción de actividades, mala reputación a la institución, multas, entre otras.

1.1.1.3. Control del pronóstico

Existen varias metodologías para realizar un análisis de vulnerabilidades entre estos métodos está OSSTMM (Manual de metodología abierta de testeo de seguridad), NIST (Guía técnica de pruebas de seguridad de la información y evaluación), CVSS (Sistema de puntuación de vulnerabilidad común), entre otras. Se analizarán estas metodologías y se seleccionará la que mejor que se adapte a una entidad como la Bolsa de Valores de Quito, con este análisis de vulnerabilidades se pretende identificar los huecos de seguridad de la red con el propósito de generar un plan de acción que permita controlar y mitigar estos riesgos, como también que en un futuro estos huecos localizados no sea una puerta abierta para posibles ataques de personas mal intencionadas.

1.1.2. Formulación del problema

El constante incremento de delitos cibernéticos hacia entidades financieras provoca que estas tomen las medidas necesarias para evitarlos. Los delincuentes cibernéticos al localizar los huecos de seguridad, los explotan para su beneficio o únicamente realizar algún daño provocando la mala reputación de las empresas, pérdidas económicas o sanciones por el ente de control.

En la Bolsa de Valores de Quito se desconoce los huecos de seguridad a los que pueden estar expuestos, ya que no se ha realizado ningún tipo de escaneo de vulnerabilidades a profundidad, esto puede provocar ataques mal intencionados hacia la institución con el fin de provocar la indisponibilidad de servicio, encriptación de la información o en el peor de los casos pérdida de la información y multas.

1.1.3. Objetivo General

Realizar un estudio de vulnerabilidades utilizando una metodología de ethical hacking para la detección de las debilidades de la infraestructura de red de la Bolsa de Valores de Quito.

1.1.4. Objetivos Específicos

Analizar diferentes metodologías de ethical hacking; mediante la comparación de cada una de estas se seleccionará la más cercana que se pueda aplicar a la Bolsa de Valores de Quito, para el descubrimiento de las vulnerabilidades en la infraestructura de red.

Realizar un escaneo interno y externo de la red de datos utilizando herramientas de software libre para el descubrimiento de vulnerabilidades en la red de la Bolsa de Valores de Quito.

Presentar una matriz de riesgos con las vulnerabilidades localizadas en la red de datos mediante un análisis de la probabilidad y el impacto de los riesgos localizados, para ser entregado a la Bolsa de Valores de Quito.

1.1.5. Justificación

La Bolsa de Valores de Quito dentro de la carta de observaciones de la firma auditora KPMG solicita realizar un análisis de vulnerabilidades sobre la infraestructura de red de datos para localizar posibles huecos de seguridad que tenga la institución.

Al realizar un escaneo de vulnerabilidades en la Bolsa de Valores de Quito se podrá detectar a tiempo los huecos de seguridad y tratarlos con la brevedad del caso, esto con el fin de mitigar posibles ataques en un futuro que puedan causar la mala reputación de la institución.

Al realizar este análisis de vulnerabilidades se podrá generar una matriz de riesgos en la cual se indicará el grado de afectación y el posible control que se puede implementar para mitigar la vulnerabilidad.

Justificación Metodológica

Para el análisis de vulnerabilidades de este proyecto se analizará las metodologías OSSTMM (Manual de metodología abierta de testeo de seguridad), NIST (Guía técnica de pruebas de seguridad de la información y evaluación), CVSS (Sistema de puntuación de vulnerabilidad común), para alinearse a las mejores prácticas, estándares y guías de seguridad informática.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

La seguridad de la información es una serie de medidas preventivas que se utilizan para salvaguardar la información de una empresa con el objetivo que esta información se encuentre disponible cuando se la necesite.

La seguridad de la información tiene tres pilares importantes que son la confidencialidad, integridad y disponibilidad.



Figura 1. Pilares de la seguridad de la información. Fuente: Introducción a la seguridad informática y el análisis de vulnerabilidades Romero et al. (2018).

2.1.1. Confidencialidad

Según Romero et al. (2018) la confidencialidad de la información se refiere a asegurar el acceso a la información solo a las personas autorizadas y dueñas de la información, para garantizar la confidencialidad de la información, ésta se debe apoyar con los siguientes recursos:

- Autenticación de usuarios
- Gestión de privilegios
- Cifrado de información

Autenticación de usuarios: por medio de la autenticación del usuario se relaciona a la persona con el usuario y contraseña dentro de un sistema.

Gestión de privilegios: las personas al ser autorizadas para el acceso de una determinada información deben contar con los permisos de acuerdo con la necesidad, es decir permisos de lectura o permisos de escritura (Romero et al., 2018).

Cifrado de información: según Romero et al. (2018) el cifrado de la información es la protección de datos por medio de contraseñas para que la información no se encuentre expuesta, esto se aplica incluso para las personas que tengan autorización para el uso de la información.

2.1.2. Integridad

La integridad de la información es evitar que los datos no sean modificados por personas no autorizadas y sin autorización con el fin que se evite errores al usar esta información (Romero et al., 2018).

Romero et al. (2018) indica que para garantizar la integridad de la información se debe considerar lo siguiente:

- Revisión del tráfico de la red
- Auditar sistemas (implementación de auditorías en los sistemas)
- Sistemas de gestión de cambios
- Copias de seguridad (backups)

Revisión del tráfico de la red: Cashman (2019) indica que la revisión del tráfico de la red es la recopilación de información que circula por una red de datos con el fin de ser analizada y detectar posibles vulnerabilidades o robo de información.

Auditar sistemas (implementación de auditorías en los sistemas): Pacheco (2018) menciona que la auditoría de sistemas verifica y evalúa todos los aspectos relacionados con los recursos informáticos, así como la efectividad de los controles implementados sobre los procedimientos que involucra el procesamiento de información perteneciente a una empresa.

Sistema de gestión de cambios: Rincón & Ruiz (2017) indican que el sistema de gestión de cambios supervisa y garantiza que todas las solicitudes de cambio sean

cuidadosamente autorizadas y priorizadas, se debe contar con los recursos necesarios para para realizar los cambios requeridos.

Copias de seguridad: Según Born et al. (2008) las copias de seguridad son consideradas en la fase de producción, la información física o lógica generada en esta fase se debe copiar de forma íntegra con una determinada frecuencia, para garantizar la gestión de servicios TI.

2.1.3. Disponibilidad

Según Romero et al. (2018) la disponibilidad de la información hace referencia que los datos se encuentren disponibles cuando se los necesite de forma confiable y fiable, para garantizar la disponibilidad se debe tener presente lo siguiente:

- Acuerdos de servicios internos SLA
- Copias de seguridad (backups)
- Disponer recursos alternativos a los primarios

Acuerdos de nivel de servicios (SLA): Born et al. (2008) menciona que los acuerdos de nivel de servicio son convenios o contratos que los proveedores de servicios acuerdan con su clientes internos o externos a cumplir sobre sus servicios contratados y/o utilizados.

Disponer recursos alternos a los primarios: Hace referencia en contar con un centro alternativo ubicado en otro lugar geográficamente diferente, ya que el tener concentrada la información en un solo lugar implica un riesgo alto.

2.1.4. Riesgos de Seguridad de la Información

La posible pérdida de información forma parte de los factores tanto internos como externos que generan complicaciones al momento de alcanzar los objetivos en las empresas; gran parte de estos objetivos tienen relación con la seguridad de la información. La seguridad absoluta no existe, pero resulta importante reducir estos riesgos, identificando evaluando y controlando las vulnerabilidades (Lawrence, Motta de Castro & Kowask, 2014).

El riesgo está dado por el producto de la probabilidad y el impacto de una determinada actividad.

2.1.5. Vulnerabilidad

La vulnerabilidad se define como el grado de debilidad que tiene un objeto o un sistema, estas debilidades son fallos de diseño, fallos de seguridad, malas prácticas de configuración, entre otras, un sistema al tener este tipo de vulnerabilidades los delincuentes sacan el mayor provecho sobre estas para realizar daños a las empresas (Romero et al., 2018).

2.1.6. Amenaza

Romero et al. (2018) menciona que las amenazas son sucesos que puede indisponer o dañar un servicio o producto con una duración e intensidad determinada.

2.1.7. Probabilidad

Es la posibilidad de ocurrencia de una actividad dependiente de factores internos o externos que influyen para que suceda o no suceda, afectando servicios o productos tangibles o intangibles (Romero et al.,2018).

2.1.8. Impacto

Es la consecuencia de la materialización del riesgo, esta materialización se analiza por niveles de medición nulo, bajo, medio y alto, dependiendo del grado de afectación que indisponer al servicio o producto sea tangible o intangible (Romero et al.,2018).

2.2. Ethical Hacking

Ethical hacking es la actividad que realizan un grupo de profesionales de forma ética para encontrar vulnerabilidades o huecos de seguridad bajo el consentimiento de sus autoridades.

2.2.1. Hacker

Gacharná (2009) indica que hacker es un individuo fanático y apasionado por la tecnología, sin embargo, en el ámbito informático la palabra hacker está asociada a la idea de una persona que golpea una red de información, llevando los elementos tecnológicos al límite para hacerlos fallar; la tarea de un hacker no es dañar, es conocer.

Los tipos de hacker son:

- White Hat Hacker
- Gray Hat Hacker
- Black Hat Hacker

White Hat Hacker: White Hat o Sombrero Blanco también conocidos como los chicos buenos, estos hackers se encargan de realizar ataques de seguridad para encontrar vulnerabilidades que puedan afectar a los sistemas de una empresa, por lo general este tipo de hackers son personas que trabajan realizando consultorías de seguridad o pertenecen alguna empresa que presta servicios de seguridad informática (Quispe, 2018).

Gray Hat Hacker: Gray Hat o Sombrero Gris este tipo de hackers tiene una ética incierta es decir que no son los buenos ni tampoco son los malos, este tipo de hackers realizan ataques sobre los sistemas sin la finalidad de mejorar los huecos de seguridad encontrados, pero tampoco con la finalidad de realizar algún tipo de daño sobre las vulnerabilidades encontradas (Quispe, 2018).

Black Hat Hacker: Black Hat o Sombrero Negro también conocidos como los chicos malos, estos hackers explotan las vulnerabilidades encontradas dentro de un sistema con el principal objetivo de realizar daños u obtener algún beneficio propio (Quispe, 2018).

2.2.2. Tipos de Ataque

Ataque pasivo: Según Kumar & Singh (2016) los ataques pasivos son difíciles de detectar, no son descubiertos en condiciones normales, el atacante puede pasar desapercibido antes, durante y después de su ataque, sin alterar la comunicación y tampoco alterar la transferencia de datos. Para hacer frente a estos ataques se requiere aplicar acciones de prevención como monitoreo frecuente y pruebas de análisis de vulnerabilidades.

Ataque Activo: Kumar & Singh (2016) indica que un ataque activo se basa en la modificación del mensaje original o en la creación de un mensaje falso para que el receptor no pueda entender el mensaje original. En este ataque el intruso intenta acceder a los sistemas o información para dañarlos, los ataques activos se dividen en:

- Alteración del mensaje
- Suplantación de identidad

- Repetición
- Denegación de servicio (DoS)

Alteración del mensaje: Es un tipo de ataque que involucra la alteración de los mensajes enviados en la red de forma no autorizada, los mensajes modificados pretenden parecer genuinos para el usuario receptor (Kumar & Singh, 2016).

Suplantación de identidad: Este tipo de ataque pretende falsificar la identidad de alguien o algo para tener accesos y realizar el ataque sobre la red de datos (Kumar & Singh, 2016).

Repetición: Los ataques de repetición se usan para el acceso o modificación de mensajes, esto ocurre cuando los paquetes de información son capturados (Kumar & Singh, 2016).

Denegación de servicio: Es un tipo de ataque que impide a los usuarios legítimos acceder algunos servicios o recursos, para lo cual son elegibles (Kumar & Singh, 2016).

2.2.3. Modalidades de ataque

Las modalidades de ataque que se conocen hoy en día son los ataques internos y externos, esto quiere decir que las amenazas existentes dentro de una empresa pueden ser explotadas desde su interior como desde su exterior.

Internos: Los ataques internos generalmente provienen del abuso en el otorgamiento de permisos de acceso entregado a los empleados, este comportamiento se presenta en empleados no conformes o insatisfechos (Sharma, Sharma, Rawal, & Narwal, 2017).

Externos: Los ataques externos se producen mediante la conexión remota o interceptación del tráfico de red; en forma ilegal de personas ajenas a una empresa (Sharma, Sharma, Rawal, & Narwal, 2017).

2.2.4. Modalidades de pruebas

Al realizar un ethical hacking se conoce dos modalidades de pruebas que son Red y Blue Team cada uno con sus características que a continuación se indica.

Red Team: Según Microsoft (2014) el equipo rojo simula técnicas y procedimientos de ataques cercanos a la vida real, estas pruebas van dirigidas a personas, procesos y tecnología de una institución, con el objetivo de medir el nivel de seguridad, estas pruebas se realizan bajo el conocimiento de ciertos directivos de la institución, pero no por todos los empleados.

Blue team: Microsoft (2014) indica que el equipo azul se encarga de la prevención, detección y respuesta de los ataques recibidos, estos controles se aplican sobre las personas, procesos y tecnología de la institución, las pruebas son realizadas bajo el conocimiento de los empleados de una empresa,

2.2.5. Tipos de pruebas de penetración

Hoy en día se conoce tres tipos de pruebas de penetración White Box, Gray Box y Black Box dependiendo de los resultados que se deseen obtener que elegirá el tipo de prueba.

White Box: Denominada como hacking transparente es la prueba de penetración más completa, al comenzar el pentest (penetration test) la persona que está realizando estas pruebas conoce información sobre la infraestructura de red, IPs, topología, logins, con el objetivo de dirigir de forma adecuada el ataque (Picouto et al., 2014).

Black Box: Conocida como Caja Negra es una prueba de penetración a ciegas, es decir no se tiene información de una empresa y es la más cercana y rigurosa cara a un ataque de los crackers, el objetivo principal es encontrar vulnerabilidades dentro de la red y explotarlas hasta el más alto nivel, al ser una prueba de ethical hacking se debe proteger la continuidad, integridad y disponibilidad de la información de la empresa (Picouto et al., 2014).

Gary Box: Esta es la modalidad media, esto quiere decir que se tiene una información limitada de la red de una empresa, pero no toda la información, con esto se pretende encontrar vulnerabilidades dentro de la red y explotarlas (Picouto et al., 2014).

2.3. Metodologías de ethical hacking

En el presente proyecto se analizará dos metodologías de ethical hacking, y se seleccionará la mejor para ser aplicada en la Bolsa de Valores de Quito y la que más se ajusta

a la realidad actual de dicha empresa, tener en cuenta que el análisis de vulnerabilidad será ejecutado sobre la infraestructura de red.

2.3.1. Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM

La metodología OSSTMM (Open Source Security Testing Methodology Manual) es una de varias metodologías de ethical hacking que existen hoy en día, fue creada por Herzong (2010) Director Ejecutivo de ISECOM (Instituto para la Seguridad de Metodologías Abiertas) en el año 2001.

Esta metodología es considerada la mejor para pruebas de seguridad dentro de un entorno de red, ya que permite evaluar la seguridad operacional de sitios físicos, las acciones humanas y las demás formas de comunicación tales como inalámbricas, cableadas, analógicas y digitales, este manual ayuda a la evaluación de los riesgos localizados a fin de que el auditor o evaluador pueda trabajar sobre estos riesgos y reducirlos.

La metodología OSSTMM está alineado para dar cumplimiento y utiliza las mejores prácticas establecidas en la ISO 27001 – 27002 e ITIL entre otras.

El manual OSSTMM muestra una serie de descripciones para llevar un proceso de testeo de seguridad, la Tabla 2 muestra las áreas de trabajo que tiene esta metodología, en resumen, cubre los aspectos de seguridad física, seguridad del espectro electromagnético y seguridad de las telecomunicaciones.

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Todos aquellos comprometidos con la organización
	Físico	Objetos tangibles de la organización
Seguridad del espectro electromagnético (SPECSEC)	Comunicaciones inalámbricas	Señales Electromagnéticas empleadas
Seguridad de las comunicaciones	Telecomunicaciones	Comunicaciones digitales y analógicas
	Redes de datos	Sistemas electrónicos y redes de datos

Tabla 2. Área de trabajo OSSTMM v3. Fuente: Ávila (2018).

El ámbito de trabajo de OSSTMM v3 se tiene los siguientes tipos de pruebas:

- Blind (Hacking Ético)
- Double Blind (Caja Negra o Pruebas de Penetración)
- Gray Box (Caja Gris)

- Double Gray Box (Doble Caja Gris)
- Tandem (Tandem o Secuencial)
- Reversal (Inverso)

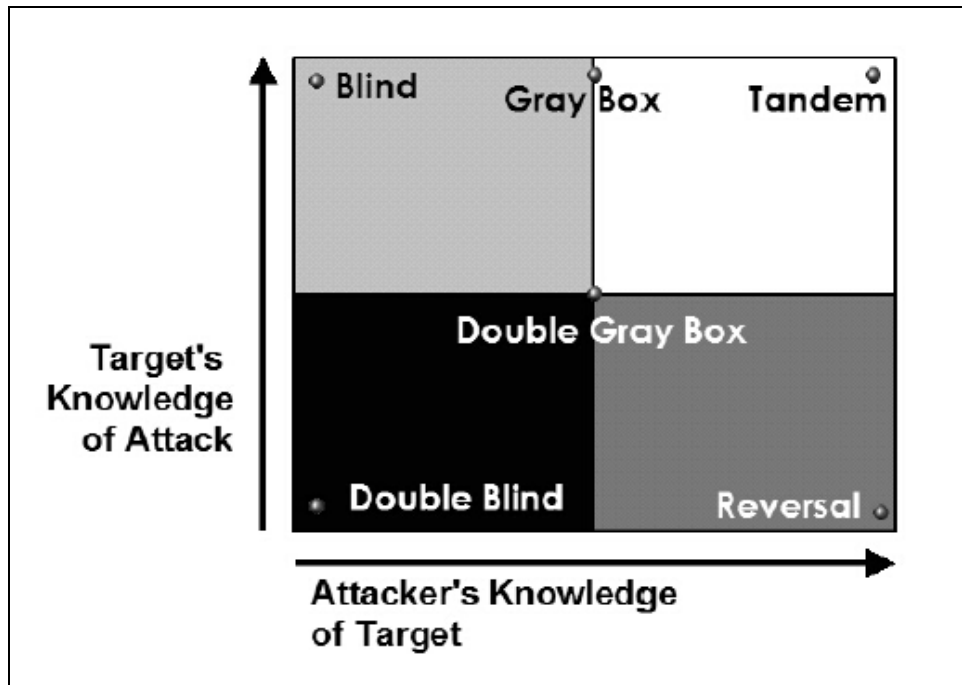


Figura 2. Tipos de test OSSTMM v3. Fuente: Open Source Security Testing Methodology Manual Herzong (2010).

Herzong (2010) establece los módulos de pruebas de OSSTMM se los utilizan dependiendo de la minuciosidad, el tipo de negocio, la asignación de tiempo y los requisitos de la auditoría, estos módulos tienen cuatro fases que son:

- Fase de inducción
- Fase de interacción
- Fase de investigación
- Fase de intervención

Cada fase presenta una profundidad diferente durante la auditoría, pero ninguna fase individual es menos importante que otra.

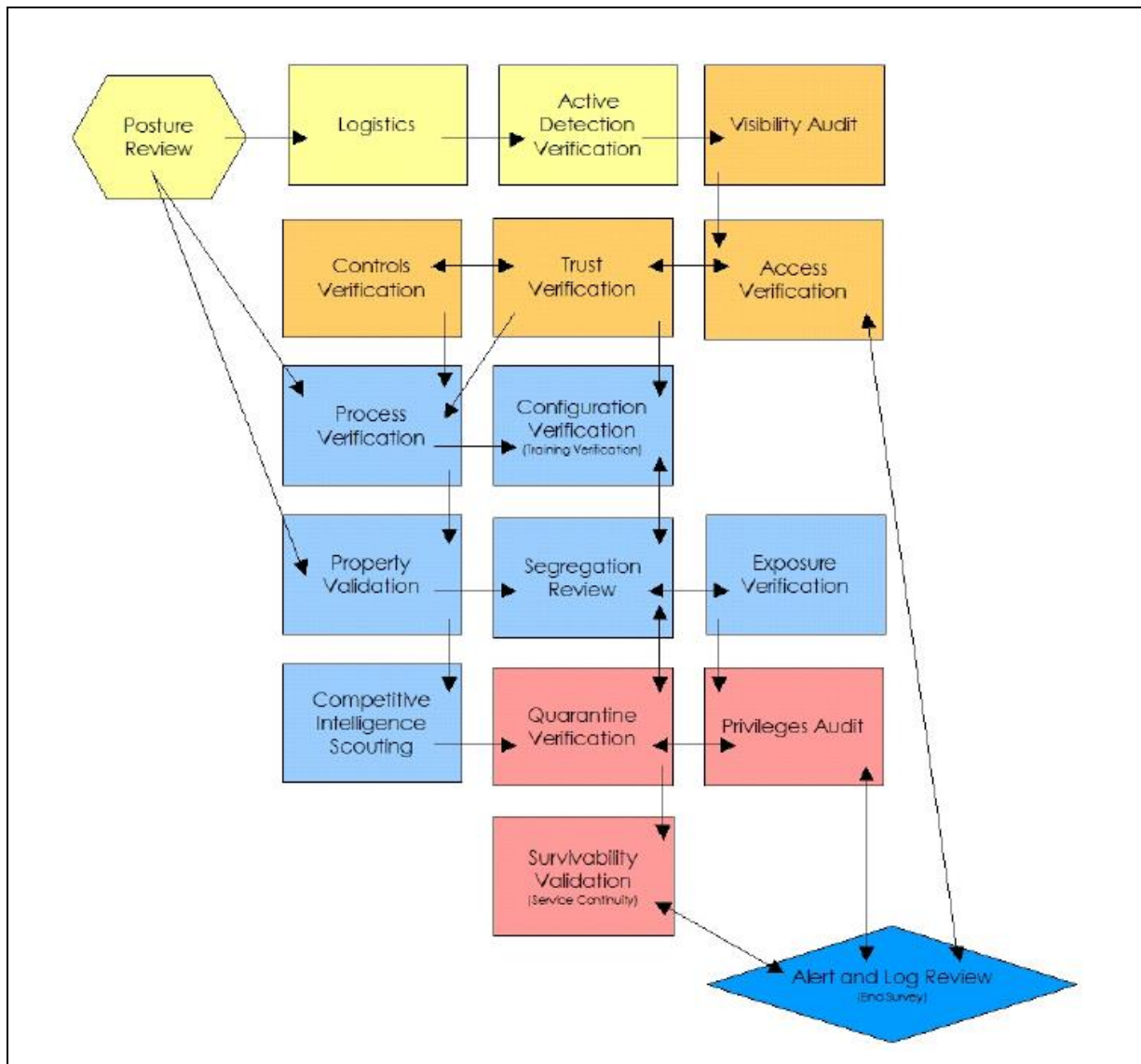


Figura 3. Metodología OSSTMM. Fuente: Open Source Security Testing Methodology Manual Herzong (2010).

Colocar juntos los módulos proporciona una metodología completa la cual puede aplicarse sobre los tipos de pruebas de seguridad, si el objetivo es un sistema en particular, una ubicación, una persona, un proceso o procesos (Herzong, 2010).

Esta metodología pretende que la pruebas sean lo más completas y eficientes posibles.

2.3.2. Sistema de puntuación de vulnerabilidad común (CVSS)

La metodología CVSS (Common Vulnerability Score System), está bajo la custodia de Forum of Incident Response and Security Teams (FIRST), pero se trata de una metodología completamente abierta, por lo que puede ser utilizado libremente (Quintero & Novoa, 2015).

La metodología CVSS es un sistema de puntaje que está diseñado para proveer un método abierto y estándar que permite estimar el impacto de las vulnerabilidades identificadas en un entorno informático, es decir, contribuye a cuantificar la gravedad que pueden representar dichas vulnerabilidades (Quintero & Novoa, 2015).

CVSS se compone de tres grupos métricos: base, temporal y ambiental.

La puntuación base refleja la gravedad de una vulnerabilidad de acuerdo con sus características intrínsecas que son constantes a lo largo del tiempo y supone el impacto razonable del peor de los casos en diferentes entornos implementados (First, 2019).

Las métricas temporales ajustan la gravedad de la base de una vulnerabilidad en función de factores que cambian con el tiempo, como la disponibilidad.

Las métricas de entorno ajustan las severidades base y temporal a un entorno informático específico. Consideran factores como la presencia de mitigaciones en ese entorno.

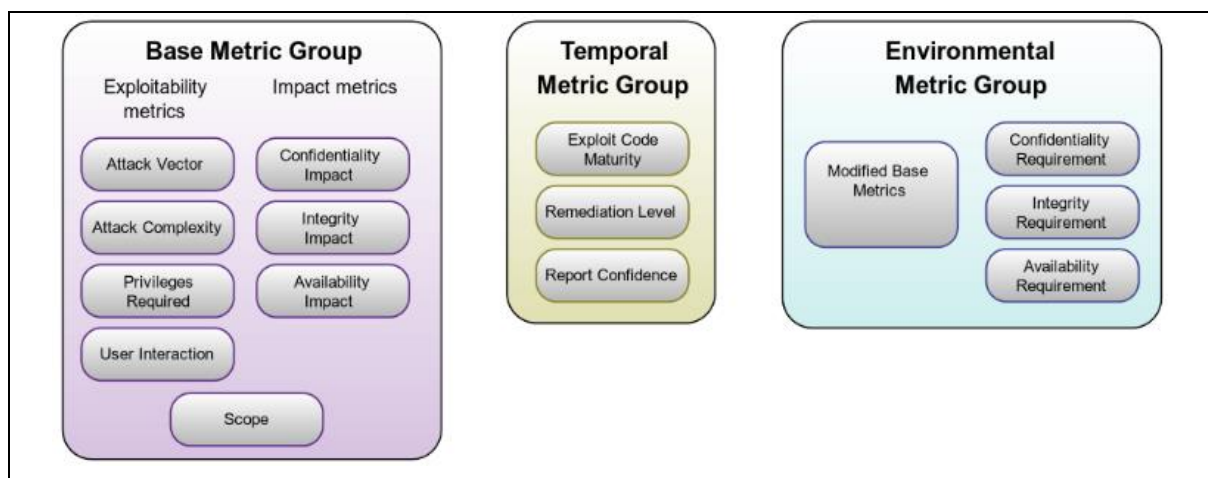


Figura 4. Grupo de métricas CVSS. Fuente: UIT (2012).

En el grupo de métricas base representa las características intrínsecas de una vulnerabilidad que son constantes a lo largo del tiempo y en los entornos de los usuarios. Se compone de dos conjuntos de métricas: las métricas de explotabilidad y las métricas de impacto.

El grupo de métricas temporales refleja las características de una vulnerabilidad que puede cambiar con el tiempo, pero no en los entornos de los usuarios.

El grupo de métricas de entorno representa las características de tipos de vulnerabilidad que son relevantes y únicas para el entorno de un usuario en particular. Las consideraciones incluyen la presencia de controles de seguridad que pueden mitigar algunas o todas las consecuencias de un ataque exitoso.

La metodología CVSS empieza a funcionar cuando un auditor o evaluador asigna valores a las métricas que varía de 0.0 a 10.0 como se muestra en la figura cinco.

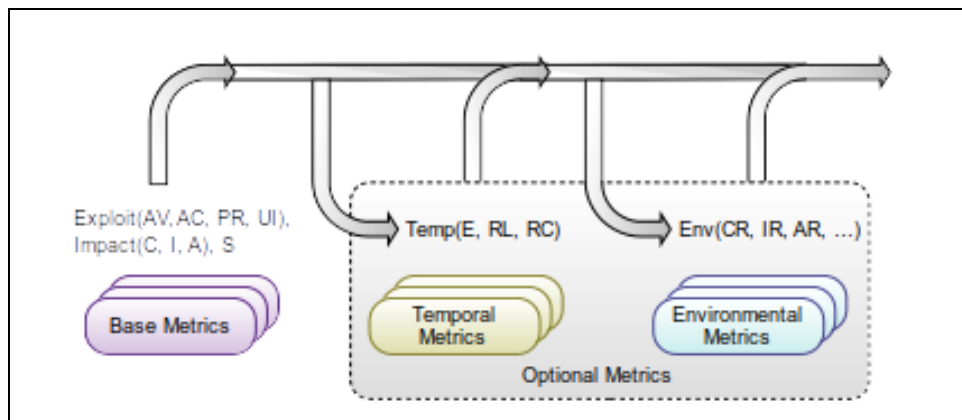


Figura 5. Métricas y Ecuaciones CVSS. Fuente: First (2019).

Los valores obtenidos en el puntaje base generalmente son producidos por la organización que mantiene el producto vulnerable, o un tercero que califica en su nombre.

Es normal que sólo se publiquen las métricas base, ya que estas no cambian con el tiempo y son comunes en todos los entornos. Los auditores o evaluadores que utilizan CVSS deben complementar el puntaje base con puntajes temporales y ambientales específicos para su uso del producto vulnerable para producir una severidad más precisa para su entorno organizacional (First, 2019).

2.3.3. Análisis comparativo de las metodologías analizadas

En la Tabla 3 se presenta un cuadro comparativo de las dos metodologías OSSTMM (Open Source Security Testing Methodology Manual) y CVSS (Common Vulnerability Score System), en las cuales se indican las características principales como también sus ventajas y desventajas.

Característica	OSSTMM	CVSS
Rigor de la metodología	La metodología OSSTMM se actualiza constantemente, la empresa que la actualiza es Institute for Security and Open Methodologies (ISECOM), es una metodología con alto rigor.	La metodología CVSS se actualiza de manera regular, está bajo la custodia de Forum of Incident Response and Security Teams (FIRST), es una metodología de alto rigor.
Ámbito y enfoque de la metodología	Esta metodología tiene enfoque operativo que permite evaluar los huecos de seguridad de una empresa.	CVSS está enfocada al análisis y evaluación de riesgos de cualquier empresa.
Facilidad de uso de la metodología	Esta metodología tiene un grado de dificultad medio, ya que se requiere que el auditor tenga experticia sobre el manejo de herramientas para cubrir las técnicas que se menciona en esta metodología.	CVSS a pesar de ser muy técnica y específica ya que trabaja sobre redes de datos, comunicaciones abiertas y seguridad, existen en internet varios ejemplos de uso, por lo cual su facilidad de uso es alta.
Métricas de la metodología	La métrica de medida es el RAV (Valores de evaluación de riesgo), la cual permite medir con valor numérico la cantidad de interacciones no controladas en contra de un objetivo.	CVSS tiene tres tipos de métricas las métricas bases, métricas temporales y métricas de ámbito, las cuales ayudan a evaluar el riesgo.
Alcance de la metodología	La metodología OSSTMM pretende cubrir todos los elementos de una red para localizar vulnerabilidades y determinar el RAV (Valores de evaluación de riesgo), y con ello el auditor pueda mitigar sus vulnerabilidades.	El alcance de CVSS es proporcionar un enfoque normalizado de los impactos de las vulnerabilidades de las tecnologías de la información, para reflejar con mayor exactitud el riesgo de estas.
Profundidad de la metodología	OSSTMM da una serie de vectores para analizar las vulnerabilidades desde el ámbito físico de las instalaciones de una empresa hasta ámbito lógico de las comunicaciones.	CVSS cuenta con métricas bases, temporales y de entorno que permite cubrir los elementos de una red.

Entornos de aplicabilidad de la metodología	OSSTMM al ser una metodología completa puede ser utilizada en diferentes empresas sean grandes o Pymes, estas empresas pueden ser públicas, privadas, sector financiero, sector manufacturero, sector alimenticio entre otras.	CVSS al tener un alcance específico y estar orientada a la localización de vulnerabilidades en redes de datos, comunicaciones abiertas y seguridad, lo utilizan proveedores de boletines de vulnerabilidades, vendedores de aplicaciones de software, investigadores entre otras.
Ventajas metodología	* Existe guías y documentación en Internet sobre esta metodología. * Se tiene soporte sobre esta metodología mediante una comunidad a nivel global. * Posee un alto grado en la calidad en los resultados. * Hace énfasis en estándares de seguridad de la información y seguridad informática. Cuenta con una calculadora para el RAV (Valores de evaluación de riesgo).	* CVSS proporciona métricas muy detalladas para la selección de objetivos a ser analizados. * CVSS está bajo el cargo de Forum of Incident Response and Security Teams (FIRST) que es líder y líder mundial reconocido en respuesta a incidentes. * Existe documentación y ejemplos en la web para aplicar esta metodología. * Cuenta con una calculadora de puntuación de vulnerabilidades.
Desventajas metodología	* OSSTMM no es adaptable con otras metodologías. * Al tener vectores de análisis la metodología no indica los objetivos que se debe seleccionar para el análisis.	* Los valores colocados de 0 a 10 en las métricas de entorno son colocados por los usuarios, en consecuencia, el valor de la vulnerabilidad podría variar. * CVSS lo utilizan mayoritariamente los vendedores de aplicaciones de software, proveedores de boletines de vulnerabilidades, entre otros.
Evaluación del riesgo	Se utilizan los RAVS para medir los niveles de riesgos.	Se define la puntuación de las vulnerabilidades de acuerdo a los criterios establecidos en la metodología, para aplicar la calculadora y fórmulas establecidas para la valoración.

Opinión personal sobre la metodología	OSSTMM es una metodología completa en la cual muestra los criterios que se debe considerar para auditar o evaluar las vulnerabilidades dentro de una organización, no establece ningún objetivo de análisis, pero dicta las directrices para la selección más adecuada del objetivo a ser analizado, para la evaluación de riesgos se utilizan los RAVS, por otra parte, se cuenta en la web con una gran cantidad de información sobre esta metodología.	CVSS es una metodología abierta que se la puede utilizar para la evaluación de vulnerabilidades dentro de una empresa, sin embargo, la utilizan de mayor medida los vendedores de boletines de vulnerabilidades, vendedores de aplicaciones de software, investigadores, entre otros. Esta metodología indica las métricas a considerarse para el análisis de vulnerabilidades, de igual forma indica la ponderación de cada vulnerabilidad para ser aplicada en la calculadora y fórmulas establecidas para valorar el riesgo.
---------------------------------------	---	---

Tabla 3. Cuadro comparativo de metodologías de análisis de vulnerabilidades. Fuente: Henry Daniel Calero Suntasig.

2.4. Herramientas de análisis de vulnerabilidades

2.4.1. Tráfico de red

Existen varias herramientas para el análisis de tráfico de red en tiempo real, las aplicaciones más utilizadas son:

- Wireshark
- Tcpdump
- Snort

Estas aplicaciones se ejecutan sobre plataforma de software libre y en algunos casos como Wireshark se puede encontrar para multiplataforma (Windows, MAC, Linux, entre otros).

Wireshark: Es una aplicación multiplataforma (Windows, MAC, Linux, entre otros), que permite analizar los paquetes de datos de ida y vuelta dentro de una red, como también los protocolos de comunicación que se están ejecutando.

Una de las ventajas que tiene esta herramienta es la presentación de resultados, ya que cuenta con un entorno gráfico de fácil interpretación para el auditor o evaluador.

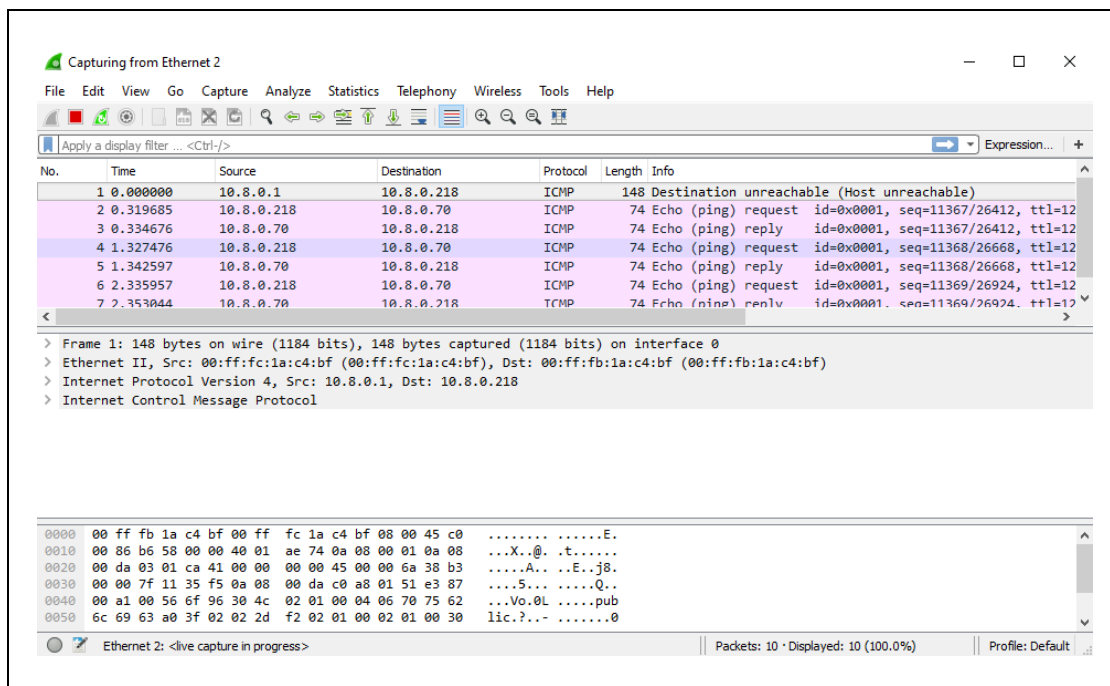


Figura 6. Interfaz gráfica de Wireshark. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Disponible para varias plataformas entre las más importantes Linux y Windows
- Captura de paquetes en tiempo real desde una o más interfaz de red.
- Muestra los paquetes con información detallada.
- Admite el formato estándar de archivos tcpdump.
- Permite abrir y guardar paquetes capturados.
- Permite el filtrado de información por paquetes, protocolos, IP's, etc.
- Resalta el resultado de paquetes dependiendo el filtro.
- Permite crear estadísticas.

TCPDUMP: Es una aplicación original de Linux, se ejecuta por la línea de comandos, a diferencia de Wireshark esta aplicación no es multiplataforma, la captura de paquetes se la realiza por medio de una interfaz de red, esta información se almacena en un fichero previamente determinado, para la interpretación de resultados se debe abrir el fichero guardado en otra aplicación como Wireshark.

```

root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:09:58.402244 ARP, Request who-has 192.168.159.2 tell 192.168.159.1, length 46
13:09:58.405073 IP 192.168.159.131.43437 > 192.168.159.2.domain: 59002+ PTR? 2.1
59.168.192.in-addr.arpa. (44)
13:09:58.411389 IP 192.168.159.2.domain > 192.168.159.131.43437: 59002 NXDomain
0/1/0 (103)
13:09:58.427564 IP 192.168.159.131.57903 > 192.168.159.2.domain: 1977+ PTR? 1.15
9.168.192.in-addr.arpa. (44)
13:09:58.434122 IP 192.168.159.2.domain > 192.168.159.131.57903: 1977 NXDomain 0
/1/0 (103)
13:09:58.435099 IP 192.168.159.131.47105 > 192.168.159.2.domain: 17782+ PTR? 131
.159.168.192.in-addr.arpa. (46)
13:09:58.441186 IP 192.168.159.2.domain > 192.168.159.131.47105: 17782 NXDomain
0/1/0 (105)
13:09:58.961866 ARP, Request who-has 192.168.159.2 tell 192.168.159.1, length 46
13:09:59.962272 ARP, Request who-has 192.168.159.2 tell 192.168.159.1, length 46

```

Figura 7. TCPDUMP línea de comandos. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Captura de paquetes en tiempo real desde una interfaz de red.
- Permite guardar paquetes capturados en ficheros.

SNORT: Es una aplicación que permite realizar un análisis de tráfico de red en tiempo real, pero se la utiliza de mayor forma para la detección de intrusiones y el escaneo de puertos dentro de una red.

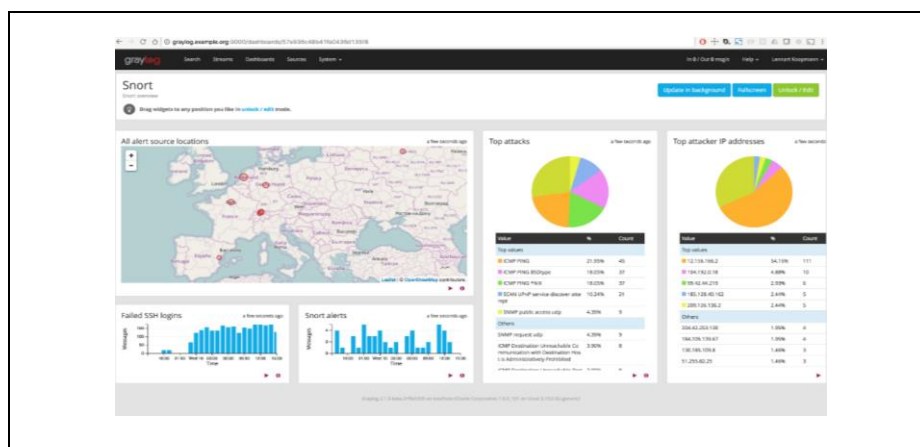


Figura 8. Interfaz gráfica de resultados SNORT. Fuente: Github (2019).

Principales características:

- Captura de paquetes en tiempo real desde una o más interfaz de red.
- Analiza protocolos de red.

- Presenta informe detallado de resultados.
- Captura paquetes en tiempo real.

Examinadas las tres herramientas de tráfico de red se determina que la mejor opción es Wireshark, ya que la principal función de Wireshark es la captura de paquetes dentro de la red a diferencia de Snort que su principal función es la detección de intrusiones, por otro lado, los resultados obtenidos en Wireshark son de fácil interpretación a diferencia de los resultados obtenidos por medio de Tcpdump.

2.4.2. Verificación de puertos

NAMP: Network Mapper (NAMP) es una aplicación de código abierto, su utilidad es escanear la red de datos para localizar puertos TCP o UDP abiertos, cuando localiza un puerto abierto se intenta realizar una conexión para identificar qué aplicación se encuentra ejecutando sobre el puerto abierto.

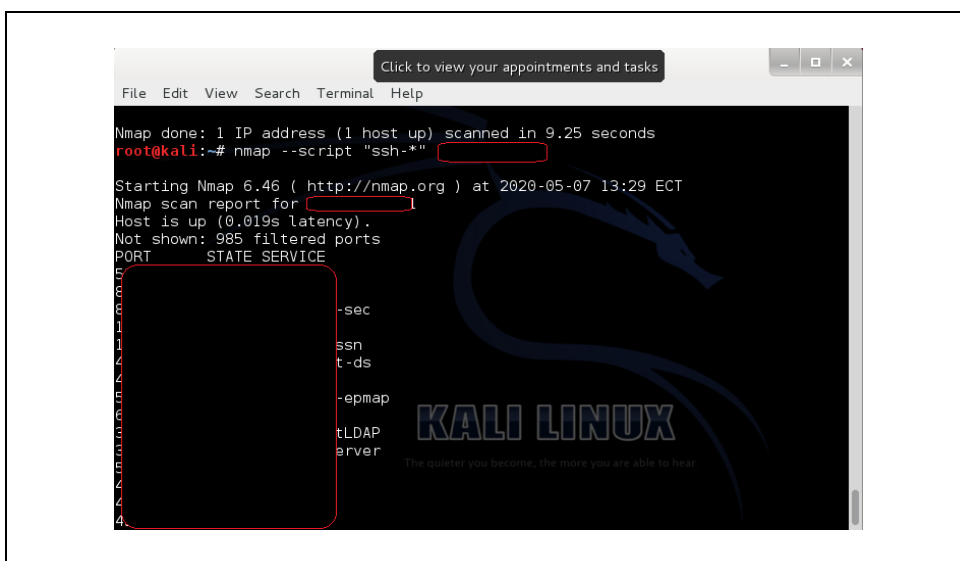


Figura 9. NMAP interfaz de línea de comandos. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Descubrimiento de equipos sobre una red.
- Escaneo de puertos TCP y UDP.
- Identificar puertos abiertos en un objetivo determinado.
- Detectar los servicios que se están ejecutando sobre un puerto abierto.

- Identificar qué sistema operativo y versión utiliza dicho objetivo.
- Descubrir ciertas características del hardware de red de la máquina objeto de prueba.

NESSUS: Es una aplicación muy similar a NMAP, realiza escaneos de red para localizar posibles vulnerabilidades, la diferencia radica que **NESSUS** al localizar vulnerabilidades utiliza exploits para explotarlas, otra de las diferencias de **NESSUS** con respecto a NMAP es sus resultados que los presenta dentro de un entorno gráfico para que el auditor o evaluador lo puedan interpretar.

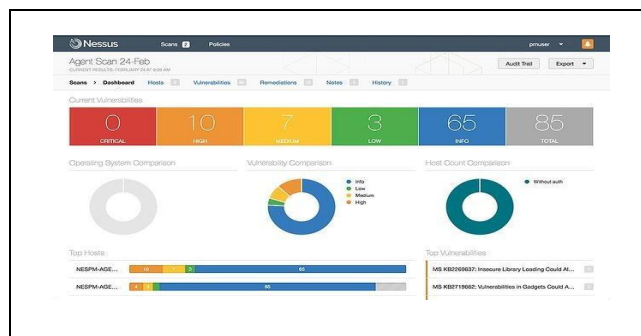


Figura 10. **NESSUS** Interfaz gráfica de resultados. Fuente: Security (2020).

Principales características:

- Explotación de vulnerabilidades por medio de exploits.
- Presentación de resultados de forma gráfica.
- Actualizaciones constantes.

NETCAT: Esta aplicación es de código abierto, permite el escaneo sobre una red para localizar puertos abiertos por medio de un Shell y forzar las conexiones TCP / UDP con el propósito de rastrear puertos o transferencias de archivos entre equipos.

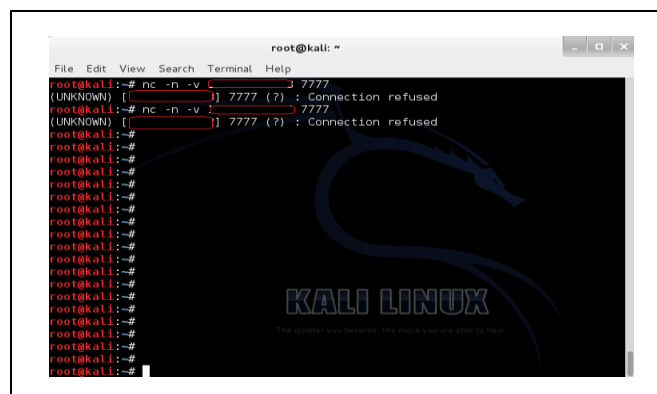


Figura 11. **NETCAT** consola de línea de comandos. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Escaneo de puertos TCP y UDP.
- Escaneo sobre protocolos IPv4 / IPv6

Al realizar el análisis entre las tres herramientas para la verificación de puertos se determina que la mejor opción a utilizar es NMAP, ya que permite el escaneo de puertos y validar cual se encuentra abierto y que aplicación se está ejecutando sobre ese puerto, además es software libre por lo que no se paga ninguna licencia, a diferencia de NESSUS se requiere contar con una licencia de pago para ser utilizado, por otra parte NMAP a diferencia de NETCAT entrega un informe detallado, los informes que entrega NMAP lo realiza por medio de una interfaz gráfica y NETCAT entrega la información por línea de comandos.

2.4.3. Captura de contraseñas

KISMET: Es una aplicación de software libre, considerado como un sistema de detecciones de intrusiones para redes inalámbricas, es decir que es un sniffer que se encuentra de forma pasiva dentro de la red, que no envía paquetes detectables, con el objetivo de detectar la presencia de puntos de acceso y clientes inalámbricos.

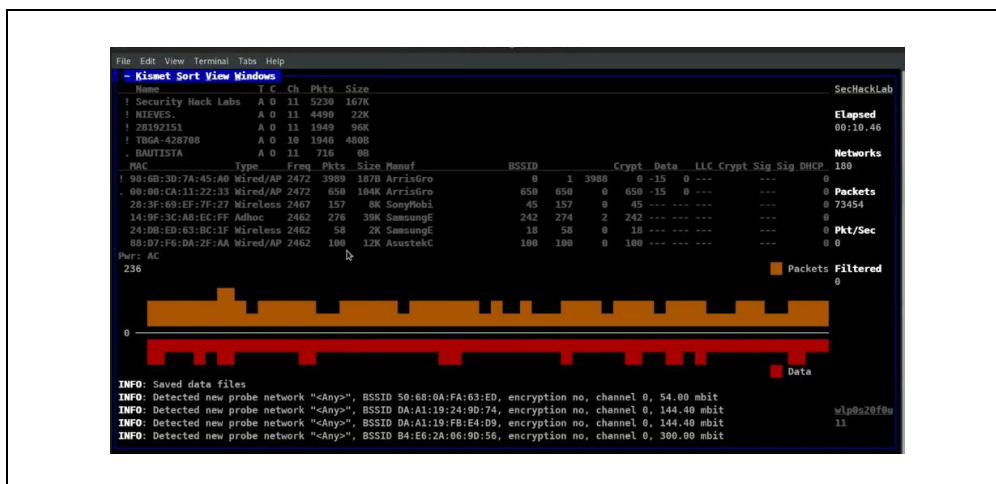


Figura 12. KISMET consola de monitoreo. Fuente: Carrera (2018).

Principales características:

- Funcionamiento de forma pasiva.
- Contiene sistema de detección de intrusos.
- Permite exportar archivos de tráfico guardados a Wireshark.
- Soportado sobre Linux y Windows (limitado).

AIRCRAK-NG: Es una aplicación de código abierto que permite analizar e inyectar paquetes multiplataforma con el objetivo de descifrar claves de redes inalámbricas, las contraseñas que se pueden descifrar son de tipo WEP y WPA/WPA2-PSK.

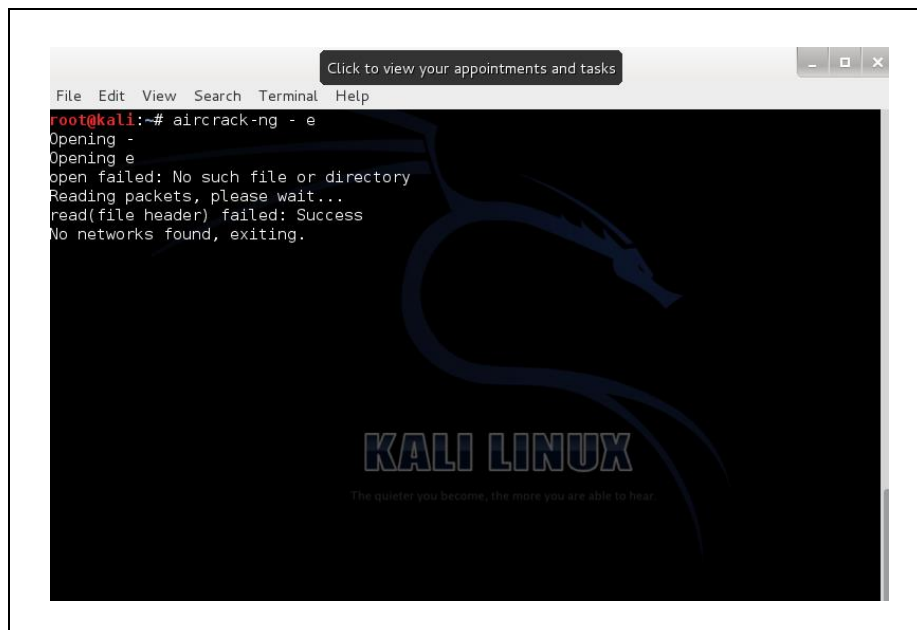
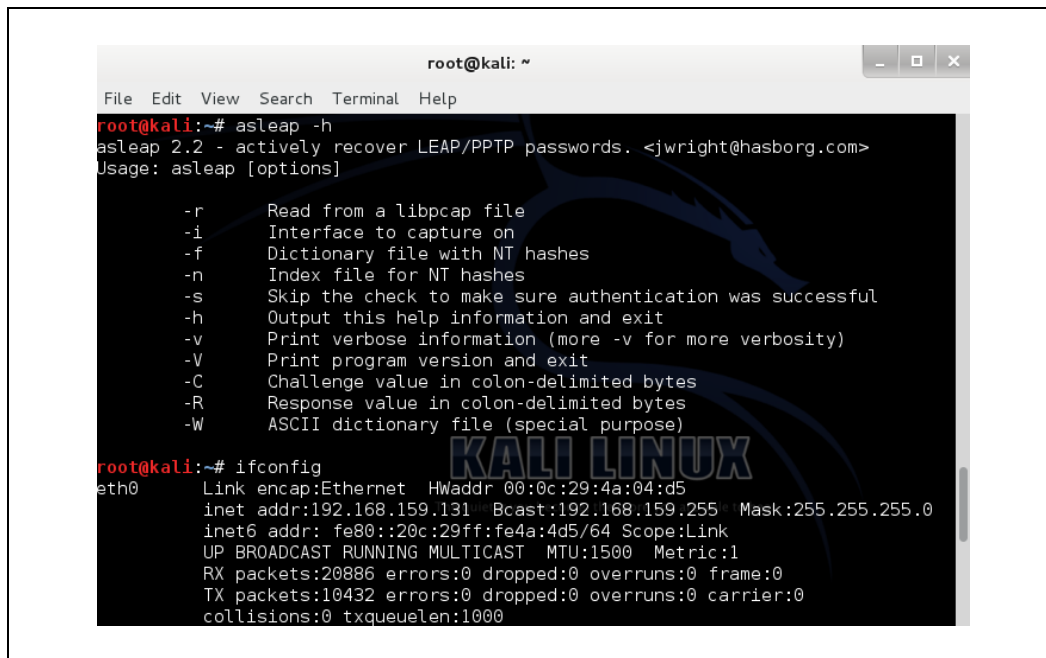


Figura 13. AIRCRACK-NG Consola. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Contiene una suite completa para el análisis de redes inalámbricas.
- Permite barrido y descubrimiento de claves en redes inalámbricas.
- Compatible con numerosas antenas inalámbricas.
- Permite realizar monitoreo de red inalámbrica.
- Permite realizar ataques dentro de la red inalámbrica.
- Permite realizar pruebas con las antenas inalámbricas directamente conectadas.

ASLEAP: Es una aplicación que permite capturar y descifrar contraseñas del protocolo LEAP (Protocolo de Autenticación Ampliable Desarrollado por Cisco), también permite leer y capturar el tráfico de cualquier tarjeta de red inalámbrica en el modo RFMON (modo de monitor), por otra parte, ASLEAP puede obtener claves de sesiones PPTP (Point to Point Tunneling Protocol) y descifrar tráfico de una VPN.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# asleap -h  
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>  
Usage: asleap [options]  
  
-r      Read from a libpcap file  
-i      Interface to capture on  
-f      Dictionary file with NT hashes  
-n      Index file for NT hashes  
-s      Skip the check to make sure authentication was successful  
-h      Output this help information and exit  
-v      Print verbose information (more -v for more verbosity)  
-V      Print program version and exit  
-C      Challenge value in colon-delimited bytes  
-R      Response value in colon-delimited bytes  
-W      ASCII dictionary file (special purpose)  
  
root@kali:~# ifconfig  
eth0    Link encap:Ethernet  HWaddr 00:0c:29:4a:04:d5  
        inet addr:192.168.159.131  Bcast:192.168.159.255  Mask:255.255.255.0  
        inet6 addr: fe80::20c:29ff:fe4a:4d5/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:20886 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:10432 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000
```

Figura 14. ASLEAP Consola de línea de comandos. Fuente: Henry Daniel Calero Suntasig.

Principales características:

- Captura paquetes y descifra contraseñas del protocolo LEAP.
- Integración con Air-Jack.
- Presentación de resultados en consola de línea de comandos.
- No permite realizar inyección de paquetes

Examinadas las tres herramientas para la captura de contraseñas se determina que la mejor opción con respecto a KISMET y ASLEAP es AIRCRCK-NG ya que cuenta con una suite completa para realizar este tipo de capturas.

2.5. Legislación Ecuatoriana que regula delitos informáticos

Antes de hacer mención a las fases de la metodología OSSTMM se menciona las leyes y decretos vigentes en el Ecuador contra los delitos informáticos.

- Código Orgánico Integral Penal (COIP).
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley Especial de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos.
- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

El COIP (2014) en el artículo 232 indica lo siguiente: Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

2.6. Valores Evaluados de Riesgo (RAV) métrica operacional

La métrica RAV es proporcionada por la metodología OSSTMM, para medir con un valor numérico las vulnerabilidades en contra de un objetivo, para cálculo del RAV se utiliza los valores obtenidos entre operaciones, limitaciones y controles existentes como muestra la Tabla 4.

El RAV no mide el riesgo de una superficie de ataque, sino que permite medirlo. No puede decir si un objetivo en particular será atacado, sin embargo, puede decir en qué lugar será atacado, contra qué tipos de ataques puede defenderse el objetivo con éxito, qué tan profundo puede llegar un atacante y cuánto daño puede hacerse. Con esa información, es posible evaluar los riesgos con mucha más precisión. (Herzong, 2010, p.63).

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad (PV)	Exposición (LE)
	Acceso (PA)	Vulnerabilidad (LV)
	Confianza (PT)	
	Autenticación (LCAu)	
Clase A	Indemnización (LCId)	Debilidad (LW)
	Resiliencia (LCRe)	
	Subyugación (LCSu)	
	Continuidad (LCCT)	
Controles	No repudio (LCNR)	Preocupación (LC)
	Confidencialidad (LCCf)	
	Privacidad (LCPr)	
	Integridad (LCIt)	
Clase B	Ala rama (LCAI)	Anomalías (LA)

Tabla 4. Estructura métrica operacional RAV. Fuente: Henry Daniel Calero Suntasig.

Según la metodología OSSTMM para el cálculo del RAV se obtiene lo siguiente:

$$\text{RAV} = \text{Controles Verdaderos} - \text{Porosidad} - \text{Limitaciones}$$

Figura 15. Cálculo de la seguridad. Fuente: Herzong (2010).

2.6.1. Seguridad Operacional (Porosidad)

La seguridad operacional es el primer factor para la obtención de la medición real actual de seguridad para los diferentes canales de la metodología OSSTMM, la seguridad operacional se obtiene de la sumatoria de la Visibilidad (PV), Acceso (PA) y Confianza (PT) (Herzong, 2010).

$$OpSec_{sum} = P_V + P_A + P_T$$

Figura 16. Cálculo Seguridad Operacional (Porosidad). Fuente: Herzong (2010).

2.6.2. Controles verdaderos (TC)

El segundo factor para el cálculo del RAV son los controles verdaderos, es decir los mecanismos implementados para proteger la seguridad, el valor TCsum se obtiene con la sumatoria de los Controles A: Autenticación (TCAu), Identificación (TCId), Resistencia (TCRe), Subyugación (TCSu), Continuidad (TC Ct) y Controles B: No repudio (TCNr), Confidencialidad (TCCf), Privacidad (TCPr), Integridad (TCIt), Alarama (TCAI). (Herzong, 2010)

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{It} + TC_{Pr} + TC_{Cf} + TC_{Al}$$

Figura 17. Cálculo Controles Verdaderos (TC). Fuente: Herzong (2010)

Los controles ausentes (MC) de autenticación está dado por el siguiente cálculo:

$$MC_{Au} = OpSec_{sum} - TC_{Au}$$

Figura 18. Cálculo de Control Ausentes de Autenticación. Fuente: Herzong (2010).

Los controles ausentes (MC) están dados por la siguiente fórmula:

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{It} + MC_{Pr} + MC_{Cf} + MC_{Al}$$

Figura 19. Cálculo de Controles Ausentes (MC). Fuente: Herzong (2010).

2.6.3. Limitaciones

Las limitaciones se contabilizan de forma individual, el valor de las vulnerabilidades, debilidades y preocupaciones se basa en una relación inversa de la porosidad o suma OpSecsum (Herzong, 2010).

Las exposiciones y anomalías no plantean problemas por sí solas, sin embargo, estas se presentan cuando existe una vulnerabilidad, debilidad o preocupación. (Herzong, 2010).

2.6.4. Exposición

“La exposición es una acción, falla o error injustificable que proporciona visibilidad directa o indirecta de objetivos o activos dentro del canal de alcance elegido” (Herzong, 2010, p.28).

2.6.5. Vulnerabilidad

Es permitir el acceso de forma privilegiada a los activos de información o procesos internos de forma no autorizada (Herzong, 2010).

2.6.6. Debilidad

Es un fallo que anula los efectos de los controles de Clase A estos son: Autenticación (FCAu), Identificación (FCId), Resistencia (FCRe), Subyugación (FCSu), Continuidad (FCCt), la debilidad está dada por la sumatoria de los controles de Clase A.

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

Figura 20. Cálculo de la debilidad (L_W). Fuente: Herzong (2010).

2.6.7. Preocupación

Es un fallo que anula los efectos de los controles Clase B estos son: No Repudio (FCNr), Confidencialidad (FCCf), Privacidad (FCPr), Integridad (FCIt), Alarma (FCAI), la preocupación está dada por la sumatoria de los controles de Clase B.

$$L_C = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{AI}$$

Figura 21. Cálculo de la Preocupación. Fuente: Herzong (2010).

2.6.8. Anomalía

Es toda acción que no se identifica con facilidad, estas acciones no pueden ser medidas en operaciones normales (Herzong, 2010).

CAPÍTULO II

ANÁLISIS DE VULNERABILIDADES

3.1. Aplicación OSSTMM sobre la infraestructura de red de la Bolsa de Valores de Quito

Como se indicó anteriormente la metodología OSSTMM es un tipo de prueba completa para el análisis de vulnerabilidades, esta se va aplicar sobre la infraestructura de red de la Bolsa de Valores de Quito, esta metodología menciona el Proceso de Cuatro Puntos (4PP), que señala lo siguiente: “No confunda la formalidad de la presentación de los informes finales, no tiene que mostrar cada paso que se está haciendo, pero debe entender cómo llegar de la A a la C” (Herzong, 2010, p.43).

3.1.1. Fase de inducción

La fase de inducción es el comienzo del análisis de vulnerabilidades, en esta fase se debe tener presente el alcance y las limitaciones de las tareas que se van a realizar, así como también se debe contar con la autorización por escrito de la máxima autoridad de la Bolsa de Valores de Quito que es el Gerente General, Jeffry Illingworth, a fin de que el evaluador lleve este proceso dentro de los márgenes que son permitidos por la ley y que la información obtenida mediante las pruebas realizadas sea únicamente para fines evaluativos.

3.1.2. Fase de interacción

El evaluador en esta fase deberá interactuar de forma directa con los objetivos analizados para desencadenar respuestas para este análisis, además, recopilará información mediante diversas técnicas (entrevistas, encuestas y observaciones), para evaluar la seguridad actual de un canal, seguridad operacional, controles y limitaciones.

3.1.3. Fase de indagación

En la indagación el auditor o evaluador realizará una serie de pruebas u observaciones donde los resultados permitan detectar fortalezas y debilidades del sistema que está siendo auditado con el fin de justificar esas fortalezas y debilidades con evidencias.

3.1.4. Fase de intervención

La fase de intervención es la última fase de la evaluación de vulnerabilidades donde se centran en los recursos de los objetivos requeridos en la aplicación, mismos que se pueden intercambiar, cambiar, sobrecargar, o morir a causa de la penetración, esta es la fase final de una prueba de seguridad (Herzong, 2010).

Durante esta fase se genera informes por cada canal auditado con ayuda de la hoja de cálculo RAV la cual permite evaluar la eficiencia o deficiencia del canal auditado o evaluado, esta hoja de cálculo está disponible para la descarga en la siguiente página <https://www.isecom.org/research.html#content5-9d>.

3.2. Pruebas de seguridad humana Bolsa de Valores de Quito (BVQ)

Según Herzong (2010) este canal comprende el elemento humano de la comunicación donde la interacción es física o psicológica, este canal cubre la participación de personal operativo, el objetivo de estas pruebas es la concientización de seguridad del personal y la medición de brechas con las políticas de la organización.

Para estas pruebas se realizaron encuestas, observaciones y entrevistas a funcionarios de la BVQ, estas técnicas fueron utilizadas de la mejor manera con el fin de no comprometer la integridad y confidencialidad de las personas, las encuestas fueron de carácter anónimo.

En el Anexo 1 y 2 se puede observar las preguntas realizadas a los funcionarios de la BVQ.

3.2.1. Seguridad operacional

3.2.1.1. Visibilidad (PV)

Dentro de la visibilidad se debe enumerar el personal autorizado y el no autorizado para el acceso a la BVQ.

Técnica utilizada		Observación
Objetivo		Bolsa de Valores de Quito
Personal	Autorizado	No Autorizado
	1.- Presidente	
	2.- Gerente	
	3.- Departamento Administrativo RRHH	
	4.-Departamento Comercial	10.- Personal de Casas de Valores
Departamentos / Áreas	5.- Departamento Legal	11.- Accionistas
	6.- Departamento de Finanzas	12.- Personas Particulares
	7.- Departamento Operaciones / Estadístico	
	8.- Departamento de Tecnología	
	9.- Empresa de limpieza externa	

Tabla 5. Visibilidad canal Humano. Fuente: Henry Daniel Calero Suntasig.

Estos datos se obtuvieron mediante una entrevista verbal entre el Guardia de Seguridad del edificio Londres y la Asistente Administrativa (Recepcionista) de la BVQ, de igual forma, se observó alrededor de 5 días este comportamiento, contabilizando los ítems numéricos para visibilidad se obtuvo **PV=12**

3.2.1.2. Acceso (PA)

Para determinar el acceso se debe considerar todas las variables que se pueden presentar para el acceso a la información de la BVQ desde la entrada al edificio hasta el ingreso a las instalaciones.

Técnica utilizada	Encuesta y Observación
Objetivo	Bolsa de Valores de Quito. Funcionarios (BVQ)
	1.- Interacción Personal
	2.- Tarjetas de Acceso
Información Obtenida	3.- Computadoras de trabajo
	4.- Dispositivos móviles
	5.- Información física

Tabla 6. Acceso Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Los diferentes puntos de acceso para dentro del canal humano se muestran en la tabla 6, con esto se determina que **PA=5**

3.2.1.3. Confianza (PT)

La confianza dentro del personal hace referencia a l acceso y no divulgación a la información clasificada de la institución, también se analiza la información publicada de los funcionarios en redes sociales.

Técnica utilizada	Ingeniería Social y Encuestas
Objetivo	Bolsa de Valores de Quito funcionarios (BVQ) 1.- Acceso a instalaciones 2.- Acceso a tarjetas magnéticas 3.- Acceso a los activos de la información
Información Obtenida	4.- Obtención de credenciales 5.- Obtención de fotografías personales 6.- Obtención de correos personales 7.- Obtención de cuentas de redes sociales

Tabla 7 Confianza Canal Humano Fuente: Henry Daniel Calero Suntasig.

Para esta prueba se realizaron encuestas y se utilizó herramientas de redes sociales para buscar la información de los funcionarios de la BVQ.

Experiencia  Bolsa de Valores de Quito 2019 – actualidad · 1 año Quito	Experiencia  Comercial Bolsa de Valores de Quito · Jornada completa ene. de 2020 – actualidad · 3 meses Ecuador
Experiencia  Analista Comercial Senior Bolsa de Valores de Quito sept. de 2018 – actualidad · 1 año y 7 meses Quito, Ecuador	Experiencia  Analista Comercial Bolsa de Valores de Quito mar. de 2009 – actualidad · 11 años y 1 mes Quito, Ecuador

Figura 22. Búsqueda de funcionarios en LinkedIn. Fuente: Henry Daniel Calero Suntasig.

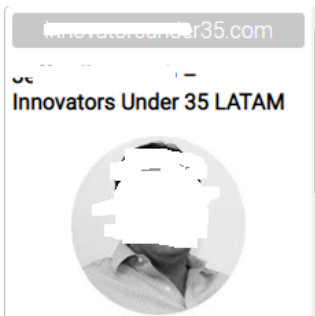
	
---	--

Figura 23. Búsqueda de funcionarios en WebMii. Fuente: Henry Daniel Calero Suntasig.

Mediante las herramientas como LinkedIn, WebMii, Pipl, Facebook, entre otros se pudo obtener información personal de los funcionarios de la BVQ, como fotografías, cuentas de correo electrónico, cuentas de redes sociales, etc. Como resultado se obtuvo el valor numérico para confianza es **PT = 7**.

3.2.2. Controles

Se deben enumerar los controles existentes para la protección de la información institucional.

3.2.2.1. Autenticación (LCAu)

En la autenticación pretende enumerar los medios para la interacción en las instalaciones de la BVQ.

Técnica utilizada	Observación
Objetivo	Edificio Londres Bolsa de Valores de Quito
Medios de comunicación autorizados	1.- Interacción con guardia de seguridad (PB) 2.- Autorización para el acceso 3.- Autorización vía telefónica 4.- Agendamiento de reuniones autorizadas

Tabla 8. Autenticación Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Mediante la observación se pudo obtuvo los datos que pueden utilizar las personas para tener acceso a las instalaciones de la BVQ, primero deben tener acceso al edificio Londres y seguido a la BVQ, el valor numérico para la autenticación es **LCAu= 4**.

3.2.2.2. Indemnización (LCId)

Se refiere a verificar la documentación de políticas, procedimientos, acuerdos de confidencialidad y otros que maneja la institución con todo el personal de la BVQ.

Técnica utilizada	Observación y cumplimiento del Reglamento Interno
Objetivo	Funcionarios BVQ Visitantes Público en general
Compromisos y obligaciones del reglamento interno de la BVQ	1.- Horario de ingreso y salida personal BVQ 2.-Horario de atención a las visitas y público en general 3.- Llamado de atención verbal 4.- Llamando de atención por escrito 5.- Acuerdos de confidencialidad

6.- Normas internas de la institución

Tabla 9 Indemnización Canal Humano Fuente: Henry Daniel Calero Suntasig

Para este control se recurrió al reglamento interno de la institución y a los compromisos y obligaciones de los funcionarios de la BVQ, como resultado para la Indemnización es **LCId=6**.

3.2.2.3. Resiliencia (LCRe)

La resiliencia hace referencia al libre acceso a la BVQ del personal autorizado, con esto se tendrá acceso directo a los activos de la institución.

Técnica utilizada	Observación y Encuesta
Objetivo	Bolsa de Valores de Quito
Acceso sin restricciones	1.- Funcionarios BVQ 2.-Empresa de limpieza externa

Tabla 10. Resiliencia Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Para este control se realizó una encuesta y se utilizó la técnica de observación determinando los accesos sin restricciones a la BVQ, teniendo como resultado un valor para la Resiliencia de **LCRe = 2**.

3.2.2.4. Subyugación (LCSu)

Es el control que permite asegurar las interacciones que se producen de acuerdo con los procedimientos, procesos y políticas predefinidos dentro de la institución.

Técnica utilizada	Observación y Encuesta
Objetivo	Funcionarios BVQ Visitantes Público en general
Controles no regulados	**

Tabla 11. Subyugación Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Existen acuerdos de confidencialidad y de no divulgación de información que aplican a los funcionarios de la BVQ, visitantes y público en general, se tiene procesos definidos para el uso de correos electrónicos personales, uso de redes sociales y uso de teléfonos personales dentro de la institución, en tal virtud para la subyugación se obtuvo un valor de **LCSu= 0**.

3.2.2.5. Continuidad (LCCT)

Dentro de la metodología sugiere que se debe verificar y enumerar los escenarios en los que los retrasos de los funcionarios se canalizan de forma adecuada a través de personal o un medio automatizado para el acceso oportuno a servicios, procesos y operaciones (Herzong, 2010).

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito. Funcionarios (BVQ) * Calamidad domestica
Razón de ausencia	* Enfermedad * Retrasos (tráfico, avería de auto, transporte público, etc.) * Vacaciones
Inconvenientes	1.- Departamento Operaciones / Estadístico 2.- Departamento de Tecnología

Tabla 12. Continuidad Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Mediante la observación se determina que si existe ausencia o retraso del personal que realiza la apertura de puertas de la BVQ pueden generar inconvenientes a las áreas de Tecnología y Operaciones para subir los procesos de negociación, para este control se obtuvo un valor de **LCCT = 2**.

3.2.2.6. No repudio LCNR

Este control permite enumerar y verificar el uso de los sistemas de monitoreo y control de accesos para identificar y registrar adecuadamente el acceso o interacciones con activos de la institución, para contar con evidencia suficiente y afrontar el repudio, se debe documentar la profundidad de la interacción que se registra (Herzong, 2010).

Técnica utilizada	Observación y Encuesta
Registro de acceso / identificación	Funcionarios BVQ 1.- Biométrico, tarjetas de acceso Personal de Limpieza Externa 2.- Bitácora de ingreso

Tabla 13. No Repudio Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Los funcionarios de la BVQ para acceder deben registrar su hora de entrada en el biométrico y para el ingreso de las instalaciones deben utilizar su tarjeta magnética de acceso,

el personal de limpieza externa se registra en una bitácora, para No Repudio se obtuvo el valor de **LCNR=2**.

3.2.2.7. Confidencialidad (LCCf)

En la confidencialidad se debe enumerar y verificar el tipo de comunicación interpersonal que existe dentro de la institución, se debe considerar la comunicación física y los elementos que se transportan entre los procesos internos y externos, el personal utilizar códigos, lenguaje indescifrable, interacciones personales para garantizar la confidencialidad de la comunicación (Herzong, 2010).

Técnica utilizada	Observación y Encuesta
Tipos de comunicación	1.- Documex
	2.- Correo electrónico institucional
	3.- Herramientas de colaboración (office 365)
	4.- Videoconferencias
	5.- Vía telefónica (entre extensiones)

Tabla 14. Confidencialidad Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Se cuenta con líneas de comunicación segura dentro de la BVQ, el control de confidencialidad obtuvo un valor de **LCCf = 5**.

3.2.2.8. Privacidad (LCPr)

En la privacidad se debe enumerar y probar el uso de los controles implementados dentro de la institución, que permita proteger la privacidad de los activos.

Técnica utilizada	Observación y Encuesta
Interacción segura	1.- Entrega de Documentos de forma personal
	2.- Interacciones personales dentro de espacios seguros

Tabla 15. Privacidad Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Para precautelar la información se entregan los documentos físicos de forma personal además se cuenta con espacios seguros para la interacción entre personal interno o externo, el control de privacidad tiene un valor de **LCPr = 2**.

3.2.2.9. Integridad (LCIt)

En el control de integridad se debe enumerar y probar los controles implementados dentro de la institución, que permita garantizar la integridad de los activos, estos activos

pueden ser transportados dentro o fuera de la institución para precautelar su integridad, se debe usar sellos, firmas, hash o marcas cifradas para proteger y asegurar que los activos no se puedan cambiar (Herzong, 2010).

Técnica utilizada	Observación y Encuesta
Trasporte o envío de activos	1.- Registro en bitácora o sistema Documex
	2.- Asignación de número único de documento
	3.- Firmas y sellos.
	4.- Firmas electrónicas

Tabla 16. Integridad Canal Humano. Fuente: Henry Daniel Calero Suntasig

El transporte de documentos sean estos internos o externos se realiza de forma segura y son registrados con un número único para ser procesados, estos deben tener firma y sello físico o contar con firma electrónica, para la integridad se obtuvo un valor de **LCIt= 4**.

3.2.2.10. Alarma (LCAI)

En el control de alarma se debe verificar y enumerar los sistemas implementados dentro de la institución, los cuales se utilizan para el registro o mensaje de advertencia para cada puerta de acceso, donde el personal pueda observar una situación sospechosa o bajo sospecha de intentos de elusión, actividad fraudulenta, traspaso o incumplimiento previamente establecidos en las políticas, procedimiento o procesos de la empresa (Herzong, 2010).

Técnica utilizada	Observación y Encuesta
Métodos de seguridad de acceso	1.- Sistema de alarma (registro)
	2.- Llamadas telefónicas de verificación
	3.- Cámaras de seguridad
	4.- Guardia
	5.- Sistema de accesos de puertas (registro)

Tabla 17. Alarma Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Ante una actitud sospechosa se cuenta con un sistema de alarma, guardia del edificio y cámaras de seguridad, el control de alarma se obtuvo un valor de **LCAI = 5**.

3.2.3. Limitaciones

3.2.3.1. Exposición (LE)

Se considera a la divulgación de información de forma no intencional como intencional, por ejemplo: entregar información institucional vía telefónica; que los mecanismos de seguridad no funcionen de forma adecuada, como dejar abierta la puerta de acceso para cualquier persona ajena a la entidad.

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Exposición	1.- Personas no autorizadas tengan ingreso a las instalaciones de la BVQ sin supervisión. 2.- Bitácora de visitas de guardia expuesto al público.

Tabla 18. Exposición Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Los datos obtenidos en la exposición son **LE = 2**.

3.2.3.2. Vulnerabilidad (LV)

Permite el acceso privilegiado o entrega de información a personas no autorizados.

Técnica utilizada	Encuesta y Observación
Objetivo	Bolsa de Valores de Quito. Funcionarios (BVQ)
Vulnerabilidad	1.- Extraviar la tarjeta de acceso y no reportar oportunamente con el encargado para el bloqueo. 2.- No cumplir con la política de bloqueo de equipos en caso de ausencia temporal del lugar de trabajo. 3.- Entregar información de uso interno vía telefónica. 4.- Entregar información privilegiada a funcionarios en periodo de prueba o practicantes. 5.- Uso de dispositivos de almacenamiento externo. 6.- Uso de correo personal para compartir información institucional.

Tabla 19. Vulnerabilidad Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Los datos obtenidos en la Vulnerabilidad es **LV = 6**.

3.2.3.3. Debilidad (Lw)

La debilidad es la falla o mal funcionamiento que impide, reduce, abusa o invalida los efectos de los cinco controles de Clase A: autenticación, indemnización, resiliencia, subyugación y continuidad (Herzong, 2010).

Técnica utilizada	Observación y cumplimiento del Reglamento Interno
Autenticación	1.- Suplantación de identidad
Indemnización	1.- Incumplimiento del reglamento interno 2.- Incumplimiento de los procedimientos o procesos institucionales

Tabla 20. Debilidad Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Para resiliencia y continuidad se repite la misma debilidad “*Incumplimiento del reglamento interno*” por tal razón no se la coloca nuevamente, en el control de subyugación no se localiza debilidades.

Aplicando la fórmula de la figura 20 se obtiene:

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ci}$$

$$L_W = 1 + 2 + 0 + 0 + 0$$

$$L_W = 3$$

3.2.3.4. Preocupación (Lc)

La preocupación es la falla o mal funcionamiento que impide, reduce, abusa o invalida los efectos de los cinco controles de Clase B: no repudio, confidencialidad, privacidad, integridad y alarma.

Técnica utilizada	Observación y Encuesta
No Repudio	1.- Personal de limpieza compañía externa o funcionarios de la BVQ no registran su ingreso o salida.
Confidencialidad	1.- No registrar el ingreso o salida de documentos de la institución
Privacidad	1.- Funcionarios dejen información física sobre sus escritorios (incumplimiento de políticas y procesos institucionales).
Integridad	1.- Alteración de sellos y firmas.
Alarma	1.- Funcionamiento irregular de cámaras por falta de mantenimiento. 2.- Funcionamiento irregular del sistema de alarma por falta de revisión de la empresa contratada.

Tabla 21 Preocupación Canal humano Fuente Henry Daniel Calero Suntasig

Aplicando la fórmula de la figura 21 se obtiene:

$$L_C = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{Al}$$

$$L_C = 1 + 1 + 1 + 1 + 2$$

$$L_C = 6$$

3.2.3.5. Anomalía (LA)

Se considera a la anomalía toda acción que no se identifica con facilidad, estas acciones no se pueden medir en operaciones normales y tampoco se las puede contabilizar.

Técnica utilizada	Observación y Encuesta
Anomalía	1.- Préstamo de tarjetas de acceso entre usuarios. 2.- Usar equipo de trabajo o extensión telefónica sin autorización del dueño del equipo. 3.- Ingreso de correspondencia de dudosa procedencia. 4.- Utilizar dispositivos personales de almacenamiento externo para compartir información institucional. 5.- Visitas guiadas por las instalaciones de la BVQ.

Tabla 22. Anomalía Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Los datos obtenidos en la anomalía es **LA = 5**.

Para el Canal Humano se obtuvo los siguientes resultados.

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad PV = 12	Exposición LE = 2
	Acceso PA = 5	Vulnerabilidad LV = 6
	Confianza PT = 7	
	Autenticación LCAu = 4	
	Controles	Indemnización LCId = 6
Clase A Resiliencia LCRé = 2		
Subyugación LCSu = 0		
Continuidad LCCt = 2		
No repudio LCNr = 2		
Controles	Confidencialidad LCCf = 5	Preocupación LC = 6
	Clase B Privacidad LCPr = 2	
	Integridad LCIt = 4	
	Alarma LCAI = 5	
	Anomalías LA = 5	

Tabla 23. Datos Canal Humano RAV. Fuente: Henry Daniel Calero Suntasig.

Con los datos obtenidos se ingresa a la calculadora de RAVS, producto de la descarga del sitio web <https://www.isecom.org/research.html#content5-9d>, para comprobar los resultados se utiliza la siguiente fórmula:

$$\text{RAV} = \text{CONTROLES VERDADEROS} - \text{POROSIDAD} - \text{LIMITACIONES}$$

$$\text{RAV} = 6.28 - 11.42 - 16.41$$

$$\text{RAV} = - 21.55$$

Este valor determina un 21.55 de insuficiencia y carencia de controles dentro de los controles implementados.

La información digital o física de la BVQ se encuentra parcialmente vulnerable a posibles ataques informáticos.

Pruebas de Seguridad Humana

OSSTMM versión 3

Inserte en los espacios en blanco los valores numéricos para OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC		
Visibilidad		12
Acceso		5
Confianza		7
Total (Porosidad)		24

CONTROLES		
Clase A		Ausentes
Autenticación		20
Indemnización		18
Resiliencia		22
Subyugación		24
Continuidad		22
Total Clase A	14	106

Clase B		Ausentes
No-Repudio		22
Confidencialidad		19
Privacidad		22
Integridad		50
Alarma		19
Total Clase B	18	102

		Ausentes Verdaderos
Total Controles	32	208
Cobertura Total	13,33%	86,67%

LIMITACIONES			Valor Numérico	Valor Total
Vulnerabilidad		6	9,666667	58,000000
Debilidad		3	5,416667	16,250000
Preocupación		6	5,250000	31,500000
Exposición		2	1,238889	2,477778
Anomalia		5	0,877778	4,388889
Total # Limitaciones	22			112,6167



OPSEC
11,427051

Controles Verdaderos
6,282567

Controles Completos
6,282567

Cobertura Verdadera A
11,67%

Cobertura Verdadera B
15,00%

Total Cobertura Verdadera
13,33%



Limitaciones
16,415797

Seguridad Δ
-21,56

Protección Verdadera
78,44

Seguridad Actual: 78,5663 ravs

OSSTMM RAV - Creative Commons 3,0 atribution-Nom Commercial-No Derivs 2011, ISECOM

Figura 24. Calculadora RAVS – Seguridad Canal Humano. Fuente: Henry Daniel Calero Suntasig

3.3. Pruebas de seguridad física Bolsa de Valores de Quito (BVQ)

Las pruebas de seguridad del canal físico no requieren actividad interpersonal con el personal de la institución, se basa principalmente en la observación de la seguridad de las instalaciones, (Herzong, 2010).

El canal físico aborda la interacción entre el investigador y los objetivos a ser analizados, el principal objetivo del cumplimiento de estas pruebas de seguridad es la verificación física y lógica de la brecha de seguridad con el estándar de seguridad requerido de acuerdo con las políticas internas, las regulaciones de la industria o la legislación regional que se encuentre la institución (Herzong, 2010).

Para el análisis de esta prueba se realizaron observaciones, entrevistas y encuestas; la encuesta fue realizada al Analista de Soporte TI, observar Anexo 1, Anexo 2 y Anexo 3.

3.3.1. Seguridad operacional

3.3.1.1. Visibilidad (PV)

La metodología sugiere realizar pruebas de verificación para la visibilidad de objetivos y activos, los activos también se puede considerar suministros como alimentos, agua, combustible y procesos operativos que puedan afectar los suministros como la eliminación adecuada de desechos y otros contaminantes, carga y descarga de suministros. (Herzong, 2010).

De acuerdo con la Metodología se debe considerar lo siguiente:

- Mapear y detallar el perímetro del alcance determinado, utilizando técnicas que el investigador las considere (Herzong, 2010).
- Enumerar y detallar el comportamiento de circulación en las instalaciones de la institución tales como tráfico peatonal, tráfico en áreas ocupadas, sensores visibles y cámaras de seguridad (Herzong, 2010).
- Detallar los directorios y agendas telefónicas internas, que identifiquen posibles ubicaciones de procesamiento de información a las que el público, visitantes o personas ajenas a la institución no puedan acceder fácilmente.

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito 1.- Piso 8 Presidencia Gerencia Departamento Administrativo RRHH Departamento Comercial Departamento Legal Recepción Directorio
Áreas de acceso	2.- Piso 9 Departamento de Finanzas Departamento Operaciones / Estadístico Departamento de Tecnología Rueda 3.- Piso 10 Auditorio / Cafetería 4.- Parqueaderos 5.- Bodega Subsuelo

Tabla 24. Visibilidad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Mediante la observación se determinan cinco áreas de acceso dentro de la BVQ donde se puede procesar información, para la visibilidad se obtuvo un valor de PV= 5.

3.3.1.2. Acceso (PA)

A través de las pruebas de acceso se deben enumerar los puntos existentes para interactuar con los activos la institución, el investigador se limita a la observación de puntos de acceso que se tendría a las instalaciones de la institución, estos accesos pueden ser físicos o ambientales (Herzong, 2010).

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito 1.- Acceso a puerta de parqueaderos 2.- Acceso puerta principal 3.- Acceso a gradas
Accesos Físicos	4.- Acceso Piso 8 5.- Acceso Piso 9 6.- Acceso Piso 10 7.- Externos (ruido, olores, frio, calor)

Tabla 25. Acceso Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de acceso se determina **PA = 7**.

3.3.1.3. Confianza (PT)

Las pruebas de confianza se refieren al acceso de los activos de la institución sin requerir identificación o autenticación, es decir a personal autorizado para acceder a la institución (Herzong, 2010).

Técnica utilizada	Observación y Encuesta
Objetivo	Bolsa de Valores de Quito
Accesos - confianza	1.- Acceso a oficinas (durante el horario de trabajo)

Tabla 26. Confianza Canal Físico. Fuente: Henry Daniel Calero Suntasig

Para las pruebas de confianza se determina un valor **PT= 1**.

3.3.2. Controles

3.3.2.1. Autenticación (LCAu)

Dentro de los controles de autenticación la metodología considera lo siguiente:

- Verificar el proceso de autenticación del personal autorizado y no autorizado.
- Validar las deficiencias a las que se requieren privilegios para acceder, el proceso de obtener esos privilegios y garantizar que solo sean las partes identificables y autorizadas.
- Verificar el proceso de registro de acceso y qué elementos se ingresaron y eliminaron.

Técnica utilizada	Observación y Encuesta
Objetivo	Bolsa de Valores de Quito 1.- Personal de la BVQ 2.- Empresa de limpieza externa 3.- Practicantes 4.- Público en general (visitas, accionistas, público en general)
Autenticación	5.- Elementos llevados al objetivo (solicitudes, facturas, documentos) 6.- Elementos que salen del objetivo (ofertas económicas, informes, documentos) 7.- Elementos en el objetivo (computadores, impresoras, documentos, etc.)

Tabla 27. Autenticación Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de autenticación se determina **LCAu = 7**.

3.3.2.2. Indemnización (LCId)

Dentro de los controles de Indemnización la metodología indica lo siguiente:

- Validar el contrato de la póliza de seguros de los empleados e instalaciones de la institución, también se deben validar los acuerdos de no divulgación, acuerdos de confidencialidad y renunciaciones (Herzong, 2010).
- Revisar y validar el uso de señaléticas de advertencia de peligro, incendios, salida de emergencias, alarmas, y publicaciones de información general (Herzong, 2010).

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
	1.- Póliza de seguros
	2.- Convenios de confidencialidad y no divulgación
Indemnización	3.- Normativa interna de la empresa
	4.- Señales de Advertencia
	5.- Señalética de evacuación
	6.- Acciones Legales

Tabla 28. Indemnización Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de indemnización se obtuvo el valor **LCId= 6**.

3.3.2.3. Resiliencia (LCRe)

Dentro de los controles de Resiliencia la metodología solicita que se considere lo siguiente:

- Enumerar y verificar que la ausencia o distracción del personal de recepción, mensajería no permita el acceso inmediato a los activos de la institución u operaciones (Herzong, 2010).
- Enumerar y verificar que la omisión o falta de conocimiento de las políticas de seguridad físicas de la institución no permita el acceso directo a los activos institucionales u operaciones (Herzong, 2010).
- Verificar que los recursos que la institución adquiera con proveedores externos tales como alimentos, agua, servicio de lavandería, combustibles, material de oficina o comunicaciones no permita el acceso directo a los activos u operaciones de la empresa (Herzong, 2010).

Verificar que las situaciones de amenaza que generan una alerta alta no suspendan, detengan o minimicen la seguridad operativa (Herzong, 2010).

Técnica utilizada	Observación – Ingeniería Social
Objetivo	Bolsa de Valores de Quito
Indemnización	1.- Controles, procesos y políticas (no permiten el acceso) 2.- Recursos externos (comunicaciones, telefonía, internet) 3.- Condiciones de amenazas (terremoto, inundaciones, amenaza de bombas)

Tabla 29. Resiliencia Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de resiliencia se obtuvo el valor de **LCRe= 3**.

3.3.2.4. Subyugación (LCSu)

Para el control de subyugación se debe enumerar y probar los accesos no controlados a los activos de la institución, es decir, PIN, fotos de identificación, etc. (Herzong, 2010).

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Subyugación	● Tarjetas de acceso (código) ● Biométrico (huella digital) ● Tokens (certificados digitales)

Tabla 30. Subyugación Control Físico. Fuente: Henry Daniel Calero Suntasig.

Como consecuencia de las pruebas de subyugación el valor obtenido es **LCSu = 0**.

3.3.2.5. Continuidad LCCt

Dentro de los controles de Continuidad la metodología indica lo siguiente:

- Validar que los atrasos del personal no afecten a la continuidad del negocio y en el caso que se presente esta situación los backups de estas personas deben permitir el acceso oportuno a servicios, procesos y operaciones (Herzong, 2010).
- Verificar que la ausencia, distracción, remoción o silenciamiento del personal de recepción, mensajería o personal de la puerta no detiene o rechaza el acceso oportuno a servicios, procesos y operaciones de la institución (Herzong, 2010).
- Comprobar que el aislamiento de los materiales tales como alimentos, agua, servicio de lavandería, combustible, comunicaciones, etc., no detendrán el acceso a servicios, procesos y operaciones de la institución (Herzong, 2010).

- Identificar que las situaciones de amenaza que generan una alerta alta no paralicen o indispongan el acceso a servicios, procesos y operaciones de la institución (Herzong, 2010).

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Continuidad	1.- Retrasos del personal (Backup o personal de apoyo)
	2.- Personal de recepción o mensajería (distracción, remoción o silenciamiento)
	3.- Aislamiento de recursos (combustible, energía eléctrica, alimentos, agua)
	4.- Eliminación de desechos

Tabla 31. Continuidad canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de Continuidad se obtiene un valor de **LCCT= 4**.

3.3.2.6. No Repudio (LCNR)

Para las pruebas de no repudio se debe enumerar y verificar los sistemas que tiene la compañía para registrar adecuadamente los acceso o interacciones con activos, para tener evidencia específica para afrontar el repudio (Herzong, 2010).

Técnica utilizada	Observación
No Repudio	1.- Biométrico
	2.- Sistema de Alarma
	3.- Tarjetas de Acceso
	4.- Video cámaras de seguridad

Tabla 32. No Repudio Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de No Repudio registra un valor de **LCNR= 4**.

3.3.2.7. Confidencialidad (LCCf)

Para las pruebas de confidencialidad se enumera y prueba el uso de todas las señales, la comunicación física y objetos transportados entre procesos internos y externos, se debe contar con lugares seguros para intercambiar información verbal con el objetivo de promover la confidencialidad de la comunicación (Herzong, 2010).

Técnica utilizada	Observación
Confidencialidad	1.- Interacciones personales en lugares seguros

Tabla 33. Confidencialidad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de Confidencialidad da como resultado **LCCf= 1**.

3.3.2.8. Privacidad (LCPr)

Para la prueba de privacidad se debe verificar el tipo de comunicación que existe en las institución, comunicación escrita y comunicación verbal; la comunicación escrita debe utilizar empaquetado o etiquetado no marcado o no obvio, las comunicaciones verbales deben generarse "a puerta cerrada", y dentro de habitaciones elegidas para proteger la privacidad (Herzong, 2010).

Técnica utilizada	Observación - Encuesta
Privacidad	1.- Sitios seguros de reuniones 2.- Salas virtuales privadas para reuniones

Tabla 34. Privacidad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de Privacidad se obtuvo el resultado de **LCPr = 2**.

3.3.2.9. Integridad (LCIt)

Dentro de los controles de Integridad la metodología indica lo siguiente:

- Verificar los procedimientos, políticas y procesos internos que la institución utiliza para garantizar la integridad de la información, estos pueden ser marcas cifradas, firmas, sellos, hash, para resguardar y certificar que los activos de información no puedan cambiar o redirigirse a otra persona no autorizada sin el previo conocimiento de las partes involucradas (Herzong, 2010).
- Validar los procedimientos, políticas y procesos internos que la institución utiliza para el transporte seguro de documentos internos o externos, estos pueden utilizar sellos, firmas, marcas, cinta adhesiva, etiquetas, o marcas encriptadas para resguardar y certificar que los activos no puedan cambiar o ser alterados por terceros sin que las partes involucradas lo sepan (Herzong, 2010).
- Verificar que los dispositivos de almacenamiento de información físicos y digitales no se encuentren expuestos a la descomposición de factores naturales, como humedad, calor o desvanecimiento de la luz solar (Herzong, 2010).

Técnica utilizada	Observación - Entrevista
Integridad	1.- Clasificación de la información
	2.- Movimiento de equipos informáticos
	3.- Archivo físico pasivo

Tabla 35. Integridad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de Integridad se obtuvo un valor de **LCIt= 3**.

3.3.2.10. Alarma (LCAI)

Para las pruebas de alarma se debe verificar el uso de un sistema o registro de advertencia, este sistema debe estar en cada puerta de acceso debe contar con sensores para que el personal al observar una situación dudosa o de actividad engañosa pueda notificar al personal encargado de estas anomalías (Herzong, 2010).

Técnica utilizada	Observación - Entrevista
Alarma	1.- Sistema de alarma (Llamadas telefónicas, monitoreo)

Tabla 36. Alarma Control Físico. Fuente: Henry Daniel Calero Suntasig.

Para las pruebas de Integridad registra un valor de **LCAI= 1**.

3.3.3. Limitaciones

3.3.3.1. Exposición (LE)

Para la exposición se debe indicar los accesos no controlados que posee la institución, estos permiten el acceso a múltiples ubicaciones sin autorización previa.

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Exposición	1.- Segunda puerta de auditorio (salida posterior)
	2.- Segunda de Directorio (ingreso y salida de directivos)

Tabla 37. Exposición Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para la exposición se obtuvo un valor de **LE= 2**.

3.3.3.2. Vulnerabilidad (LV)

La vulnerabilidad está dada por el acceso y la confianza por lo que se analiza los ítems de acceso y confianza para determinar las vulnerabilidades.

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Vulnerabilidad	1.- Puerta de parqueadero al encontrarse abierta y en caso de que el guardia no esté en su lugar, las personas no autorizadas puedan ingresar. 2.- Guardia de entrada puede dar acceso sin confirmar el ingreso de las personas.

Tabla 38. Vulnerabilidad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para la Vulnerabilidad se obtiene un valor de **LV= 2**.

3.3.3.3. Debilidad (Lw)

Para la debilidad debemos revisar los controles de clase A y buscar o enumerar las posibles debilidades sobre estos controles.

Técnica utilizada	Observación
Indemnización	1.- La no renovación de pólizas de seguros podrían causar riesgo.
Subyugación	2.- Dejar tokens personales a la vista del público o visitas.

Tabla 39. Debilidad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para los controles autenticación, resiliencia y continuidad no se observaron debilidades, pero se localizaron debilidades para indemnización y subyugación.

Aplicando la fórmula de la figura 20 se obtiene el siguiente resultado:

$$L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$Lw = 0 + 1 + 0 + 1 + 0$$

$$Lw = 2$$

3.3.3.4. Preocupación (Lc)

Para la preocupación es importante revisar los controles de clase B y buscar o enumerar los posibles riesgos sobre estos controles.

Técnica utilizada	Observación
Privacidad	1.- No programar el uso de espacios destinados para reuniones y tenerlas que hacer en otros sitios.
Alarma	2.- No renovar a tiempo con el proveedor del monitoreo de alarma.

Tabla 40. Preocupación Canal Humano. Fuente: Henry Daniel Calero Suntasig.

Para los controles no repudio, confidencialidad e integridad no se localizó preocupaciones, pero se localizó para privacidad y alarma.

Aplicando la fórmula de la figura 21 se obtiene el siguiente resultado:

$$L_C = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{Al}$$

$$Lc = 0 + 0 + 1 + 0 + 1$$

$$Lc = 2$$

3.3.3.5. Anomalía (LA)

Las anomalías pueden darse por factores externos, pero son elementos no comunes que no pueden ser medidos durante un periodo de tiempo.

Técnica utilizada	Observación
Objetivo	Bolsa de Valores de Quito
Anomalía	1.- Ingresos de personas de comida rápida (entrega a diferentes pisos). 2.- Fallo de generador eléctrico este aspecto está a cargo del edificio Londres.

Tabla 41. Anomalía Canal Físico. Fuente: Henry Daniel Calero Suntasig.

Para la anomalía se obtuvo un valor de **LA= 2**.

Para el Canal Físico se obtuvo la siguiente información:

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad PV = 5	Exposición LE = 2
	Acceso PA = 7	Vulnerabilidad LV = 2
	Confianza PT = 1	
	Autenticación LCAu = 7	
Controles	Indemnización LCId = 6	
	Clase A Resiliencia LCRe = 3	Debilidad LW = 2
	Subyugación LCSu = 0	
	Continuidad LCCt = 4	
	No repudio LCNr = 4	
	Confidencialidad LCCf = 1	
	Clase B Privacidad LCPr = 2	Preocupación LC = 2
	Integridad LCIt = 3	
	Alarma LCAI = 1	
Anomalías LA = 2		

Tabla 42 Datos Canal Físico RAV Fuente: Henry Daniel Calero Suntasig

Una vez analizados y procesados los resultados se los somete a comprobación de la siguiente manera:

$$RAV = \text{CONTROLES VERDADEROS} - \text{POROSIDAD} - \text{LIMITACIONES}$$

$$RAV = 6.21 - 9.69 - 12.96$$

$$RAV = -16.44$$

Este valor determina un 16.44 de insuficiencia y carencia en los controles previamente implementados.

La información digital o física de la BVQ se encuentra parcialmente vulnerable a posibles ataques informáticos y en el peor de los casos robo o sustracción de documentos físicos.

Pruebas de Seguridad Física

OSSTMM versión 3

Inserte en los espacios en blanco los valores numéricos para OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC

Visibilidad	5
Acceso	7
Confianza	1
Total (Porosidad)	13



OPSEC
9,698723

CONTROLES

Clase A		Ausentes
Autenticación	7	6
Indemnización	6	7
Resiliencia	3	10
Subyugación	0	13
Continuidad	4	9
Total Clase A	20	45

Controles Verdaderos
6,213854

Controles Completos
6,213854

Cobertura Verdadera A
30,77%

Cobertura Verdadera B
16,92%

Total Cobertura Verdadera
23,85%

Clase B		Ausentes
No-Repudio	4	9
Confidencialidad	1	12
Privacidad	2	11
Integridad	3	10
Alarma	1	12
Total Clase B	11	54

		Ausentes Verdaderos
Total Controles	31	99
Cobertura Total	23,85%	76,15%



LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	2	8,615385	17,230769
Debilidad	2	4,461538	8,923077
Preocupación	2	5,153846	10,307692
Exposición	2	1,164497	2,328940
Anomalia	2	0,520118	1,040237
Total # Limitaciones	10		39,8308

Limitaciones
12,962360

Seguridad Δ
-16,45

Protección Verdadera
83,55

Seguridad Actual: 83,4018 ravs

OSSTMM RAV - Creative Commons 3,0 attribution-Nom Commercial-No Derivs 2011, ISECOM

Figura 25. Calculadora RAVS – Seguridad Canal Físico. Fuente: Henry Daniel Calero Suntasig.

3.4. Pruebas de seguridad Inalámbrica Bolsa de Valores de Quito (BVQ)

Para realizar las pruebas del canal inalámbrico la metodología indica que este canal cubra la interacción del investigador dentro del rango de los objetivos seleccionados. Los objetivos para el cumplimiento de estas pruebas son las barreras físicas y lógicas, que permitan la medición de los estándares de seguridad implementados o descritos en los procedimientos, procesos o política de la compañía (Herzong, 2010).

Para estas pruebas se utilizó lo siguiente:

Encuesta al Analista Senior de Infraestructura y entrevista al Analista de Soporte TI

Para estas pruebas se debe revisar las políticas de la BVQ para el uso del Wireless institucional, dentro de la política se indica que existen dos tipos de redes una red pública en la cual se pueden unir visitantes, directivos o público en general y otra red privada en la cual solo se permite la conexión a dispositivos que pertenecen a la institución.

Mediante el análisis de las encuestas al Analista de desarrollo TI / Soporte Técnico TI, ver Anexo 2, Anexo 3 y Anexo 5.

3.4.1. Seguridad operacional

3.4.1.1. Visibilidad (PV)

En la visibilidad se deben verificar los componentes que conforman el sistema inalámbrico de la institución.

A través de estas pruebas se obtuvo información mediante la consola de administración del Wi-Fi de la institución.

Técnica utilizada	Observación, Power Bi, Encuesta y Entrevista
Visibilidad	1.- Frecuencias detectada 2,4 GHz
	2.- Frecuencias detectada 5 GHz
	3.- SSID cercanos
	4.- Firewall
	5.- Canales de señal para propagación
	6.- Canales ocupados por otros SSID

Tabla 43. Visibilidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Dentro de la visibilidad se obtuvo acceso a la información que genera la consola del Wireless y con ayuda de Power BI se realizó un dashboard para realizar gráficos e identificar

los SSID que afectan a las señales inalámbricas de la BVQ, los canales que están utilizando y a que señal Wireless afectan, para la visibilidad se obtiene un valor de **PV= 6**.

3.4.1.2. Acceso (PA)

La metodología recomienda lo siguiente:

- Evaluar el método de acceso a la administración de los dispositivos inalámbricos (Herzong, 2010).
- Revisar los puntos de acceso de la red inalámbrica y detectar si están desactivados a ciertos horarios durante el día (Herzong, 2010).
- Configurar los dispositivos inalámbricos con la potencia de emisión más adecuada, para que su operación se mantenga dentro del límites seguros de la institución (Herzong, 2010).
- Verificar que se haya cambiado el identificador del conjunto de servicios (SSID) de fábrica (Herzong, 2010).
- Evaluar los controles de acceso, comprobar la seguridad del perímetro y la capacidad de interceptar o interferir con comunicación de la red inalámbrica (Herzong, 2010).

Técnica utilizada	Observación, Encuesta y Entrevista
Acceso	1.- El acceso a dispositivos inalámbricos: se cuenta con una controladora Wireless, está ubicada en un lugar restringido de la organización. 2.- Por políticas internas los dispositivos de usuarios se encuentran configurados para que utilicen la red cableado como predeterminada, por tal razón el componente Wireless está desactivado. 3.- Los equipos Wireless al tener una controladora se encuentran configurados para la selección del mejor canal y el que no tenga mucha interferencia, por otra parte, irradian potencia necesaria para el funcionamiento este dentro del perímetro de la BVQ. 4.- Todo equipo Wireless de la BVQ no tiene configuraciones por defecto o de fábrica. 5.- Los controles de accesos a las instalaciones están controlados por los diferentes medios (guardias, tarjetas de acceso, cámaras y alarmas)

Tabla 44. Acceso Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Dentro del acceso Wireless se describe cada una de las recomendaciones que indica la metodología, el valor numérico para el acceso es **PA=5**.

3.4.1.3. Confianza (PT)

De acuerdo con la metodología las pruebas de confianza se refieren al acceso a la información física o digital sin necesidad de identificación o autenticación. (Herzong, 2010)

La metodología recomienda considerar lo siguiente:

- Probar el método de autenticación de los clientes. (Herzong, 2010)
- Probar la profundidad de los requisitos para acceder a dispositivos inalámbricos. (Herzong, 2010)

Técnica utilizada	Observación y Entrevista
Confianza	1.- Autenticación mediante usuario y contraseñas proporcionadas por departamento de Tecnología, por política interna todos los equipos inalámbricos de propiedad de la BVQ pueden ingresar al Wi-Fi corporativo.
	2.- Para acceder a dispositivos inalámbricos existen tres niveles.
	Usuario y contraseña
	Clave de dispositivo inalámbrico
	Código de verificación de equipo aceptable dentro de la red
	3.- Ingreso al Wireless por visitantes o autoridades eventuales.
	Verifica SO actualizado
	Verifica Antivirus actualizado
	Clave de dispositivo inalámbrico
	Código de verificación de equipo aceptable dentro de la red pública

Tabla 45. Confianza Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la confianza se obtiene un valor numérico de **PT=3**.

3.4.2. Controles

3.4.2.1. Autenticación (LCAu)

Enumerar y probar los componentes necesarios para de autenticación y autorización a la red inalámbrica (Herzong, 2010).

Al tener acceso a la controladora del Wireless institucional se obtuvo lo siguiente.

Técnica utilizada	Observación y Entrevista
Autenticación	1.- SSID 1 - BVQ - XXX encriptación XXX. 2.- SSID 2 - BVQ - XXX encriptación XXX. 3.- Confirmación del administrador para ingreso a la red. 4.- Visitas debe contar con código de autenticación para el ingreso.

Tabla 46. Autenticación Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Al tener acceso a la consola del Wireless y con el procedimiento interno para acceso a dispositivos a la red inalámbrica institucional, se obtuvo para la autenticación un valor de **LCAu = 4**.

3.4.2.2. Indemnización (LCId)

Dentro de la indemnización se debe revisar los activos y servicios que se encuentran protegidos contra el abuso u omisión en la política del empleado, como también los activos asegurados por hurto o averías (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Indemnización	1.- Equipos dentro de póliza de seguros 2.- Equipos dentro de contrato de mantenimientos preventivos 3.- Políticas internas del buen uso de los recursos institucionales 4.- Equipos ubicados en sitios seguros

Tabla 47. Indemnización Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para el control de indemnización se obtuvo un valor de **LCId = 4**.

3.4.2.3. Resiliencia (LCRe)

En la resiliencia se debe revisar el proceso de los encargados de activos fijos que desconectan los equipos debido a una violación o preocupaciones de seguridad de acuerdo con la política de seguridad interna de la institución.

Técnica utilizada	Observación y Entrevista
Resiliencia	1.- Los funcionarios que desconecten equipos deben notificar a la Gerencia de Tecnología y encargado de activos fijos (reglamento interno). 2.- El personal de guardianía revisa las pertenencias de visitantes al salir e ingresar a las instalaciones, si identifican algún comportamiento fuera de lo normal, notifican enseguida.

Tabla 48. Resiliencia Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la saliencia se obtuvo un valor numérico de **LCRe = 2**.

3.4.2.4. Subyugación LCSu

Se debe revisar la configuración de los dispositivos inalámbricos y desactivar todo control que provenga de fábrica. (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Subyugación	1.- Los equipos inalámbricos no cuentan con la configuración predeterminada de fábrica. 2.- Actualización de firmware y certificados de comunicación.

Tabla 49. Subyugación Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la subyugación se obtiene un valor numérico de **LCSu = 2**.

3.4.2.5. Continuidad (LCCT)

Para el control de continuidad se debe enumerar y probar los equipos que están asignados como backup y puedan entrar a funcionar en el caso de avería del equipo principal, con el objetivo de evitar demoras en el acceso a los servicios prestados (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Continuidad	1.- Se cuenta con equipos de back-up para ser reemplazados inmediatamente. 2.- Equipos se dan mantenimiento preventivo para correcto funcionamiento. 3.- Equipos Wireless no son considerados como servicio de alto riesgo para seguir operando.

Tabla 50. Continuidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la continuidad se obtiene el valor de **LCCT = 3**.

3.4.2.6. No Repudio (LCNR)

Dentro de control no repudio se debe verificar y probar los sistemas donde se generen un historial de eventos de la red inalámbrica con el propósito de evidenciar las acciones ejecutadas sobre éste y desafiar el repudio en el caso que se presente (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
No Repudio	1.- Se registra eventos de ingreso a la consola de administración indicando la fecha, hora, usuario y desde que dirección IP se realizó el ingreso. 2.- Se registra los canales de interferencia, los equipos Wireless se autoconfiguran en otro canal para no ser interferidos.

3.- Se registra bloqueo de equipos no permitidos dentro del ámbito Wireless de la BVQ.

Tabla 51. No Repudio Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para no repudio se obtiene un valor de **LCNR = 3**.

3.4.2.7. Confidencialidad LCCf

Para el control de confidencialidad se debe enumerar el uso de equipos para amortiguar las señales de transmisión hacia los exteriores de la empresa y los controles establecidos para asegurar o encriptar la red inalámbrica (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Confidencialidad	1.- Las instalaciones de BVQ están en los pisos 8, 9 y 10 del edificio Londres, por lo cual no se utiliza amortiguadores de señales inalámbricas. 2.- Dentro del ámbito inalámbrico de la BVQ el sistema se encuentra encriptado.

Tabla 52. Confidencialidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para confidencialidad se obtiene un valor de **LCCf = 2**.

3.4.2.8. Privacidad LCPr

Para el control de la privacidad se debe determinar los controles de ingreso físico a los puntos de comunicación y módulos que los controlan. (cerraduras con llave, lectores de tarjetas, cámaras, etc.) (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Privacidad	Para acceder a la controladora del Wireless se debe pasar por lo siguiente: 1.- Guardia planta baja 2.- Acceso piso nueve (Credenciales de la BVQ) 3.- Acceso a la Gerencia de Tecnología (credenciales de la BVQ) 4.- Acceso al centro de cómputo (tarjeta de acceso) 5.- Cámaras de Seguridad 6.- Sistema de Accesos

Tabla 53. Privacidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Existen varios controles para acceder a la controladora del Wireless, el valor numérico para la privacidad es **LCPr = 6**.

3.4.2.9. Integridad LCIt

Para el control de la integridad se debe determinar que los datos son accedidos y modificados por el personal que están previamente autorizados, la red inalámbrica debe utilizar un cifrado adecuado para garantizar la confidencialidad de comunicaciones (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Integridad	1.- Se cuenta con el uso de usuario y contraseña. 2.- Se monitorea el sistema inalámbrico donde se observa qué equipo se encuentra conectado, que IP fue asignada y que AP le está dando señal, revisión de tráfico y en el caso de darse se tiene la opción de bloqueo. 3.- Red inalámbrica cuenta con uso de cifrado y encriptación.

Tabla 54. Integridad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la integridad se registra un valor de **LCIt = 3**.

3.4.2.10. Alarma (LCAI)

En el control de alarma se debe validar el uso de un sistema, registro o mensaje de información para enviar alertas sobre las anomalías que existen dentro del sistema inalámbrico, también se debe enumerar los sistemas con los que cuenta la institución en el caso de observar una situación sospechosa, intentos de elusión o actividad fraudulenta. (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Alarma	1.- Sistema de alarma 2.- Notificaciones por correo electrónico de la consola Wireless. 3.- Antivirus institucional

Tabla 55. Alarma Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para control de alarma se registra un valor numérico de **LCAI= 3**.

3.4.3. Limitaciones

Las limitaciones son las vulnerabilidades encontradas que pueden afectar de forma directa a los controles implementados.

3.4.3.1. Exposición (LE)

Las limitaciones de exposición son aquellas que pueden estar provocando mal funcionamiento del sistema Wireless.

Técnica utilizada	Observación y Entrevista
Exposición	1.- Interferencia co-canal
	2.- Interferencia de canal adyacente

Tabla 56. Exposición Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la exposición se registra un valor numérico de **LE=2**.

3.4.3.2. Vulnerabilidad (LV)

La limitación de la vulnerabilidad puede estar dada por la omisión de actualizar el firmware del AP, como también por no revisar la estructura física donde se encuentra instalado y puede averiarse por daños climáticos.

Técnica utilizada	Observación y Entrevista
Vulnerabilidad	1.- Por estar instalados en el techo y existir una filtración de agua podría afectar el funcionamiento.
	2.- Omitir actualizaciones de firmware.

Tabla 57. Vulnerabilidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la vulnerabilidad se registra un valor numérico de **LV= 2**.

3.4.3.3. Debilidad (LW)

La limitación de la debilidad se debe analizar los controles de clase A e identificar las debilidades que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación y Entrevista
Autenticación	1.- No utilizar códigos de autenticación de forma ética (visitantes).
Continuidad	2.- No contar con equipos de backup por mantenimiento.

Tabla 58. Debilidad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para los controles indemnización, resiliencia y subyugación no se localiza debilidades, pero si se encuentran debilidades para autenticación y continuidad.

Aplicando la fórmula de la figura 20 se obtiene:

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$L_W = 1 + 0 + 0 + 0 + 1$$

$$L_W = 2$$

3.4.3.4. Preocupación (LC)

Para la limitación de la preocupación se debe analizar los controles de clase B e identificar las posibles inconvenientes que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación y Entrevista
No repudio	1.- Si el servicio de la consola de administración se encuentra deshabilitado, no se podría tener registros de los equipos Wireless.
Alarma	2.- Por cambio de cuentas de correo electrónico las notificaciones no podrían llegar a la cuenta de correo configurada.

Tabla 59. Preocupación Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para los controles integridad, confidencialidad e integridad no se localizó preocupaciones, pero se localizó para no repudio y alarma.

Aplicando la fórmula de la figura 21 se registra lo siguiente:

$$L_C = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{Al}$$

$$L_C = 1 + 0 + 0 + 0 + 1$$

$$L_C = 2$$

3.4.3.5. Anomalía (LA)

Las anomalías son factores externos que pueden provocar el mal funcionamiento de los equipos.

Técnica utilizada	Observación y Entrevista
Anomalía	1.- Un código de autenticación de visitante pueda ser utilizado en dos dispositivos. 2.- Desbloqueo de equipos no autorizados dentro de la consola.

Tabla 60. Anomalía Canal inalámbrico. Fuente: Henry Daniel Calero Suntasig.

Para la anomalía se registra un valor numérico de **LA = 2**.

Para el Canal Inalámbrico se obtuvo la siguiente información:

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad PV = 6	Exposición LE = 2
	Acceso PA = 5	Vulnerabilidad LV = 2
	Confianza PT = 3	
	Autenticación LCAu = 4	
	Indemnización LCId = 4	
Controles	Clase A Resiliencia LCRé = 2	Debilidad LW = 2
	Subyugación LCSu = 2	
	Continuidad LCCt = 3	
	No repudio LCNr = 3	
	Confidencialidad LCCf = 2	
	Clase B Privacidad LCPr = 6	Preocupación LC = 2
	Integridad LClt = 3	
	Alarma LCAI = 3	
		Anomalías LA = 2

Tabla 61. Datos Canal Inalámbrico RAV. Fuente: Henry Daniel Calero Suntasig.

Una vez que se obtiene los resultados estos pueden ser comprobados de la siguiente manera:

$$RAV = \text{CONTROLES VERDADEROS} - \text{POROSIDAD} - \text{LIMITACIONES}$$

$$RAV = 6.28 - 9.90 - 12.98$$

$$RAV = -16.6$$

Este valor determina un 16.6 de insuficiencia y carencia de controles dentro de los controles implementados.

La información digital o física de la BVQ se encuentra parcialmente vulnerable a posibles ataques informáticos y en el peor de los casos robo o sustracción de documentos físicos.

Pruebas de Seguridad Inalámbrico

OSSTMM versión 3

Inserte en los espacios en blanco los valores numéricos para OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC

Visibilidad	6
Acceso	5
Confianza	3
Total (Porosidad)	14

CONTROLES

Clase A

Autenticación	4	Ausentes	10
Indemnización	4		10
Resiliencia	2		12
Subyugación	2		12
Continuidad	3		11
Total Clase A	15		55

Clase B

No-Repudio	3	Ausentes	11
Confidencialidad	2		12
Privacidad	6		8
Integridad	3		11
Alarma	3		11
Total Clase B	17		53

Total Controles	32	Ausentes Verdaderos	108
Cobertura Total	22,86%		77,14%

LIMITACIONES

Vulnerabilidad	2	Valor Numérico	8,714286	Valor Total	17,428571
Debilidad	2		4,928571		9,857143
Preocupación	2		4,785714		9,571429
Exposición	2		1,034694		2,069388
Anomalia	2		0,593878		1,187755
Total # Limitaciones	10				40,1143



OPSEC
9,900073

Controles Verdaderos
6,282567

Controles Completos
6,282567

Cobertura Verdadera A
21,43%

Cobertura Verdadera B
24,29%

Total Cobertura Verdadera
22,86%



Limitaciones
12,984544

Seguridad Δ
-16,60

Protección Verdadera
83,40

Seguridad Actual: 83,2457 ravs

OSSTMM RAV - Creative Commons 3,0 atribution-Nom Commercial-No Derivs 2011, ISECOM

Figura 26. Calculadora RAVS – Seguridad Canal Inalámbrico. Fuente: Henry Daniel Calero Suntasig.

3.5. Evaluación de seguridad de Telecomunicaciones Bolsa de Valores de Quito (BVQ)

Para las pruebas de Seguridad de Telecomunicaciones este canal resguarda la interacción del investigador con los objetivos analizados. Si bien algunos servicios consideran esto simplemente como "phreaking" es decir un hacking del sistema telefónico, el verdadero objetivo es la evidencia de brechas de seguridad determinadas en el estándar de seguridad, política de la compañía, industria regulaciones o legislación regional. (Herzong, 2010)

La metodología indica que los objetivos de ataque son:

- Prueba de PBX
- Prueba de buzón de voz
- Inspección, sondeo y pruebas de fax / módem
- Pruebas de servicios de acceso remoto (RAS)
- Prueba de líneas ISDN de respaldo
- Prueba de voz sobre IP
- Prueba de red conmutada por paquetes X.25

Para el caso de estudio dentro de la Bolsa de Valores de Quito, el sistema de telefonía es digital y analógico, no tiene telefonía IP, para estas pruebas se aplicará las recomendaciones que indica la metodología adaptándose a la situación real de la compañía.

Se realizó una encuesta al Analista de Desarrollo TI / Analista de Soporte TI, ver Anexo 3.

3.5.1. Seguridad operacional

3.5.1.1. Visibilidad (PV)

Para la seguridad de operaciones se debe enumerar los objetivos en el alcance a través de la interacción directa e indirecta, en este caso será la central PBX de la organización (Herzong, 2010).

Para estas pruebas la metodología indica lo siguiente:

- Evaluación de PBX: enumerar los sistemas de telefonía dentro de la institución (Herzong, 2010).

- Evaluación de buzones de voz: probar buzones de voz dentro del sistema de telefonía (Herzong, 2010).
- Evaluación de FAX: enumere los sistemas de FAX dentro del sistema de telefonía (Herzong, 2010).
- Encuesta de módem: encontrar todos los sistemas con módems de escucha e interactivos dentro del sistema telefónico (Herzong, 2010).
- Identificar los tipos y versiones de SO en uso en sistemas telefónico (Herzong, 2010).
- Identificar los tipos de módem, FAX y los programas operativos (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Visibilidad	1.- Sistema PBX
	La BVQ no utiliza FAX
	La BVQ no utiliza Módems

Tabla 62. Visibilidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la visibilidad un valor de **PV = 1**.

3.5.1.2. Acceso (PA)

Para estas pruebas la metodología indica lo siguiente:

- Pruebas de PBX: encontrar sistemas PBX que admitan el manejo remoto o el acceso al terminal de mantenimiento, ya sea a través de marcado telefónico o red IP (Herzong, 2010).
- Evaluación de buzones de voz: encontrar buzones de voz que tengan salida al mundo (Herzong, 2010).
- Evaluación de FAX: validar los procedimientos de FAX que permiten la gestión remota o el acceso a la terminal de mantenimiento (Herzong, 2010).
- Verificación de las líneas ISDN de respaldo (Herzong, 2010).
- Evaluación de voz sobre IP: verificar los escuchas telefónicas o seguimiento, secuestro de llamadas, sustitución de CLID y negativa de servicio (Herzong, 2010).
- Solicitar servicios remotos conocidos y comunes (Herzong, 2010).
- Identifique los dispositivos de servicios y sus versiones (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Acceso	1.- Central Telefónica PBX ubicada centro de cómputo. 2.- Se cuenta con una línea análogas de respaldo. • Pruebas de buzones de voz expuestos no se considera ya que al ser una central digital se tiene solo un IVR general. • La BVQ no utiliza FAX. • La BVQ no cuenta con telefonía IP.

Tabla 63. Visibilidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Para la visibilidad se obtuvo un valor numérico de **PA = 2**.

3.5.1.3. Confianza (PT)

Los controles de confianza hacen referencia al acceso de la información o al sitio físico sin la necesidad de credenciales de autenticación (Herzong, 2010).

La metodología indica lo siguiente:

- Revisar las técnicas de acceso implementadas que no requieren la presentación de documentos de autenticación (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Confianza	1.- Para el acceso a la central telefónica PBX se debe tener credencial de acceso ya que está ubicada en un área segura.

Tabla 64. Confianza Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la confianza un valor numérico de **PT = 1**.

3.5.2. Controles

3.5.2.1. Autenticación (LCAu)

Para la autenticación la metodología recomienda lo siguiente:

- Especificar los recursos de telecomunicaciones que solicitan autenticación (Herzong, 2010).
- Comprobar las técnicas de autorización y la identificación requerida (Herzong, 2010).

- Verificar que las cuentas administrativas no posean credenciales predeterminadas (Herzong, 2010).
- Asegurar que las cuentas de usuario no tengan credenciales predeterminadas (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Autenticación	1.- Para ingresar a la central PBX se lo realiza por medio de un equipo ubicado en el centro de cómputo, este equipo cuenta usuario y contraseña seguros. 2.- Claves de Accesos a la central PBX tiene alto grado de complejidad y se encuentra desactivado usuario y parámetros de configuración por defecto. Solo existe un usuario y contraseña que puede acceder a la central PBX, clientes no tienen permisos para la administración, ya que es una central digital.

Tabla 65. Autenticación Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la autenticación un valor de **LCAu = 2**.

3.5.2.2. Indemnización (LCId)

Para los controles de indemnización la metodología recomienda lo siguiente:

- Los activos de telefonía deben estar incluidos en la póliza por robo o daños, identificar los controles de responsabilidad y descargos de responsabilidad (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Indemnización	1.- La central PBX si está dentro del seguro de la póliza de la BVQ

Tabla 66. Indemnización Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Para la indemnización se obtuvo un valor de **LCId = 1**.

3.5.2.3. Resiliencia (LCRe)

Identificar el proceso de las personas encargadas que desconectan los dispositivos del sistema telefónico debido a una violación de seguridad (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Resiliencia	1.- Mantenimiento preventivo se desconectan los terminales de la PBX. 2.- Por averías y cambios de equipos se desconectan los terminales de la PBX.

Tabla 67. Resiliencia Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig

Se registra para la resiliencia un valor de **L_{CRe} = 2**.

3.5.2.4. Subyugación (L_{CSu})

Para el control de subyugación se debe enumerar las condiciones para usar o habilitar los controles de pérdida no habilitados por defecto (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Subyugación	1.- Central PBX no está habilitado controles o configuración por defecto. 2.- Equipo de acceso a la central PBX no cuenta con una configuración por defecto. 3.- Equipo de acceso cumple con las políticas de seguridad de la institución. 4.- Equipos terminales de la PBX no están habilitado controles por defecto.

Tabla 68. Subyugación Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la subyugación un valor de **L_{CSu} = 4**.

3.5.2.5. Continuidad L_{CCt}

Para los controles de continuidad la metodología recomienda lo siguiente:

- Enumerar los respaldos existentes del sistema telefónico para evitar retrasos en el acceso y el servicio en el caso de falla del sistema principal, como también el tiempo de respuesta a través de personal de respaldo o medios automatizados para acceso alternativo (Herzong, 2010).
- Enumerar los problemas de calidad de servicio del proveedor del servicio telefónico y el rendimiento de las tecnologías de telecomunicaciones (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Continuidad	1.-Se tiene línea telefónica analógica de backup. 2.-Funcionarios cuentan con servicio telefónico móvil para comunicación. 3.-Se socializa con los cliente internos y externos métodos alternativos de comunicación. 4.-Por política interna se obtiene un respaldo semanal de la configuración de la central PBX.

Tabla 69. Continuidad Canal de Telecomunicaciones. Fuente Henry: Daniel Calero Suntasig.

Se registra para la continuidad un valor de **LCCt = 4**.

3.5.2.6. No Repudio (LCNR)

Para los controles de no repudio la metodología recomienda lo siguiente:

- Enumerar los controles que tiene la institución para registrar el acceso o las interacciones a la propiedad del sistema telefónico para evidenciar y desafiar el repudio (Herzong, 2010).
- Contar con un visor de eventos para verificar el ingreso y conexión del sistema telefónico (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
No repudio	1.- Registro de acceso al centro de cómputo a la central PBX. 2.- Registro de acceso al equipo para conexión a la central PBX. 3.- Registro de acceso a la central PBX.

Tabla 70. No Repudio Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para el no repudio un valor de **LCNR = 3**.

3.5.2.7. Confidencialidad (LCCf)

Para los controles de confidencialidad la metodología recomienda lo siguiente:

- Enumerar las interacciones que utilizan líneas seguras, cifrado, interacciones para proteger la confidencialidad de la propiedad de información entre las partes involucradas (Herzong, 2010).

- Validar las técnicas aceptables utilizadas para mantener la confidencialidad de la comunicación (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Confidencialidad	1.- No divulgar información confidencial vía telefónica. 2.- Utilizar canales de comunicación de acuerdo con las políticas de seguridad de la BVQ.

Tabla 71. Confidencialidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la confidencialidad un valor de **LCNR = 2**.

3.5.2.8. Privacidad (LCPr)

Para el control de la privacidad se debe enumerar los canales utilizados, cifrado, líneas seguras, interacciones "silenciadas" o "cerradas" para resguardar la privacidad de la interacción (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Privacidad	1.- Comunicación interna entre extensiones es privada y esta comunicación no sale al exterior (canal seguro). 2.- Comunicación externa limita por tiempo y se debe seguir normas internas de la institución.

Tabla 72. Privacidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la privacidad un valor de **LCPr = 2**.

3.5.2.9. Integridad (LCIt)

Enumerar las deficiencias de integridad cuando utilice el sistema de comunicación telefónico para garantizar que el activo no se pueda cambiar, redirigir, o revertir sin que las partes involucradas lo sepan (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Integridad	1.- La telefonía es una comunicación en tiempo real 2.- Para brindar información vía telefónica se debe asegurar el funcionario con que persona está interactuando.

Tabla 73. Privacidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la privacidad un valor de **LCIt = 2**.

3.5.2.10. Alarma (LCAI)

Para los controles de alarma la metodología recomienda lo siguiente:

- Revisar el uso de un método, registro o mensaje de advertencia para cada puerta de acceso, ante una situación sospechosa, intentos de intrusión o actividad fraudulenta (Herzong, 2010).
- Revisar los registros y detalles de llamadas que ingresan y salen del sistema de telefonía en busca de signos de abuso o fraude (Herzong, 2010).

Técnica utilizada	Observación y Entrevista
Alarma	1.- En la ubicación de la central PBX se cuenta con sistema de alarma. 2.- Por política interna de la empresa indica que se debe obtener un registro de llamadas telefónicas por usuario.

Tabla 74. Alarma Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la privacidad un valor de **LCAI = 2**.

3.5.3. Limitaciones

3.5.3.1. Exposición (LE)

Para la exposición se debe revisar la información de los registros telefónicos que se publica fuera de la institución como páginas web, directorios telefónicos, redes sociales, entre otros (Herzong, 2010).

Al tener una central PBX digital, la información que se publica al exterior son los números de contacto de los funcionarios de la BVQ como también las extensiones, esta información es aceptable y no se tiene ninguna otra información publicada sobre la PBX, el valor registrado para la exposición es **LE = 0**.

3.5.3.2. Vulnerabilidad (LV)

La vulnerabilidad está dada por las operaciones de acceso y confianza, en consecuencia, la central PBX al estar dentro del centro de cómputo y tener un acceso restringido la vulnerabilidad de acceso es **LV = 0**.

3.5.3.3. Debilidad (Lw)

Para la limitación de la debilidad se debe analizar los controles de clase A e identificar las debilidades que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación y Entrevista
Indemnización	1.- Por obsolescencia tecnológica, la póliza no pueda cubrir la central PBX.
Subyugación	1.-Versión del sistema operativo central PBX no tiene soporte técnico por parte del proveedor.

Tabla 75. Debilidad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Para los controles autenticación, resiliencia y continuidad no se localizó debilidades, pero se localizó para indemnización y subyugación.

Aplicando la fórmula de la figura 20 se obtiene:

$$L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$
$$Lw = 0 + 1 + 0 + 1 + 0$$
$$Lw = 2$$

3.5.3.4. Preocupación (Lc)

Para la limitación de la preocupación se debe analizar los controles de clase B e identificar las posibles inconvenientes que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación y Entrevista
No repudio	1.- No tener registro telefónico por mal funcionamiento de la central PBX.

Tabla 76. Preocupación Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Para los controles integridad, confidencialidad, integridad y alarma no se localizó preocupaciones, pero se localizó para no repudio.

Aplicando la fórmula de la figura 21 se obtiene:

$$L_c = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{Al}$$
$$Lc = 1 + 0 + 0 + 0 + 0$$
$$Lc = 1$$

3.5.3.5. Anomalía (LA)

Las anomalías son factores externos que pueden provocar el mal funcionamiento de los equipos.

Técnica utilizada	Observación y Entrevista
Anomalía	1.- Fallo o intermitencias del servicio por proveedor de telefonía.

Tabla 77. Anomalía Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

Se registra para la anomalía un valor de **LA = 1**.

Para el Canal Inalámbrico se obtuvo la siguiente información:

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad PV = 1	Exposición LE = 0
	Acceso PA = 2	Vulnerabilidad LV = 0
	Confianza PT = 1	
	Autenticación LCAu = 2	
Controles	Indemnización LCId = 1	
	Clase A	Debilidad LW = 2
	Resiliencia LCRé = 2	
	Subyugación LCSu = 4	
	Continuidad LCCt = 4	
	No repudio LCNr = 3	
	Confidencialidad LCCf = 2	
	Clase B	Preocupación LC = 1
	Privacidad LCPr = 2	
	Integridad LCIt = 2	
	Alarma LCAI = 2	
Anomalías LA = 1		

Tabla 78. Datos Canal Telecomunicaciones RAV. Fuente: Henry Daniel Calero Suntasig.

Una vez que se obtienen los resultados estos son comprobables de la siguiente manera:

$$RAV = \text{CONTROLES VERDADEROS} - \text{POROSIDAD} - \text{LIMITACIONES}$$

$$RAV = 5.67 - 6.77 - 8.89$$

$$RAV = -9.99$$

Este valor determina un 9.99 de insuficiencia y carencia de controles dentro de los controles implementados.

Las comunicaciones de la BVQ se encuentran parcialmente vulnerables se puede mejorar la seguridad para evitar algún ataque informático.

Pruebas de Seguridad Telecomunicaciones

OSSTMM versión 3

Inserte en los espacios en blanco los valores numéricos para OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC

Visibilidad	1
Acceso	2
Confianza	1
Total (Porosidad)	4

CONTROLES

Clase A		Ausentes
Autenticación	2	2
Indemnización	1	3
Resiliencia	2	2
Subyugación	4	0
Continuidad	4	0
Total Clase A	13	7

Clase B		Ausentes
No-Repudio	3	1
Confidencialidad	2	2
Privacidad	2	2
Integridad	2	2
Alarma	2	2
Total Clase B	11	9

		Ausentes Verdaderos
Total Controles	24	16
Cobertura Total	60,00%	40,00%

LIMITACIONES

		Valor Numérico	Valor Total
Vulnerabilidad	0	5,000000	0,000000
Debilidad	2	2,750000	5,500000
Preocupación	1	3,250000	3,250000
Exposición	0	1,050000	0,000000
Anomalia	1	0,850000	0,850000
Total # Limitaciones	4		9,6000

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC

6,776361

Controles Verdaderos

5,674005

Controles Completos

5,674005

Cobertura Verdadera A

65,00%

Cobertura Verdadera B

55,00%

Total Cobertura Verdadera

60,00%



Limitaciones

8,896639

Seguridad Δ

-10,00

Protección Verdadera

90,00

Seguridad Actual: 89,7146 ravs

OSSTMM RAV - Creative Commons 3.0 atribution-Nom Commercial-No Derivs 2011, ISECOM

Figura 27. Calculadora RAVS – Seguridad Canal Telecomunicaciones. Fuente: Henry Daniel Calero Suntasig.

3.6. Evaluación de la seguridad de Redes de Datos Bolsa de Valores de Quito (BVQ)

Para las pruebas de seguridad de redes de datos se solicitan las interacciones con los datos existentes salvaguardas operacionales de la red de comunicación utilizadas para vigilar el acceso a la propiedad (Herzong, 2010).

En este canal cubre la participación de las redes operativas, mientras que algunas organizaciones consideran esto simplemente como "prueba de penetración", el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la interacción del sistema y la calidad operativa prueba con mediciones de brecha al estándar de seguridad requerido descrito en la política de la compañía (Herzong, 2010).

Para estas pruebas se utilizó:

Encuestas al Analista Senior de Infraestructura y Analista de Desarrollo TI / Analista de Soporte TI.

Herramienta libre Kali Linux (Virtualizado)

- Equipo Físico:
Equipo: HP Elitebook 8470p
Sistema Operativo: Windows 10 Pro (Licenciado)
Procesador: Intel (R) Core (TM) i7-3520U
Memoria: 16 Gb
- Equipo Virtual
Sistema Operativo: Kali GNU/Linux 1.0.8
Procesador: Intel (R) Core (TM) i7-3520U
Memoria: 8 GB

Revisar Anexo 5 y Anexo 6, en los anexos se observa la encuesta realizada al Analista Senior de Infraestructura y las pruebas realizadas.

3.6.1. Seguridad operacional

3.6.1.1. Visibilidad (PV)

Enumerar los objetivos del alcance a través de la interacción directa e indirecta (Herzong, 2010)

La metodología indica lo siguiente:

- Identificar el perímetro de los segmentos de la red de destino y el objetivo a ser analizado (Herzong, 2010).
- Utilizar el rastreo de la red para localizar protocolos que envían respuestas o solicitudes del servicio de red donde corresponda (Herzong, 2010).
- Examinar todos los servidores de nombres y los servidores de nombres del ISP o proveedor de alojamiento (Herzong, 2010).
- Validar las solicitudes de propagación y las respuestas de todos los objetivos (Herzong, 2010).
- Verificar respuestas ICMP (Herzong, 2010).

Técnica utilizada	Observación, Entrevista, Kali Linux
Visibilidad	1.-Directorio Activo Principal
	2.-Directorio Activo Secundario
	3.-Base de Datos Principal
	4.-Base de Datos Secundario
	5.-Capa de Servicios Principal
	6.-Capa de Servicios Secundario
	7.-Servidor de VPNs
	8.-Servidor de consultas externas
	9.-Equipos activos
	10.-Equipos pasivos
	11.-Correo electrónico
	12.-Antivirus
	13.-Salida a internet
	14.-Dominio 1
	15.-Dominio 2
	16.-Dominio 3
	17.-Dominio 4

Tabla 79. Visibilidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Para la visibilidad se registra un valor de **PV= 17**.

3.6.1.2. Acceso (PA)

Se debe realizar pruebas para contabilizar los puntos de acceso hacia la red de datos. (Herzong, 2010)

La metodología menciona las siguientes sugerencias:

- Revisar los servicios comunes conocidos que utilizan UDP para conexiones desde todas las direcciones (Herzong, 2010).
- Solicitar servicios VPN comunes (Herzong, 2010).
- Revisar el servicio de red y enrutamiento para acceder a restricciones anteriores dentro del alcance (Herzong, 2010).
- Verificar el tiempo de actividad de los sistemas operativos en comparación con las últimas vulnerabilidades y versiones de parches (Herzong, 2010).
- Verificar la aplicación para el sistema y la versión.

Por confidencialidad del proyecto no se indica en el escrito que puertos se encuentran abiertos, las pruebas de verificación se pueden observar en el Anexo 6, se indica el número total de puertos abiertos comunes dentro de la red de la BVQ número de puertos **32**.

Los puertos utilizados para servicios dentro de la BVQ **10**.

Los puertos para servicios de VPN **1**.

Técnica utilizada	Observación, Entrevista, Kali Linux
Acceso	Puertos comunes = 32
	Puertos para servicios = 10
	Puertos VPN = 1

Tabla 80. Acceso Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para acceso un valor de **PA = 43**.

3.6.1.3. Confianza (PT)

La operación de confianza hace referencia al acceso a la información sin necesidad de identificación o autenticación, es decir a personal autorizado (Herzong, 2010).

Para las pruebas de spoofing se intentó de acceder vía inalámbrica a la red, pero al tener niveles de autenticación no se pudo realizar esta prueba, por otra parte, para acceder a la red inalámbrica se debe pasar por la autorización del administrador.

Al conectarse a un punto de red de la BVQ se detecta que no brinda servicio, ya que están configurados para que solo las MAC de los equipos de la BVQ se puedan conectar.

Se realizó pruebas de phishing enviando un enlace vía mail de una supuesta página de la BVQ, pero el personal de la BVQ notifica al departamento de tecnología de lo ocurrido y no ingresan a los enlaces enviados. Ver Anexo 6.

Para la confianza se obtiene un valor de **PT = 0**

3.6.2. Controles

3.6.2.1. Autenticación (LCAu)

Para la autenticación la metodología recomienda lo siguiente:

- Especificar los accesos que requieren autenticación (Herzong, 2010).
- Especificar el procedimiento para obtener la credencial adecuada para la autenticación (Herzong, 2010).
- Especificar el procedimiento de identificación adecuada para recibir la autenticación. (Herzong, 2010).
- Especificar el procedimiento lógico de autenticación (Herzong, 2010).
- Especificar la solidez de la autenticación (Herzong, 2010).
- Verificar de errores lógicos en la aplicación de la autenticación (Herzong, 2010).

Técnica utilizada	Observación, Entrevista, Kali Linux
Autenticación	1.- Mac registrada se conecta a la red BVQ.
	2.- Usuario válido en el AD de la BVQ se logea.
	3.- Política de contraseñas.
	4.- Intentos fallidos inhabilita al usuario.
	5.- Acceso VPN

Tabla 81. Acceso Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para el control de acceso un valor de **LCAu = 5**.

3.6.2.2. Indemnización (LCId)

- Contabilizar los servicios o objetivos que están resguardados contra el abuso o elusión de la política del empleado o el reglamento interno de la institución, estos deben estar asegurados por avería o robo, por otra parte, deben contar con los descargos respectivos de responsabilidad (Herzong, 2010).
- Examinar el contrato de la póliza de seguro para evidenciar las limitaciones en los tipos de daños que cubren la póliza (Herzong, 2010).

Técnica utilizada	Observación, Entrevista, Kali Linux
Indemnización	1.- Póliza de seguros cubre (robo, daños eléctricos, incendios, inundaciones y desastres naturales) 2.- La póliza cubre todo el equipo tecnológico de la BVQ (servidores, impresoras equipos de cómputo, UPS). 3.- La póliza tiene cobertura dentro y fuera de la BVQ. 4.- La póliza tiene la ventaja de agregar equipos o disminuir de acuerdo con la necesidad.

Tabla 82. Indemnización Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para control de indemnización un valor de **LCId = 4**.

3.6.2.3. Resiliencia LCRe

- Examinar los puntos de falla en la infraestructura de red donde el cambio o la falla pueden causar una indisponibilidad del servicio (Herzong, 2010).
- Verificar el impacto en el acceso que causará una falla del sistema o servicio (Herzong, 2010).

Técnica utilizada	Observación, Entrevista, Kali Linux
Resiliencia	1.- Software base 2.- Obsolescencia de hardware 3.- Incompatibilidad de nuevas aplicaciones 4.- Alto consumo de recursos del equipo por obsolescencia

Tabla 83. Resiliencia Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para el control de resiliencia un valor de **LCRe = 4**.

3.6.2.4. Subyugación (LCSu)

Para control de subyugación se debe enumerar las autenticaciones seguras a sitios externos como páginas web, dominios de acuerdo con el alcance del objetivo.

Técnica utilizada	Observación, Entrevista
Subyugación	1.- https://dominio1
	2.- https://dominio2

Tabla 84. Subyugación Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la subyugación un valor de **LCSu = 2**.

3.6.2.5. Continuidad (LCCT)

Para la continuidad la metodología recomienda lo siguiente:

- Enumerar los procedimiento y controles que cuenta la institución con respecto a demoras en el acceso y servicio, tiempos de réplica a través de sistemas de backups o el cambio a canales alternos (Herzong, 2010).
- Validar los sistemas de bloqueo que tiene implementado la institución a intentos de ingreso de intrusos con usuarios inválidos. (Herzong, 2010).

Técnica utilizada	Observación, Entrevista
Continuidad	1.- La BVQ tiene levantado el BIA para tiempos de recupero.
	2.- Ausencia de proveedores críticos
	3.- Ausencia de personal Clave
	4.- No acceso a las instalaciones
	5.- Fallas tecnológicas
	6.- Desastres Naturales
	7.- Seguridades detecta las instrucciones hacia la BVQ.

Tabla 85. Continuidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la continuidad un valor de **LCCT = 7**.

3.6.2.6. No Repudio (LCNR)

Para el control de no repudio la metodología recomienda lo siguiente:

- Enumerar el uso de los sistemas que se utilizan para identificar o registrar el acceso o las interacciones a la propiedad para obtener evidencia específica para el repudio (Herzong, 2010).

- Revisar la profundidad de la interacción registrada y el proceso de identificación (Herzong, 2010).
- Verificar que todos los procedimientos de interacción estén debidamente registrados con una identificación adecuada (Herzong, 2010).
- Identifique los procedimientos que minimicen el repudio (Herzong, 2010).

Técnica utilizada	Observación, Entrevista
No Repudio	1.- Rastreo de dirección IP 2.- Identificación de logs. 3.- Identificación de logs servidor VPNs 4.- Sistemas de seguridad 5.- Sistema de acceso de puertas

Tabla 86. No Repudio Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para el no repudio un valor de **LCNR = 5**.

3.6.2.7. Confidencialidad (LCCf)

Para el control de confidencialidad la metodología recomienda lo siguiente:

- Enumerar las interacciones con los servicios dentro del objetivo analizado de las comunicaciones o activos transportado a través del canal utilizando líneas seguras, cifrado (Herzong, 2010).
- Enumerar los métodos admisibles para el manejo de la confidencialidad (Herzong, 2010).
- Enumerar los límites externos de comunicación que pueden protegerse mediante los métodos aplicados de confidencialidad (Herzong, 2010).

Técnica utilizada	Observación, Entrevista
Confidencialidad	1.- La arquitectura de las aplicaciones y servicios están diseñada con las mejores prácticas recomendadas. 2.- La manipulación de datos está a cargo de los funcionarios de la BVQ de acuerdo con su acceso. 3.- Para aplicaciones web cuenta con la seguridad necesaria para precautelar la confidencialidad.

Tabla 87. Confidencialidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la confidencialidad un valor de **LCCf = 3**.

3.6.2.8. Privacidad (LCPr)

Para el control de la privacidad la metodología recomienda lo siguiente:

- Se debe contabilizar los objetivos dentro del alcance de las comunicación o activos transportados utilizando servicios específicos, interacciones personales, identificación personal, firmas individuales, para resguardar la privacidad de la interacción (Herzong, 2010).

Técnica utilizada	Observación, Entrevista
Privacidad	1.- Capa de servicios, cuenta con seguridad de certificados
	2.- Conexión VPN.
	3.- Aplicaciones no se encuentra expuestas al exterior.

Tabla 88. Privacidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la privacidad un valor de **LCPr = 3**

3.6.2.9. Integridad (LCIt)

Para el control de integridad de debe verificar el proceso donde se determine la frecuencia de respaldo, réplicas, control de cambios, entre otros, como también la información que utiliza firmas, cifrado, hash o marcas para avalar que el activo no se redirige, pueda cambiar o revertir sin que las partes implicadas lo sepan. (Herzong, 2010)

Técnica utilizada	Observación, Entrevista
Integridad	1.- Política de respaldos
	2.- Control de cambios software.
	3.- Control de cambios de información.

Tabla 89. Privacidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la integridad un valor de **LCIt = 3.**

3.6.2.10. Alarma (LCAI)

Verificar el uso de un sistema, mensaje o registro de advertencia localizado para cada acceso a través de cada canal donde el personal observa una situación sospechosa de intentos de elusión, actividad fraudulenta (Herzong, 2010).

Técnica utilizada	Observación, Entrevista
Alarma	1.- Notificaciones de monitoreo
	2.- Notificaciones de antivirus
	3.- Notificaciones de firewall
	4.- Notificaciones de respaldos

Tabla 90. Alarma Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la alarma un valor de **LCAI = 4**.

3.6.3. Limitaciones

3.6.3.1. Exposición (LE)

La exposición está dada por la operación de visibilidad, dentro de este proyecto la exposición son los dominios externos, para mitigar esta exposición se cuenta con certificados de seguridad, el valor numérico para la exposición es **LE = 1**.

3.6.3.2. Vulnerabilidad (LV)

Las vulnerabilidades vienen dadas las operaciones de acceso y confianza.

Técnica utilizada	Observación, Entrevista
Vulnerabilidad	1.- Discontinuidad de software

Tabla 91. Vulnerabilidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la vulnerabilidad un valor de **LV = 1**.

3.6.3.3. Debilidad (LW)

Para la limitación de la debilidad se debe analizar los controles de clase A e identificar las debilidades que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación, Entrevista
Resiliencia	1.- Obsolescencia de hardware.
	2.- Discontinuidad de software.
Subyugación	3.- Renovación de certificados digitales.

Tabla 92. Debilidad Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Para los controles autenticación, indemnización y continuidad no se localizó debilidades, pero se localizó para resiliencia y subyugación.

Aplicando la fórmula de la figura 20 se obtiene:

$$L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$Lw = 0 + 0 + 2 + 1 + 0$$

$$Lw = 3$$

3.6.3.4. Preocupación (LC)

Para la limitación de la preocupación se debe analizar los controles de clase B e identificar las posibles inconvenientes que pueden existir dentro de esos controles o la implementación de nuevos controles adicionales.

Técnica utilizada	Observación, Entrevista
No Repudio	1.- Features de logs deshabilitados.

Tabla 93. Preocupación Canal Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Para los controles integridad, confidencialidad, integridad y alarma no se localizó preocupaciones, pero se localizó para no repudio.

Aplicando la fórmula de la figura 21 se obtiene:

$$L_c = FC_{NR} + FC_{It} + FC_{Pr} + FC_{Cf} + FC_{Al}$$

$$Lc = 1 + 0 + 0 + 0 + 0$$

$$Lc = 1$$

3.6.3.5. Anomalías (LA)

La anomalía para el canal red de datos está dada por:

Técnica utilizada	Observación, Entrevista
Anomalía	1.- No tener servicio de proveedor externo. 2.- Avería de equipos de proveedores externos.

Tabla 94. Anomalía Redes de Datos. Fuente: Henry Daniel Calero Suntasig.

Se registra para la anomalía un valor de **LA = 2**.

Para el Canal Red de Datos se obtiene la siguiente información:

Categoría	Seguridad Operacional	Limitaciones
Operaciones	Visibilidad PV = 17	Exposición LE = 1
	Acceso PA = 43	Vulnerabilidad LV = 1
	Confianza PT = 0	
	Autenticación LCAu = 5	
	Indemnización LCId = 4	Debilidad LW = 3
Controles	Clase A Resiliencia LCre = 4	
	Subyugación LCSu = 2	
	Continuidad LCCt = 7	
	No repudio LCNr = 5	
	Confidencialidad LCCf = 3	
Clase B	Privacidad LCPr = 3	Preocupación LC = 1
	Integridad LCIt = 3	
	Alarma LCAI = 4	
	Anomalías LA = 2	

Tabla 95 Datos Canal Red de Datos RAV Fuente Henry Daniel Calero Suntasig

Una vez que se obtienen los resultados pueden ser comprobados de la siguiente manera:

$$RAV = \text{CONTROLES VERDADEROS} - \text{POROSIDAD} - \text{LIMITACIONES}$$

$$RAV = 6.77 - 14.27 - 12.48$$

$$RAV = -19.98$$

Este valor determina un 19.98 de insuficiencia y carencia de controles dentro de los controles implementados.

La red de datos de la BVQ se encuentra parcialmente vulnerable a posibles ataques informáticos y en el peor de los casos robo o sustracción de información.

Pruebas de Seguridad Redes de Datos

OSSTMM versión 3

Inserte en los espacios en blanco los valores numéricos para OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC

Visibilidad	17
Acceso	43
Confianza	0
Total (Porosidad)	60

CONTROLES

Clase A		Ausentes
Autenticación	5	55
Indemnización	4	56
Resiliencia	4	56
Subyugación	2	58
Continuidad	7	53
Total Clase A	22	278

Clase B		Ausentes
No-Repudio	5	55
Confidencialidad	3	57
Privacidad	3	57
Integridad	3	57
Alarma	4	56
Total Clase B	18	282

		Ausentes Verdaderos
Total Controles	40	560
Cobertura Total	6,67%	93,33%

LIMITACIONES

		Valor Numérico	Valor Total
Vulnerabilidad	1	10,333333	10,333333
Debilidad	3	5,633333	16,900000
Preocupación	1	5,700000	5,700000
Exposición	1	1,016667	1,016667
Anomalia	2	0,083333	0,166667
Total # Limitaciones	8		34,1167

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC
14,274794

Controles Verdaderos
6,776361

Controles Completos
5,674005
6,776361

Cobertura Verdadera A
7,33%

Cobertura Verdadera B
6,00%

Total Cobertura Verdadera
6,67%



Limitaciones
12,482752

Seguridad Δ
-19,98

Protección Verdadera
80,02

Seguridad Actual: 79,9873 ravs

OSSTMM RAV - Creative Commons 3,0 attribution-Nom Commercial-No Derivs 2011, ISECOM

Figura 28. Calculadora RAVS – Seguridad Canal Red de Datos. Fuente: Henry Daniel Calero Suntasig.

3.7. Interpretación de resultados

Los valores obtenidos aplicando la metodología OSSTMM sobre la Red de Datos de la Bolsa de Valores de Quito son los siguientes:

Clase	Canal	Seguridad Actual /100
Seguridad Física	Humano	78,56
Seguridad Humana	Físico	83,40
Seguridad Inalámbrica	Comunicaciones inalámbricas	83,24
Seguridad de las Comunicaciones	Telecomunicaciones	89,71
	Redes de datos	79,98

Tabla 96. Resultados obtenidos de la seguridad actual de la BVQ. Fuente: Henry Daniel Calero Suntasig.

Clase	Canal	Riesgo Actual /100
Seguridad Física	Humano	21,56
Seguridad Humana	Físico	16,45
Seguridad Inalámbrica	Comunicaciones inalámbricas	16,60
Seguridad de las Comunicaciones	Telecomunicaciones	10,00
	Redes de datos	19,98

Tabla 97. Resultados obtenidos de riesgo actual de la BVQ. Fuente: Henry Daniel Calero Suntasig.

Para la medición del riesgo se hará uso de la escala de Likert, Bedoya (2017) indica que para el uso de esta escala es necesario asignar valores numéricos en cinco rangos del total de la medición. El total para el caso de estudio es cien puntos, por tal motivo cada escala será cada veinte puntos, y los niveles para estas escalas son:

Escala de Likert	
Escala puntos	Niveles de escala
Escala de: 1-20	Muy Bajo
Escala de: 21-40	Bajo
Escala de: 41-60	Medio
Escala de: 61-80	Alto
Escala de: 81-100	Muy Alto

Tabla 98. Escala de Likert medición de Riesgo. Fuente: Henry Daniel Calero Suntasig.

Aplicando la escala de Likert dentro de los riesgos actuales se obtiene los siguientes resultados:

Clase	Canal	Muy alto	Alto	Medio	Bajo	Muy bajo
Seguridad Física	Humano				21,56	
Seguridad Humana	Físico					16,45
Seguridad Inalámbrica	Comunicaciones inalámbricas					16,60
Seguridad de las Comunicaciones	Telecomunicaciones					10,00
	Redes de datos					19,98

Tabla 99. Resultados de riesgos actuales de la BVQ utilizando escala de Likert. Fuente: Henry Daniel Calero Suntasig.

Si bien el canal de seguridad física tiene un nivel de riesgo bajo se debe tomar medidas para que este canal quede dentro de la escala “muy bajo”, por otro lado los canales de seguridad físico, comunicaciones inalámbricas, telecomunicaciones y redes de datos se encuentran dentro de la escala “muy bajo”, esto no quiere decir que no se tiene vulnerabilidades en estos canales, se deben revisar las vulnerabilidades localizadas para implementar controles con el objetivo que se mantenga dentro de esa escala aceptable.

A continuación, se presenta la matriz de riesgos con las vulnerabilidades encontradas.

ACTIVO/FACTOR/PROCESO						ANÁLISIS DE RIESGO								
CANAL	FACTOR O COMPONENTE	RIESGO	TIPO RIESGO	DESCRIPCION RIESGO	CONSECUENCIAS QUE DEJARÍA EL RIESGO	CONTROL	TIPO DE CONTROL	PERIODICIDAD DE REVISION	PROBABILIDAD	IMPACTO	RIESGO BRUTO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Seguridad canal Humano	Exposición	Ingreso de personas no autorizadas a la BVQ sin confirmación (guardia PB)	EXTERNO	Guardia de PB permite paso a personas ajenas a la institución	Acceso no controlado a las instalaciones de la BVQ	Notificar a empresa de seguridad que toda persona debe ser anunciada antes del ingreso	PREVENTIVO	DEMANDA	1	2	2	X		
		Bitácora de vistas expuestas al publico	INHERENTE	La bitácora de registro de visitas a la BVQ del guardia de PB esta expuesta al publico	Al estar expuesta un visitante puede hacer uso de un nombre visualizado en la bitácora y realizar suplantación de identidad para solicitar información vía telefónica	Notificar a empresa de seguridad normas básicas de protección de información.	PREVENTIVO	DEMANDA	2	2	4	X		
	Vulnerabilidad	Tarjetas de accesos extraviadas	INHERENTE	El personal de la BVQ al extraviar la tarjeta de acceso no informa al personal asignado para su bloqueo	Personas ajenas a la institución pueden utilizar estas tarjetas	Difusión del reglamento interno de la BVQ	CORRECTIVO	SEMESTRAL	1	3	3	X	X	X
		Divulgación de información vía telefónica	INHERENTE	Entregar información institucional por canales no autorizados	Confidencialidad de la información	Difusión del reglamento interno de la BVQ	PREVENTIVO	SEMESTRAL	1	3	3	X	X	
		Entrega de información privilegiada	INHERENTE	Entregar información privilegiada a funcionarios en periodo de prueba o pasantes	Confidencialidad, integridad de la información	Inducción al personal al ingresar a la BVQ	PREVENTIVO	DEMANDA	2	3	6	X	X	X
		Uso de dispositivos de almacenamiento externo	INHERENTE	Usar dispositivos no autorizados para guardar o trasladar información de propiedad de la BVQ	Confidencialidad, integridad y disponibilidad de la información	Difusión de la política de seguridad de la BVQ	PREVENTIVO	SEMESTRAL	1	3	3	X	X	
		Uso de correos personales	INHERENTE	Utilizar correos personales para el envío de infoamción de propiedad de la BVQ	Confidencialidad, integridad y disponibilidad de la información	Difusión de la política de seguridad de la BVQ	PREVENTIVO	SEMESTRAL	1	3	3	X		
		Suplantación de identidad en vistas externas	INHERENTE	Personas que visitan a la BVQ se anuncian con nombre diferente.	Acceso no controlado a las instalaciones de la BVQ	Notificar a empresa de seguridad que toda persona que ingresa a la BVQ debe presentar alguna identificación.	PREVENTIVO	DEMANDA	1	3	3	X		
	Indemnización / No Repudio / Privacidad / Integridad	Incumplimiento de l reglamento interno, políticas o procesos institucionales	INHERENTE	Al no cumplir con el reglamento, políticas o procesos internos, los funcionarios podrán estar incurriendo en faltas graves dentro de la institución.	Confidencialidad, integridad y disponibilidad de la información	Difusión de la política de seguridad de la BVQ	PREVENTIVO	SEMESTRAL	2	3	6	X	X	X
	Confidencialidad	Fallas para el registro de documentos internos y externos	INHERENTE	Si no se registra los documentos internos y externo no se tendría trazabilidad de la información física	Perdida de información física	Difusión de la política de activos de la información	PREVENTIVO	SEMESTRAL	1	3	3	X	X	X
	Alarma	Fallas del sistema de video cámaras de seguridad	INHERENTE	Fallas de grabación de sistema de cámaras por mal funcionamiento	No contar con el registro de sistema de video de las personas que ingresan o salen de las instalaciones de la BVQ	Mantenimiento trimestral del sistema de video cámaras	PREVENTIVO	TRIMESTRAL	1	3	3	X	X	X
		Fallas del sistema de alarma	INHERENTE	El sistema de alarma no este funcionado de forma correcta	No tener protección en las instalaciones de la BVQ durante la noche.	Contactar con proveedor para mantenimiento cada seis meses	PREVENTIVO	SEMESTRAL	1	3	3	X	X	X

Figura 29. Análisis de la probabilidad y el impacto. Fuente: Henry Daniel Calero Suntasig

ACTIVO/FACTOR/PROCESO									ANÁLISIS DE RIESGO					
CANAL	FACTOR O COMPONENTE	RIESGO	TIPO RIESGO	DESCRIPCION RIESGO	CONSECUENCIAS QUE DEJARÍA EL RIESGO	CONTROL	TIPO DE CONTROL	PERIODICIDAD DE REVISION	PROBABILIDAD	IMPACTO	RIESGO BRUTO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Seguridad canal Físico	Exposición	Ingreso no autorizado por puerta de auditorio (salida posterior)	INHERENTE	Ingreso de personas no autorizadas por puerta posterior del auditorio de la BVQ	Ingreso de personas no autorizadas	Habilitar puerta posterior en fechas de seminarios, conferencias, el resto del tiempo tenerlo bajo llave	PREVENTIVO	DEMANDA	1	3	3	X	X	X
		Ingreso no autorizado por segunda puerta directorio	INHERENTE	Ingreso de personas no autorizadas por puerta segunda puerta del directorio de la BVQ	Ingreso de personas no autorizadas	Habilitar puerta en fechas de directorios de la BVQ el resto del tiempo tenerlo bajo llave	PREVENTIVO	DEMANDA	1	3	3	X	X	X
	Vulnerabilidad	Ingreso no autorizado por puerta de parqueadero	EXTERNO	Ingreso de personas no autorizadas por puerta del parqueadero	Ingreso de personas no autorizadas	Notificar a empresa de seguridad que toda persona ajena al edificio Londres debe ingresar por la puerta principal del Edificio	PREVENTIVO	DEMANDA	1	3	3	X		
	Indemnización	No renovar de pólizas de seguros	INHERENTE	Por caducidad de la póliza de seguros no realizar la renovación	No tener cobertura ante una emergencia dentro	Revisión de coberturas y caducidad de pólizas de la BVQ	PREVENTIVO	ANUAL	1	3	3		X	
	Privacidad	Indisponibilidad de lugar destinados para reuniones o recibir visitas laborales	INHERENTE	No contar con espacio para recibir visitas de trabajo o realizar reuniones con personas externas o internas	Divulgación de información	Asignar espacios físicos para recibir visitas de trabajo y realizar reuniones internas y externas	PREVENTIVO	DEMANDA	1	3	3	X		
	Alarma	Renovación del sistema de alarma	INHERENTE	Por caducidad del contrato del sistema de alarma y no realizar la renovación	No tener protección en las instalaciones de la BVQ durante la noche.	Revisión de caducidad del contrato para proceder con la renovación	PREVENTIVO	ANUAL	1	3	3	X	X	X
	Anomalías	Fallos del generador eléctrico del edificio Londres	EXTERNO	Hace referencia al mal funcionamiento del generador eléctrico del edificio	Que el equipo no funcione adecuadamente ni cumpla sus funciones de respaldo y regulación de energía.	Solicitar al administrador del edificio contrato de mantenimiento del generador	PREVENTIVO	ANUAL	1	3	3			X

Figura 30. Análisis de la probabilidad y el impacto. Fuente: Henry Daniel Calero Suntasig

ACTIVO/FACTOR/PROCESO									ANÁLISIS DE RIESGO					
CANAL	FACTOR O COMPONENTE	RIESGO	TIPO RIESGO	DESCRIPCION RIESGO	CONSECUENCIAS QUE DEJARÍA EL RIESGO	CONTROL	TIPO DE CONTROL	PERIODICIDAD DE REVISIÓN	PROBABILIDAD	IMPACTO	RIESGO BRUTO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Seguridad canal Inalámbrico	Exposición	Interferencia de transmisión	EXTERNO	Hace referencia al envío de señales radiales para interferir con el tráfico de una red inalámbrica.	Desconexión continua de la red inalámbrica.	Configuración automática de canales.	PREVENTIVO	DEMANDA	3	1	3			X
	Vulnerabilidad	Fallos externos del dispositivo inalámbrico	INHERENTE	Hace referencia a fallas del equipo por factores externos (humedad, calor, filtraciones de agua, etc.)	Interrupción de servicio	Revisión periódica por parte de auxiliar de servicios generales	PREVENTIVO	SEMANAL	1	2	2			X
		Fallos de actualización de firmware	INHERENTE	Hace referencia a la actualización de sistema de los dispositivos inalámbricos	Interrupción de servicio	Política de código malicioso	PREVENTIVO	SEMANAL	1	3	3			X
	Continuidad	Mantenimiento de equipos de backup	INHERENTE	Hace referencia al mantenimiento de equipos de backup durante la avería de un equipo principal	Interrupción de servicio	Programar mantenimientos preventivos y/o correctivos de equipos de backup fuera del horario de operaciones	PREVENTIVO	TRIMESTRAL	1	1	1			X
	No repudio	Fallos de consola administración Wireless	INHERENTE	Hace referencia al fallo de la consola de Wireless	Pérdida de monitoreo de equipos Wireless y registro de eventos	Generar backup de configuración para ser restaurados en otro equipo	PREVENTIVO	DEMANDA	1	3	3		X	X
	Alarma	Cambio de cuentas de correo electrónico para notificaciones	INHERENTE	Hace referencia de cambio de claves o cuentas de correo electrónico para recibir notificaciones del sistema Wireless	No contar con alarmas de los eventos del sistema Wireless	Informar cambios de cuentas y contraseñas para servicios de notificaciones	PREVENTIVO	DEMANDA	1	3	3			X
	Anomalías	Fallo de código de autenticación Wireless para ser utilizado en dos dispositivos	INHERENTE	Hace referencia a utilizar un voucher de acceso en dos dispositivos inalámbricos de visitantes	Conexión a recursos de la BVQ sin autorización	Política de seguridad de la información	PREVENTIVO	DEMANDA	1	2	2			X
		Desbloqueo de equipos no autorizados	INHERENTE	Hace referencia al desbloqueo de equipos sin autorización	Conexión a recursos de la BVQ sin autorización	Política de seguridad de la información	PREVENTIVO	DEMANDA	1	3	3	X	X	
Seguridad canal de Telecomunicaciones	Indemnización / No Repudio	Obsolescencia de central PBX	INHERENTE	Equipo ha cumplido su vida útil.	Daño parcial o total del equipo.	Mantenimiento preventivo y/o correctivo	PREVENTIVO	DEMANDA	3	3	3	X	X	X
	Subyugación	Discontinuidad del sistema operativo central PBX	INHERENTE	Hace referencia a la discontinuidad del sistema operativo de la central PBX	No contar con actualizaciones por parte del proveedor	Considerar renovación de central PBX	PREVENTIVO	DEMANDA	3	3	3	X	X	X
	Anomalías	Fallas de servicio proveedor de telefonía	EXTERNO	Cualquier motivo atribuible al proveedor o terceros, que origine	Interrupción del servicio telefónico.	Cumplimiento del SLA.	PREVENTIVO	DEMANDA	1	2	2			X
Seguridad canal Red de Datos	Exposición	Exposición de dominios	INHERENTE	Hace referencia a los dominios de la BVQ expuestos a internet	Interrupción de servicio	Contratar certificados digitales SSL	PREVENTIVO	DEMANDA	3	2	6	X	X	X
	Vulnerabilidad	Discontinuidad de Software	INHERENTE	Hace referencia a la discontinuidad de software interno de la institución	No contar con actualizaciones para la plataforma diseñada	Actualización de software interno	CORRECTIVO	SEMANAL	2	3	6	X	X	X
	Resiliencia	Obsolescencia de hardware	INHERENTE	Equipos han cumplido su vida útil.	Daño parcial o total del equipo, con riesgo de pérdidas de información.	Mantenimiento preventivo y/o correctivo	PREVENTIVO	DEMANDA	3	3	3			X
	Subyugación	Caducidad del certificado	INHERENTE	Que se cumpla el tiempo de vigencia del certificado adquirido.	Imposibilidad de acceder o hacer uso de servicios críticos contratados.	Política de gestión de certificados digitales	PREVENTIVO	DEMANDA	1	3	3			X
	Anomalías	Fallo de servicio de proveedores externos	EXTERNO	Cualquier motivo atribuible al proveedor principal, que origine un corte del servicio.	Operaciones que necesiten internet para efectuarse se ven afectadas	Cumplimiento del SLA y respaldo.	PREVENTIVO	DEMANDA	1	3	3			X

Figura 31. Análisis de la probabilidad y el impacto. Fuente: Henry Daniel Calero Suntasig

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- En el presente proyecto se realizó un análisis de vulnerabilidades sobre la infraestructura de red de la Bolsa de Valores de Quito, precautelando los tres principios de la seguridad de la información que son confidencialidad, integridad y disponibilidad, para no afectar los servicios operacionales de la institución.
- Para el análisis de vulnerabilidades se realizó una comparación entre dos metodologías, para seleccionar la que más se adapte a la realizada de la Bolsa de Valores de Quito, las metodologías analizadas fueron:

Manual de la Metodología Abierta de Testeo de Seguridad OSSTMMv3
Sistema de puntuación de vulnerabilidad común (CVSS)

La metodología seleccionada fue el Manual de la Metodología Abierta de Testeo de Seguridad OSSTMMv3 ya que es una metodología completa la cual nos muestra los criterios que se deben considerar para auditar o evaluar las vulnerabilidades dentro de una organización, no establece ningún objetivo de análisis, pero dicta las directrices para la selección más adecuada del objetivo a ser analizado, para la evaluación de riesgos la metodología utiliza RAVS,

- En el presente proyecto se realizó escaneos internos y externos para localizar vulnerabilidades, se utilizó varias técnicas tales como observación, entrevista, encuestas y cada una de estas técnicas proporcionó información importante para localizar huecos de seguridad, por otra parte se utilizó software libre como Kali Linux que cuenta con una gran variedad de herramientas de escaneo de vulnerabilidades, este software se utilizó para escanear desde el interior como el exterior la red de la Bolsa de Valores de Quito, como resultado proporcionó información sobre posibles huecos de seguridad que se detallan dentro de este documento.

- En este proyecto se utilizó la metodología OSSTMMv3 para la detección de vulnerabilidades, producto de esta investigación se levantó una matriz de riesgos analizando la probabilidad y el impacto de cada una de las vulnerabilidades detectadas, así también se indica dentro de la matriz que riesgos ameritan tomar una acción inmediata.
- Se examinó la cantidad de riesgos obtenidos por cada canal de la metodología OSSTMMv3, para la cual se obtuvieron los siguientes resultados:

Canal Humano: Doce riesgos que equivalen al 21.56% de vulnerabilidades.

Canal Físico: Siete riesgos que equivalen al 16.45% de vulnerabilidades.

Canal Inalámbrico: Ocho riesgos que equivalen al 16.60% de vulnerabilidades.

Canal de Telecomunicaciones: Tres riesgos que equivalen al 10% de vulnerabilidades.

Canal de Red de Datos: Cinco riesgos que equivalen al 19.98% de vulnerabilidades.

5.2. Recomendaciones

- Al revisar el organigrama de la institución se detecta que el Oficial de Seguridad de la Información es el Analista Senior de Infraestructura por lo que se recomienda de acuerdo con la norma ISO 27001, el Oficial de Seguridad de la Información debe ser una persona que trabaje en colaboración con el departamento de Tecnología, pero no dentro del departamento de Tecnología porque puede llegar a ser juez y parte dentro de una auditoría.
- Para evitar la obsolescencia de hardware por el paso de los años, se recomienda migrar algunos servicios a la nube gradualmente, teniendo en cuenta las seguridades necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información.

Bibliografía

- Ávila, M. (2018). *Estudio de las mejores prácticas de ethical hacking, para generar un nuevo método que facilite la ejecución de análisis de seguridad enfocados a pruebas de penetración*. Universidad Nacional Abierta y Distancia UNAD, Bogotá, Colombia.
- Bedoya, C (2017). *Diseño de un instrumento tipo escala Likert para la descripción de las actitudes hacia la tecnología por parte de los profesores de un colegio público de Bogotá* (Maestría). Universidad Distrital Francisco José de Caldas, Bogotá.
- Born, J. van, de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Veen, A. van der, & Verheijen, T. (2008). *Gestión de Servicios de TI basada en ITIL* (1.ª ed.). Holanda: Van Haren Publishing.
- Carrera, E. (29 de mayo de 2018). *Pentesting WiFi: Usando Kismet para ver la actividad de un usuario de Wi-Fi a través de las paredes*. Recuperado de: <https://securityhacklabs.net/articulo/usando-kismet-para-ver-la-actividad-de-un-usuario-de-wi-fi-a-traves-de-las-paredes>
- Cashman, J. (26 de agosto de 2019). *WhatsUp® Gold*. Obtenido de WhatsUp® Gold. Recuperado de: <https://es.ipswitch.com/monitoreo-de-redes/analisis-de-trafico-de-red>
- Código Orgánico Integral Penal [COIP] (2014). *Código Orgánico Integral Penal*. Asamblea Nacional. Registro Oficial, Suplemento 180.
- First, O. (03 de 12 de 2019). *Common Vulnerability Scoring System v3.1: Specification Document*. Recuperado de: <https://www.first.org/cvss/v3.1/specification-document>.
- Gacharná, F. (2009, junio). Hacker ético vs delincuente informático: Una mirada en el contexto colombiano. *Inventum*, 4(6), 46-49.
- Github. (11 de abril de 2019). *How to send Snort IDS alert logs into Graylog*. Recuperado de: <https://github.com/Graylog2/graylog-guide-snort>

- Herzong, P. (2010). *Open Source Security Testing Methodology Manual*. ISECOM.
- Kumar, K., & Singh, S. (2016). Intrusion Detection Using Soft Computing Techniques . *International Journal of Computer Science & Communication Networks*, 6(3), 153-169.
- Lawrence, I., Motta de Castro, A., & Kowask, E. (2014). *Planeación y Gestión Estratégica de las TI* (1.ª ed., pp. 19–20). Bogotá: Renata-Cedia.
- Microsoft. (2014). Microsoft Enterprise Cloud Red Teaming (sf). Recuperado de : https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf.
- Pacheco, O. (2018). *Auditoría de Sistemas* (1.ª ed.). Lima - Perú: OEPC.
- Picouto, F., Ramos, A., Barbero, C., González, J., & Serrano, E. (2014). *Redes seguridad perimetral monitorización y ataques en redes* (2.ª ed.). España: Ediciones De La U.
- Quispe, C. A. (2018). *Tipos de Hackers*. La Paz, Bolivia Universidad Mayor de San Andrés.
- Quinteros, P., & Novoa , H. (2015). Common Vulnerability Score System (CVSS) para calcular la severidad de una vulnerabilidad en los Sistemas de Información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, II, 95-105.
- Rincón A., & Ruiz C., (2017). *Diseño de un proceso de gestión de cambios, aplicado a redes móviles, con base en las buenas prácticas ITIL*. (Especialización). Universidad Santo Tomas, Bogotá.
- Rivas, C. (2017). *Informe general KPMG – Auditoría Departamento de Tecnología*. Quito.
- Romero, M. I., Figueroa, G. L., Vera, D. S., Álava, J. E., Parrales, G. R., Álava, C. J., Murillo, A. L., Castillo, M. A., (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1ª ed.). Alicante: 3 Ciencias Editorial Área de Innovación y Desarrollo, S.L.
- Security, I. S. (27 de enero de 2020). *Tenable Network Security – IT Vulnerability Management & Scanner*. Recuperado de: <https://www.infoguard.ch/de-ch/partner/tenable-network-security-vulnerability-management>

Sharma U., Sharma P., Rawal V. & Narwal P. (2017). Network Security: Internal and External Attacks. *Journal of Engineering and Applied Sciences*, 12 (24), 7494-75000. doi:10.3923/jeasci.2017.7494.7500.

UIT, S. D. (2012). *Sistema común de puntuación de vulnerabilidades*. Guinebra - Suiza: UIT.

Anexos

Dentro de anexos podrá visualizar los datos obtenidos durante este proyecto tales como encuestas, resultados de encuestas, captura pantalla de uso de herramientas libres del escaneo de vulnerabilidades, etc.

Anexo 1.- Encuesta Pruebas de Seguridad Humana, Física e Inalámbrica BVQ

Pruebas de Seguridad Humana, Física e Inalámbrica de la BVQ

1. ¿Comparte usted la contraseña de acceso a su equipo?

- ☐ SI
☐ NO

2. ¿Las contraseñas asignadas a usted para el uso de aplicaciones de la BVQ las ha compartido con otras personas?

- ☐ SI
☐ NO

3. ¿Para recordar su contraseña la escribe y lo deja cerca de su equipo?

- ☐ SI
☐ NO

4. ¿Considera que la información de la BVQ se encuentra totalmente segura ?

- ☐ SI
☐ NO

5. ¿Utiliza correos personales como gmail, hotmail, yahoo, para el envío de información relacionada con su trabajo?

- ☐ SI
☐ NO

6. ¿Ha notado alguna vez que la información de su equipo a sido manipulada o modificada de forma parcial o total?

- ☐ SI
- ☐ NO

7. Cuando comparte información que pertenece a la BVQ, ¿Está seguro que la información fue recibida únicamente por la persona con quien la compartió?

- ☐ SI
- ☐ NO

8. ¿Ha detectado que su equipo a sido utilizado por otras personas desde que lo asignaron a usted?

- ☐ SI
- ☐ NO

9. ¿Para compartir información de trabajo ha utilizado en alguna ocasión dispositivos de almacenamiento extraíbles como flash memory, cds, etc?

- ☐ SI
- ☐ NO

10. ¿Durante el período que usted a trabajado en la BVQ se le ha perdido algún dispositivo de almacenamiento con información de trabajo, por ejemplo flah memory, cd, etc?

- ☐ SI
- ☐ NO

11. ¿Conoce si pueden manipular su equipo de forma remota sin su conocimiento?

- ☐ SI
- ☐ NO

12. ¿Para acceder a áreas restringidas de la BVQ, usted debe pasar por algún filtro de seguridad?

- ☐ SI
- ☐ NO

13. ¿A compartido información personal o de trabajo con funcionarios de la BVQ vía telefónica?

- ☐ SI
- ☐ NO

14. ¿Considera Ud que el sistema de acceso en las puertas de la BVQ es un método seguro y confiable para la restricción de ingreso a personal no autorizado?

- ☐ SI
- ☐ NO

15. ¿Para ingresar al departamento de tecnología necesita autorización?

- ☐ SI
- ☐ NO

16. ¿Para acceder al centro de cómputo de la BVQ necesita tener autorización?

- ☐ SI
- ☐ NO

17. ¿Si tiene autorización para acceder al centro de cómputo de la BVQ debe registrar su acceso en una bitácora de visitas?

- ☐ SI
- ☐ NO

18. ¿Al ingresar dispositivos de almacenamiento externos en su equipo de trabajo muestra alertas de seguridad para analizar el dispositivo?

- ☐ SI
- ☐ NO

19. ¿En alguna ocasión ha tenido claves o accesos con privilegios altos para el ingreso a sistemas, aplicaciones o instalar software no autorizado en su equipo?

- ☐ SI
- ☐ NO

20. ¿Utiliza su computadora portátil institucional fuera de trabajo?

- ☐ SI
- ☐ NO

21. ¿Cuando se le ha perdido o se ha dañado su credencial de acceso lo ha reportado para su bloqueo ?

- ☐ SI
- ☐ NO

22. ¿Al olvidar su credencial de acceso a solicitado a su compañero que le preste para movilizarse dentro de la BVQ?

- ☐ SI
- ☐ NO

23. ¿Para conectarse dispositivos móviles personales a la red WIFI de la BVQ usted debe solicitar autorización?

- ☐ SI
- ☐ NO

24. ¿Para el uso de aplicaciones que usted utiliza necesita tokens, certificados digitales u otros tipos de autenticación?

- ☐ SI
- ☐ NO

25. ¿Usted a observado si el público en general o personas externas que visita la BVQ tiene libre acceso dentro de las instalaciones de la BVQ?

- ☐ SI
- ☐ NO

26. Dentro de las instalaciones de la BVQ ha observado señalética de prevención de accidentes como por ejemplo área de peligro, sistema contraincendios, piso mojado, etc.?

- ☐ SI
- ☐ NO

27. ¿Caundo usted tiene prevista una visita o reunión de trabajo le notifica el guardia de PB que lo están buscando para autorizar el acceso?

- ☐ SI
- ☐ NO

28. ¿Dentro de la BVQ tiene áreas destinadas para realizar reuniones o atender visitas?

- ☐ SI
- ☐ NO

29. ¿Para trasladar su equipo de trabajo fuera de la instalaciones de la BVQ usted debe tener autorización para hacerlo?

- ☐ SI
- ☐ NO

30. ¿Conoce usted el reglamento interno de la BVQ?

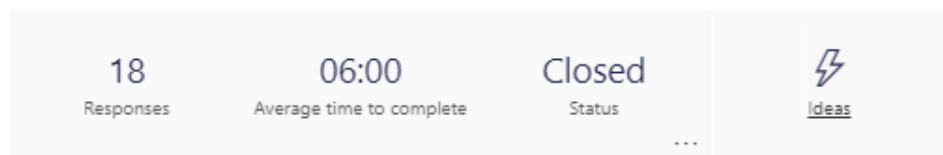
- ☐ SI
- ☐ NO

31. ¿Dentro de su contrato o reglamento interno le mencionaron sobre acuerdo de confidencialidad y no divulgación de información de la BVQ?

- ☐ SI
- ☐ NO

Submit

Anexo 2.- Resultados de la encuesta de Pruebas de Seguridad Humana, Física e Inalámbrica BVQ



View results

 Open in Excel

1. ¿Comparte usted la contraseña de acceso a su equipo?

[More Details](#)

- ☒ SI 6
- ☐ NO 13



2. ¿Las contraseñas asignadas a usted para el uso de aplicaciones de la BVQ las ha compartido con otras personas?

[More Details](#)

- ☒ SI 6
- ☐ NO 13



3. ¿Para recordar su contraseña la escribe y lo deja cerca de su equipo?

[More Details](#)

- ☒ SI 2
- ☐ NO 17



3. ¿Para recordar su contraseña la escribe y lo deja cerca de su equipo?

[More Details](#)



4. ¿Considera que la información de la BVQ se encuentra totalmente segura ?

[More Details](#)



5. ¿Utiliza correos personales como gmail, hotmail, yahoo, para el envío de información relacionada con su trabajo?

[More Details](#)



6. ¿Ha notado alguna vez que la información de su equipo a sido manipulada o modificada de forma parcial o total?

[More Details](#)



7. Cuando comparte información que pertenece a la BVQ. ¿Está seguro que la información fue recibida únicamente por la persona con quien la compartió?

[More Details](#)



8. ¿Ha detectado que su equipo a sido utilizado por otras personas desde que lo asignaron a usted?

[More Details](#)



9. ¿Para compartir información de trabajo ha utilizado en alguna ocasión dispositivos de almacenamiento extraíbles como flash memory, cds, etc?

[More Details](#)



10. ¿Durante el período que usted a trabajado en la BVQ se le ha perdido algún dispositivo de almacenamiento con información de trabajo, por ejemplo flah memory, cd, etc?

[More Details](#)



11. ¿Conoce si pueden manipular su equipo de forma remota sin su conocimiento?

[More Details](#)



12. ¿Para acceder a áreas restringidas de la BVQ, usted debe pasar por algún fitro de seguridad?

[More Details](#)



13. ¿A compartido información personal o de trabajo con funcionarios de la BVQ vía telefónica?

[More Details](#)



14. ¿Considera Ud que el sistema de acceso en las puertas de la BVQ es un método seguro y confiable para la restricción de ingreso a personal no autorizado?

[More Details](#)



15. ¿Para ingresar al departamento de tecnología necesita autorización?

[More Details](#)



16. ¿Para acceder al centro de cómputo de la BVQ necesita tener autorización?

[More Details](#)



17. ¿Si tiene autorización para acceder al centro de cómputo de la BVQ debe registrar su acceso en una bitácora de visitas?

[More Details](#)



18. ¿Al ingresar dispositivos de almacenamiento externos en su equipo de trabajo muestra alertas de seguridad para analizar el dispositivo?

[More Details](#)



19. ¿En alguna ocasión ha tenido claves o accesos con privilegios altos para el ingreso a sistemas, aplicaciones o instalar software no autorizado en su equipo?

[More Details](#)



20. ¿Utiliza su computadora portátil institucional fuera de trabajo?

[More Details](#)



21. ¿Cuando se le ha perdido o se ha dañado su credencial de acceso lo ha reportado para su bloqueo ?

[More Details](#)



22. ¿Al olvidar su credencial de acceso a solicitado a su compañero que le preste para movilizarse dentro de la BVQ?

[More Details](#)



23. ¿Para conectarse dispositivos móviles personales a la red WIFI de la BVQ usted debe solicitar autorización?

[More Details](#)



24. ¿Para el uso de aplicaciones que usted utiliza necesita tokens, certificados digitales u otros tipos de autenticación?

[More Details](#)



25. ¿Usted a observado si el público en general o personas externas que visita la BVQ tiene libre acceso dentro de las instalaciones de la BVQ?

[More Details](#)



26. Dentro de las instalaciones de la BVQ ha observado señalética de prevención de accidentes como por ejemplo área de peligro, sistema contra incendios, piso mojado, etc.?

[More Details](#)



27. ¿Cuándo usted tiene prevista una visita o reunión de trabajo le notifica el guardia de PB que lo están buscando para autorizar el acceso?

[More Details](#)



28. ¿Dentro de la BVQ tiene áreas destinadas para realizar reuniones o atender visitas?

[More Details](#)



29. ¿Para trasladar su equipo de trabajo fuera de la instalaciones de la BVQ usted debe tener autorización para hacerlo?

[More Details](#)



30. ¿Conoce usted el reglamento interno de la BVQ?

[More Details](#)



31. ¿Dentro de su contrato o reglamento interno le mencionaron sobre acuerdo de confidencialidad y no divulgación de información de la BVQ?

[More Details](#)



Anexo 3.- Resultados de la encuesta realizada al Analista de Desarrollo TI / Analista de Soporte TI

Encuesta Analista de Desarrollo TI / Analista de soporte TI



5. ¿Para el ingreso al WIFI de un equipo que pertenece a la BVQ se debe tener autorización?

[More Details](#)



6. ¿Para el ingreso al WIFI de un equipo personal de un funcionario de la BVQ se debe tener autorización?

[More Details](#)



7. ¿Para el ingreso al WIFI de un equipo de un visitante a la BVQ se debe tener autorización?

[More Details](#)



8. ¿Existe solo una red WIFI dentro de la BVQ?

[More Details](#)



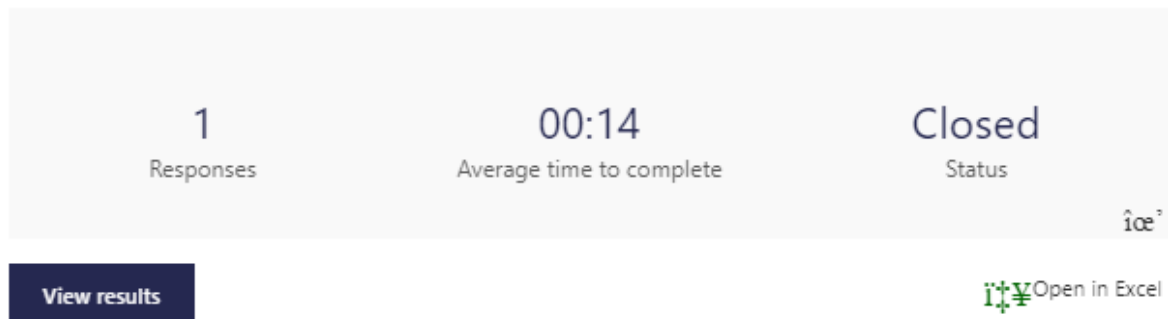
9. ¿Revisa usted la consola de WIFI para revisar que equipos están conectados y de ser el caso bloquear equipos que no están autorizados?

[More Details](#)



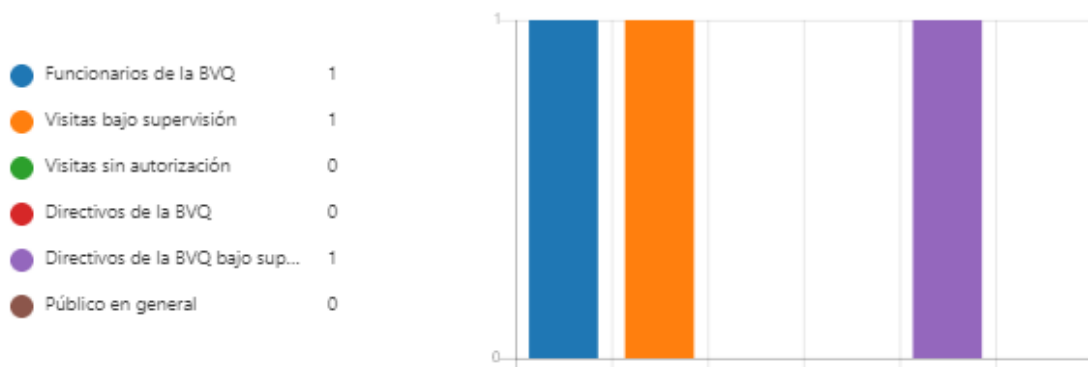
Anexo 4.- Resultados de la encuesta realizada al Analista Senior de Infraestructura

Encuesta Analista Senior de Infraestructura



1. ¿Que personas tiene acceso a la Gerencia de Tecnología?

[More Details](#)



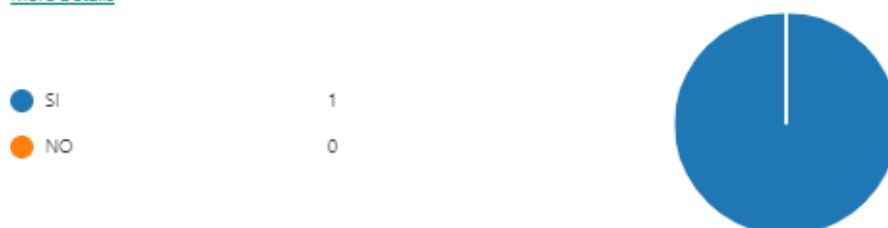
2. ¿Qué personas tienen acceso al centro de cómputo?

[More Details](#)



3. ¿Cuenta con políticas definidas para el acceso a la información?

[More Details](#)



4. ¿Cuenta con políticas de respaldo de información?

[More Details](#)

SI	1
NO	0



5. ¿Cuenta políticas de uso aceptable de internet?

[More Details](#)

SI	1
NO	0



6. ¿Para comunicaciones confiables utilizan métodos de encriptación?

[More Details](#)

SI	1
NO	0



7. ¿Qué tipo de servicios de comunicaciones tiene la BVQ?

[More Details](#)

Telefonía analógica	1
Telefonía digital	1
Telefonía IP	0



8. ¿Cuentan con un manual de Plan de Continuidad del Negocio?

[More Details](#)



9. ¿Cuenta con alertas en el caso de fallo de aplicaciones o sistemas?

[More Details](#)



10. ¿Dentro de la institución tienen conformado el Comité de Tecnología?

[More Details](#)



Anexo 5.- Recolección de datos e interpretación de resultados de la consola de WIFI de la BVQ

WIRELESS CLIENTS (PER RADIO TYPE)



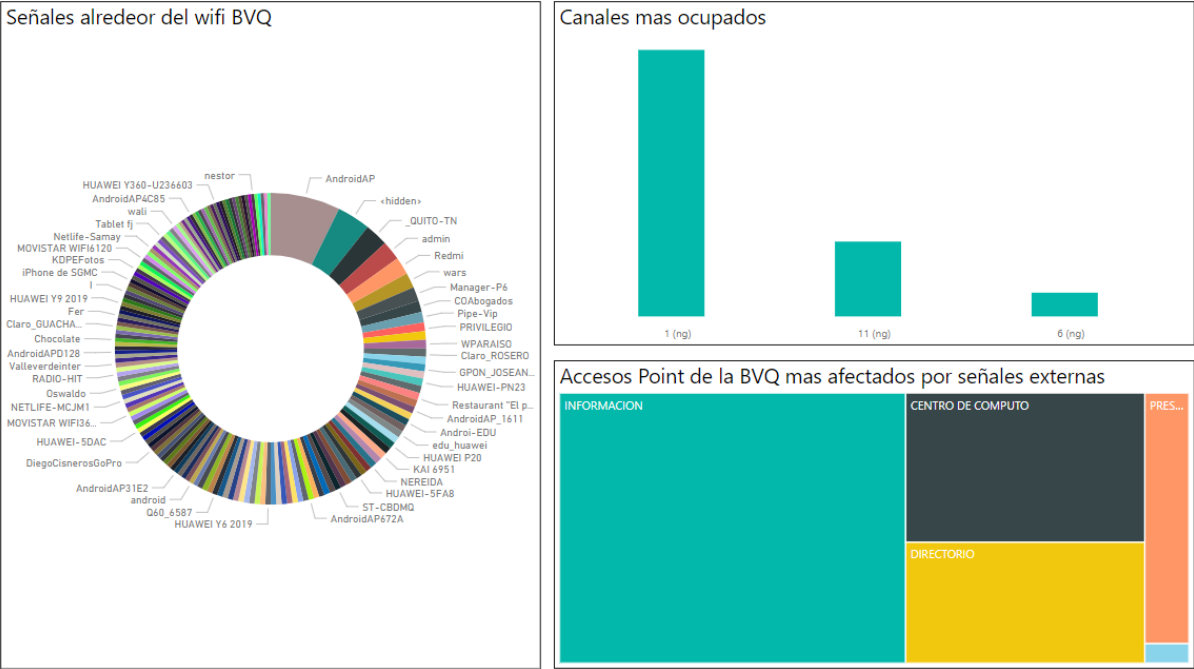
Número de frecuencias de trabajo.

	NAME/SSID	BSSID	CHANNEL	BW [MHz]	SECURITY	MANUFACTURER	LOCATION	SIGNAL ↓
☐ 3	_QUITO-TN	a4:6c:2a:d4:05:00	1 (ng)	20	Open	Cisco	Near C... Near II... Near P...	45% (-72 dBm) 32% (-77 dBm) 22% (-81 dBm)
1	COAbogados	68:7f:74:d0:df:67	11 (ng)	40	WPA/WPA2 (TKIP/AES/CCMP)	Cisco-Li	Near C...	42% (-73 dBm)
1	<hidden>	84:78:ac:96:f2:e5	1 (ng)	20	WPA/WPA2 (AES/CCMP)	Cisco	Near I...	35% (-76 dBm)
☐ 2	WPARAISO	84:78:ac:96:f2:e0	1 (ng)	20	WPA2 (AES/CCMP)	Cisco	Near I... Near P...	35% (-76 dBm) 5.0% (-88 dBm)
☐ 3	Wifi-Casa	48:57:02:62:24:d0	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	Near F... Near I... Near D...	32% (-77 dBm) 25% (-80 dBm) 12% (-85 dBm)
☐ 2	<hidden>	84:78:ac:96:f2:e4	1 (ng)	20	WEP	Cisco	Near I... Near F...	32% (-77 dBm) 0% (-90 dBm)
1	ECUADOR_DIGITAL	7c:57:3c:6d:38:e0	1 (ng)	20	Open		Near I...	30% (-78 dBm)
1	Manager-P6	26:18:d6:cf:e2:2e	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	25% (-80 dBm)
1	Tvcable_CEMAA	c4:04:15:8f:2c:ac	6 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	Netgear	Near f...	25% (-80 dBm)
1	Pipe-Vip	76:d9:e7:cd:d1:88	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	22% (-81 dBm)
1	HUAWEI Y5 2019	46:59:e3:0c:d1:87	1 (ng)	20	WPA2 (AES/CCMP)		Near C...	20% (-82 dBm)
☐ 4	INGCAJAS	d0:65:cad7:bd:a8	11 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	HuaweiTe	Near C... Near I... Near D... Near F...	20% (-82 dBm) 20% (-82 dBm) 5.0% (-88 dBm) 0% (-90 dBm)
1	_QUITO-TN	a4:6c:2a:d4:1b:a0	11 (ng)	20	Open	Cisco	Near C...	20% (-82 dBm)
1	Manager-P6	66:d9:e7:cd:d1:88	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	20% (-82 dBm)
1	admin	56:d9:e7:cd:d1:88	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	20% (-82 dBm)
1	wars	06:18:d6:cf:e2:2e	1 (ng)	20	WPA/WPA2 (AES/CCMP)	Ubiquiti	Near I...	20% (-82 dBm)
1	admin	56:d9:e7:59:64:86	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	20% (-82 dBm)
1	CJ-FUNCIONARIOS	c0:7b:bc:76:e3:50	1 (ng)	20	WPA/WPA2 (AES/CCMP)	Cisco	Near I...	20% (-82 dBm)
1	Pipe-Vip	36:18:d6:cf:e2:2e	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	Near I...	20% (-82 dBm)
☐ 3	Tvcable-Luis_2GEXT	a0:04:60:88:79:cd	1 (ng)	20	WPA2 (AES/CCMP)	Netgear	Near I... Near D... Near P...	20% (-82 dBm) 7.4% (-87 dBm) 0% (-90 dBm)

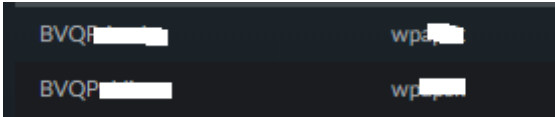
Datos de señales alrededor de equipos Wifi BVQ

	BSSID	MAC	Canal	Frecuencia BW	Seguridad	Marca	Afectación	Porcentaje Señal	Señal	Unidad
1	_QUITO-TN	a46c2ad40500	1 (ng)	20	Open	Cisco	DIRECTORIO	47%	-71	d8m
2	COAbogados	687f74d0df67	11 (ng)	40	WPA/WPA2 (TKIP/AES/CCMP)	Cisco-Li	CENTRO DE COMPUTO	42%	-73	d8m
4	PRIVILEGIO	c05627197b82	6 (ng)	40	WPA2 (AES/CCMP)	Belkinln	PRESIDENCIA	32%	-77	d8m
5	chidden	8478ac96f2e4	1 (ng)	20	WEP	Cisco	INFORMACION	32%	-77	d8m
6	WPARAISO	8478ac96f2e0	1 (ng)	20	WPA2 (AES/CCMP)	Cisco	INFORMACION	32%	-77	d8m
7	Wifi-Casa	4857026224d0	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	PISO 10	32%	-77	d8m
8	Redmi	1cccd6818833	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	30%	-78	d8m
9	Claro_ROSERO	3cb74b794c82	1 (ng)	20	WPA/WPA2 (AES/CCMP)		INFORMACION	30%	-78	d8m
10	chidden	8478ac96f2e5	1 (ng)	20	WPA/WPA2 (AES/CCMP)	Cisco	INFORMACION	30%	-78	d8m
11	Restaurant "El primo"	6689f18076d5	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	27%	-79	d8m
12	NETLIFE-PPPJ	1caecba8a33c	6 (ng)	20	WPA2 (TKIP/AES/CCMP)		PRESIDENCIA	27%	-79	d8m
13	HUAWEI Mate 20 lite	902bd2a48bd7	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	27%	-79	d8m
14	HUAWEI-PN23	b0e5ed6d1714	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	27%	-79	d8m
15	GPON_JOSEANTONI	0067622515a8	1 (ng)	20	WPA/WPA2 (AES/CCMP)		INFORMACION	27%	-79	d8m
16	ECUADOR_DIGITAL	7c573c6d38e0	1 (ng)	20	Open		INFORMACION	27%	-79	d8m
17	Huawei	3cfa4371e6da	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	25%	-80	d8m
18	MOVISTAR wif7981	92633b0e1df95	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	25%	-80	d8m
19	KAI 6951	b6ae2b21795e	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	25%	-80	d8m
20	AndroidAPB386	06ba8d31b386	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	25%	-80	d8m
21	edu_huawei	88f56ea59dce	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	25%	-80	d8m
22	NEREIDA	009a0cd467a18	1 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	HuaweiTe	DIRECTORIO	25%	-80	d8m
23	AndroidAP_1611	20326c9a806c	1 (ng)	20	Open		INFORMACION	25%	-80	d8m
24	Claro_ALHAMOUD00	6018715cf8d0	1 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	AriseGro	INFORMACION	25%	-80	d8m
25	HUAWEI P20	347916425f6e	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	25%	-80	d8m
26	Androi-EDU	306a85c64149	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	INFORMACION	25%	-80	d8m
27	INGCAJAS	d065cad7bd8a	11 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	HuaweiTe	CENTRO DE COMPUTO	25%	-80	d8m
28	ST-CBDMQ	30eb1f10b2c5	11 (ng)	20	WPA2 (AES/CCMP)	SkyLabMx	CENTRO DE COMPUTO	22%	-81	d8m
29	HUAWEI Y7	0c8fffe231f9	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	22%	-81	d8m
30	HUAWEI-5FA8	b08900af5fa8	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	22%	-81	d8m
31	AndroidAP	b8bcb1b13aef	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	22%	-81	d8m
32	MOVISTAR wif13095	9ce0635149c4	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	DIRECTORIO	22%	-81	d8m
33	NETLIFE-MIMI	ccbbfe3708a8	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	22%	-81	d8m
34	HUAWEI-93A6	a057e32583a6	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	22%	-81	d8m
35	SYNC_XT9H995	0026b489eed4	1 (ng)	20	WPA2 (TKIP/AES/CCMP)	FordMoto	INFORMACION	22%	-81	d8m
36	AndroidAP7B0C	ce2119667b0c	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	22%	-81	d8m
37	_QUITO-TN	a46c2ad41ba0	11 (ng)	20	Open	Cisco	CENTRO DE COMPUTO	22%	-81	d8m
38	wars	46d9e7cdd188	1 (ng)	20	WPA/WPA2 (AES/CCMP)	Ubiquiti	INFORMACION	22%	-81	d8m
39	Pipe-Vip	3618d6cfe22e	1 (ng)	20	WPA2 (AES/CCMP)	Ubiquiti	INFORMACION	22%	-81	d8m
40	Tucable-Luis_2GEXT	a004608873cd	1 (ng)	20	WPA2 (AES/CCMP)	Netgear	INFORMACION	22%	-81	d8m
41	solex	04b429165087	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	20%	-82	d8m
163	wars	46d9e7cdd1b7	11 (ng)	20	WPA/WPA2 (AES/CCMP)	Ubiquiti	CENTRO DE COMPUTO	15%	-84	d8m
164	INTERNET CNT	0026b682eb8a	11 (ng)	20	WPA (AES/CCMP)	AskeyCom	CENTRO DE COMPUTO	15%	-84	d8m
165	CBDMQ	8c25050b35f2	6 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	PRESIDENCIA	12%	-85	d8m
166	MW4INF_2881	942790072881	1 (ng)	20	WPA2 (TKIP/AES/CCMP)		INFORMACION	12%	-85	d8m
167	AndroidAP4C85	d611a3364c85	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	12%	-85	d8m
168	AndroidAPDFE4	b26fe035fde4	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
169	AndroidAP	26920e27b88a	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	12%	-85	d8m
170	AndroidAP	888322aeb4ec	11 (ng)	20	WPA2 (AES/CCMP)	SamsungE	CENTRO DE COMPUTO	12%	-85	d8m
171	T_Mercure_Alameda_	f29fc02a0af0d	1 (ng)	20	Open	Ubiquiti	INFORMACION	12%	-85	d8m
172	fernanda2	0ad46aeaf6fe	1 (ng)	20	WPA (TKIP/AES/CCMP)		INFORMACION	12%	-85	d8m
173	Xperia XAI Ultra_7oad	d6389c5e6ea2	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	12%	-85	d8m
174	Landeaus	26181d9ce387	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	12%	-85	d8m
175	CNT-GAMBOA	d07ab55c3728	11 (ng)	20	WPA/WPA2 (AES/CCMP)	HuaweiTe	CENTRO DE COMPUTO	12%	-85	d8m
176	HUAWEI Y360-U23680	d265ca0a3d6a	6 (ng)	20	WPA2 (AES/CCMP)		PRESIDENCIA	12%	-85	d8m
177	WSENECYT	74a02145a300	1 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	Cisco	INFORMACION	12%	-85	d8m
178	AndroidAP2471	a0a4d0fb2471	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	INFORMACION	12%	-85	d8m
179	ambaseg matriz	fc0a21ad1e94	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
180	AndroidAP	24dbedac3901	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	INFORMACION	12%	-85	d8m
181	HUAWEI-59FC	b08900af59fc	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	12%	-85	d8m
182	JawgTm	804e705e1ddb	11 (ng)	20	WPA2 (AES/CCMP)	SamsungE	CENTRO DE COMPUTO	12%	-85	d8m
183	AndroidAPBEF4	b26fe018be44	6 (ng)	20	WPA2 (AES/CCMP)		PRESIDENCIA	12%	-85	d8m
184	HUAWEI-50E4	b08900af50e4	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	INFORMACION	12%	-85	d8m
185	HUAWEI-5546	8c25050b5546	1 (ng)	20	WPA2 (AES/CCMP)		DIRECTORIO	12%	-85	d8m
186	AndroidAP	48c07963c6507	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	INFORMACION	12%	-85	d8m
187	nestor	68e7c266a46b	6 (ng)	20	WPA2 (AES/CCMP)	SamsungE	PRESIDENCIA	12%	-85	d8m
188	HUAWEI Mate 9	021a1f183076	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	12%	-85	d8m
189	Q6_1205	d4c94b1fdb7e	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	12%	-85	d8m
190	Macho Alfa	ec107b68d0ce	11 (ng)	20	WPA2 (AES/CCMP)	SamsungE	CENTRO DE COMPUTO	12%	-85	d8m
191	MOVISTAR wif9592	92633b0e09b7	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
192	AndroidAP	3e0518842312	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
193	AMBULANCIA NOVA	a407b6b86671	1 (ng)	20	WPA2 (AES/CCMP)	SamsungE	DIRECTORIO	12%	-85	d8m
194	NETLIFE-AMBIENTAL	10bef5d953d8	1 (ng)	20	WPA/WPA2 (TKIP/AES/CCMP)	D-Linkln	INFORMACION	12%	-85	d8m
195	SYNC_XTAA7F9w	0026b48f8f84	1 (ng)	20	WPA2 (TKIP/AES/CCMP)		INFORMACION	12%	-85	d8m
196	JF De la Torre	e0dc0ff265674	1 (ng)	20	WPA2 (AES/CCMP)		INFORMACION	12%	-85	d8m
197	dayana	58c05cbb0ce017	11 (ng)	20	WPA2 (AES/CCMP)	SamsungE	CENTRO DE COMPUTO	12%	-85	d8m
198	AndroidAP389E	da5575c5389e	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
199	AndroidAP_1773	ecaa250915f5	11 (ng)	20	WPA2 (AES/CCMP)		CENTRO DE COMPUTO	12%	-85	d8m
200	MOVISTAR wif7001	1496e5c6afb1	1 (ng)	20	Open	SamsungE	INFORMACION	12%	-85	d8m
201	HUAWEI-95DA	a057e32585da	1 (ng)	20	WPA2 (AES/CCMP)	HuaweiTe	DIRECTORIO	12%	-85	d8m

Importación de datos a EXCEL para Dashboard Power BI



Dashborad Power BI – Equipo wifi afectado



Número de SSID de la BVQ

Mode WP Encryption

	DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTIONS
	CM	192.168.1.1	CONNECTED	CM	3.0.0.0	125d 1h 22m 48s	LOCATE RESTART
	DI	192.168.1.2	CONNECTED	DI	3.0.0.0	35d 5h 13m 1s	LOCATE RESTART
	Il	192.168.1.3	CONNECTED	Il	3.0.0.0	35d 5h 12m 54s	LOCATE RESTART
	PL	192.168.1.4	CONNECTED	PL	3.0.0.0	35d 5h 13m 19s	LOCATE RESTART
	PL	192.168.1.5	CONNECTED	PL	3.0.0.0	65d 15h 55m 36s	LOCATE RESTART

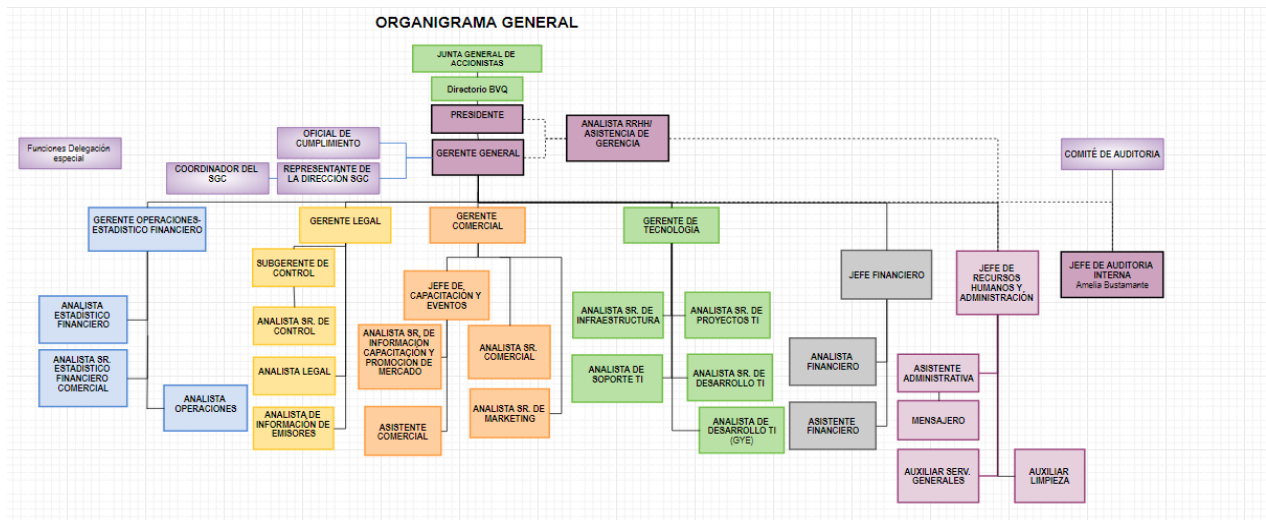
Consola de actualización de firmware AP - BVQ

EVENT	TIME
Admin min [redacted] log in from 1[redacted]	1:28 pm 0[redacted]
Admin [redacted] log in from [redacted]	12:45 pm 04[redacted]
Admin [redacted] log in from 1[redacted]	8:58 pm 0[redacted]
[redacted] was encountering some interference on channel 6	1:18 pm 0[redacted]
[redacted] was encountering some interference on channel 6	11:07 am 03[redacted]
[redacted] was encountering some interference on channel 6	3:54 pm 0[redacted]
Admin Admin [redacted] in log in from 1[redacted]	2:04 pm 03[redacted]
[redacted] was encountering some interference on channel 6	4:10 pm 03[redacted]
[redacted] was encountering some interference on channel 6	11:11 am [redacted]
GABY-PC has become unauthorized	5:25 pm [redacted]
[redacted] was encountering some interference on channel 6	2:28 pm [redacted]
[redacted] was encountering some interference on channel 11	1:05 pm [redacted]
GABY-PC is authorized by Admin bvqadmin for 480 minutes	5:22 pm [redacted]
GABY-PC has become unauthorized	5:20 pm [redacted]
[redacted] was used by GABY-PC	4:50 pm [redacted]
Admin [redacted] in log in from [redacted]	3:20 pm [redacted]
[redacted] was encountering some interference on channel 6	10:25 am [redacted]
LAPTOP-CARLOS-INTELEC is blocked by Admin [redacted]	11:40 am [redacted]
[redacted] was encountering some interference on channel 1	11:27 am [redacted]
[redacted] was used by LAPTOP-CARLOS-INTELEC	11:11 am [redacted]
Admin [redacted] in log in from [redacted]	11:08 am [redacted]
[redacted] was encountering some interference on channel 1	1:44 pm [redacted]
[redacted] was encountering some interference on channel 1	1:44 pm [redacted]
[redacted] was encountering some interference on channel 6	4:06 pm [redacted]

Consola de monitoreo de logs WIFI - BVQ

	NAME	IP ADDRESS	CONNECTION	AP/PORT	UPTIME	ACTIONS
	[redacted]	19[redacted]	BVQ[redacted]	[redacted]	1[redacted]	BLOCK RECONNECT
	[redacted]	19[redacted]	BVQ[redacted]	[redacted]	1[redacted]	BLOCK RECONNECT
	[redacted]	19[redacted]	BVQ[redacted]	[redacted]	1[redacted]	BLOCK RECONNECT
	[redacted]	19[redacted]	BVQ[redacted]	[redacted]	1[redacted]	BLOCK RECONNECT
	[redacted]	19[redacted]	BVQ[redacted]	[redacted]	1[redacted]	BLOCK RECONNECT

Consola de monitoreo de clientes autorizados dentro de la red WIFI



Organigrama de la institución - BVQ

Tarifación

Buscar: Usuarios En nmc

Donde: Extensión Empezar por

Tarifación **Alarmas**

Meta empresa : nmc

Fecha de comienzo	Núm llamado	Duración	Extensión	Coste operador directo	Coste operador indirecto	Coste RDSI
24/03/20 11:39:07	0992556641	0:02:24	573	0,48	0,0	0,0
24/03/20 10:47:49	0999559835	0:02:22	531	0,71	0,0	0,0
24/03/20 10:47:49	023319518	0:02:22	531	0,0	0,0	0,0
24/03/20 10:42:41	0988181723	0:00:07	530	0,04	0,0	0,0
24/03/20 10:39:01	022999000	0:02:21	532	0,0	0,0	0,0
24/03/20 10:39:01	0982432807	0:02:21	532	1,18	0,0	0,0
24/03/20 10:34:42	0982432807	0:00:00	532	0,0	0,0	0,0
24/03/20 10:34:39	022999000	0:00:00	532	0,0	0,0	0,0
24/03/20 10:32:35	0982432807	0:00:00	532	0,0	0,0	0,0

10 justificantes (sobre 10 requeridos)

Propiedades Justificantes Máscaras Costes Monitorización

[11:52:16] > Lanzar la aplicación Tarifación.

Registro de llamadas telefónicas central PBX

Anexo 6.- Herramientas de Kali Linux utilizadas para este proyecto.

LEVANTAMIENTO DE INFORMACIÓN

Nombre de cliente:	Bolsa de Valores de Quito
Nombre de contacto	Marcelo Aguilar - Gerente de Tecnología
Preparado por:	Henry Daniel Calero Suntasig - Investigador
Teléfono:	23988500
Correo electrónico:	marceloaguilar@bolsadequito.com

Número de direcciones IP - Internas			
Item	Dispositivos	Número de direcciones	Direcciones
1	Directorio Activo Principal	1	192
2	Directorio Activo Secundario	1	192
3	Base de Datos Principal	1	192
4	Base de Datos Secundario	1	192
5	Capa de Servicios Principal	1	192
6	Capa de Servicios Secundario	1	192
7	Servidor de VPNs	1	192
8	Servidor de consultas externas	1	192
9	Switches LAN	8	192.168.1.1 - 192.168.1.8 192.168.2.1 - 192.168.2.8
10	Routers de red WAN	2	Proveedor externo
11	Firewall IPS / IDS	2	Proveedor externo
12	Antivirus	1	Nube
13	Access Point	5	192.168.1.1 - 192.168.1.5 192.168.2.1 - 192.168.2.5
14	Estaciones de trabajo	1	Segmento 192.1
15	Impresoras	3	192.168.1.1 - 192.168.1.3
17	Biométrico	1	192.168.1.1
Número de direcciones IP - Públicas			
Cant	Dispositivos	Número de direcciones	IP Pública
1	Salida a internet	1	157.140.1.1
2	Capa de servicios (bvqservicesot.com)	1	157.140.1.1
3	Servidor de VPNs	1	157.140.1.1
4	Servidor de consultas externas	1	157.140.1.1
5	intrabvq.com	1	N/A
6	iegc.ec	1	N/A
4	bolsadequito.com	1	157.140.1.1
5	sicav.ec	1	N/A

1.- La infraestructura tecnológica interna se encuentra en las instalaciones de la empresa?

Si	☒	No	☐
		Territorio Nacional	☒
		Territorio Internacional	☒

2.- Mantiene más de un DataCenter?

Si	☐	No	☒
Cuántos?			

3.- Se cuenta con enlaces dedicados para interconexión de sucursales o DataCenter?

Si	☒	No	☐
----	-------------------------------------	----	--------------------------

Levantamiento de información red BVQ

```

root@kali:~# nmap -sV 19[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted] ECT
Nmap scan report for [redacted]
Host is up (0.014s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE      VERSION
38[redacted] p    open  ld[redacted]
40[redacted] p    open  kp[redacted]
63[redacted] p    open  ld[redacted]
32[redacted] cp   open  gl[redacted]  AP?
32[redacted] cp   open  gl[redacted]  APssl?
59[redacted] cp   open  fr[redacted]
49[redacted] tcp  open  un[redacted]
49[redacted] tcp  open  un[redacted]
49[redacted] tcp  open  un[redacted]
49[redacted] tcp  open  unknown

```

Escaneo Directorio Activo

```

root@kali:~# nmap -sV 19[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted] ECT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 1[redacted]
Host is up (2.3s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
8[redacted]  open  h[redacted]  Mic
1[redacted]  open  m[redacted]  Mic
4[redacted]  open  n[redacted]
5[redacted]  filtered s[redacted]
1[redacted]  open  m[redacted]  Mic
2[redacted]  open  h[redacted]  Com
2[redacted]  open  c[redacted]
2[redacted]  open  m[redacted]
3[redacted]  open  m[redacted]
4[redacted]  open  u[redacted]
4[redacted]  open  u[redacted]
4[redacted]  open  u[redacted]
4[redacted]  open  u[redacted]

```

Escaneo Base de Datos

```

@kali:~# nmap -sV 19[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted] to hear.
: Host seems down. If it is really up, but blocking our ping probes, try -Pn
done: 1 IP address (0 hosts up) scanned in 3.19 seconds
@kali:~#

```

Escaneo Capa de Servicios

```

root@kali:~# nmap -sV 15[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted]
Nmap scan report for 1[redacted]
Host is up (2.1s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
15[redacted] open  [redacted] S[redacted]R)
4[redacted] open  [redacted] S[redacted]R)
5[redacted] filtered s[redacted]
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.61 seconds

```

Escaneo Servidor VPNs

```

root@kali:~# nmap -sV 15[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted]
Nmap scan report for host-1[redacted]ecua.net.ec ([redacted])
Host is up (0.0034s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
[redacted] open [redacted]
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.43 seconds

```

Escaneo Servidor de consultas externas

```

root@kali:~# nmap -sV 157[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted]
Nmap scan report for host-15[redacted].ecua.net.ec (1[redacted])
Host is up (0.047s latency).
All 1000 scanned ports on host-15[redacted].ecua.net.ec (15[redacted]3) are filtered
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.28 seconds
root@kali:~#

```

Escaneo IP salida a internet BVQ

```

root@kali:~# nmap -sV 157[redacted]
Starting Nmap 6.46 ( http://nmap.org ) at [redacted]
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.25 seconds

```

Escaneo IP servidor VPN expuesto con IP publica

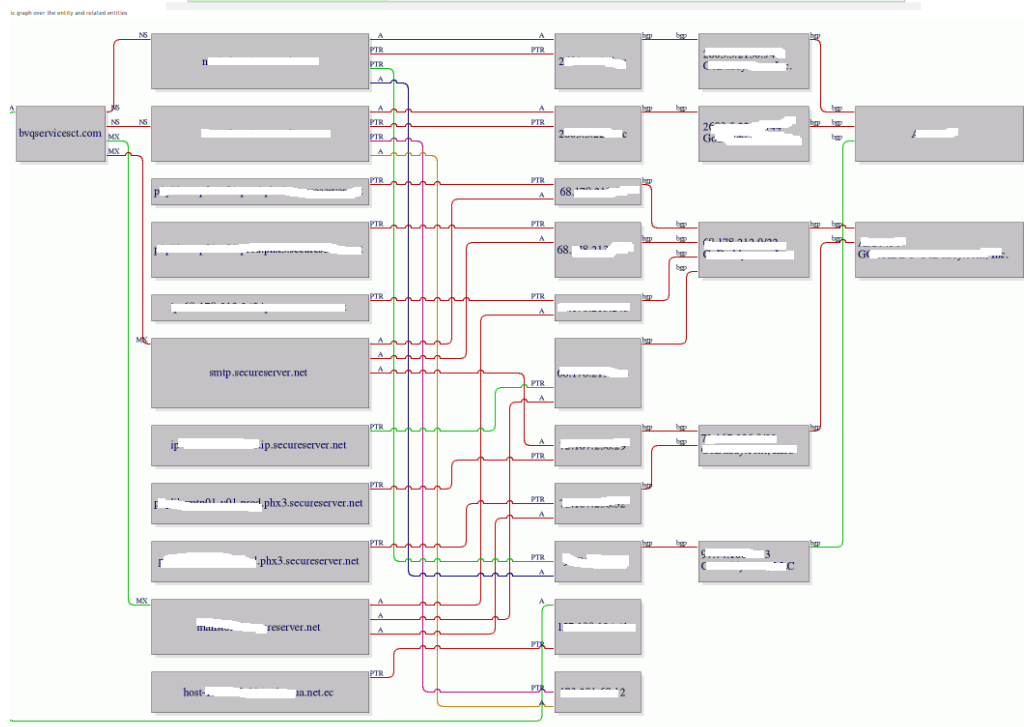
```

root@kali:/# nmap -sV 157.140.12.11
Starting Nmap 6.46 ( http://nmap.org ) a
Nmap scan report for host-1.157.140.12.11.ecua.net.ec (157.140.12.11)
Host is up (0.0095s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6p1 Ubuntu
80/tcp    open  http         Apache/2.4.6-2ubuntu
443/tcp   open  https        Apache/2.4.6-2ubuntu
8080/tcp   open  http         Apache/2.4.6-2ubuntu
SMB/445   info: CIFS
Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 77.15 seconds

```

bvqservicesct.com quick info

General	
FQDN	bvqservicesct.com
Host Name	
Domain Name	bvqservicesct.com
Registry	com
TLD	com
DNS	
IP numbers	157.140.12.11
Name servers	ns1.dnscontrol.com ns2.dnscontrol.com
Mail servers	mailstore.secureserver.net smtp.secureserver.net



Escaneo Capa de Servicios desde IP pública

```

root@kali:~# nslookup
> intrabvq.com
Server:
Address:

Non-authoritative answer:
Name: intrabvq.com
Address: 5
root@kali:~# nmap 5
Starting Nmap 6.46 ( http://nmap.org ) at
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds

```

intrabvq.com quick info

General	
FQDN	intrabvq.com
Host Name	
Domain Name	intrabvq.com
Registry	com
TLD	com
DNS	
IP numbers	50.97.150.22
Name servers	ns01.intrabvq.com ns02.intrabvq.com
Mail servers	mail.intrabvq.com

Escaneo dominio1

```

root@kali:~# nslookup
> bolsadequito.com
Server:
Address:

Non-authoritative answer:
Name: bolsadequito.com
Address: 15
> ^Croot@kali:~# nmap -sV 1
Starting Nmap 6.46 ( http://nmap.org )
Nmap scan report for bolsadequito.com (1)
Host is up (0.010s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu
80/tcp    open  httpd    Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind  rpcbind
135/tcp   open  msrpc    Microsoft RPC
139/tcp   open  smb      SMB 1.0.0
445/tcp   open  smb      SMB 1.0.0
8080/tcp  open  httpd    Apache/2.4.18 (Ubuntu)
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 212.20 seconds

```

QUICK INFO

Quick summary of the host name

www.bolsadequito.com quick info

General	
FQDN	www.bolsadequito.com
Host Name	www
Domain Name	bolsadequito.com
Registry	com
TLD	com
DNS	
IP numbers	157.140.147.11
Domain DNS	
Name servers	ns1.bolsadequito.com ns2.bolsadequito.com ns3.bolsadequito.com
Mail servers	mail.bolsadequito.com
IP Numbers	157.140.147.11

Escaneo dominio2

```

root@kali:~# nslookup
> sicav.ec
Server:      192.168.1.1
Address:     192.168.1.1

Non-authoritative answer:
Name:   sicav.ec
Address: 192.168.1.1

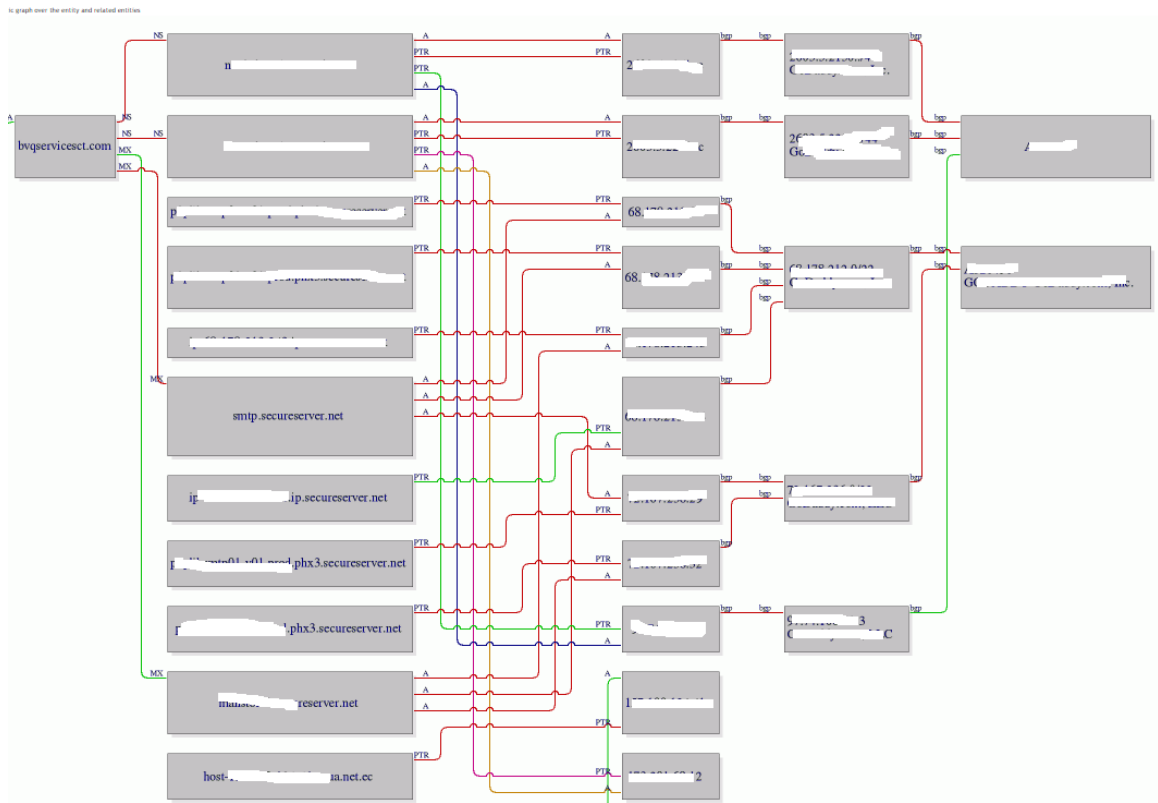
root@kali:~# nmap -sV 192.168.1.1

Starting Nmap 6.46 ( http://nmap.org ) at 2017-10-14 14:11:11
Nmap scan report for 192.168.1.1 (192.168.1.1)
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.1.1 (192.168.1.1) are filtered
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.43 seconds

```

sicav.ec quick info

General	
FQDN	sicav.ec
Host Name	
Domain Name	sicav.ec
Registry	ec
TLD	ec



Escaneo dominio4

*Ethernet 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
2584	36.522069	192.168.1.10	192.168.1.10	TCP	54	3389 → 59469 [ACK] Seq=1304 Ack=33157 Win=63022 Len=0
2585	36.538012	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2586	36.540811	192.168.1.10	192.168.1.10	UDP	60	56885 → 3389 Len=12
2587	36.568873	192.168.1.10	192.168.1.10	ARP	60	Who has 192.168.1.10? Tell 192.168.1.10
2588	36.568895	192.168.1.10	192.168.1.10	ARP	60	Who has 192.168.1.10? Tell 192.168.1.10
2589	36.582122	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2590	36.582148	192.168.1.10	192.168.1.10	TCP	54	3389 → 59469 [ACK] Seq=1304 Ack=33359 Win=62820 Len=0
2591	36.582297	192.168.1.10	192.168.1.10	ICMP	82	Redirect (Redirect for host)
2592	36.589961	192.168.1.10	192.168.1.10	TLSv1.2	139	Application Data
2593	36.606264	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2594	36.606287	192.168.1.10	192.168.1.10	TCP	54	3389 → 59469 [ACK] Seq=1304 Ack=33545 Win=64000 Len=0
2595	36.618263	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2596	36.633863	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2597	36.633884	192.168.1.10	192.168.1.10	TCP	54	3389 → 59469 [ACK] Seq=1304 Ack=33747 Win=63798 Len=0
2598	36.646392	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2599	36.662246	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2600	36.662269	192.168.1.10	192.168.1.10	TCP	54	3389 → 59469 [ACK] Seq=1304 Ack=33949 Win=63596 Len=0
2601	36.682215	192.168.1.10	192.168.1.10	TLSv1.2	155	Application Data
2602	36.707817	192.168.1.10	192.168.1.10	UDP	179	3389 → 56885 Len=137
2603	36.708036	192.168.1.10	192.168.1.33	ICMP	207	Redirect (Redirect for host)

Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{0359F2AE-E8D8-44A1-A86D-750025BEAA66}, id 0

Ethernet II, Src: Micro-St_85:71:a9 (6c:62:6d:85:71:a9), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

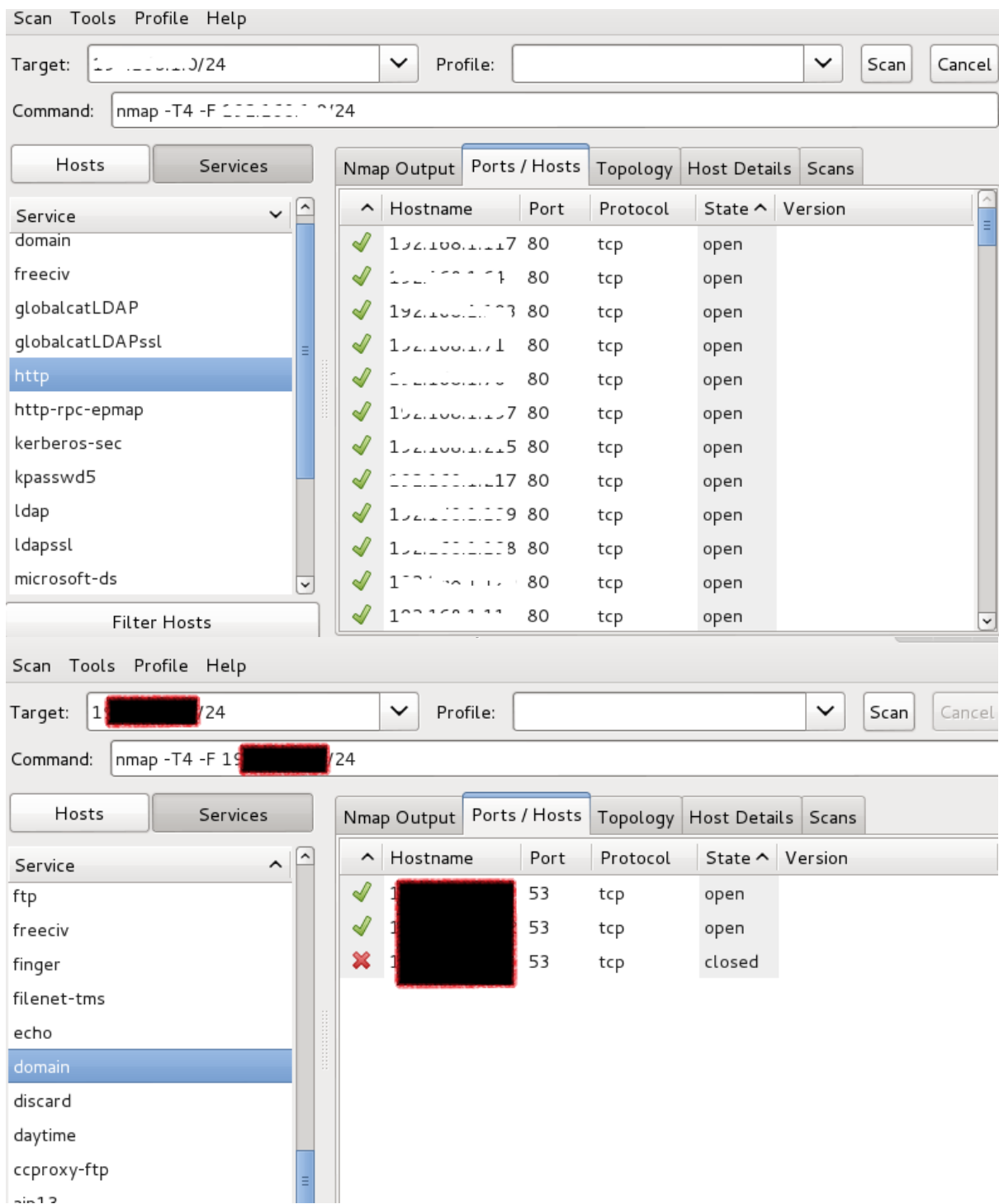
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 56885, Dst Port: 1000

```

0000  01 00 5e 7f ff fa 6c 62 6d 85 71 a9 08 00 45 00  ...A...
0010  00 ca 58 a2 00 00 01 11 ae bb c0 a8 01 23 ef ff  ...X...
0020  ff fa d8 15 07 6c 00 b6 6d 81 4d 2d 53 45 41 52  ...
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH *
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST:
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssd
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  -HX:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial
0090  2d 6f 72 6f 3a 73 65 72 76 69 63 65 3a 64 69 61  -org
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  l:1
00b0  20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 38  Goo
00c0  30 2e 30 2e 33 39 38 37 2e 31 33 32 20 57 69 6e  0.0.
00d0  64 6f 77 73 0d 0a 0d 0a  ...dows
  
```

Captura de tráfico ICMP



Puertos habilitados dentro de la red 192.x.x.x /x

RV: Nueva página de la BVQ



Hector Almeida

Para Marcelo Aguilar; Daniel Calero

Respondió a este mensaje el 02/12/2019 10:23.
Mensaje enviado con importancia Alta.

Responder

Responder a todos

Reenviar



lu. 02/12/2019 9:1

Me lleo esto

Saludos Cordiales

H

GEREN

Av. Amazonas N21-252 y Carrión,
Edificio Londres Piso 8
T: +5932 3988 500 W: www.bolsadequito.com

BVQ
BOLSA
DE VALORES
DE QUITO



MÁS INVERSIÓN
MÁS FINANCIAMIENTO
PARA EL ECUADOR

¡[Suscríbete](#) a nuestro Boletín Semanal y entérate de todo lo que pasa en el mercado de valores ecuatoriano ahora!

¡Síguenos en Facebook! ¡Da click [Aquí!](#)

RV: Nueva página de la BVQ



Sebastian Herrera

Para Daniel Calero

Responder

Responder a todos

Reenviar



ju. 02/01/2020 12:57

Hola Dani,

Me lleo este correo.

Cualquier requerimiento que necesiten por favor dirigirlo al siguiente correo: operacionesbvq@bolsadequito.com.

Saludos Cordiales

Sebastian H
ANALIS

Av. Amazonas N21-252 y Carrión,
Edificio Londres Piso 8
T: +5932 3988 500 W: www.bolsadequito.com

BVQ
BOLSA
DE VALORES
DE QUITO



MÁS INVERSIÓN
MÁS FINANCIAMIENTO
PARA EL ECUADOR

¡[Suscríbete](#) a nuestro Boletín Semanal y entérate de todo lo que pasa en el mercado de valores ecuatoriano ahora!

¡Síguenos en Facebook! ¡Da click [Aquí!](#)

El personal no ingresa a páginas desconocidas; notifican inmediatamente al departamento de Tecnología

Account Policies/Password Policy

Policy

Enforce password history
Maximum password age
Minimum password age
Minimum password length
Password must meet complexity requirements
Store passwords using reversible encryption

Setting

passwords remembered
days
days
characters
Enabled
Disabled

Política de contraseñas para accesos

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

Bloqueo de accesos al ingresar contraseñas incorrectas

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Auditoría de accesos habilitadas

Nombre	Fecha de modificación	Tipo	Tamaño
[Redacted]	18/08/2023 12:53	Comprimido	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	16/08/2023 17:13	Archivo	1 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
[Redacted]	18/08/2023 13:31	Comprimido	5 KB
[Redacted]	18/08/2023 13:30	Archivo	2 KB
cliente10.key	18/08/2023 13:30	Archivo KEY	2 KB

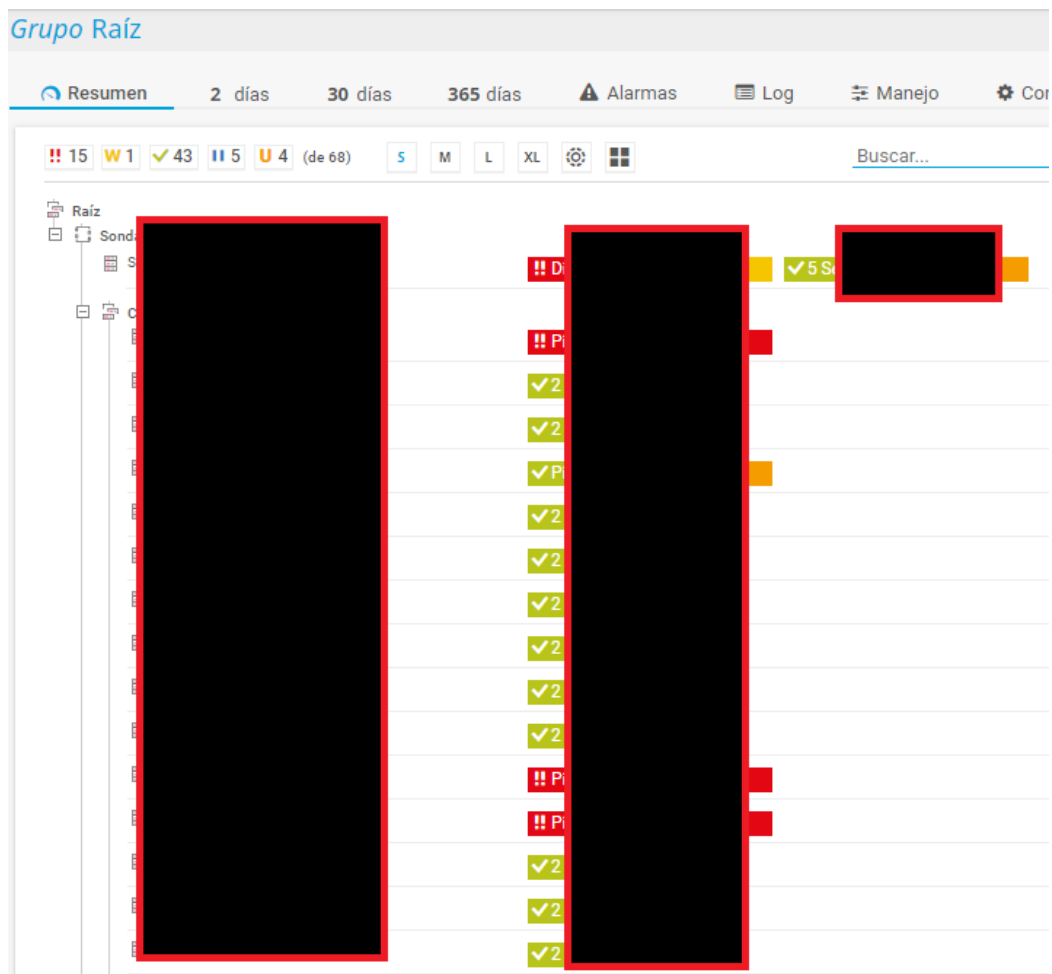
Para autenticarse por VPN se utilizan certificados

dt	31/05/2019	04	Archivo BAK	
dt	30/05/2019	04	Archivo BAK	
dt	29/05/2019	04	Archivo BAK	
dt	28/05/2019	05	Archivo BAK	
dt	27/05/2019	04	Archivo BAK	
dt	24/05/2019	04	Archivo BAK	
dt	23/05/2019	04	Archivo BAK	
dt	22/05/2019	51	Archivo BAK	
dt	21/05/2019	04	Archivo BAK	
dt	20/05/2019	04	Archivo BAK	
dt	17/05/2019	04	Archivo BAK	
dt	16/05/2019	04	Archivo BAK	
dt	15/05/2019	04	Archivo BAK	
dt	14/05/2019	04	Archivo BAK	
dt	13/05/2019	04	Archivo BAK	
dt	10/05/2019	04	Archivo BAK	
dt	09/05/2019	04	Archivo BAK	
dt	08/05/2019	04	Archivo BAK	
dt	07/05/2019	04	Archivo BAK	
dt	06/05/2019	04	Archivo BAK	
dt	05/05/2019	57	Archivo BAK	
dt	03/05/2019	04	Archivo BAK	
dt	02/05/2019	04	Archivo BAK	
dt	01/05/2019	04	Archivo BAK	
dt	31/04/2019	04	Archivo BAK	
dt	30/04/2019	04	Archivo BAK	
dt	27/04/2019	04	Archivo BAK	
dt	26/04/2019	04	Archivo BAK	
dt	25/04/2019	04	Archivo BAK	
dt	24/04/2019	05	Archivo BAK	
dt	23/04/2019	05	Archivo BAK	
dt	20/04/2019	04	Archivo BAK	
dt	19/04/2019	04	Archivo BAK	

Respaldo diario de información

Nombre	Modificado	Modificado por
Ir...	04/11/2019	H...
...	06/11/2019	D...
bi...	06/11/2019	D...
Cal...	06/06/2019	D...
Com...	06/06/2019	D...
Com...	06/06/2019	D...
Com...	06/11/2019	D...
Dat...	11/06/2019	J...
I...	06/11/2019	D...
I...	15/11/2019	H...
I...	06/06/2019	D...
I...	06/11/2019	D...

Control de cambios en documentos



Herramienta de monitoreo PRTG

[PRTG Network Monitor] mo...

DC [Redacted]

Responder Responder a todos Reenviar ...

Mensaje enviado con importancia Alta.
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

PRTG NETWORK MONITOR

!!! Sensor [Redacted] ***

Sonda local > CASAS DE VALORES > PLUSVALORES (10.8.0.146)

Nuevo estado en 07/03/2020 2:35:00 (SA Pacific Standard Time):

Fallo

Ultimo mensaje:

1 hora intervalo promedio de 371 mseg (Tiempo de respuesta) es inusualmente alto para esta hora de la semana (Connection timed out Socket Error # 10060 Connection timed out. (error de socket # 10060))

Último escaneo:	Último disponible:	Último fallo:	Tiempo disponible:	Tiempo de fallo:	Cobertura:	Tipo de sensor:	Intervalo:
14 s	12 m 35 s	14 s	95,3671%	4,6329%	98%	RDP (Escritorio remoto)	60 s

Escanear ahora Confirmar alarma Pausa Reanudar

Pausar por 5 minutos Pausar por 60 minutos Pausar por 24 horas

Mensaje de alarma de servicio PRTG

D [REDACTED] Report



notificaciones_seguridad@[REDACTED].com

Responder

Responder a todos

Reenviar



Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.



[REDACTED] Activity Report - 18.01.2020.zip

Bitdefender
GravityZone



Notificación de informe

Se ha generado automáticamente un informe programado conforme a los ajustes configurados en el Control Center. Para ver el informe, abra el adjunto.

Activar Windows

Ve a Configuración para activar Windows.

Mensaje de alarma antivirus

F [REDACTED] 001



notificaciones_seguridad@[REDACTED]

Para [REDACTED]

Responder

Responder a todos

Reenviar



[REDACTED] 1903.pdf

[REDACTED]
Se adjunta reporte correspondiente a su dispositivo de seguridad.

Mensaje de alarma firewall

Informe de BCK y Replicas [REDACTED] Satisfactorio)



Para Soporte Sistemas
CC Daniel Calero

Informe de BCK y Replicas BD's

Informe de [REDACTED] Sin novedad

[REDACTED]		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK

Informe de [REDACTED] Sin novedad

[REDACTED]		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK
		OK

Importante: "Hemos atendido su requerimiento, en caso de no existir una respuesta al presente co

Mensaje de revisión diaria de respaldos

Anexo 7.- Convenio BVQ.



CONVENIO DE CONFIDENCIALIDAD

Comparecen a la celebración del presente Convenio de Confidencialidad, por una parte, la **BOLSA DE VALORES DE QUITO BVQ SOCIEDAD ANÓNIMA**, debidamente representada por el señor Jeffry Illingworth, en su calidad Gerente General, a quien en adelante se la denominará "**La Bolsa**"; y, por otra parte, el señor Henry Daniel Calero Suntasig, con Cédula de Identidad No. 1716997828, por sus propios derechos, a quien en adelante se lo denominará "**El Investigador**".

Los comparecientes son legalmente capaces, y de manera libre y voluntaria comparecen a la celebración del presente Convenio al tenor de las siguientes cláusulas:

PRIMERA: ANTECEDENTES. -

- a. **La Bolsa** es una Sociedad Anónima, creada al amparo de la Ley de Mercado de Valores, cuyo objeto es brindar a las Casas de Valores e Instituciones del Sector Público autorizados para operar en el mercado de valores, los mecanismos y servicios necesarios para la negociación de valores.
- b. **El Investigador** se encuentra desarrollando un proyecto de investigación para obtener su título de maestría, con el tema "Análisis de Vulnerabilidades para la Infraestructura de Red de la Bolsa de Valores de Quito, aplicando una metodología de Ethical Hawking", para cuyo efecto se le ha otorgado acceso a la infraestructura de red y a información de diversos procesos operativos de **La Bolsa**.
- c. **La Bolsa** y **El Investigador** han resuelto suscribir el presente Convenio de Confidencialidad por la información que será provista por **La Bolsa** y/o accedida por **El Investigador** en el mercado del desarrollo de su proyecto de titulación.

SEGUNDA: OBJETO. -



www.bolsadequito.com
Av. Amazonas N21-252 y Carrión
Edif. Londres, Piso 8
PBX: (593 2) 398 8500

[Empty rectangular box for stamp or signature]

DECIMÓ CUARTA: RATIFICACIÓN. -

[Empty rectangular box for stamp or signature]


Jeffrey Illingworth
GERENTE GENERAL
BOLSA DE VALORES DE QUITO


Henry Daniel Calero Suntasig
EL INVESTIGADOR