



FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS.

ANÁLISIS Y DISEÑO DE CONTROLES DE SEGURIDAD PERSONAL EN
REDES SOCIALES.

Trabajo de Titulación presentado en conformidad con los requisitos
establecidos para optar por el título de Ingeniera en Sistemas de Computación
e Informática.

Profesor Guía

Mgt. Eddy Mauricio Armas Pallasco.

Autor

Michelle Elizabeth Benítez Dávila.

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Eddy Mauricio Armas Pallasco.
Mgt. en Gerencia de Sistemas y TI.
CI: 1711715803

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Michelle Elizabeth Benítez Dávila.

CI: 1719216861

AGRADECIMIENTO

Agradezco a Dios por todas sus bendiciones, a mis padres por su esfuerzo y sacrificio, a mi hermano por su respaldo, y a mis abuelos por el amor que me han sabido brindar. Un agradecimiento especial al Mgt. Eddy Armas por hacer posible la realización de este trabajo.

DEDICATORIA

Este trabajo y los frutos de mis estudios los dedico a Dios, a mis padres, hermano y abuelos por todo el apoyo en esta etapa de mi vida. Así mismo se lo dedico a todos los niños, niñas y adolescentes que han sido víctimas por medio de las redes sociales.

RESUMEN

En el presente trabajo de titulación se trata la problemática de la inseguridad de los usuarios en las redes sociales en el Ecuador. Las vulnerabilidades y amenazas en un sistema informático incrementan de la misma forma que evolucionan las funciones, por lo que se requieren controles de seguridad que minimicen los riesgos para el usuario. En el primer capítulo se recopila los antecedentes, problemática y estadísticas de la seguridad personal en redes sociales en el Ecuador. En el siguiente capítulo vamos a revisar varias definiciones concernientes a red social, delitos cibernéticos, la red social Facebook y metodología de análisis de riesgos. Para posteriormente analizar los riesgos de los usuarios en la red social Facebook con el uso de la metodología de análisis de riesgos NIST SP 800-30 para poder comprender de mejor manera la problemática y poder en el último capítulo diseñar controles recomendados de seguridad personal en redes sociales.

ABSTRACT

The goal of this study examines the lack of safety Ecuadorian people have when carrying out activities online. One of the most popular tools used online is social networking tools and their developing is endless; however, users may currently be unconscious of the dangers, threats and attacks that these sites imply. In this context, it is essential to implement a safeguarding system to minimize the risks on the social networking use. The first chapter highly focuses on the problems social networking sites involve. Then a complete review of the literature about social networking in Ecuador has been performed. Subsequent to it, Facebook users' risks are analyzed using NIST SP 800-30 methodology. To come to an end, it is suggested best practices to users to guard against potential malware by means of a social networking safeguarding system.

Keywords: social network, safeguarding system, NIST SP 800-30 methodology.

INDICE

Introducción.....	1
1. Capitulo I. Redes Sociales en Ecuador.....	3
1.1. Antecedente	4
1.2. Problemática	5
1.3. Estadísticas	5
1.3.1. Tabulación de Resultados de la Encuesta “Seguridad Personal en Redes Sociales” en el Ecuador	7
1.3.1.1. Tabulación de Resultados del Rango de 10 a 12 Años.....	8
1.3.1.2. Tabulación de Resultados del Rango de 13 a 18 Años.....	15
1.3.1.3. Tabulación de Resultados del Rango de 19 a 55 Años.....	22
2. Capitulo II. Marco Teórico	30
2.1. Redes Sociales.....	30
2.1.1. Definición de Red Social.....	30
2.1.2. Historia de la Web 2.0.....	31
2.1.3. Tipos de Redes Sociales	32
2.1.3.1. Redes Sociales Directas	32
2.1.3.1.1. Según Finalidad.....	33
2.1.3.1.1.1. De Ocio	33
2.1.3.1.1.2. De Uso Profesional.....	33
2.1.3.1.2. Según Modo de Funcionamiento	34
2.1.3.1.2.1. De Contenidos.....	34
2.1.3.1.2.2. Basada en Perfiles: Personales/Profesionales	35
2.1.3.1.2.3. Microblogging	35

2.1.3.1.3. Según Grado de Apertura.....	35
2.1.3.1.3.1. Públicas.....	36
2.1.3.1.3.2. Privadas	36
2.1.3.1.4. Según Nivel de Integración.....	36
2.1.3.1.4.1. De Integración Vertical	37
2.1.3.1.4.2. De Integración Horizontal	37
2.1.3.2. Redes Sociales Indirectas	37
2.1.3.2.1. Foros	38
2.1.3.2.2. Blogs	38
2.1.4. Redes Sociales más Conocidas	39
2.1.4.1. Facebook.....	39
2.1.4.2. YouTube.....	40
2.1.4.3. Wikipedia	41
2.1.4.4. Twitter.....	41
2.1.4.5. LinkedIn	42
2.1.4.6. Instagram.....	42
2.1.4.7. Google+	42
2.1.5. Diferencias de las Redes Sociales.....	43
2.1.5.1. Matriz de Tipos de Redes Sociales.....	43
2.1.5.2. Matriz de Diferencias de Redes Sociales.....	43
2.2. Seguridad Cibernética	44
2.2.1. Delitos Cibernéticos	44
2.2.1.1. Cyberbullying.....	46
2.2.1.2. Falsificación de Identidad	46
2.2.1.3. Grooming.....	46
2.2.1.4. Fraude informático.....	47

2.2.1.5. Robo de Información	47
2.3. Red Social Facebook	47
2.3.1. Concepto de Facebook	48
2.3.2. Historia de Facebook	49
2.3.3. Controles Actuales de Seguridad del Usuario en Facebook ...	50
2.3.3.1. Consejo de Seguridad de Facebook	50
2.3.3.2. Condiciones y Políticas de Facebook	51
2.3.3.2.1. Política de Datos	51
2.3.3.2.2. Declaración de Derechos y Responsabilidades	53
2.3.3.2.3. Normas Comunitarias	54
2.3.3.2.3.1. Ayudar a estar Seguros	54
2.3.3.2.3.2. Fomentar el Comportamiento Respetuoso	56
2.3.3.2.3.3. Proteger Cuentas e Información Personal	56
2.3.3.2.3.4. Proteger la Propiedad Intelectual	58
2.3.3.3. Tecnologías Utilizadas para la Seguridad de Facebook	58
2.3.3.3.1. Cookies	59
2.3.3.3.2. Almacenamiento Local	60
2.3.3.3.3. Etiquetas Pixel	61
2.4. Metodología de Análisis de Riesgos	62
2.4.1. Riesgo	62
2.4.2. Análisis de Riesgos	63
2.4.2.1. Controles	63
2.4.2.1.1. Control Preventivo	63
2.4.2.1.2. Control de Detección	63
2.4.2.1.3. Control de Protección	63

2.4.2.1.4. Control Correctivo.....	64
2.4.3. Principales Metodologías de Análisis de Riesgos Informáticos.....	64
2.4.3.1. MAGERIT	64
2.4.3.2. CRAMM.....	65
2.4.3.3. NIST SP 800-30.....	65
2.4.3.1. OCTAVE.....	65
2.4.4. Diferencias de las Metodologías de Análisis de Riesgos Informáticos.....	66
2.4.5. Metodología NIST SP 800-30	67
2.4.5.1. Evaluación de Riesgos en NIST SP 800-30.....	68
2.4.5.1.1. Caracterización del Sistema	68
2.4.5.1.2. Identificación de Amenazas	69
2.4.5.1.3. Identificación de Vulnerabilidad	70
2.4.5.1.4. Análisis de Control.....	71
2.4.5.1.5. Determinación de Probabilidad.....	72
2.4.5.1.6. Análisis de Impacto.....	73
2.4.5.1.7. Determinación del Riesgo.....	74
2.4.5.1.8. Recomendaciones de Control.....	75
2.4.5.1.9. Documentación de Resultados	76
3. Capitulo III. Análisis de Riesgos	77
3.1. Caracterización del Sistema	77
3.1.1. Alcance de la Evaluación de Riesgos	78
3.1.2. Entorno de Procesamiento del Sistema de Información de la Red Social Facebook.....	78
3.1.2.1. Software	79

3.1.2.2. Tecnologías que Utiliza el Software	79
3.1.2.3. Datos e Información.....	80
3.1.2.4. Usuarios del Sistema	81
3.1.2.5. Procesos Actualmente Utilizados en el Software	81
3.1.2.5.1. Registrar Cuenta en Facebook. (PRO-REG01)	83
3.1.2.5.2. Autenticar en Facebook. (PRO-AUT01).....	85
3.1.2.5.3. Configuración de la Cuenta	99
3.1.2.5.4. Compartir Contenido. (PRO-COM01)	113
3.1.2.5.5. Reportar Abuso y Bloquear Usuarios, Paginas, Aplicaciones, etc	121
3.1.2.6. Controles de Gestión, Técnicos y Operacionales	126
3.1.2.6.1. Controles de Gestión. (CON-GES01)	126
3.1.2.6.2. Algoritmos para Reconocimiento de Patrones. (CON-TEC01).....	127
3.1.2.6.3. Advertencias. (CON-TEC02)	127
3.1.2.6.4. Limite en el Uso de Funciones. (CON-TEC03)	128
3.1.2.6.5. Controles de Seguridad en Menores de Edad. (CON-TEC04).....	129
3.1.2.6.6. Inhabilitar Cuentas. (CON-OPE01)	131
3.1.2.6.7. Control Operativo en Caso de Falsificación de Información. (CON-OPE02).....	131
3.2. Identificación de Amenaza.....	132
3.3. Identificación de Vulnerabilidad	133
3.4. Análisis de Control.....	135
3.5. Determinación de Probabilidad. (PROB)	138
3.6. Análisis de Impacto. (IMP)	145

3.7. Determinación del Riesgo	152
3.8. Recomendaciones de Control.....	161
3.9. Documentación de Evaluación de Riesgos.....	163
4. Capitulo IV. Diseño de Controles Propuestos de Seguridad Personal en Redes Sociales	175
4.1. Proceso Recomendado para Registrar Cuenta en Redes Sociales. (DIS-REG01).....	180
4.1.1. Proceso Recomendado para Configurar Controles de Seguridad. (DIS-REG02)	183
4.2. Proceso Recomendado para Autenticar en Redes Sociales. (DIS-AUT01).....	186
4.2.1. Proceso Recomendado para Restablecer Cuenta en Redes Sociales. (DIS-AUT02)	189
4.3. Proceso Recomendado para Compartir Información. (DIS-COM01).....	192
4.3.1. Proceso Recomendado para Revisión de Publicaciones y Comentarios. (DIS-COM02).....	195
4.3.2. Proceso Recomendado para Reportar Contenido. (DIS-COM03).....	197
4.4. Proceso Recomendado para Configurar Cuenta	198
4.4.1. Proceso Recomendado para Configurar Sobrenombre. (DIS-CON01).....	198
4.4.2. Proceso Recomendado para Configurar Pregunta de Seguridad. (DIS-CON02)	200
4.4.3. Proceso Recomendado para Editar la Configuración de Seguridad. (DIS-SEG01)	201

4.4.4. Proceso Recomendado para Eliminar Cuenta. (DIS-ELI01)....	203
4.5. Proceso Recomendado para Controles Automáticos del Sistema	205
4.5.1. Proceso Recomendado para Limitar el Uso de Funciones. (DIS-LIM01)	205
4.5.2. Proceso Recomendado para Control de Seguridad en un Menor de Edad. (DIS-MEN01)	207
4.6. Análisis de Control	209
5. Conclusiones y Recomendaciones	213
Referencias	218
Anexos	223

INDICE DE FIGURAS

Figura 1. Distribución de la encuesta por edad	8
Figura 2. ¿Qué redes sociales utiliza? Rango de 10-12 años	9
Figura 3. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 10-12 años	9
Figura 4. ¿Todos los datos publicados en su red social son reales? Rango de 10-12 años.....	10
Figura 5. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 10-12 años	11
Figura 6. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 10-12 años.....	11
Figura 7. ¿Qué configuración de privacidad contiene su red social? Rango de 10-12 años.....	12
Figura 8. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 10-12 años.....	13
Figura 9. ¿Ha sido amenazado o insultado a través de su red social? Rango de 10-12 años.....	13
Figura 10. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 10-12 años.....	14
Figura 11. ¿Qué le preocupa de las redes sociales? Rango de 10-12 años	15
Figura 12. ¿Qué redes sociales utiliza? Rango de 13-18 años	16
Figura 13. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 13-18 años	16
Figura 14. ¿Todos los datos publicados en su red social son reales? Rango de 13-18 años.....	17
Figura 15. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 13-18 años	18

Figura 16. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 13-18 años.....	18
Figura 17. ¿Qué configuración de privacidad contiene su red social? Rango de 13-18 años.....	19
Figura 18. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 13-18 años.....	20
Figura 19. ¿Ha sido amenazado o insultado a través de su red social? Rango de 13-18 años.....	20
Figura 20. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 13-18 años.....	21
Figura 21. ¿Qué le preocupa de las redes sociales? Rango de 13-18 años.....	22
Figura 22. ¿Qué redes sociales utiliza? Rango de 19-55 años	23
Figura 23. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 19-55 años.....	23
Figura 24. ¿Todos los datos publicados en su red social son reales? Rango de 19-55 años.....	24
Figura 25. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 19-55 años.....	25
Figura 26. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 19-55 años.....	25
Figura 27. ¿Qué configuración de privacidad contiene su red social? Rango de 19-55 años.....	26
Figura 28. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 19-55 años.....	27
Figura 29. ¿Ha sido amenazado o insultado a través de su red social? Rango de 19-55 años.....	27
Figura 30. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 19-55 años.....	28

Figura 31. ¿Qué le preocupa de las redes sociales? Rango de 19-55 años	29
Figura 32. Crear una página en Facebook	57
Figura 33. Cookies en Facebook sin Iniciar Sesión	59
Figura 34. Cookies en Facebook al Iniciar Sesión.....	60
Figura 35. Almacenamiento Local de Facebook.....	61
Figura 36. Código Fuente de un Pixel de Facebook.....	62
Figura 37. Pasos para la Evaluación de Riesgos	77
Figura 38. Entorno de Procesamiento del Sistema de Información de la Red Social Facebook	78
Figura 39. Proceso del Usuario en Facebook.....	82
Figura 40. Diagrama de Flujo de Registrar Cuenta en Facebook.....	84
Figura 41. Diagrama de Flujo de Autenticar Cuenta en Facebook	86
Figura 42. Diagrama de Flujo de Autenticar Cuenta en Facebook con Contraseña de un Solo Uso	88
Figura 43. Diagrama de Flujo de Autenticar Cuenta de Facebook en Aplicaciones con Uso de la Contraseña de Aplicaciones	89
Figura 44. Diagrama de Flujo de Restablecer Contraseña de Facebook....	91
Figura 45. Diagrama de Flujo de Restablecer Contraseña de Facebook por Medio de la Pregunta de Seguridad.....	92
Figura 46. Diagrama de Flujo de Restablecer Contraseña de Facebook con Ayuda de los Amigos de Confianza	93
Figura 47. Diagrama de Flujo de Autenticar en Facebook con Uso de Alerta de Inicio de Sesión.....	95
Figura 48. Diagrama de Flujo de Autenticar en Facebook con Uso de la Aprobación de Inicio de Sesión	97
Figura 49. Diagrama de Flujo de Proteger Cuenta en Facebook.....	98
Figura 50. Diagrama de Flujo de Configurar Nombre en Facebook.....	100
Figura 51. Diagrama de Flujo de Configurar Fecha de Nacimiento en Facebook	101
Figura 52. Diagrama de Flujo de Configurar Anuncios en Facebook.....	103
Figura 53. Diagrama de Flujo de Desactivar Cuenta en Facebook.....	104

Figura 54. Diagrama de Flujo de Eliminar Cuenta en Facebook	106
Figura 55. Diagrama de Flujo del Control de Privacidad en la Información del Perfil en Facebook	108
Figura 56. Diagrama de Flujo del Control de Privacidad en la Dirección Electrónica en Facebook.....	109
Figura 57. Diagrama de Flujo del Control de Privacidad en Secciones de Facebook	110
Figura 58. Diagrama de Flujo del Control de Privacidad de la Lista de Amigos en Facebook	111
Figura 59. Diagrama de Flujo del Control de Privacidad de Solicitud y Búsqueda de Usuario en Facebook	113
Figura 60. Diagrama de Flujo de Compartir Contenido en Facebook	115
Figura 61. Diagrama de Flujo del Control de Privacidad de Publicaciones Realizadas en Facebook.....	116
Figura 62. Diagrama de Flujo del Control de Privacidad de Publicaciones de Otros Usuarios en la Biografía	118
Figura 63. Diagrama de Flujo del Control de Privacidad de Revisión de la Biografía	119
Figura 64. Diagrama de Flujo de Visualizar Como Otros Usuarios Ven la Biografía	120
Figura 65. Diagrama de Flujo de Reportar Abuso	122
Figura 66. Diagrama de Flujo de Reportar Abuso por Medio de Formulario.....	123
Figura 67. Diagrama de Flujo de Reportar Cuenta de Menor de 13 Años ..	124
Figura 68. Diagrama de Flujo de Bloquear en Facebook	125
Figura 69. Diagrama de Flujo de Limitar el Uso de Funciones	129
Figura 70. Diagrama de Flujo del Control de Seguridad de un Menor de Edad	130
Figura 71. Procesos Recomendados en una Red Social	180
Figura 72. Diagrama de Flujo Recomendado para Registrar Cuenta en Redes Sociales	182

Figura 73. Diagrama de Flujo Recomendado para Configurar Controles de Seguridad en Redes Sociales	185
Figura 74. Diagrama de Flujo Recomendado para Autenticar en Redes Sociales	188
Figura 75. Diagrama de Flujo Recomendado para Restablecer Contraseña en Redes Sociales	191
Figura 76. Diagrama de Flujo Recomendado para Compartir Contenido en Redes Sociales	194
Figura 77. Diagrama de Flujo Recomendado para Revisión de Publicaciones y Comentarios en Redes Sociales.....	196
Figura 78. Diagrama de Flujo Recomendado para Reportar Contenido en Redes Sociales	197
Figura 79. Diagrama de Flujo Recomendado para Configurar Sobrenombre en Redes Sociales.....	199
Figura 80. Diagrama de Flujo Recomendado para Configurar la Pregunta de Seguridad en Redes Sociales	200
Figura 81. Diagrama de Flujo Recomendado para Editar la Configuración de Seguridad en Redes Sociales	202
Figura 82. Diagrama de Flujo Recomendado para Eliminar Cuenta en Redes Sociales	204
Figura 83. Diagrama de Flujo Recomendado para Limitar el Uso de Funciones en Redes Sociales.....	206
Figura 84. Diagrama de Flujo Recomendado para el Control de Seguridad de un Menor de Edad en Redes Sociales	208

INDICE DE TABLAS

Tabla 1. Distribución de la encuesta por edad.....	8
Tabla 2. ¿Qué redes sociales utiliza? Rango de 10-12 años.....	9
Tabla 3. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 10-12 años.....	10
Tabla 4. ¿Todos los datos publicados en su red social son reales? Rango de 10-12 años.....	10
Tabla 5. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 10-12 años.....	11
Tabla 6. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 10-12 años.....	12
Tabla 7. ¿Qué configuración de privacidad contiene su red social? Rango de 10-12 años.....	12
Tabla 8. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información personal a los propietarios de la aplicación? Rango de 10-12 años.....	13
Tabla 9. ¿Ha sido amenazado o insultado a través de su red social? Rango de 10-12 años.....	14
Tabla 10. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 10-12 años.....	14
Tabla 11. ¿Qué le preocupa de las redes sociales? Rango de 10-12 años.....	15
Tabla 12. ¿Qué redes sociales utiliza? Rango de 13-18 años.....	16
Tabla 13. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 13-18 años.....	17
Tabla 14. ¿Todos los datos publicados en su red social son reales? Rango de 13-18 años.....	17
Tabla 15. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 13-18 años.....	18

Tabla 16. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 13-18 años.....	19
Tabla 17. ¿Qué configuración de privacidad contiene su red social? Rango de 13-18 años.....	19
Tabla 18. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 13-18 años.....	20
Tabla 19. ¿Ha sido amenazado o insultado a través de su red social? Rango de 13-18 años.....	21
Tabla 20. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 13-18 años.....	21
Tabla 21. ¿Qué le preocupa de las redes sociales? Rango de 13-18 años	22
Tabla 22. ¿Qué redes sociales utiliza? Rango de 19-55 años.....	23
Tabla 23. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 19- 55 años	24
Tabla 24. ¿Todos los datos publicados en su red social son reales? Rango de 19-55 años.....	24
Tabla 25. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 19-55 años	25
Tabla 26. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 19-55 años.....	26
Tabla 27. ¿Qué configuración de privacidad contiene su red social? Rango de 19-55 años.....	26
Tabla 28. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 19-55 años.....	27
Tabla 29. ¿Ha sido amenazado o insultado a través de su red social? Rango de 19-55 años.....	28
Tabla 30. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 19-55 años.....	28
Tabla 31. ¿Qué le preocupa de las redes sociales? Rango de 19-55 años	29

Tabla 32. Matriz de tipos de redes sociales	43
Tabla 33. Matriz de diferencias de redes sociales	44
Tabla 34. Matriz de diferencias de las metodologías de análisis de riesgos	66
Tabla 35. Ejemplo de Amenazas Humanas	69
Tabla 36. Ejemplo de Pares de la Vulnerabilidad / Amenaza	71
Tabla 37. Matriz – Nivel de riesgos	75
Tabla 38. Sensibilidad de Información.	80
Tabla 39. Mapa de Calor - Sensibilidad de información	81
Tabla 40. Amenazas Humanas – Red Social Facebook.....	132
Tabla 41. Pares de la Vulnerabilidad / Amenaza – Red Social Facebook ..	133
Tabla 42. Tipo del Control – Red Social Facebook	135
Tabla 43. Automatización del Control – Red Social Facebook	135
Tabla 44. Escalas y Niveles de la Efectividad de Controles – Red Social Facebook	136
Tabla 45. Mapa de Calor de la Efectividad de Controles – Red Social Facebook	136
Tabla 46. Evaluación de Controles – Red Social Facebook	136
Tabla 47. Criterios de Evaluación de la Probabilidad – Red Social Facebook	138
Tabla 48. Determinación de Probabilidad – Red Social Facebook	139
Tabla 49. Criterios de Evaluación del Impacto – Red Social Facebook.....	145
Tabla 50. Análisis de Impacto – Red Social Facebook.....	146
Tabla 51. Acciones a Realizar – Red Social Facebook	152
Tabla 52. Escalas y Niveles del Riesgo – Red Social Facebook	152
Tabla 53. Mapa de Calor del Riesgo – Red Social Facebook.....	152
Tabla 54. Matriz de Riesgos – Red Social Facebook	154
Tabla 55. Tipo del Control – Recomendaciones de Control de la Red Social Facebook	161
Tabla 56. Automatización del Control – Recomendaciones de Control de la Red Social Facebook	161

Tabla 57. Escalas y Niveles de la Efectividad de Controles - Recomendaciones de Control de la Red Social Facebook	162
Tabla 58. Mapa de Calor de la Efectividad de Controles - Recomendaciones de Control de la Red Social Facebook	162
Tabla 59. Evaluación de Controles – Recomendaciones de Control de la Red Social Facebook	162
Tabla 60. Acciones a Realizar – Red Social Facebook	164
Tabla 61. Resumen de la Evaluación de Riesgos - Red Social Facebook..	166
Tabla 62. Controles recomendados para minimizar los riesgos por amenaza	175
Tabla 63. Tipo del Control – Diseño de Controles	209
Tabla 64. Automatización del Control – Diseño de Controles.....	210
Tabla 65. Escalas y Niveles de la Efectividad de Controles – Diseño de Controles	210
Tabla 66. Mapa de Calor de la Efectividad de Controles – Diseño de Controles	210
Tabla 67. Evaluación de Controles – Diseño de Controles.....	211
Tabla 68. Conclusiones de la encuesta “SEGURIDAD PERSONAL EN REDES SOCIALES” por rangos de edad	213
Tabla 69. Conclusión y Recomendación – Vulnerabilidades y Controles Recomendados a la Red Social Facebook.....	215

INTRODUCCIÓN.

Se ha observado que en la última década, las redes sociales se han vuelto importantes para la comunicación del ser humano. De la misma forma que se crean y evolucionan los sistemas de información se presentan nuevos riesgos para los usuarios, motivo por el que se requieren nuevos controles de seguridad informática que minimicen dichas inseguridades.

El objetivo es diseñar controles de seguridad personal que minimicen los peligros existentes en las redes sociales, a partir de la recopilación de información, procesos y controles actuales de la red social Facebook para el análisis de riesgos de las inseguridades pertenecientes a los usuarios de las plataformas, con el fin de recomendar a las empresas que implementen los controles diseñados en el presente trabajo de titulación.

Los objetivos específicos del presente trabajo de titulación son:

- Analizar las metodologías de evaluación de riesgos y las diferentes redes sociales.
- Identificar los puntos débiles de inseguridad personal de los usuarios en redes sociales que permiten ser susceptibles a las amenazas.
- Proponer controles de seguridad que minimicen los peligros existentes en redes sociales.

La metodología de evaluación de riesgos NIST 800-30, es la más apropiada en este caso para ser la guía del análisis de riesgos de la inseguridad personal de los usuarios en las redes sociales, dando énfasis en los delitos cibernéticos. El proceso se realiza en nueve pasos principales en el que se caracteriza el sistema informático, identifican y describen las amenazas y vulnerabilidades, analizan los controles actuales, determinan las probabilidades e impacto, se miden las amenazas obteniendo los riesgos y sus respectivos niveles con la matriz de riesgo, se generan recomendaciones para aplicar controles y así ser implementados en el proceso de gestión de riesgo y por último, la documentación de resultados que consiste en el informe de evaluación de riesgo.

Es importante que el usuario se sienta seguro al tener disponibilidad, confidencialidad e integridad en las redes sociales, por lo que los controles deben ser en lo posible proactivos para evitar la existencia de cuentas falsas, acoso cibernético, agresiones contra el honor, hurto de cuenta, etc.

1. Capítulo I. Redes Sociales en Ecuador.

Se ha observado que en los últimos años, las redes sociales en Ecuador han sido claves en la comunicación actual de las personas, llegando a ser las más utilizadas. Así como aparecieron otorgando beneficios también contienen falencias, las cuales son aprovechadas por los delincuentes como medio para realizar sus fechorías.

En el tomo II del libro serie memorias y debates del XVI Congreso Iberoamericano de Derecho e Informática, Mariliana Rico Carrillo expresa sobre las redes sociales que “La evolución de las Tecnologías de la Información y las Comunicaciones (TIC) ha favorecido la presencia de nuevas herramientas en Internet, representadas principalmente por la existencia de espacios abiertos de comunicación e interacción. La participación activa y el creciente número de los usuarios de las redes sociales en este ámbito han producido importantes consecuencias en el ejercicio de algunos derechos fundamentales.” (Barzallo, J, Téllez, J, Reyes, P y Amoroso, Y, 2012, p.403)

En las páginas web de ranking como Alexa, indican que una de las redes sociales más utilizada a nivel mundial es Facebook. Dicha red social tiene su política de datos, normas de uso, sesión de derechos y responsabilidades, en las que contiene la información de cómo el usuario debe comportarse y usar de mejor manera la red social. Las normas de uso en gran parte no son proactivas, ya que esperan a que suceda para que se reporte o se tome medidas en el asunto. Por ejemplo el mínimo de edad para ingresar a la red social es de 13 años, pero se pueden encontrar perfiles de niños de 10 a 12 años que dicen tener de 15 en adelante. Existe la norma ISO/IEC 27032 que contiene las directrices para la Seguridad en Internet, pero no intervienen directamente en la seguridad de las redes sociales como son los delitos cibernéticos.

1.1. Antecedentes.

En el Segundo Encuentro Latinoamericano sobre Seguridad Cibernética realizado el 10 y 11 de septiembre, el Doctor Julio Téllez Valdés expuso que la tecnología puede potenciar a los individuos y a la sociedad, por medio de las aplicaciones móviles, educación e-learning y el Cloud-Computing pero que al mismo tiempo pueden ser instrumentos para vulnerar derechos fundamentales como la guerra cibernética, espionaje cibernético, usurpación de identidad, acoso cibernético y terrorismo a distancia. (García, 2015, pp.21-22)

A las conclusiones que llegaron en el Segundo Encuentro Latinoamericano sobre Seguridad Cibernética, fue que la protección debe darse antes del acto y no cuando ya ocurrió, de tal forma que tenga un enfoque preventivo y no reactivo. Incorporar a la familia para poder ayudar a los niños, niñas y adolescentes que tengan una navegación segura, un uso seguro de las redes de telecomunicaciones y sobre todo la conciencia ética y cívica para hacer un uso asertivo e inteligente del Internet. (García, 2015, p.25)

Manuel Castells en el discurso de Internet, libertad y sociedad: una perspectiva analítica del 2001, dijo: "Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces." (Temperani, 2013, párr. 6)

En el taller de Legislación en materia de Ciberdelincuencia en América Latina, se puede apreciar que las víctimas del crimen cibernético a nivel mundial tiene un incremento de 255 millones de personas en el 2011 a 556 millones en el 2013, eso tiene un incremento de 118%, lo cual indica que existe más de 1.5 millones de víctimas cada día, aproximadamente 18 víctimas cada segundo. (SEGOB, 2014, p.5)

Es importante tener ambientes tecnológicos seguros para los usuarios, sobre todo para los adolescentes, porque es el medio en el que actualmente se

desenvuelven desde temprana edad, llegando a ser fundamentales en su vida cotidiana para el aprendizaje, investigación y crecimiento personal.

1.2. Problemática.

La seguridad y delincuencia cibernética es un tema de preocupación mundial, sobre todo cuando se involucra a menores de edad. En la última década, la evolución de la tecnología y avances en la comunicación ha incrementado de forma rápida, a tal punto en que los cambios sociales han resultado impredecibles, teniendo como consecuencia los nuevos riesgos que se han generado para la sociedad. Los crímenes en las redes sociales han sido varios, por ejemplo, el robo de información, falsificación de identidad, acceso sin autorización, crímenes contra el honor, falta de privacidad, grooming, cyberbullying, etc.

De la investigación llevada a cabo, no se encontraron hallazgos sobre estadísticas y análisis de crímenes cibernéticos en las redes sociales en el Ecuador. Por tal motivo se realizó la encuesta “Seguridad Personal en Redes Sociales” para establecer los indicadores de privacidad, seguridad, veracidad de información y lo que preocupa principalmente a los usuarios de las redes sociales que utilizan.

1.3. Estadísticas.

Según la herramienta Alexa Internet (s.f.), en el top tiene a Facebook sobre todas las redes sociales a nivel mundial, teniendo el segundo lugar del top de sitios web. La red social es utilizada más en Estados Unidos, el género femenino es mayor que el masculino y en ubicación de navegación predomina en los colegios.

En la página de Facebook (s.f.) newsroom, en la historia se puede observar el incremento de los usuarios de Facebook de un año a otro. En el año 2004

contaba con un millón de usuarios, para el 2005 alcanzó los 6 millones de usuarios, en el 2007 llegó a los 58 millones, para el 2010 contaba con 600 millones de personas activas en la red social y en el 2015 tuvo mil millones de usuarios activos que utilizaron la red social por día.

Según Formación Gerencial Business Training Center (s.f.) en la estadística realizada el 30 de Enero del 2016 de Facebook. “Ecuador cuenta con una audiencia de 8'900.000 usuarios, de los cuales 1'400.000 son administradores de páginas Facebook, muchas de las cuales pertenecen a marcas, emprendimientos e intereses comunes de grupos de usuarios.”

La red social que le sigue a Facebook en la herramienta Alexa Internet (s.f.), es YouTube. YouTube es más utilizado en Estados Unidos, el género masculino es mayor que el femenino y en ubicación de navegación predomina en el hogar.

A diferencia de Ecuador, España cuenta con la estadística del número de los delitos cibernéticos ocurridos en el año 2014. La estadística fue a base de los informes del Ministerio de Justicia del país. Ocupando la estafa el primer puesto con 17.328 casos, seguido por la pornografía y corrupción de menores o discapacitados con 581 casos, amenazas y coacciones con 527 casos, acceso sin autorización con 297 casos, falsificación documental con 156 casos, daños y sabotaje informático con 143 casos, contra la integridad moral con 130 casos, denuncias por suplantación de identidad con 117 casos y acoso a menores de 13 años con 60 casos. Los delitos informáticos aumentaron 71.21% del año 2013 al 2014. Llegando así a darnos cuenta cómo crecen las amenazas de un año a otro en un ritmo rápido. Statista (s.f.)

1.3.1. Tabulación de Resultados de la Encuesta “Seguridad Personal en Redes Sociales” en el Ecuador.

El objetivo de la encuesta es obtener los indicadores de la seguridad personal de los usuarios en las redes sociales en el Ecuador. La encuesta se puede observar en el Anexo A.

Los rangos de las encuestas se basan de 10 a 12 años porque son pre-adolescentes que comienzan a evadir los controles de seguridad para poder ingresar a las redes sociales. Dichas encuestas se realizaron en la Unidad Educativa San Francisco de Sales, contando con 147 en total.

Muchas de las redes sociales son creadas en Estados Unidos, por lo que la edad mínima es de 13 años para crear un perfil.

“Antes de permitirle a tus hijos crear sus propios perfiles sociales, revisa con atención los Términos de Uso de estas redes. Debido a que muchas de ellas han sido creadas en los Estados Unidos, la edad mínima para crear un perfil en una red social será de 13 años de edad. Esto se debe a ley federal de 1998 de los Estados Unidos llamada *Children's Online Privacy Protection Act*, y que tiene relación con el uso de la información confidencial de los menores de edad y el cómo la almacenan las empresas de tecnología. Debido a que la información personal de los menores de 13 años debe manejarse de manera diferente, muchas redes sociales han optado por no permitir que ellos utilicen sus servicios.” (About, s.f.)

El rango de 13 a 18 años es porque en la adolescencia son más vulnerables a las amenazas de las redes sociales por el comportamiento que tienen a esa edad. Dichas encuestas se realizaron en la Unidad Educativa San Francisco de Sales, contando con 191 en total.

El rango de 19 a 55 años es porque a partir de los 55 disminuye la cantidad de usuarios que utilizan las redes sociales, ya que se les dificulta su uso. Dichas encuestas se realizaron a usuarios de Facebook en Ecuador por medio de una

encuesta web., contando con 130 en total. Son menos encuestas ya que son usuarios que tienen más conciencia y responsabilidad sobre el uso de información personal en las redes sociales.

El total de encuestas realizadas es de 567. De las cuales el 51% fueron de adolescentes entre 13 y 18 años, el 26% entre 10 y 12 años y el 23% de entre el rango de 19 a 55 años.

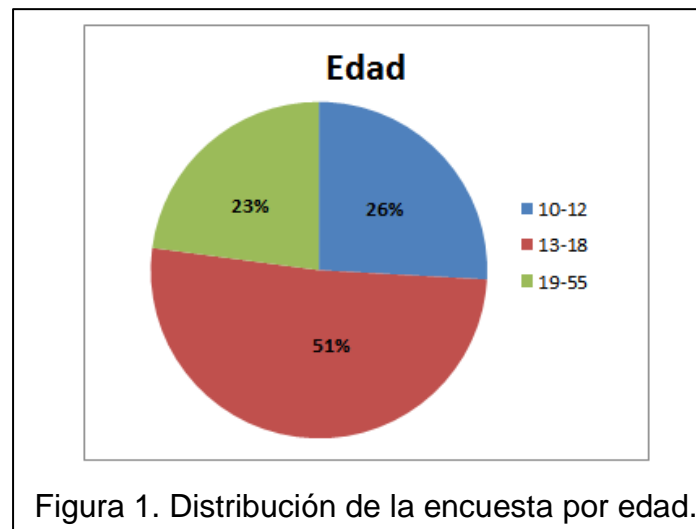


Tabla 1. Distribución de la encuesta por edad.

Rango de edad	Total	Porcentaje
10-12	147	25.9%
13-18	291	51.2%
19-55	130	22.9%

1.3.1.1. Tabulación de Resultados del Rango de 10 a 12 Años.

El total de encuestas realizadas a personas que pertenecen al rango de edad de 10 a 12 años fueron de 147 encuestas. Las cuales indican que el 89,8% utiliza YouTube, el 69,4% Facebook, el 61,9% Wikipedia, el 35,4% Instagram, el 19% Twitter y el 3,4% utiliza otra red social como Snapchat.

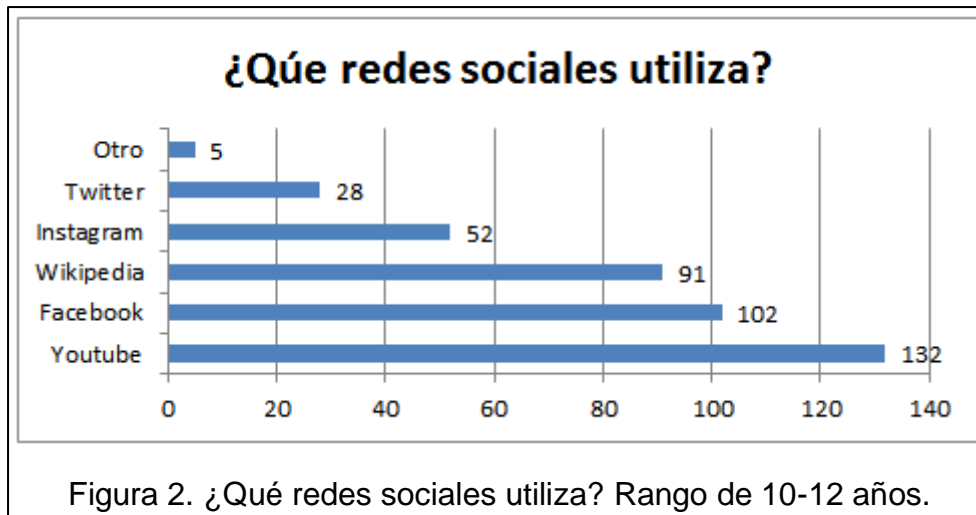


Tabla 2. ¿Qué redes sociales utiliza? Rango de 10-12 años.

Red Social	Total	Porcentaje
Youtube	132	89.8%
Facebook	102	69.4%
Wikipedia	91	61.9%
Instagram	52	35,4%
Twitter	28	19.0%
Otro	5	3.4%

De las 147 encuestas, el 49% utilizó el código al e-mail para la verificación de creación de la cuenta, el 29,9% el código al celular y el 34% ningún tipo de verificación.

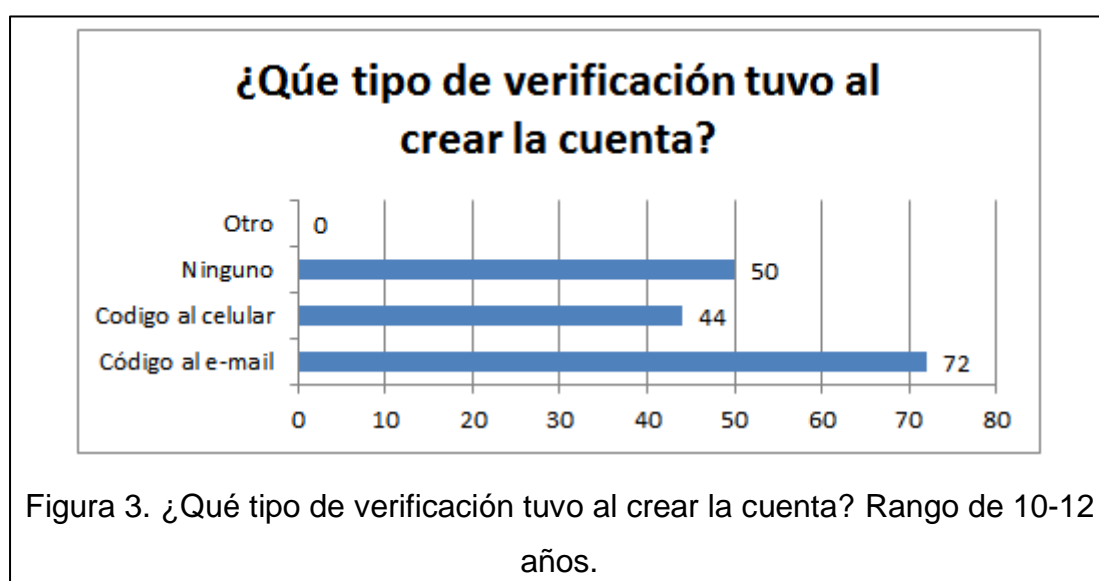


Tabla 3. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 10-12 años.

Tipo de Verificación	Total	Porcentaje
Código al e-mail	72	49.0%
Código al celular	44	29.9%
Ninguno	50	34.0%
Otro	0	0.0%

De las 147 encuestas, el 24,5% publico datos reales en las redes sociales y el 76,2% no publico información real.

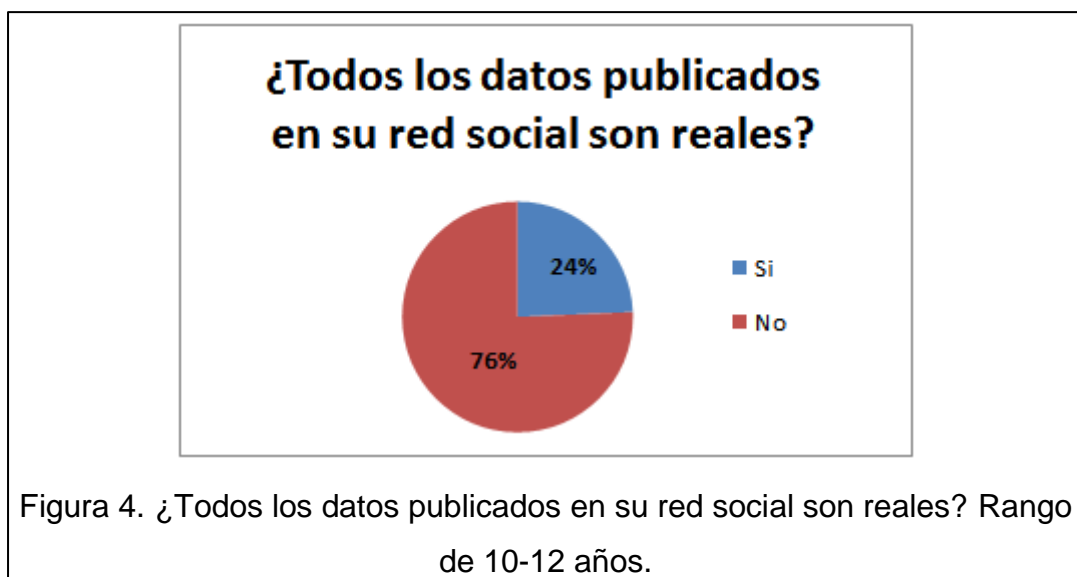


Tabla 4. ¿Todos los datos publicados en su red social son reales? Rango de 10-12 años.

¿Son los datos reales?	Total	Porcentaje
Si	36	24.5%
No	112	76.2%

De las 147 encuestas, el 83% considera su contraseña segura y el 17% no.

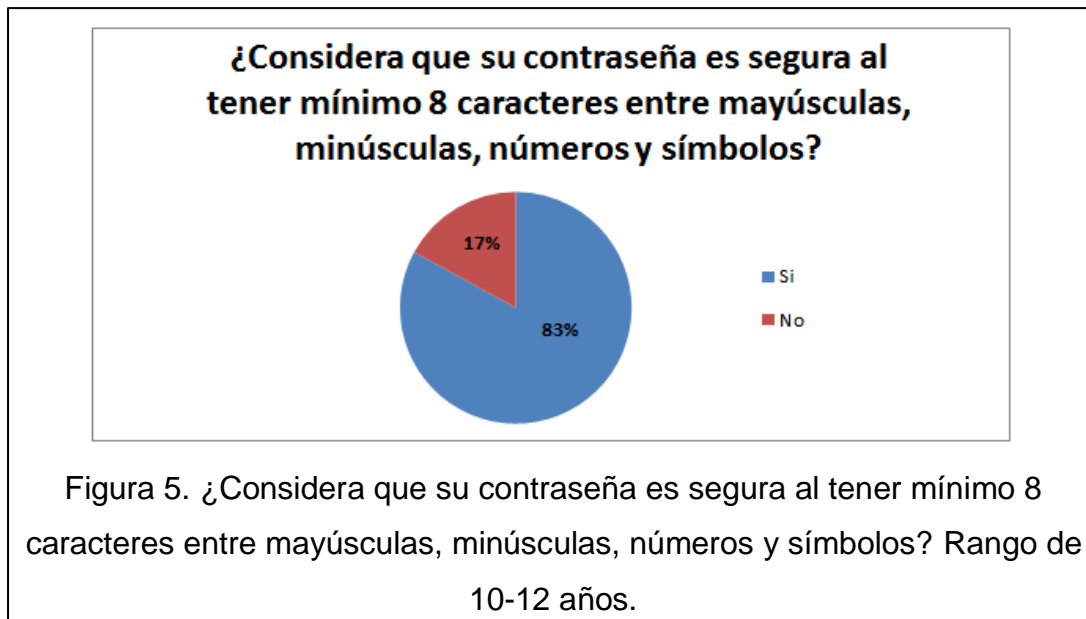


Tabla 5. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 10-12 años.

¿Es segura la contraseña?	Total	Porcentaje
Si	122	83.0%
No	25	17.0%

De las 147 encuestas, el 69,4% nunca cambia la contraseña, el 17% cambia cada 6 meses y el 13,6% cambia anualmente.

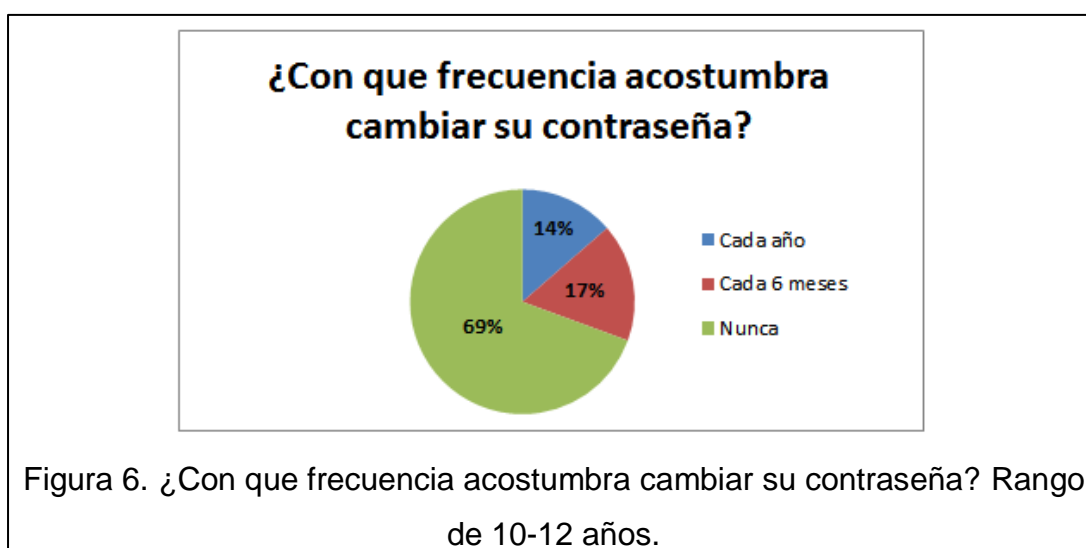


Tabla 6. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 10-12 años.

Frecuencia del cambio de contraseña	Total	Porcentaje
Cada año	20	13.6%
Cada 6 meses	25	17.0%
Nunca	102	69.4%

De las 147 encuestas, el 42,2% desconoce la configuración de privacidad en las redes sociales, el 40,8% tiene para que sea visible solo para amigos, el 10,2% solo para amigos específicos y el 6,8% para todos.

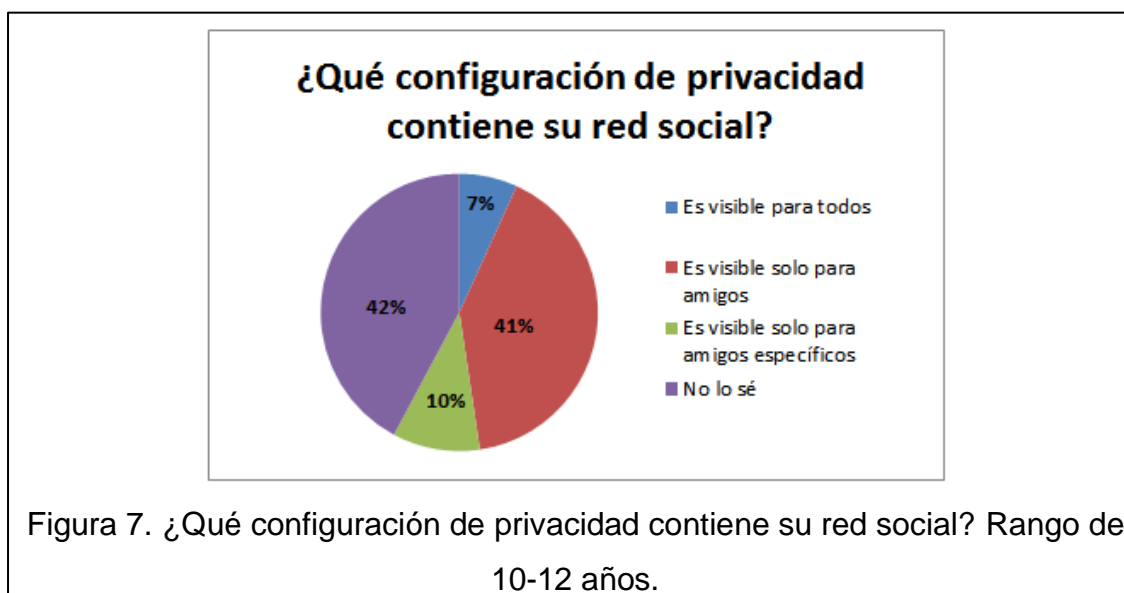


Tabla 7. ¿Qué configuración de privacidad contiene su red social? Rango de 10-12 años.

Configuración de privacidad	Total	Porcentaje
Es visible para todos	10	6.8%
Es visible solo para amigos	60	40.8%
Es visible solo para amigos específicos	15	10.2%
No lo sé	62	42.2%

De las 147 encuestas, el 62,6% tiene conocimiento de la información proporcionada a las aplicaciones asociadas y el 37,4% desconoce.

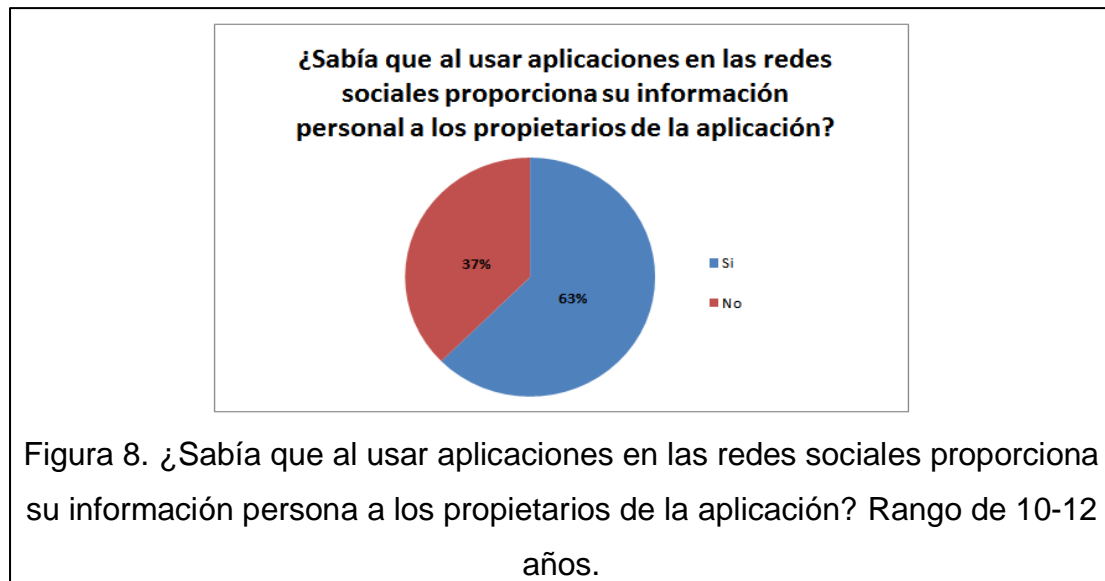


Tabla 8. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 10-12 años.

Conocimiento de la información proporcionada a las aplicaciones	Total	Porcentaje
Si	92	62.6%
No	55	37.4%

De las 147 encuestas, el 91,8% no ha sido amenazado o insultado a través de su red social y el 8,2% si lo ha sido.



Tabla 9. ¿Ha sido amenazado o insultado a través de su red social? Rango de 10-12 años.

Ha sido amenazado o insultado	Total	Porcentaje
Si	12	8.2%
No	135	91.8%

De las 147 encuestas, el 93,2% no aceptado invitaciones de amistad de desconocidos y el 6,8% si aceptado.



Tabla 10. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 10-12 años.

Aceptado invitaciones de amistad de desconocidos	Total	Porcentaje
Si	10	6.38%
No	137	93.2%

De las 147 encuestas, al 91,8% le preocupa el robo de información, al 87,1% la falsificación de identidad, al 81,6% el grooming, al 74,8% el acoso, al 66,7% el acceso sin autorización y la falta de privacidad, al 62,6% los crímenes contra el honor, al 2% nada y al 0,7% otro como por ejemplo el Spam.

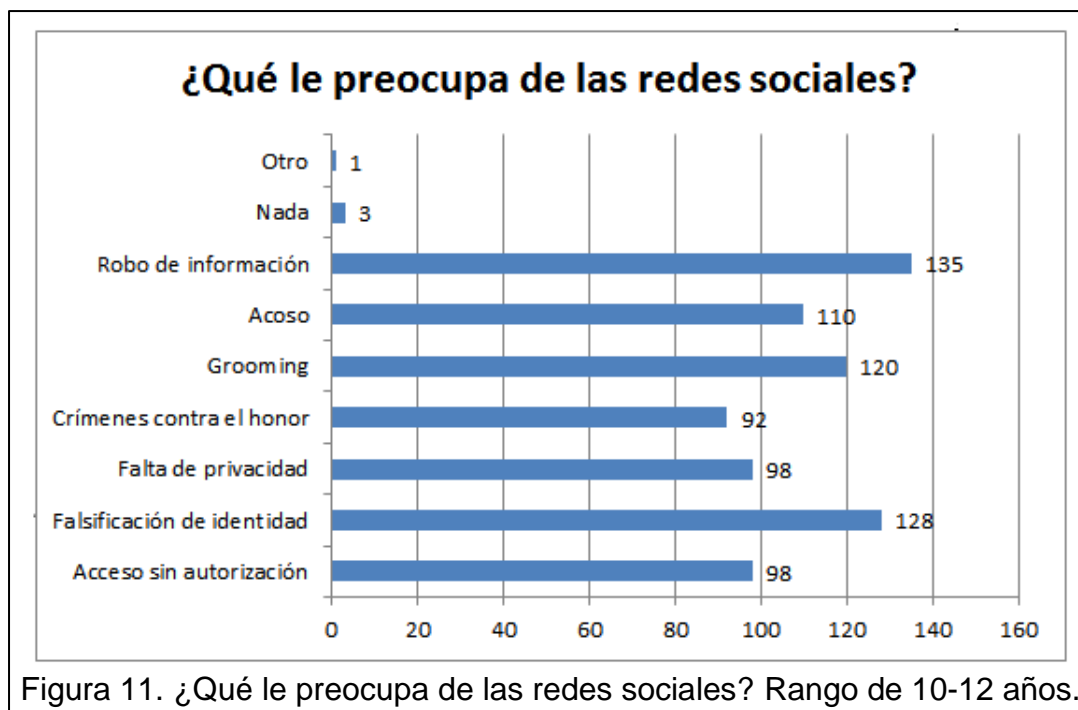


Tabla 11. ¿Qué le preocupa de las redes sociales? Rango de 10-12 años.

¿Qué le preocupa de las Redes Sociales	Total	Porcentaje
Acceso sin autorización	98	66.7%
Falsificación de identidad	128	87.1%
Falta de privacidad	98	66.7%
Crímenes contra el honor	92	62.6%
Grooming	120	81.6%
Acoso	110	74.8%
Robo de información	135	91.8%
Nada	3	2.0%
Otro	1	0.7%

1.3.1.2. Tabulación de Resultados del Rango de 13 a 18 Años.

El total de encuestas realizadas a personas que pertenecen al rango de edad de 13 a 18 años fueron 291 encuestas. Las cuales indican que el 90,4% utiliza YouTube, el 90,0% Facebook, el 65,3% Instagram, el 56,4% Wikipedia, el 32,6% Twitter, el 0,3% LinkedIn y el 18,9% utiliza otra red social como Snapchat.

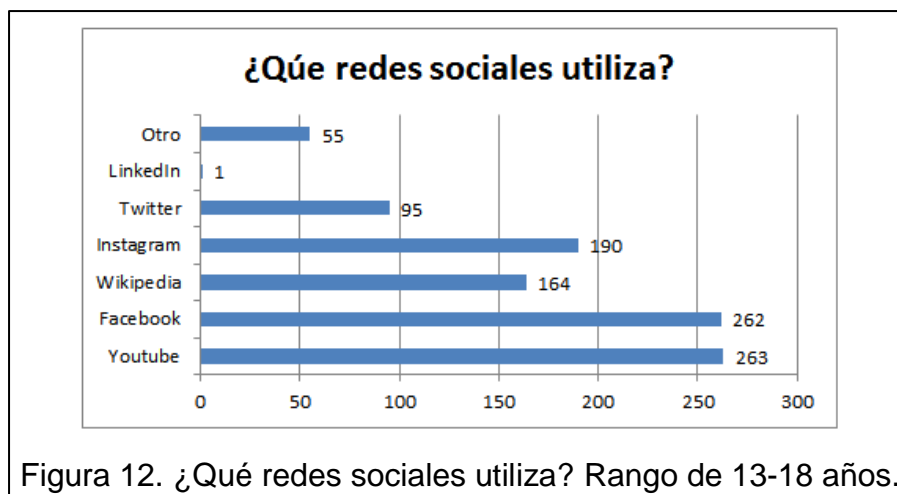


Tabla 12. ¿Qué redes sociales utiliza? Rango de 13-18 años.

Red Social	Total	Porcentaje
Youtube	236	89.8%
Facebook	262	69.4%
Wikipedia	164	61.9%
Instagram	190	35,4%
Twitter	95	19.0%
LinkedIn	1	0.3%
Otro	55	18.9%

De las 291 encuestas, el 87,6% utilizó el código al e-mail para la verificación de creación de la cuenta, el 49,8% el código al celular, el 2,1% ningún tipo de verificación y el 1% otro tipo de verificación.

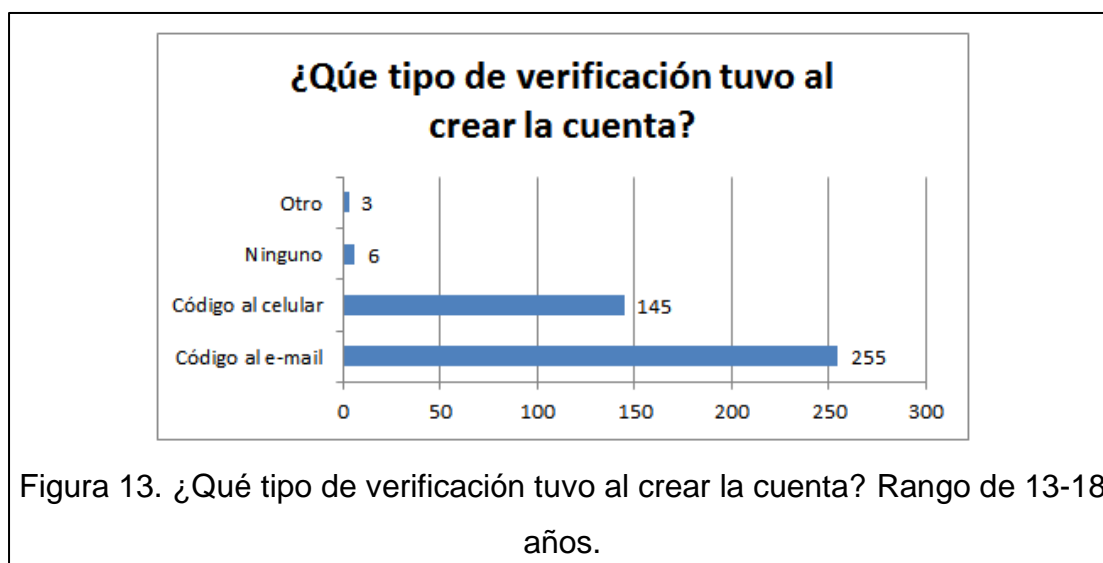


Tabla 13. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 13-18 años.

Tipo de Verificación	Total	Porcentaje
Código al e-mail	255	87.6%
Código al celular	145	49.8%
Ninguno	6	2.1%
Otro	30	1.0%

De las 291 encuestas, el 81,1% publico datos reales en las redes sociales y el 18,9% no publico información real.

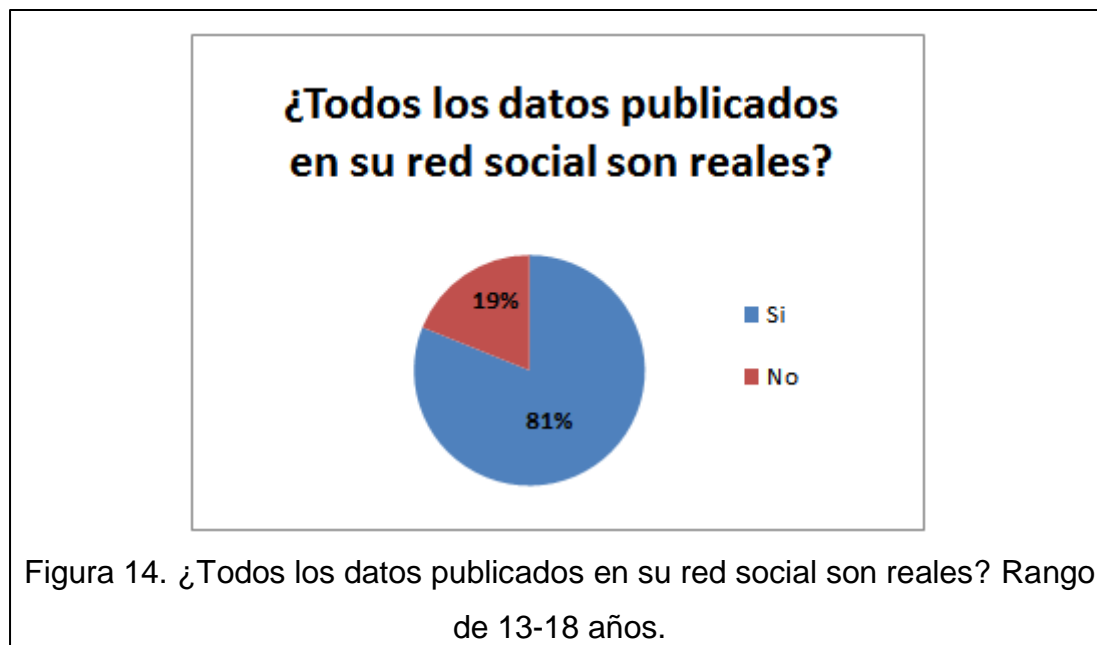


Tabla 14. ¿Todos los datos publicados en su red social son reales? Rango de 13-18 años.

¿Son los datos reales?	Total	Porcentaje
Si	236	81.1%
No	55	18.9%

De las 291 encuestas, el 83,2% considera su contraseña segura y el 16,8% no.

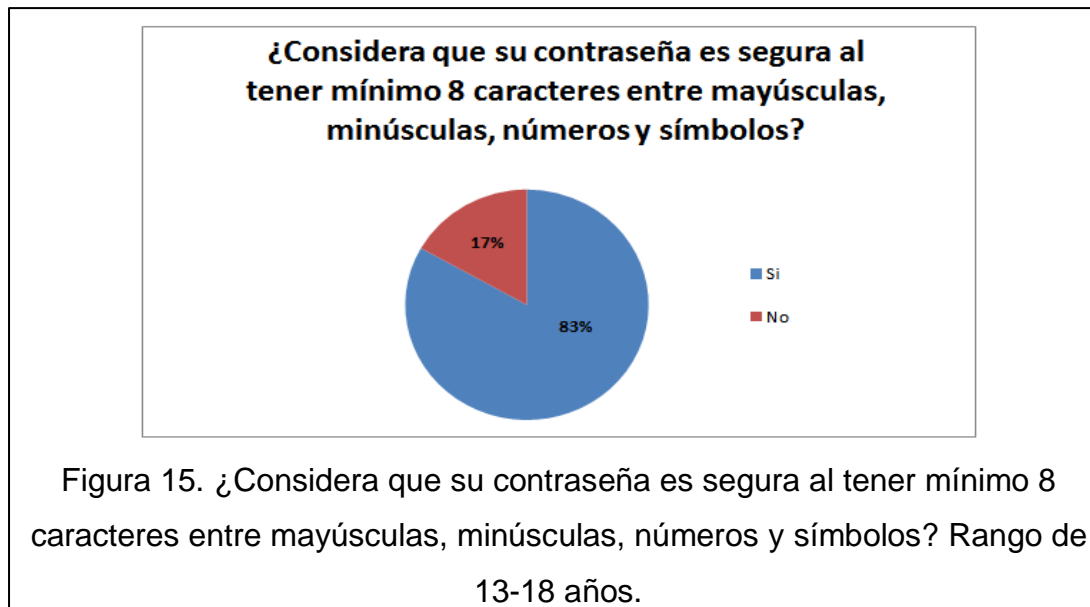


Tabla 15. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 13-18 años.

¿Es segura la contraseña?	Total	Porcentaje
Si	242	83.2%
No	49	16.8%

De las 291 encuestas, el 49,5% nunca cambia la contraseña, el 28,2% cambia cada 6 meses y el 22,3% cambia anualmente.

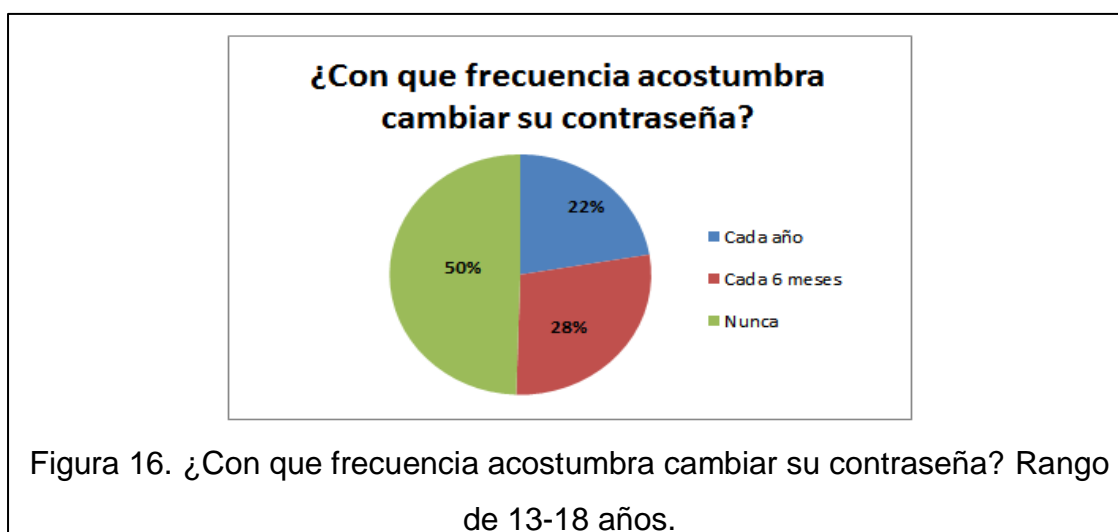


Tabla 16. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 13-18 años.

Frecuencia del cambio de contraseña	Total	Porcentaje
Cada año	65	22.3%
Cada 6 meses	82	28.2%
Nunca	144	49.5%

De las 291 encuestas, el 6,5% desconoce la configuración de privacidad en las redes sociales, el 67% tiene para que sea visible solo para amigos, el 11,3% solo para amigos específicos y el 15,1% para todos.



Tabla 17. ¿Qué configuración de privacidad contiene su red social? Rango de 13-18 años.

Configuración de privacidad	Total	Porcentaje
Es visible para todos	44	15.1%
Es visible solo para amigos	195	67.0%
Es visible solo para amigos específicos	33	11.3%
No lo sé	19	6.5%

De las 291 encuestas, el 81,4% tiene conocimiento de la información proporcionada a las aplicaciones asociadas y el 18,6% desconoce.

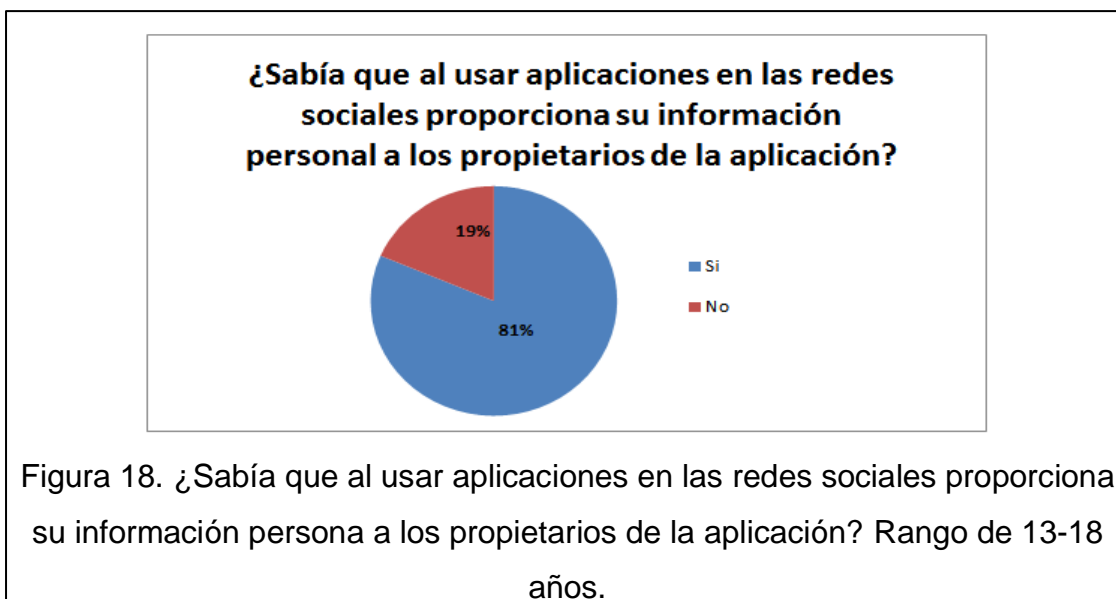


Tabla 18. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 13-18 años.

Conocimiento de la información proporcionada a las aplicaciones	Total	Porcentaje
Si	237	81.4%
No	54	18.6%

De las 291 encuestas, el 74,6% no ha sido amenazado o insultado a través de su red social y el 25,4% si lo ha sido.

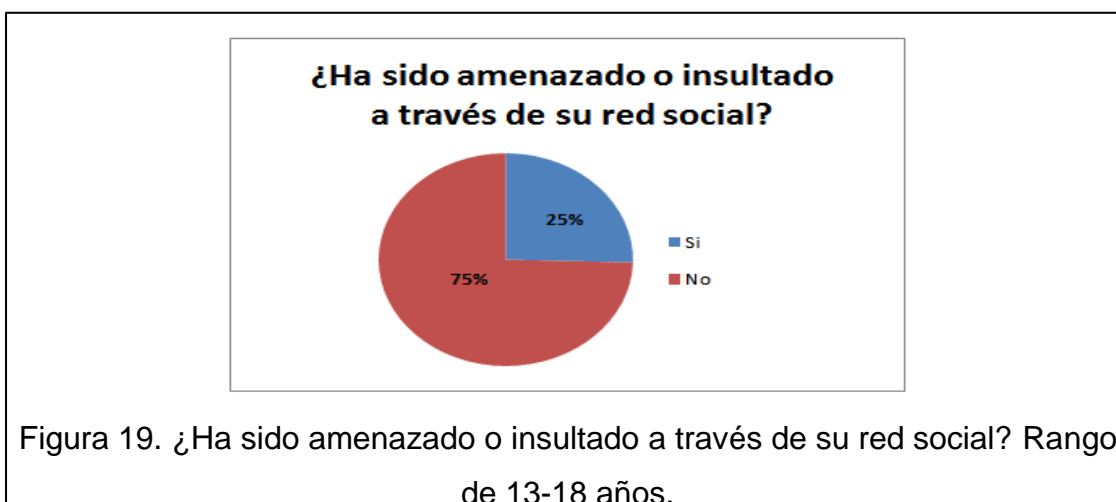


Tabla 19. ¿Ha sido amenazado o insultado a través de su red social? Rango de 13-18 años.

Ha sido amenazado o insultado	Total	Porcentaje
Si	74	25.4%
No	217	74.6%

De las 291 encuestas, el 51,9% aceptado invitaciones de amistad de desconocidos y el 48,1% no aceptado.



Tabla 20. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 13-18 años.

Aceptado invitaciones de amistad de desconocidos	Total	Porcentaje
Si	151	51.9%
No	140	48.1%

De las 291 encuestas, al 83,5% le preocupa el robo de información, al 75,3% la falsificación de identidad, al 47,8% el grooming, al 70,4% el acoso, al 48,8% el acceso sin autorización, al 52,9% la falta de privacidad, al 30,9% los crímenes contra el honor, al 2,1% nada y al 0,3% otro como por ejemplo el Spam.

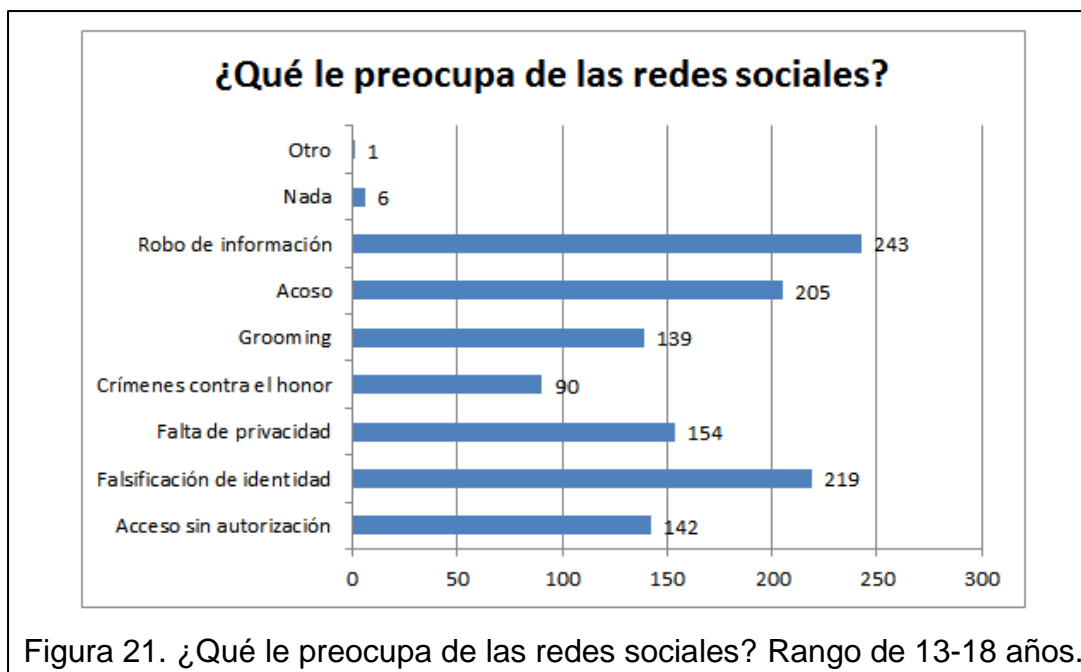


Tabla 21. ¿Qué le preocupa de las redes sociales? Rango de 13-18 años.

¿Qué le preocupa de las Redes Sociales	Total	Porcentaje
Acceso sin autorización	142	48.8%
Falsificación de identidad	219	75.3%
Falta de privacidad	154	52.9%
Crímenes contra el honor	90	30.9%
Grooming	139	47.8%
Acoso	205	70.4%
Robo de información	243	83.5%
Nada	6	2.1%
Otro	1	0.3%

1.3.1.3. Tabulación de Resultados del Rango de 19 a 55 Años.

El total de encuestas realizadas a personas que pertenecen al rango de edad de 19 a 55 años fueron 130 encuestas. Las cuales indican que el 67,7% utiliza YouTube, el 93,8% Facebook, el 40% Instagram, el 32,3% Wikipedia, el 30% Twitter, el 30% LinkedIn y el 6,9% utiliza otra red social como Snapchat.

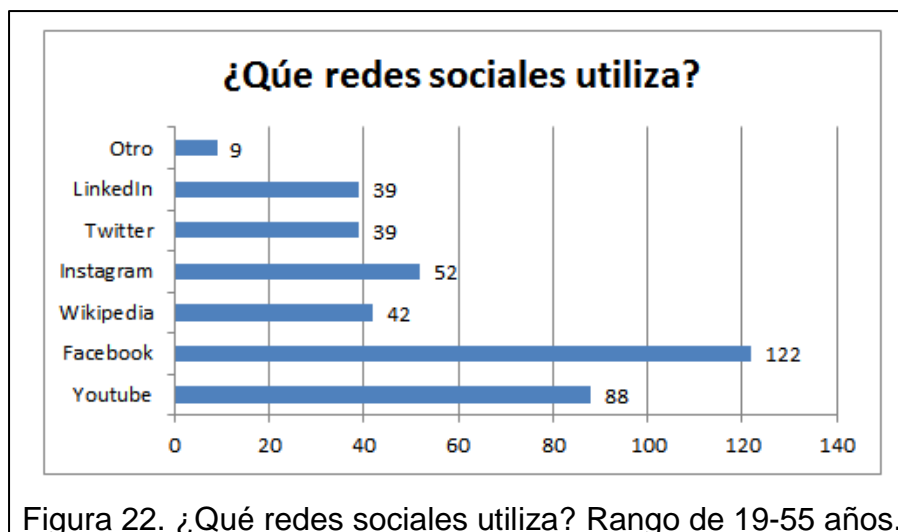


Tabla 22. ¿Qué redes sociales utiliza? Rango de 19-55 años.

Red Social	Total	Porcentaje
Youtube	88	67.7%
Facebook	122	93.8%
Wikipedia	42	32.3%
Instagram	52	40.0%
Twitter	39	30.0%
LinkedIn	39	30.0%
Otro	9	6.9%

De las 130 encuestas, el 88,5% utilizo el código al e-mail para la verificación de creación de la cuenta, el 37,7% el código al celular y el 4,6% ningún tipo de verificación.

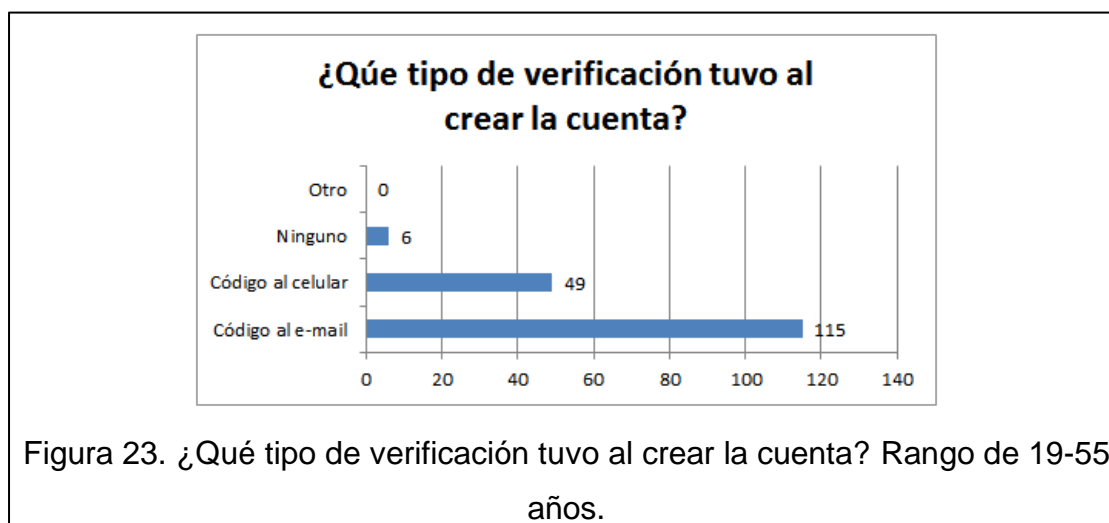


Tabla 23. ¿Qué tipo de verificación tuvo al crear la cuenta? Rango de 19-55 años.

Tipo de Verificación	Total	Porcentaje
Código al e-mail	115	88.5%
Código al celular	49	37.7%
Ninguno	6	4.6%
Otro	0	0.0%

De las 130 encuestas, el 67,7% publico datos reales en las redes sociales y el 32,3% no publico información real.

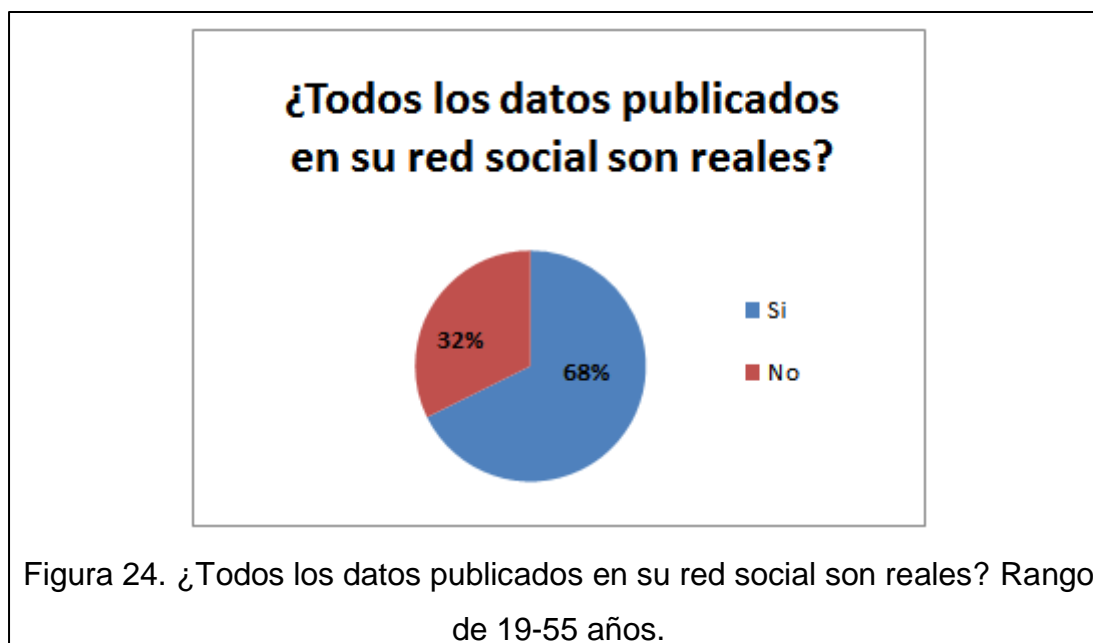


Tabla 24. ¿Todos los datos publicados en su red social son reales? Rango de 19-55 años.

¿Son los datos reales?	Total	Porcentaje
Si	88	67.7%
No	42	32.3%

De las 130 encuestas, el 73,1% considera su contraseña segura y el 26,9% no.

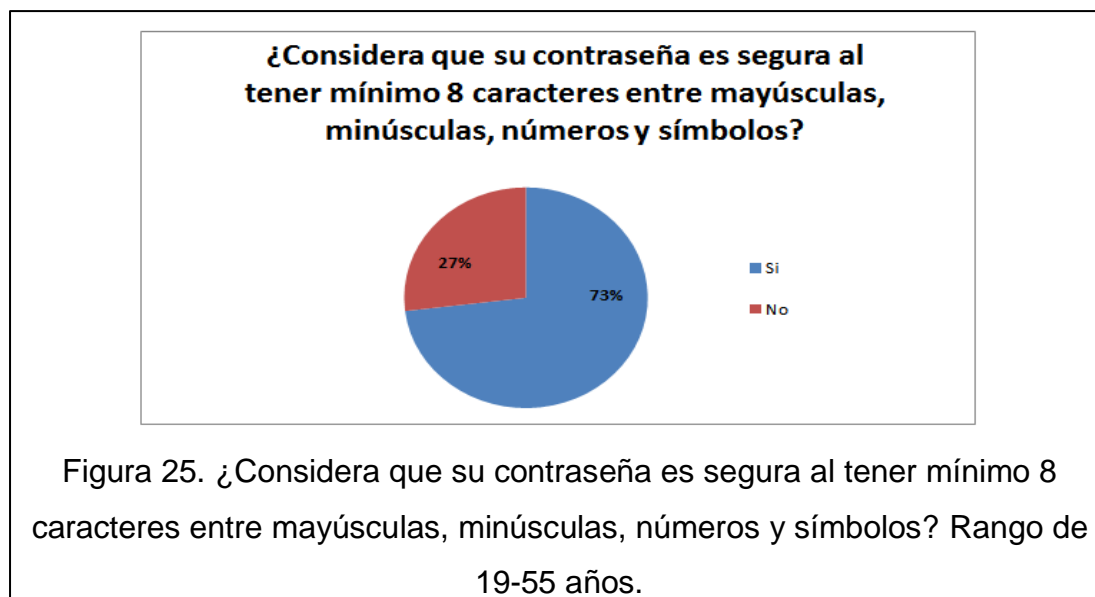


Tabla 25. ¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? Rango de 19-55 años.

¿Es segura la contraseña?	Total	Porcentaje
Si	95	73.1%
No	35	26.9%

De las 130 encuestas, el 41,5% nunca cambia la contraseña, el 30,0% cambia cada 6 meses y el 28,5% cambia anualmente.

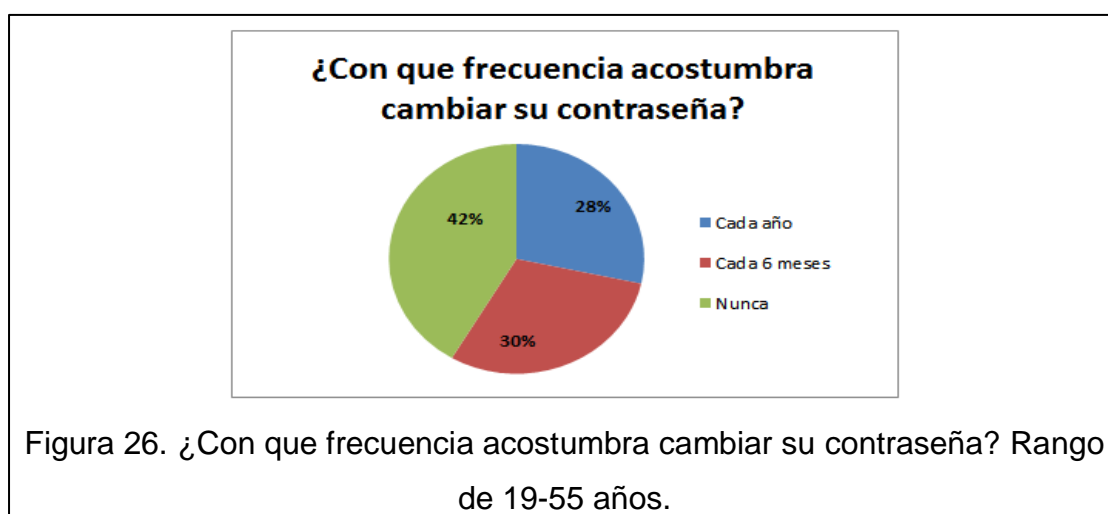


Tabla 26. ¿Con que frecuencia acostumbra cambiar su contraseña? Rango de 19-55 años.

Frecuencia del cambio de contraseña	Total	Porcentaje
Cada año	37	28.5%
Cada 6 meses	39	30.0%
Nunca	54	41.5%

De las 130 encuestas, el 4,6% desconoce la configuración de privacidad en las redes sociales, el 60,8% tiene para que sea visible solo para amigos, el 14,6% solo para amigos específicos y el 20% para todos.

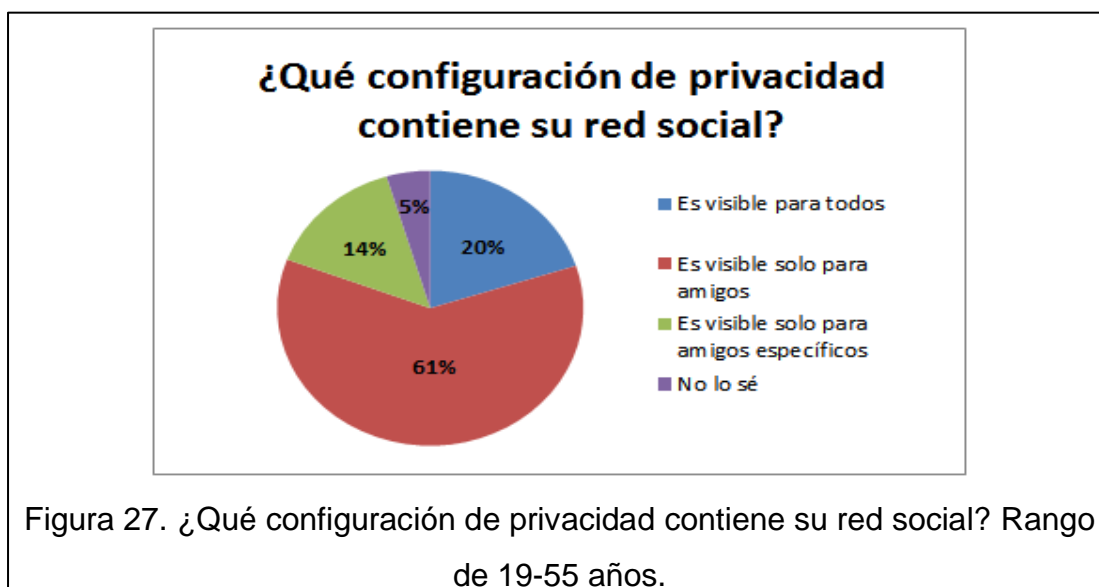


Tabla 27. ¿Qué configuración de privacidad contiene su red social? Rango de 19-55 años.

Configuración de privacidad	Total	Porcentaje
Es visible para todos	26	20.0%
Es visible solo para amigos	79	60.8%
Es visible solo para amigos específicos	19	14.6%
No lo sé	6	4.6%

De las 130 encuestas, el 80% tiene conocimiento de la información proporcionada a las aplicaciones asociadas y el 20% desconoce.

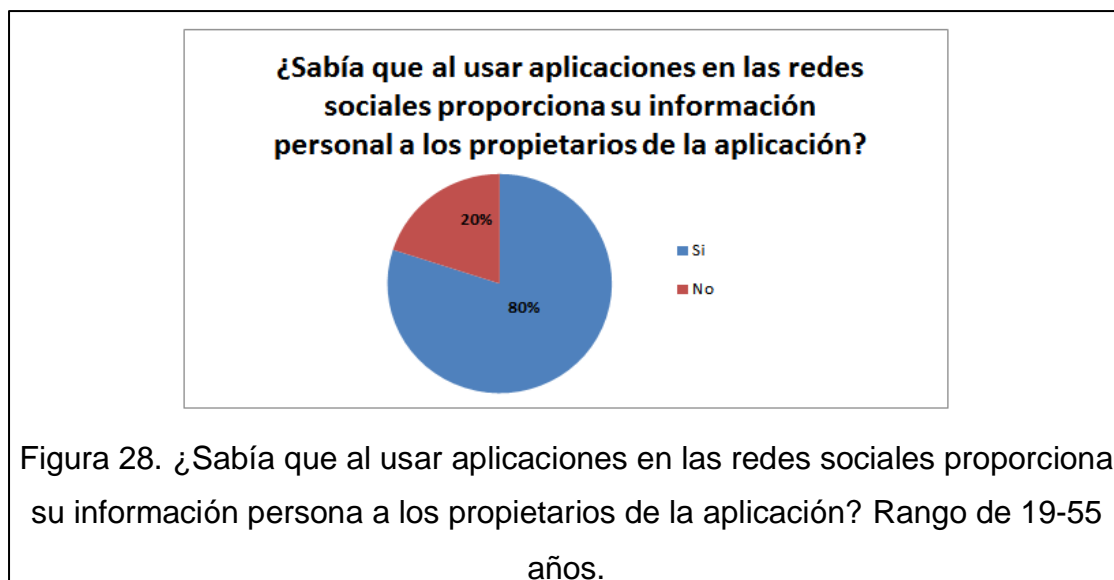


Tabla 28. ¿Sabía que al usar aplicaciones en las redes sociales proporciona su información persona a los propietarios de la aplicación? Rango de 19-55 años.

Conocimiento de la información proporcionada a las aplicaciones	Total	Porcentaje
Si	104	80.0%
No	26	20.0%

De las 130 encuestas, el 80% no ha sido amenazado o insultado a través de su red social y el 20% si lo ha sido.



Tabla 29. ¿Ha sido amenazado o insultado a través de su red social? Rango de 19-55 años.

Ha sido amenazado o insultado	Total	Porcentaje
Si	26	20.0%
No	104	80.0%

De las 130 encuestas, el 37,7% aceptado invitaciones de amistad de desconocidos y el 62,3% no aceptado.



Tabla 30. ¿Ha aceptado invitaciones de amistad de desconocidos? Rango de 19-55 años.

Aceptado invitaciones de amistad de desconocidos	Total	Porcentaje
Si	49	37.7%
No	81	62.3%

De las 130 encuestas, al 72,3% le preocupa el robo de información, al 66,9% la falsificación de identidad, al 33,1% el grooming, al 40,8% el acoso, al 53,8% el acceso sin autorización, al 53,8% la falta de privacidad, al 30% los crímenes contra el honor, al 3,1% nada y al 0,8% otro como por ejemplo el Spam.

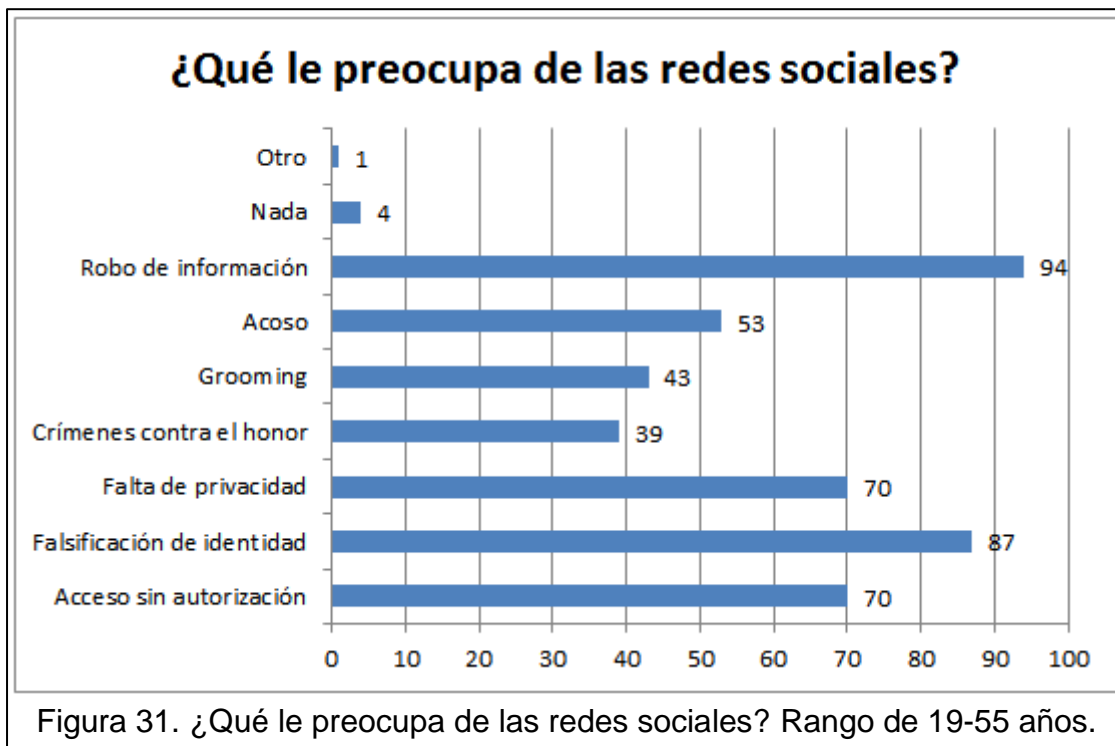


Tabla 31. ¿Qué le preocupa de las redes sociales? Rango de 19-55 años.

¿Qué le preocupa de las Redes Sociales	Total	Porcentaje
Acceso sin autorización	70	53.8%
Falsificación de identidad	87	66.9%
Falta de privacidad	70	53.8%
Crímenes contra el honor	39	30.0%
Grooming	43	33.1%
Acoso	53	40.8%
Robo de información	94	72.3%
Nada	4	3.1%
Otro	1	0.8%

2. Capítulo II. Marco Teórico.

2.1. Redes Sociales.

La tecnología ha utilizado las redes sociales como una herramienta para la comunicación entre las personas. Existen varios tipos de redes sociales, como las que se dedican al entretenimiento o a lo profesional, cada una tiene su propio objetivo.

2.1.1. Definición de Red Social.

Las redes sociales se forman a partir de las relaciones que tienen las personas con su familia, amigos, compañeros, conocidos, colegas, etc.

“Igual que para fabricar una red solo se necesitan cuerdas enlazadas entre sí mediante nudos, para construir una red social únicamente hacen falta dos elementos: las personas, que serían cada uno de los nudos (nodos) de la red, y las relaciones entre las personas, que serían los fragmentos de cuerda entre nudo y nudo.” (Gómez, 2010, p.5)

Con la tecnología web 2.0, se crearon herramientas que relacionan socialmente a las personas. Permitiendo la interacción entre ellas por medio de internet a pesar de la distancia. En la actualidad, la mayoría de estas se manejan como aplicaciones móviles con el fin de que sean más accesibles para el usuario.

Estas herramientas web permiten compartir gratuitamente fotografías, videos, música, frases, ideas, dedicatorias, conversaciones, hojas de vida, etc. Entre las redes sociales más conocidas están Facebook, Twitter, Youtube, LinkedIn etc.

“La Universidad de California publicó un largo artículo académico en el que definió en tres puntos cuándo a una red social de internet se le puede llamar así: 1) puede construirse un perfil personal, 2) pueden

establecerse conexiones (amistades) con otros usuarios y 3) puede consultarse quiénes son tus amigos y los amigos de tus amigos. La primera web que cumplió estos tres requisitos fue SixDegrees.com y apareció en 1998.” (Gómez, 2010, pp.16-17)

La estructura principal de estas herramientas web conocidas como “Redes Sociales” son similares. Sus elementos principales son los perfiles (personas), relaciones entre las personas (conexiones de amistad) y compartir algún tipo de información, según sea su temática.

2.1.2. Historia de la Web 2.0.

Los geeks, personas fascinadas por la tecnología, son los impulsores para que evolucione la tecnología y terminen apareciendo las redes sociales.

“En los años noventa, solo los geeks podían expresarse en internet mediante servidores que ofrecían información a través de hipervínculos. Después aparecieron los canales IRC, mejor conocidos como chats, pero no fue suficiente porque los usuarios querían dejar y saber las opiniones de las páginas web que visitaban.” (Gómez, 2010, p.13)

La web 2.0 crea una comunidad virtual en el que se genera contenido por parte de los usuarios permitiendo que los mismos interactúen.

“Actualmente existe la web 2.0, se basa en que existe una base de datos que almacena la “conversación” entre los usuarios. Estos pueden añadir, modificar y suprimir información de la base de datos, asociar nueva información y modificar la apariencia con la que se muestran dichos datos.” (Gómez, 2010, p.13)

La tecnología avanza de una manera rápida y la web no se podía quedar atrás creando la web 2.0. La asociación de las bases de datos y páginas web 2.0 son parte de la vida cotidiana de las personas que las usan, a tal punto que

después de nacer como páginas web se convirtieron en herramientas móviles por sus beneficios.

La web 3.0 añade metadatos semánticos a la web, llegando a ser vinculada estrechamente con la inteligencia artificial.

2.1.3. Tipos de Redes Sociales.

Las redes sociales se diferencian unas de otras por el segmento social al que se dedican, según el tipo tiene sus funcionalidades y temática.

Las redes sociales se categorizan en dos grupos que son las redes sociales directas e indirectas, llegando a tener subcategorías cada una.

2.1.3.1. Redes Sociales Directas.

Las redes sociales directas son dedicadas a grupos de usuarios que les gusta el mismo tipo de contenido, llegando a interactuar en igualdad de condiciones.

“Son redes sociales directas aquellas cuyos servicios prestados a través de Internet en los que existe una colaboración entre grupos de personas que comparten intereses en común y que, interactuando entre sí en igualdad de condiciones, pueden controlar la información que comparten.” (Urueña, Ferrari, Blanco, Valdecasa, 2011, p.13)

Para acceder a este tipo de red social es necesario tener un perfil en la misma. “El acceso a la información contenida en los perfiles suele estar condicionada por el grado de privacidad que dichos usuarios establezcan para los mismos.” (Urueña et al, 2011, p.13)

Al tener un perfil permite tener el control de la información que se comparte como por ejemplo elegir si es disponible para todos los usuarios, solo amigos o para solo una persona en específico.

Uno de los peligros que se corre es el de la falsificación de identidad, esto se debe a que pueden clonar el perfil de una persona, o hace contacto con alguien que está usando una cuenta falsa.

Las redes sociales directas se pueden clasificar por su finalidad, funcionamiento, grado de apertura y nivel de integración.

2.1.3.1.1. Según Finalidad.

Un usuario siempre tiene un objetivo para ingresar a una red social puede ser para uso personal por ejemplo entretenimiento como Facebook, Twitter, o uso profesional por ejemplo obtener contactos profesionales en LinkedIn. (Urueña et al, 2011, p.13)

2.1.3.1.1.1. De Ocio.

Este tipo de red social tiene como objetivo principal comunicar a los usuarios para potenciar las relaciones personales por medio de la publicación de videos, fotos, música, mensajes de texto, etc. Ejemplos de redes sociales de Ocio son Facebook, Twitter, Myspace, etc.

“El usuario busca fundamentalmente entretenimiento y mejorar sus relaciones personales a través de la interacción con otros usuarios ya sea mediante comentarios, comunicándose, o bien mediante el intercambio de información ya sea en soporte escrito o audiovisual.”
(Urueña et al, 2011, p.13)

2.1.3.1.1.2. De Uso Profesional.

Este tipo de red social tiene como objetivo principal establecer contacto profesional entre usuarios, generando contenido de uso laboral.

“El usuario busca principalmente promocionarse a nivel profesional, estar al día en su campo o especialidad e incrementar su agenda de contactos profesionales.” (Urueña et al, 2011, p.13)

Este tipo de red social cuenta con usuarios de una edad superior que de las redes sociales de ocio. Una de las redes sociales de uso profesional más conocida a nivel mundial es LinkedIn.

2.1.3.1.2. Según Modo de Funcionamiento.

Las funcionalidades de una red social son definidas según la temática y actividad a la que es dirigida la misma. Por ejemplo, publicar contenidos como YouTube, crear perfiles como Facebook, o de microblogging como Twitter

“Se tiene en cuenta el conjunto de procesos que estructuran las redes sociales y las orientan de forma particular hacia actividades concretas.” (Urueña et al, 2011, p.13)

2.1.3.1.2.1. De Contenidos.

El usuario crea y comparte el contenido a través de la red social, ejemplos de este tipo de red social es YouTube. Para ver dicho contenido no es necesario tener una cuenta en la red social pero para publicar contenido sí. Se puede compartir esta información en otras redes sociales como las de ocio, un ejemplo claro es que en Facebook se pueden compartir videos de Youtube.

“El usuario crea contenidos ya sea en soporte escrito o audiovisual que posteriormente distribuye y comparte a través de la red social con otros usuarios. Los contenidos publicados suelen estar sujetos a supervisión para comprobar la adecuación de los mismos y una vez validados pueden comentarse. Una característica interesante de este tipo de redes consiste en que la información suele estar disponible para todo usuario sin necesidad de tener un perfil creado.” (Urueña et al, 2011, pp.13-14)

2.1.3.1.2.2. Basada en Perfiles: Personales/Profesionales.

Los perfiles constan de los datos principales del usuario, información personal que desean compartir y una fotografía. Para este tipo de redes sociales es necesario tener una cuenta para poder tener un perfil. Un ejemplo de este tipo de red social es Facebook.

“Los perfiles consisten en fichas donde los usuarios aportan un conjunto de información de contenido personal y/o profesional que suele complementarse con una fotografía personal. En este tipo de redes suele ser obligatoria la creación de un perfil para poder ser usuario y poder emplear así todas las funciones de la red.” (Urueña et al, 2011, p.14)

2.1.3.1.2.3. Microblogging.

Este tipo de red social tiene principalmente un límite para compartir el contenido, su diseño permite ser más óptimo para dispositivos móviles. Por ejemplo, Twitter permite un máximo de 140 caracteres, llegando a ser fácil de ver el contenido compartido por los usuarios que siguen la cuenta.

“Están diseñadas para compartir y comentar pequeños paquetes de información (que suelen medirse en caracteres), pudiendo ser emitidos desde dispositivos fijos o móviles que facilitan el seguimiento activo de los mismos por parte de sus usuarios.” (Urueña et al, 2011, p.14)

2.1.3.1.3. Según Grado de Apertura.

Existen redes sociales con un grado muy alto de privacidad y seguridad, y otras como las redes sociales públicas que son accesibles para todos los usuarios de internet, por ejemplo YouTube.

“Se tiene en cuenta la capacidad de acceso a las mismas por cualquier usuario entendida ésta como el nivel de restricción que se aplica.”
(Urueña et al, 2011, p.14)

2.1.3.1.3.1. Públicas.

Un ejemplo de una red pública es YouTube, permite a todo usuario de internet ingresar para observar los videos subidos.

“Están abiertas a ser empleadas por cualquier tipo de usuario que cuente con un dispositivo de acceso a Internet sin necesidad de pertenecer a un grupo u organización concreta.” (Urueña et al, 2011, p.14)

2.1.3.1.3.2. Privadas.

Su principal objetivo es mantener la privacidad al máximo por lo que para acceder a ella se requiere ser parte de una organización o de un grupo en específico.

“Están cerradas a ser empleadas por cualquier tipo de usuario. Sólo se puede acceder a ellas por la pertenencia a un grupo específico u organización privada que suele hacerse cargo del coste de la misma.”
(Urueña et al, 2011, p.14)

2.1.3.1.4. Según Nivel de Integración.

Pueden ser de integración vertical con una temática definida u horizontal que es abierta a todo tipo de contenido.

“Se tiene en cuenta el nivel de afinidad, interés e involucración en materias o actividades de tipo, preferentemente, profesional.” (Urueña et al, 2011, p.14)

2.1.3.1.4.1. De integración Vertical.

Este tipo de red social está dirigida usuarios con una temática definida, puede ser de ocio, profesional o mixta. El grupo de usuarios es menor que la de integración horizontal.

“Su empleo suele estar acotado al uso por parte de un grupo de usuarios a los que aúna una misma formación, interés o pertenencia profesional.” (Urueña et al, 2011, p.14)

2.1.3.1.4.2. De integración Horizontal.

Este tipo de red social está dirigida a todo tipo de usuarios sin contar con una temática definida como Facebook.

“Su empleo no está acotado a un grupo de usuarios con intereses concretos en una materia.” (Urueña et al, 2011, p.14)

2.1.3.2. Redes Sociales Indirectas.

Las redes sociales indirectas tienen perfiles pero no necesariamente son expuestos a los demás. Son lugares en los que se publica contenido para que sea visto por otras personas que no necesariamente son amigos.

“Son redes sociales indirectas aquellas cuyos servicios prestados a través de Internet cuentan con usuarios que no suelen disponer de un perfil visible para todos existiendo un individuo o grupo que controla y

dirige la información o las discusiones en torno a un tema concreto.” (Urueña et al, 2011, p.16)

2.1.3.2.1. Foros.

Este tipo de red social contiene temas de interés común en el que se discute el mismo entre los diferentes usuarios. Existe una persona encargada de llevar y controlar dichas discusiones.

“Son servicios prestados a través de Internet concebidos, en un principio, para su empleo por parte de expertos dentro un área de conocimiento específico o como herramienta de reunión con carácter informativo. En los mismos se llevan a cabo intercambios de información, valoraciones y opiniones existiendo un cierto grado de bidireccionalidad en la medida en que puede responderse a una pregunta planteada o comentar lo expuesto por otro usuario.” (Urueña et al, 2011, p.16)

2.1.3.2.2. Blogs.

Este tipo de red social publica contenido de todo tipo de una forma cronológica. El dueño del blog es el encargado de supervisar su blog.

“Son servicios prestados a través de Internet que suelen contar con un elevado grado de actualización y donde suele existir una recopilación cronológica de uno o varios autores. Es frecuente la inclusión de enlaces en las anotaciones y suelen estar administrados por el mismo autor que los crea donde plasma aspectos que, a nivel personal, considera relevantes o de interés.” (Urueña et al, 2011, p.16)

2.1.4. Redes Sociales más Conocidas.

A nivel global en la herramienta de análisis Alexa Internet (s.f.) las redes sociales más utilizadas son Facebook, Youtube, Wikipedia, Twitter, LinkedIn e Instagram.

En Ecuador, según Alexa Internet (s.f.) las redes sociales más utilizadas son las mismas que a nivel global excepto LinkedIn que se encuentra en el puesto 46 del ranking de Ecuador.

“Una de las ventajas que tiene internet es que todo es cuantificable. Es muy difícil saber quién está viendo la tele o escuchando la radio, pero no sucede así con la red. Se sabe cuándo y dónde hacemos clic, de qué página procedemos, a qué página nos dirigimos y cuánto tiempo nos quedamos en ella. Las webs, a diferencia de las canciones de los 40 principales, se ordenan en función del uso de los usuarios y no en base a criterios comerciales.” (Gómez, 2010, pp. 21-22)

Facebook es una de las redes sociales más conocida a nivel mundial, ocupa siempre los primeros puestos en los rankings de herramientas de análisis como Alexa Internet y Social Networking Websites Review.

2.1.4.1. Facebook.

Consiste en tener un muro personal en el que el dueño del perfil o sus contactos comparten mensajes, fotos, videos, etc. El usuario tiene la posibilidad de elegir quien puede ver su muro y escribir en el mismo. Llegan notificaciones cuando un amigo ha comentado, compartido o gustado alguna publicación en el muro. “En concreto, tu muro no es más que una página web donde se visualiza todo lo que has ido escribiendo tú y todo lo que han escrito tus amigos.” (Gómez, 2010, p.23)

Facebook tiene aplicaciones asociadas a su web, dichas aplicaciones permiten ser más interactivos a los usuarios, por ejemplo cuando juegan en línea y desean compartir en su muro.

Facebook permite denunciar abusos o todo tipo de actos que vayan en contra de sus términos de uso, quien lo revisa y está pendiente de dichas denuncias son los administradores.

Con las páginas oficiales para fans se ha logrado disminuir increíblemente los perfiles falsos de artistas, en los que los adolescentes se hacían amigos, llegando exponerse a grandes peligros como por ejemplo el grooming. “Algunos de los famosos ya usan estas páginas como canales oficiales de comunicación con sus fans.” (Gómez, 2010, p.28)

2.1.4.2. YouTube.

Es el buscador de videos más popular en internet, teniendo canales de todo tipo de temática, por ejemplo maquillaje, bromas, música, baile, etc. Sobre todo el más usado por los artistas para compartir sus nuevos videos musicales, llegando a ser compartidos en otras redes sociales y convirtiéndose en grandes hits.

“Pese a las limitaciones en el tiempo (10 minutos máximo) y en el copyright (no se puede subir material protegido), los usuarios se las han ingeniado una y otra vez para burlar los controles y subir música, series de televisión y hasta películas enteras.” (Gómez, 2010, p.31)

Es importante tener un control de seguridad más proactivo para evitar que burlen los mismos, es grave dicho acontecimiento ya que en muchos de los casos pueden llegar a denigrar a terceras personas o cometer delitos por cuestiones de copyright, difamación, violencia, etc.

2.1.4.3. Wikipedia.

Wikipedia es una red social pública, se encuentra abierta para que todo usuario de internet pueda acceder a ella, su funcionamiento está basado en una enciclopedia libre. Wikipedia es una de las redes sociales más conocidas por tener contenido variado por ejemplo de ciencia, música, historia, etc.

2.1.4.4. Twitter.

Twitter dispone del timeline en el cual se puede ir visualizando las publicaciones de las personas que se sigue, permite compartir las publicaciones a las que se da el nombre de retweet.

“Un blog no es más que una página web con el contenido ordenado cronológicamente. Imagínate que tienes un blog con una peculiar limitación: cualquier cosa que escribas no puede superar los 140 caracteres (que es lo que cabe en un SMS). Twitter ofrece a sus usuarios precisamente eso: la posibilidad de publicar y leer pequeños mensajes, a los que se denomina *tweets*. Esos tweets se almacenan en tu perfil personal, donde pueden ser consultados por tus lectores (también llamados *followers* o seguidores). Al ser este funcionamiento similar al de una red de blogs, muchos han coincidido en otorgar a Twitter el nombre de “servicio de microblogging”. ” (Gómez, 2010, p.41)

Al tener un límite de caracteres se ingeniaron para crear el hashtag en el que se escribe de forma abreviada lo que se desea decir, así también aparecieron los cortadores de URL que permite publicar el hipervínculo sin toda su extensión.

Esta red social es usada principalmente por los artistas, así llegan a medir su popularidad, ya que mientras más seguidores tienen más famosos son.

2.1.4.5. LinkedIn.

Es una red social de enfoque profesional. Consta de un perfil que equivale a la hoja de vida, como experiencia laboral, últimas actividades profesionales, etc.

Permite agregar a los amigos o conocidos a su red para compartir sus logros profesionales. Esta red social no permite compartir, videos, fotografías y música. Es netamente orientado al ámbito profesional.

2.1.4.6. Instagram.

Esta red social es dedicada a fotografías e imágenes. Los usuarios acceden mediante un perfil que contiene una galería de fotos, pueden tomar, subir, compartir y etiquetar amigos en las imágenes. Así mismo permite dar likes y comentar.

Tiene la particularidad que tiene conexión con Facebook, Twitter, WhatsApp, etc. Por lo que al subir la imagen permite publicar en las otras redes sociales.

Lo importante de Instagram es que no permite guardar las fotos de los demás, lo cual le da un punto de seguridad y confianza al usuario. Claro que hoy en día se puede capturar la pantalla y recortar la imagen pero ya complica más el proceso.

2.1.4.7. Google+.

Google+ es la red social de Google, tiene la particularidad de permitir crear círculos ya sea de familia, trabajo, amistad, etc. Llegando a ser grupos definidos por el mismo usuario para cuando desea publicar algo específico para uno de ellos.

Igual que Facebook contiene un muro en el que se comparte videos, comentarios, imágenes, etc. Llegando a ser su rival directo para las demás redes sociales.

Para formar parte de esta red social es indispensable tener una cuenta Gmail. No llega a ser tan segura porque se pueden crear varias cuentas Gmail falsas y por lo mismo varias cuentas Google+.

2.1.5. Diferencias de las Redes Sociales.

Las diferencias de las redes sociales se pueden basar en el tipo de red social, popularidad, si usa friending o following, control de privacidad en la información, etc.

2.1.5.1. Matriz de Tipos de Redes Sociales.

Una red social puede tener más de un enfoque, por ejemplo Facebook es una red social de ocio y también de uso profesional según sea el objetivo del usuario, es una red social pública, de integración horizontal y basada en perfiles.

Tabla 32. Matriz de tipos de redes sociales.

	Según finalidad		Según modo de funcionamiento			Según grado de apertura		Según nivel de integración	
	De ocio	De uso profesional	De contenidos	Basadas en perfiles	Microblogging	Públicas	Privadas	De integración vertical	De integración horizontal
Facebook	X	X		X		X			X
Youtube	X	X	X	X		X			X
Wikipedia		X	X			X			X
Twitter	X	X		X	X	X			X
LinkedIn		X		X		X		X	
Instagram	X		X	X		X			X
Google+	X	X		X		X			X
Spotify	X		X	X		X			X

Adaptado de Urueña et al, 2011, p.15

2.1.5.2. Matriz de Diferencias de Redes Sociales.

Las diferencias de las redes sociales se pueden basar en las funciones que tiene. Facebook es la red social más completa en cuanto a las funcionalidades que proporciona a los usuarios.

Tabla 33. Matriz de diferencias de redes sociales.

	Facebook	Youtube	Twitter	LinkedIn	Instagram
Tipo de contenido.	Variado	Videos	Variado	Texto	Fotos
Perfil	X	X	X	X	X
Friending (Amigos).	X			X	
Following (Seguir).	X	X	X		X
Modificar estados.	X	X	X	X	X
Control de privacidad	X	X	X	X	X
Enviar mensaje privado.	X	X	X	X	X
Boton "Me gusta"	X	X	X	X	X
Grupos	X			X	
Chat	X				
Video Chat	X				
Ubicación.	X	X	X		X

Nota: a. La matriz de diferencias de redes sociales se basa en las funciones principales que proporcionan las redes sociales más conocidas, por ejemplo indicar que le gusta una publicación al usuario.

2.2. Seguridad Cibernética.

Con el tiempo y el avance de las amenazas cibernéticas es necesario desarrollar nuevas protecciones para controlar dichas amenazas. La seguridad cibernética tiene que estar en constante actualización por la misma razón.

“A medida que evoluciona el entorno de las amenazas cibernéticas, también debe desarrollarse la protección frente a dichas amenazas. Con la aparición de los ataques dirigidos y las amenazas persistentes avanzadas, queda claro que es necesario utilizar un nuevo enfoque de seguridad cibernética. Las técnicas tradicionales simplemente ya no resultan adecuadas para proteger los datos frente a los ciberataques.”
(Trend Micro Incorporated, s.f.)

2.2.1. Delitos Cibernéticos.

Un delito informático es la acción que daña o perjudica a una persona, empresa o entidad por medio de las vías informáticas.

“El delito cibernético es una forma emergente de la delincuencia transnacional y uno de los de más rápido crecimiento. A medida que Internet se ha convertido en una parte casi esencial de nuestras vidas, suministrando información y comunicación en todo el mundo, los delincuentes le han sacado provecho. Con unos dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal que, a sabiendas o inconscientemente, guardamos en línea. Las amenazas a la seguridad en Internet se han disparado de forma espectacular en los últimos años, y el delito cibernético afecta ahora a más de 431 millones de víctimas adultas a nivel mundial.” (Organización de las Naciones Unidas (ONU), 2015, párr.1)

La forma más sencilla de realizar un delito cibernético es con el uso de la ingeniería social y malware avanzados. El usuario llega a ser el más vulnerable de todos los componentes de un sistema cibernético porque es de fácil manipulación.

Las redes sociales son vulnerables a los delitos informáticos por la interacción existente, por medio de la tecnología y por la información sensible que se deposita en la misma. La vulnerabilidad se da por la falta de prevención y manejo de la información. Así como incrementan los usuarios en las redes sociales también incrementan los delincuentes que lo utilizan para realizar sus fechorías, las usan por la información y datos que se proporciona llegando a dar exceso de confianza y por los errores que cometen los usuarios.

“En la actualidad el mal uso, por desconocimiento y el abuso de las múltiples redes sociales, y sobre todo el uso por personas cada vez más jóvenes, y el desconocimiento de la vulnerabilidad a través de estos mecanismos, muchas veces, pensando que únicamente se llega al entorno de amistades autorizado, hace y propicia que otras personas, mal intencionadas hagan uso de la privacidad y contenidos de las

mismas para fines diferentes, en muchos casos de carácter delictivo.”
(Tu abogado defensor, s.f.)

Existen varios delitos informáticos que se realizan en las redes sociales, entre las más comunes está el cyberbullying, falsificación de identidad, pornografía infantil, fraude, robo y daño de información.

2.2.1.1. Cyberbullying.

Es el acoso por medio del ciberespacio entre dos menores de edad. Las intimidaciones y agresiones son realizadas por medio de las redes sociales. El principal objetivo es humillar al acosado, llegando a atentar contra su moral e integridad. (stopbullying.gov, s.f.)

2.2.1.2. Falsificación de Identidad.

Es la creación de perfiles falsos, con el fin de engañar ser personas reales o empresas para manipular, acosar y atentar contra la dignidad e integridad de los usuarios. La suplantación de identidad de una persona se utiliza para realizar acciones delictivas, llegando a denigrar a la persona que es dueña de la identidad. (Rodríguez, 2011, p.16)

2.2.1.3. Grooming.

Los pedófilos utilizan las redes sociales como medio para encontrar y engañar a los menores de edad, consiguiendo intercambiar la información que contiene la pornografía infantil. Los pedófilos utilizan la falsificación de identidad de menores de edad para conseguir la confianza y así ser más fácil obtener las fotografías y videos. (Rodríguez, 2011, p.17)

2.2.1.4. Fraude informático.

Los fraudes informáticos se dan en las redes sociales como medio para engañar y obtener datos sensibles de los usuarios. El Phishing se basa en que el estafador se hace pasar por una persona o empresa oficial, el cual tiene comunicación con el usuario para ofrecer servicios o productos con la finalidad de obtener la información sensible, el delincuente crea una cuenta falsa con los datos del usuario y gasta su crédito. Los fraudes generan que el usuario se quede sin acceso a sus cuentas y pérdidas económicas. (Rodríguez, 2011, pp.17-18)

2.2.1.5. Robo de Información.

El robo de información se da por la falta de cuidado del usuario al compartir la información en las redes sociales. Toda información como correos electrónicos, números de cuenta, fotos, etc. que se brinda en las redes sociales sirven a los delincuentes para secuestros, extorsiones, robos, etc. (Rodríguez, 2011, p.18)

2.3. Red Social Facebook.

Facebook es una de las redes sociales más populares a nivel mundial, ocupando los primeros puestos en el ranking de Ecuador en la herramienta de Alexa. Es una red social de ocio que también es utilizada para el ámbito profesional en ciertos casos, es pública, basada en perfiles y de integración horizontal

Del análisis realizado a las redes sociales se observó que Facebook es la red social más completa en cuanto a las funcionalidades que proporciona a los usuarios. El tipo de contenido es variado como videos, imágenes, texto, etc. Tiene las dos funcionalidades para relacionar a los usuarios que son las de seguir (following) o ser amigos (friending), permite modificar las publicaciones,

controlar la privacidad y enviar mensajes privados. También contiene el botón me gusta, mensajería instantánea, video chat y ubicación.

2.3.1. Concepto de Facebook.

Facebook es utilizada principalmente para relacionar a los usuarios con su familia, amigos, conocidos, etc. Y consiste principalmente en el perfil de usuario, contactos y su respectivo muro.

“En Facebook y el resto de redes sociales ese carnet de identidad lo construimos nosotros mismos, y se llama perfil de usuario (o simplemente perfil). Hay quien pone hasta el color de sus calzoncillos y hay quien solo da algunos datos. Hay quien siembra el perfil de mentiras y exageraciones para impresionar (fantasmas hay en todos los sitios, también en Facebook) y hay quien se ciñe más a la realidad. Una parte muy importante del perfil es la imagen asociada, también denominada “avatar”. La mayoría de personas optan por su propia cara, aunque no falta quien se pone una foto del perro, del coche e incluso de un peluche.” (Gómez, 2010, p.24)

Los usuarios pueden compartir contenido como fotografías, videos, imágenes, ideas, entre otras cosas con sus contactos. También tiene la posibilidad de elegir quien puede ver su muro y escribir en el mismo. Cada vez que un contacto comenta, comparte o le gusta una publicación que compartió recibe la notificación correspondiente.

Facebook es un software gratuito, que se encuentra en versión de página web y móvil, lo que hace más accesible el uso a los usuarios. La red social cuenta con aplicaciones asociadas lo que permite ser una herramienta más interactiva con los usuarios, por ejemplo los juegos que se conectan con Facebook permite ver las posiciones de los contactos en el mismo juego.

2.3.2. Historia de Facebook.

En la conferencia de la Universidad de Navarra, Mark Zuckerberg, fundador de Facebook, relato la historia de la red social.

“Se remonta a febrero de 2004, a sus años de estudiante en *Harvard*. Allí creó junto con dos colegas una versión digital e interactiva de *Facebook*, una especie de anuario de estudiantes que les permitía conocerse. Cuenta que construyó la primera versión en sólo dos semanas y en poco tiempo tuvo un gran éxito. Su web se extendió primero por todas las facultades de *Harvard* y después por el resto de las universidades norteamericanas, llegando a alcanzar en poco tiempo dos millones de usuarios. Según Zuckerberg este momento de la empresa fue crucial ya que implementaron la mayor parte de las aplicaciones y utilidades que aún hoy se siguen empleando.” (Torres, 2008, p.682)

La red social logro tener éxito porque comenzó con las funciones básicas y conforme iban avanzando y teniendo éxito, acoplaban las funciones más complejas, entre ellas las de seguridad del usuario.

“A partir del año 2006 comenzaron a introducir novedades realmente destacadas. Entre ellas Zuckerberg citó el ya comentado *news feed* que definió como una de las piezas clave de su producto gracias a los mecanismos de retroalimentación que genera entre los usuarios. Continuó hablando del siguiente movimiento, que consistió en permitir la entrada a todo el mundo en *Facebook*, dejando de ser una red exclusiva de estudiantes, y la apertura de su código para facilitar la interacción con otras aplicaciones. El último hito que subrayó en esta cronología del producto fue el lanzamiento de la nueva interfaz y su traducción a otros idiomas, un total de 28, entre ellos el español.” (Torres, 2008, p.683.)

Facebook creció de una forma rápida en cuanto a número de usuarios y funciones, llegando a obtener los primeros puestos en los rankings de la web.

Mark Zuckerberg demostró que el emprendimiento y esfuerzo de unos estudiantes universitarios puede causar cambios impactantes en la sociedad.

2.3.3. Controles Actuales de Seguridad del Usuario en Facebook.

Facebook contrata a 5 organizaciones que les proporcionan asesoramiento de seguridad social, dichas organizaciones conforman el consejo de seguridad de Facebook.

Algunos controles de seguridad que Facebook posee son reactivas debido a que usan el método de reporte de abusos, estos procesos se pueden apreciar en las normas comunitarias que se encuentran en su página web. Quien lo revisa y está pendiente de dichas denuncias son los administradores.

2.3.3.1. Consejo de Seguridad de Facebook.

En la página de ayuda de Facebook en la sección de Privacidad y Seguridad, explica sobre el consejo asesor de seguridad que la red social utiliza. “El consejo asesor de seguridad de Facebook integra cinco de las principales organizaciones de Norteamérica y Europa que se ocupan de la seguridad en internet. Estas organizaciones asesoran a Facebook en cuestiones relacionadas con la seguridad de la red.” (Facebook, s.f., párr.1)

Entre las organizaciones que conforman el consejo de seguridad de Facebook están Childnet International, Connect Safely y Family Online Safety Institute (FOSI), las cuales son dedicadas a la seguridad de los menores de edad en internet y National Network to End Domestic Violence (NNEDV) y WiredSafety que son especializadas en el acoso cibernético. (Facebook, s.f.)

Dichas organizaciones asesoran a la red social Facebook en la creación y actualización de sus políticas, normas comunitarias y en los casos que son reportados como abusos.

2.3.3.2. Condiciones y Políticas de Facebook.

La seguridad para Facebook parte desde su política de datos, normas comunitarias, declaración de derechos y responsabilidades en las que solicitan el compromiso por parte del usuario para no incumplirlas. En caso de no cumplir con las mismas pueden ser eliminados totalmente de la red social.

2.3.3.2.1. Política de Datos.

La política de datos que se encuentra en Facebook (s.f.), tiene el fin de que los usuarios comprendan de qué manera es usada, recopilada y compartida la información que proporcionan en la red social.

Así mismo como el usuario puede administrar o eliminar su información, como responde la red social a los requerimientos legales y cómo funcionan sus servicios a nivel mundial.

La información que recopila la red social es la actividad e información que proporciona el usuario, contenido que otros usuarios proporcionan, grupos con los que interactúa el usuario, sincronización de datos como la agenda de contactos, información de aplicaciones como juegos, información de socios externos como anunciantes, empresas de Facebook como Instagram y transacciones financieras como número de tarjeta, cuentas, autenticación, facturación, etc. También recopila los datos del dispositivo como IP, sistema operativo, idioma, zona horaria, etc. (Facebook, s.f.)

La información que se recopila es usada para mejorar y desarrollar nuevos servicios de una forma personalizada. También para la comunicación con el usuario, mostrar y medir el sistema de publicidad en anuncios y servicios.

Es utilizada en especial para fomentar la seguridad y protección, como se encuentra en la política de datos de Facebook.

“La información que tenemos nos ayuda a verificar cuentas y actividades, así como a fomentar la seguridad y la protección tanto dentro de nuestros servicios como fuera de ellos, por ejemplo, mediante la investigación de actividades sospechosas o de infracciones de nuestras condiciones o políticas. Nos esforzamos por proteger tu cuenta, para lo cual recurrimos a equipos de ingenieros, sistemas automatizados y tecnología avanzada, como el cifrado y el aprendizaje automático. Además, proporcionamos herramientas de seguridad fáciles de usar que incorporan un nivel adicional de protección a tu cuenta.” (Facebook, s.f.)

La información es compartida con las personas que se comunica y comparte contenido el usuario, terceras personas que ven el contenido publicado de familiares, amigos y conocidos. Es compartida con las aplicaciones, sitios web y servicios de terceras personas que utilizan los servicios de Facebook, así mismo es compartida con las empresas de Facebook, socios y clientes. En caso de existir un nuevo propietario se transferirá la información

Para recopilar, usar y compartir la información Facebook utiliza el marco Safe Harbor, por lo que la red social puede compartir la información con su grupo de empresas o terceros. (Facebook, s.f.)

Facebook puede acceder a la información, conservar y compartir en casos de requerimiento legal, fraudes, protección e investigaciones. (Facebook, s.f.)

El usuario puede administrar o eliminar todo el contenido que comparte en Facebook. La cuenta puede ser eliminada o desactivada en cualquier momento, al eliminar se borra toda la información proporcionada por el usuario. Facebook conserva por un año aproximadamente los datos de las cuentas inhabilitadas por incumplir las condiciones. (Facebook, s.f.)

2.3.3.2.2. Declaración de Derechos y Responsabilidades.

La declaración de derechos y responsabilidades es el documento en el que se encuentran las condiciones de servicio entre la red social y los usuarios, marcas, productos y servicios.

La declaración de derechos y responsabilidades deja claro que el usuario es el responsable absoluto de la privacidad y del contenido que comparte con otros usuarios.

En cuanto a la seguridad, en la declaración de derechos y responsabilidades Facebook (s.f., párr.7) solicita los compromisos por parte de sus usuarios de la siguiente forma:

1. No proporcionarás información personal falsa en Facebook, ni crearás una cuenta para otras personas sin su autorización.
2. No crearás más de una cuenta personal.
3. Si inhabilitamos tu cuenta, no crearás otra sin nuestro permiso.
4. No utilizarás tu biografía personal para tu propio beneficio comercial, sino que para ello te servirás de una página de Facebook.
5. No utilizarás Facebook si eres menor de 13 años.
6. No utilizarás Facebook si fuiste declarado culpable de un delito sexual.
7. Mantendrás la información de contacto exacta y actualizada.
8. No compartirás tu contraseña (o, en el caso de los desarrolladores, tu clave secreta), no dejarás que otra persona acceda a tu cuenta, ni harás nada que pueda poner en peligro la seguridad de tu cuenta.
9. No transferirás la cuenta (incluida cualquier página o aplicación que administres) a nadie sin nuestro consentimiento previo por escrito.
10. Si seleccionas un nombre de usuario o identificador similar para tu cuenta o página, nos reservamos el derecho de eliminarlo o reclamarlo si lo consideramos oportuno (por ejemplo, si el propietario de una marca comercial se queja por un nombre de usuario que no esté estrechamente relacionado con el nombre real del usuario).

2.3.3.2.3. Normas Comunitarias.

Facebook cuenta con las Normas Comunitarias, estas son políticas para saber que se puede reportar para ser eliminado. Pueden existir cosas que desagraden pero que no infringen las normas.

Las normas comunitarias se clasifican en ayudar a estar seguros, fomentar el comportamiento respetuoso, proteger las cuentas e información personal y a proteger la propiedad intelectual.

Todo el contenido de las normas comunitarias se puede observar en la página de Facebook (s.f.) en community standards.

2.3.3.2.3.1. Ayudar a estar Seguros.

En cuanto a seguridad social Facebook tiene sus procedimientos sobre amenazas directas, autolesiones, organizaciones peligrosas, acoso y/o intimidación, ataques a personajes públicos, actividades delictivas, explotación y violencia sexual y artículos regulados.

En los casos que se considera que existe riesgo, Facebook toma las medidas de eliminar el contenido, inhabilitar las cuentas y notificar a las autoridades locales. (Facebook, s.f.)

En los casos de las amenazas directas en Facebook, proceden a revisar minuciosamente los reportes intimidatorios para identificar las amenazas graves. Una vez detectadas las amenazas que son creíbles de daños físicos a personas se procede a eliminar las mismas, ya sea perfiles o contenido. (Facebook, s.f.)

Para determinar si es un riesgo o no, se toma en cuenta factores como la ubicación geográfica de la persona, son más propensas a ser creíbles las amenazas a personas que viven en regiones violentas. (Facebook, s.f.)

Facebook no permite promoción de las conductas suicidas, elimina todo contenido que identifique a las víctimas con la intención de atacarlos. Sin embargo, si permite compartir información sobre dichas conductas. (Facebook, s.f.)

Facebook no permite tener perfiles a las organizaciones peligrosas que estén vinculadas a las actividades terroristas o delictivas, igualmente se elimina todo contenido que apoye o justifique a dichos grupos o líderes de las organizaciones. (Facebook, s.f.)

Facebook elimina todo contenido que parezca acoso o intimidación a personas particulares. Tan solo la intención de avergonzarlos ya es considerado para ser eliminado. (Facebook, s.f.)

Facebook permite debates abiertos o críticos de personas públicas. Sin embargo, elimina todo contenido que sea con lenguaje ofensivo o amenazas a los mismos. (Facebook, s.f.)

En los casos de los reportes de actividades delictivas que tienen como consecuencia daños físicos o económicos a personas o empresas, Facebook procede a notificar a las autoridades locales lo sucedido. (Facebook, s.f.)

Facebook elimina todo contenido que amenace o promueva la explotación y violencia sexual. Eso quiere decir que elimina fotos y videos que muestren contenido sexual de menores, así mismo contenido que se comparte por venganza o sin el consentimiento de las personas que aparecen en ellas, amenazas y ofertas de servicios sexuales como prostitución, masajes y grabaciones sexuales. (Facebook, s.f.)

La red social no permite el uso de las herramientas de pago de Facebook para comprar o vender artículos regulados como armas de fuego, alcohol, tabaco o productos para adultos, así mismo deben contar con autorización para comercializar medicamentos con receta médica. Se puede promocionar siempre y cuando se cumpla la legislación vigente y correspondiente, en especial al determinar al público que va dirigido el contenido. (Facebook, s.f.)

2.3.3.2.3.2. Fomentar el Comportamiento Respetuoso.

Facebook pone énfasis en fomentar el comportamiento respetuoso. La mayoría de usuarios usa la red social para compartir sus experiencias y hacer tomar conciencia a los demás, aun así esto no significa que todos piensen igual, por lo que llega a existir una gran diversidad de opiniones generando conversaciones o debates de temas de gran impacto en la sociedad. Facebook para mantener el equilibrio sobre dichos asuntos llega a eliminar el contenido sensible o limita el público que puede visualizarlo.

Existen personas que comparten desnudos con un fin determinado, como campañas de concientización o proyectos artísticos. Por lo cual Facebook restringe dicho contenido para que determinados sectores sociales sensibles no se sientan incómodos por motivo de cultura o edad. (Facebook, s.f.)

La red social cuenta con políticas que se aplican a los equipos para que la revisión del contenido sea más fácil y uniforme. Por lo que se eliminan fotografías de relaciones sexuales o en el que se muestren partes íntimas como genitales, glúteos, senos, etc. Sin embargo, permite fotos de mujeres amamantando, pechos con cicatrices de mastectomía, pinturas o esculturas en las que se muestren figuras desnudas. (Facebook, s.f.)

Facebook elimina todo contenido que ataque a las personas por raza, grupo étnico, nacionalidad, religión, orientación sexual, género, discapacidades, o enfermedades. Se solicita a las personas que tienen páginas las asocien a su perfil de Facebook, así se obtiene una responsabilidad mayor por parte de los usuarios al publicar contenido en sus páginas. (Facebook, s.f.)

2.3.3.2.3.3. Proteger Cuentas e Información Personal.

Facebook tiene como objetivo proteger las cuentas y la información personal que se deposita en el mismo.

Un requisito que tiene Facebook es el de usar identidades reales para tener un entorno más seguro. Así se logra tener una mayor responsabilidad por parte de los usuarios. La red social elimina los perfiles que se hacen pasar por otras personas o si llega a tener más de un perfil una misma persona. (Facebook, s.f.)

Para mascotas, negocios, instituciones, productos, artistas o películas, se debe crear una página en lugar de un perfil. Con las páginas se permite realizar actividades comerciales. “Algunos de los famosos ya usan estas páginas como canales oficiales de comunicación con sus fans.” (Gómez, 2010, p. 28)

Con las páginas oficiales para fans se ha logrado disminuir increíblemente los perfiles falsos de artistas, en los que los adolescentes se hacían amigos, llegando exponerse a grandes peligros como por ejemplo el grooming.



Al fallecer una persona que tiene cuenta en Facebook se tienen dos alternativas, convertir en conmemorativa la cuenta o eliminar la misma. Hay que notificar a la red social por medio de un documento en el que se acredite el fallecimiento de la persona. (Facebook, s.f.)

2.3.3.2.3.4. Proteger la Propiedad Intelectual.

La red social Facebook permite compartir todo contenido si eres el propietario o tienes la autorización pertinente para realizarlo. Es importante siempre respetar los derechos de autor, marcas comerciales y derechos de propiedad intelectual. (Facebook, s.f.)

Las personas que posan para una foto aceptan tácitamente a la persona que la toma como dueño de esta, en consecuencia puede publicarla, en caso de que la foto sea tomada sin que el fotografiado se diera cuenta es necesario una autorización para publicar la misma. (Facebook, s.f.)

2.3.3.3. Tecnologías Utilizadas para la Seguridad de Facebook.

Facebook usa tecnologías como cookies, etiquetas pixel, identificador de dispositivos y almacenamiento local para la seguridad del usuario y servicios de la red social.

En la página de ayuda de Facebook en la sección de privacidad explica para que y como se utilizan dichas tecnologías.

“Las cookies son pequeños archivos que colocan el sitio web o la aplicación que usas, o el anuncio que ves, en tu navegador o dispositivo. Las etiquetas píxel (que también se denominan GIF transparentes, balizas web o píxeles) son pequeños bloques de código en las páginas web o aplicaciones que les permiten realizar acciones, como leer o colocar cookies y transmitir información a Facebook o a nuestros socios. La conexión resultante puede incluir diferentes datos, como la dirección IP de un dispositivo, la fecha y hora en que una persona vio el píxel, un identificador asociado al navegador o dispositivo, y el tipo de navegador que se usó. El almacenamiento local es una tecnología estándar del sector que permite a un sitio web o una aplicación guardar datos en la computadora, el teléfono celular u otro dispositivo de una persona y, luego, recuperarlos. Algunos ejemplos son el almacenamiento local y el

almacenamiento en caché en HTML5 o en dispositivos.” (Facebook, s.f., párr.4)

2.3.3.3.1. Cookies.

Las cookies son almacenadas en el cliente para responder en la cabecera de cada petición al servidor, por lo que son constantes es preferible que sean de pequeño tamaño para no interferir en el rendimiento. Las cookies son utilizadas principalmente en los inicios de sesión cuando se requiere que al cerrar la ventana se cierre sesión automáticamente. (Facebook, s.f.)

Se puede observar que al autenticar una cuenta se crean 7 cookies entre ellas el identificador del usuario.



Figura 33. Cookies en Facebook sin Iniciar Sesión.




2.3.3.3.2. Almacenamiento Local.

El almacenamiento local es utilizado para guardar una mayor cantidad de datos en el cliente, comúnmente de 5MB a 10MB. Los datos que se guardan no son enviados al servidor por lo que es un almacenamiento persistente y no transitorio como las cookies. En el almacenamiento local se guardan los datos cuando se selecciona no cerrar sesión, por lo que almacena dicha sesión y así se cierre el navegador no se cierra la sesión. (Facebook, s.f.)



2.3.3.3.3. Etiquetas Pixel.

En Facebook las etiquetas pixeles son mayormente usadas por los anunciantes, para medir los resultados de los anuncios de Facebook. El monitoreo de las conversiones permite medir el retorno de la inversión. Por lo que el pixel de conversión es el código que Facebook proporciona para que sea ubicado en cualquier página del sitio web después de la acción seleccionada, por ejemplo en la página de pago. Con lo cual cuando el usuario pase por el anuncio de Facebook se active el pixel y el recorrido sea rastreado. Lo utilizan para identificar si el anuncio derivó en venta real o en fracaso. (Facebook, s.f.)



Michu Ely Benítez Dávila needs your help installing the Facebook pixel on their website. This code lets you track conversions and show ads to people based on their activity on your website.

Instrucciones

Copy the code below and paste it between the <head> and </head> in your website code. You can add standard events from the list below to track specific actions people take on your website.

To confirm installation, please use the [Pixel Helper](#). Learn more in the [Help Center](#).

Facebook Pixel Code

```

<!-- Facebook Pixel Code -->
<script>
!function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;
t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','//connect.facebook.net/en_US/fbevents.js');

fbq('init', '1036105289775383');
fbq('track', "PageView");</script>
<noscript></noscript>
<!-- End Facebook Pixel Code -->

```

Figura 36. Código Fuente de un Pixel de Facebook.

2.4. Metodología de Análisis de Riesgos.

Una metodología de análisis de riesgos contempla el conjunto de procedimientos a realizar para analizar los riesgos, con el objetivo de descubrir los riesgos e identificar controles adecuados para reducir el riesgo. (Instituto Nacional de Estadística y Geografía (INEGI), s.f.)

2.4.1. Riesgo.

El riesgo es la probabilidad de que suceda un evento de impacto negativo, por medio de las vulnerabilidades existentes. (Stoneburner, Goguen, Feringa, 2002, p.8).

2.4.2. Análisis de Riesgos.

El análisis de riesgo es el proceso que permite detectar los riesgos y establecer el nivel de este. Es utilizado para determinar el grado de las amenazas, llegando a identificar los controles pertinentes para reducir el riesgo durante el proceso de mitigación de riesgos. (Stoneburner et al, 2002, p.8).

2.4.2.1. Controles.

Los controles son los procesos que se utilizan para reducir los riesgos. En el análisis de riesgos los controles se establecen de las actividades que conforman los procesos. Los controles pueden ser de prevención, detección, protección o correctivos. Un control puede ser de prevención, detección y protección al mismo tiempo. (Modelo Estándar de Control Interno del Paraguay (MECIP), s.f.)

2.4.2.1.1. Control Preventivo.

El control preventivo es el que actúa para eliminar las causas del riesgo, el objetivo es disminuir la probabilidad de que ocurra el riesgo. (MECIP, s.f.)

2.4.2.1.2. Control de Detección.

El control de detección es el que actúa al descubrir una amenaza, disminuye la probabilidad de que suceda el evento. (MECIP, s.f.)

2.4.2.1.3. Control de Protección.

El control de protección es el que disminuye las consecuencias del riesgo, disminuye el impacto del riesgo. (MECIP, s.f.)

2.4.2.1.4. Control Correctivo.

El control correctivo es utilizado para prevenir que suceda de nuevo el evento, su objetivo es mejorar los controles y disminuir el impacto del riesgo. (MECIP, s.f.)

2.4.3. Principales Metodologías de Análisis de Riesgos Informáticos.

Entre las principales metodologías de análisis de riesgos informáticos están MAGERIT, CRAMM, NIST SP 800-30 y Octave.

2.4.3.1. MAGERIT.

La metodología MAGERIT fue elaborada por el Consejo Superior de Administración Electrónica en España. La herramienta para aplicar la metodología es PILAR, desarrollada por el Centro Criptológico Nacional. (Portal de Administración Electrónica (PAE), s.f.)

MAGERIT consta de 3 tomos, método, catálogo de elementos y guía de técnicas.

- El de Método indica la metodología como conceptos, actividades del análisis de riesgos, criterios de tratamiento de riesgos, actividades de gestión de riesgos, proyectos de análisis de riesgos, plan de seguridad, desarrollo de sistemas de información y consejos prácticos. (PAE, s.f.)
- El catálogo de elementos se basa en los tipos de activos, dimensiones y criterios de valoración de activos, amenazas y salvaguardas a considerar para proteger los sistemas de información. (PAE, s.f.)
- La guía de técnicas tiene la orientación al uso de las técnicas específicas para el análisis de riesgo, como el análisis mediante tablas, análisis algorítmicos, arboles de ataque, técnicas generales y gráficas, sesiones de trabajo como entrevistas y reuniones. (PAE, s.f.)

2.4.3.2. CRAMM.

La metodología CRAMM fue elaborada por la Agencia Central de Cómputo y Telecomunicaciones en Reino Unido. La herramienta para aplicar la metodología es CRAMM EXPRESS. (Agencia Europea de Red y Seguridad de la Información (enisa), s.f.)

CRAMM consta de tres fases que son establecer los objetivos de seguridad en el que se identifica y valoriza los activos que conforman el sistema, evaluación de riesgos en el que se valorizan las amenazas y vulnerabilidad y la identificación y selección de contramedidas. (Matalobos, 2009, p.58)

2.4.3.3. NIST SP 800-30.

La metodología de evaluación de riesgos NIST SP 800-30 fue elaborada por el Instituto Nacional de Estándares y Tecnología en Estados Unidos. (Shanthamurthy, s.f.)

NIST SP 800-30 consta de 9 pasos que es la caracterización del sistema, identificación de amenazas, identificación de vulnerabilidad, análisis de control, determinación de probabilidad, análisis de impacto, determinación del riesgo, recomendaciones de control y documentación de resultados. (Shanthamurthy, s.f.)

2.4.3.4. OCTAVE.

La metodología Octave fue elaborada por el estándar internacional ISO270001 en Estados Unidos. (Urrutia, 2014)

Octave consta de 3 fases que son visión organizativa donde se definen los activos, vulnerabilidades, amenazas, exigencias de seguridad y normas existentes. En la visión tecnológica se clasifican los componentes claves y las vulnerabilidades técnicas. Y en la planificación de las medidas y reducción de

riesgos se realiza la estrategia y desarrollo del plan para reducir los riesgos. (Urrutia, 2014)

2.4.4. Diferencias de las Metodologías de Análisis de Riesgos Informáticos.

Las diferencias de las metodologías de análisis de riesgos informáticos se basan en el lugar en el que se puede aplicar dicha metodología, el tipo de valoración de los riesgos, herramientas para aplicar la metodología, resultados del análisis y las fases de la evaluación de riesgos de cada metodología.

Tabla 34. Matriz de diferencias de las metodologías de análisis de riesgos.

	Magerit	CRAMM	NIST SP 800 - 30	Octave
País que creó la metodología	España.	Reino Unido.	Estados Unidos.	Estados Unidos.
Lugar de aplicación.	Solo España.	Internacional.	Internacional.	Internacional.
Valoración	Valor del activo.	[1-5]	Alto-Medio-Bajo	Busca el riesgo más alto.
Herramienta para aplicar la metodología.	PILAR y CHINCHON	CRAMM EXPRESS	No especifica una herramienta en concreto.	No especifica una herramienta en concreto.
Resultado del análisis	Resultados ordinales y cardinales.	Tabla de valorización del riesgo sobre los activos.	Controles recomendados.	Planes de mitigación de riesgo.
Fases	1. Planificación del Proyecto de Riesgos. 2. Análisis de riesgos. 3. Gestión de riesgos. 4. Selección de salvaguardas	1. Identificación y valorización de activos. 2. Valorización de las amenazas y vulnerabilidades. 3. Selección y recomendación de contramedidas.	1. Caracterización del sistema. 2. Identificación de amenazas. 3. Identificación de vulnerabilidades. 4. Análisis de los controles. 5. Determinación de probabilidad. 6. Análisis de impacto. 7. Determinación del riesgo. 8. Recomendaciones de control. 9. Documentación de resultados.	1. Visión organizativa. 2. Visión tecnológica. 3. Estrategia y desarrollo del plan.

Adaptado de CID, 2013, pp.62-67.

Las conclusiones de las metodologías de análisis de riesgos son las siguientes:

- Magerit es una metodología que no es recomendada utilizar por lo que es de uso especial para España y es orientado a los activos del sistema.

- Octave es una metodología no recomendada por lo que es más subjetiva que las demás, al utilizar un árbol de decisiones para determinar el riesgo más alto.
- CRAMM es una metodología que no es recomendada porque es orientada al análisis de riesgos en los activos del sistema.
- NIST SP 800-30 es una metodología que da prioridad a los controles y a los perfiles claves para minimizar los riesgos.

De las diferentes metodologías de análisis de riesgos analizadas en la matriz, se llegó a la conclusión que la más óptima a utilizar es NIST SP 800-30 porque el resultado del análisis desencadena en los controles recomendados.

Hay que tomar en cuenta que para el análisis de riesgos del usuario en Facebook no se van a evaluar los activos del sistema, sino los controles actuales que se encuentran en los procesos que realiza la red social al interactuar con el usuario. Por el enfoque del análisis, lo que se busca es identificar las amenazas, vulnerabilidades y controles del sistema para determinar la probabilidad e impacto con el fin de determinar el nivel del riesgo y así diseñar controles de seguridad personal que minimicen los riesgos encontrados en las redes sociales.

2.4.5. Metodología NIST SP 800-30.

La metodología NIST SP 800-30 elaborada por Stoneburner, Goguen, Feringa (2002), es una guía para realizar una correcta gestión de riesgos relacionada con los sistemas informáticos. La gestión de riesgos en la metodología se basa en tres procesos: evaluación de riesgos, mitigación de riesgos y evaluación.

La evaluación de riesgos consiste en el proceso de identificación y análisis de riesgos para realizar las recomendaciones con el fin de reducir la valoración del riesgo. La mitigación de riesgos consiste en la priorización, ejecución y mantenimiento de las recomendaciones realizadas en la evaluación de riesgos.

La evaluación consiste en valorar los riesgos resultantes de la implementación de las recomendaciones para determinar si encuentra en un nivel aceptable.

La metodología NIST SP 800-30 tiene énfasis en los controles de seguridad que se pueden emplear para la mitigación de riesgos, con el fin de brindar mejor protección.

2.4.5.1. Evaluación de Riesgos en NIST SP 800-30.

La evaluación de riesgos es el proceso que determina el grado del riesgo para recomendar los controles adecuados con el fin de reducir los riesgos por medio del proceso de mitigación de riesgos. (Stoneburner et al, 2002, p.8.)

El proceso se deriva en nueve pasos que son: Caracterización del Sistema, Identificación de Amenazas, Identificación de Vulnerabilidad, Análisis de Control, Determinación de Probabilidad, Análisis de Impacto, Determinación del Riesgo, Recomendaciones de Control y Documentación de Resultados. (Stoneburner et al, 2002, p.8.)

La identificación de amenazas, identificación de vulnerabilidades, análisis de control y análisis de impacto de pueden realizar en paralelo. (Stoneburner et al, 2002, p.8.)

2.4.5.1.1. Caracterización del Sistema.

En este paso se define el alcance del esfuerzo, límites del sistema, recursos e información. (Stoneburner et al, 2002, p.10.)

La recolección de información se puede realizar durante todo el proceso de la evaluación de riesgos desde el paso 1 al paso 9. (Stoneburner et al, 2002, p.12.)

La información que se recopila en la caracterización del sistema por lo general es hardware, software, acoplamiento del sistema, datos e información,

usuarios, procesos, criticidad de datos, sensibilidad de datos como los niveles de protección. También se puede recopilar las políticas de seguridad, arquitectura de seguridad, flujo de información, controles técnicos, controles de gestión y controles de operación. (Stoneburner et al, 2002, p.10.)

Las técnicas que se pueden utilizar para la recopilación de información pueden ser por medio de cuestionarios, entrevistas, revisión de documentación y el uso de la herramienta de escaneo automatizado. (Stoneburner et al, 2002, pp.11-12.)

2.4.5.1.2. Identificación de Amenazas.

En este paso se busca identificar las amenazas que son probables de ocurrir en el sistema informático que se está analizando. Como resultado se obtiene el listado de todas las posibles amenazas, la motivación y quien lo realiza. (Stoneburner et al, 2002, p.12.)

Las amenazas se pueden clasificar en naturales, humanas o ambientales. Las amenazas naturales son las ocasionadas por desastres naturales como terremotos, tornados, etc. Las amenazas humanas son causadas por el ser humano, puede ser con intención maliciosa o por error. Las amenazas ambientales son las ocasionadas a largo plazo por factores como la contaminación, químicos, etc. (Stoneburner et al, 2002, p.13.)

Tabla 35. Ejemplo de Amenazas Humanas.

AMENAZA-FUENTE	MOTIVACIÓN	ACCIÓN
Hacker	<ul style="list-style-type: none"> • Ambición • Ego 	<ul style="list-style-type: none"> • Fraude cibernético • Robo de información • Ingeniería Social • Acceso no autorizado

Adaptado de Stoneburner et al, 2002, p.14.

2.4.5.1.3. Identificación de Vulnerabilidad.

En este paso se busca identificar las vulnerabilidades del sistema que son utilizadas para ejecutar las probables amenazas a ocurrir en el sistema informático que se encuentra en análisis. Como resultado se obtiene el listado de las vulnerabilidades del sistema ante cada amenaza. (Stoneburner et al, 2002, p.15.)

Las vulnerabilidades son las fallas o debilidades del sistema en los procedimientos de seguridad. Las vulnerabilidades permiten que el sistema sea susceptible a que sucedan amenazas. Es importante realizar el análisis a las vulnerabilidades del sistema, ya que si no hay una vulnerabilidad para ejecutar la amenaza, no existe riesgo. (Stoneburner et al, 2002, p.15.)

Los tipos de vulnerabilidades que pueden ocurrir y la metodología para determinar son en función del sistema informático y la fase en la que se encuentra en el SDLC. (Stoneburner et al, 2002, p.16.)

1) Si el sistema no se encuentra diseñado, las vulnerabilidades se identifican a base de las políticas y procedimientos de seguridad de la organización. (Stoneburner et al, 2002, p.16.)

2) Si el sistema se encuentra implementado, las vulnerabilidades se identifican a base de las características provistas por el sistema, la documentación del diseño de seguridad y los resultados de la certificación de prueba y evaluación del sistema. (Stoneburner et al, 2002, p.16.)

3) Si el sistema está operativo, las vulnerabilidades se identifican a base del análisis de las características, procedimientos y controles de seguridad del sistema. (Stoneburner et al, 2002, p.16.)

Los métodos que se pueden utilizar son las fuentes de vulnerabilidad, pruebas de seguridad y desarrollo de la lista de verificación de requisitos de seguridad. Una fuente de vulnerabilidad es la documentación de la evaluación de riesgos del sistema anterior, informe de auditoría, etc. (Stoneburner et al, 2002, p.16.)

Las pruebas de seguridad del sistema se realizan con herramientas automatizadas de análisis de vulnerabilidades, pruebas de penetración que permiten saber cuál es la resistencia del sistema ante intentos de violar las seguridades, etc. (Stoneburner et al, 2002, p.17.)

La lista de verificación de requisitos de seguridad contiene los estándares de seguridad básicos que se pueden utilizar para la evaluación e identificación de vulnerabilidades, se pueden dividir por zonas que son las seguridades de gestión, operativas y técnicas. (Stoneburner et al, 2002, pp.18-19.)

Tabla 36. Ejemplo de Pares de la Vulnerabilidad / Amenaza

VULNERABILIDAD	AMENAZA-FUENTE	ACCIÓN
El sistema bancario no cuenta con encriptación de contraseña en las cuentas de los usuarios.	Hacker	Fraude bancario

Adaptado de Stoneburner et al, 2002, p.15.

2.4.5.1.4. Análisis de Control.

En este paso se busca analizar los controles implementados en el sistema para minimizar o eliminar la probabilidad de que la amenaza se ejecute a través de las vulnerabilidades del sistema. Como resultado se obtiene el listado de los controles actuales o previstos utilizados para mitigar la probabilidad de que se utilice una vulnerabilidad y reducir el impacto de una amenaza. (Stoneburner et al, 2002, p.19.)

Para la calificación de la probabilidad es importante saber los controles existentes, ya que va a ser baja si existe un control que reduzca la magnitud del daño. (Stoneburner et al, 2002, p.20.)

El control es el regulador en el comportamiento del sistema, con el fin de minimizar las probabilidades de falla. Los métodos de control pueden ser técnicos como autenticación, métodos de encriptación y los no técnicos que son los controles de gestión y operativos como las políticas de seguridad, procedimientos operativos, etc. (Stoneburner et al, 2002, p.20.)

Los controles pueden ser de prevención o detección. Los controles de prevención tienen el fin de impedir los intentos de burlar las seguridades como la autenticación y encriptación, los controles de detección tienen el fin de advertir intentos de violar las seguridades como las pistas de auditoria, métodos de detección de intrusos, etc. (Stoneburner et al, 2002, p.20.)

Como técnica se puede utilizar el listado de comprobación de los requisitos de seguridad con el fin de validar el incumplimiento de seguridad. (Stoneburner et al, 2002, p.20.)

2.4.5.1.5. Determinación de Probabilidad.

En este paso se califica la probabilidad que se ejecute un evento adverso por medio de las vulnerabilidades existentes en el sistema. Como resultado se tiene la valoración de la probabilidad. (Stoneburner et al, 2002, p.21.)

Los factores a ser considerados son las amenazas con su respectiva motivación, las vulnerabilidades y los controles actuales del sistema. (Stoneburner et al, 2002, p.21.)

Los niveles de probabilidad son calificados como bajo, medio y alto.

- El nivel de probabilidad es baja, cuando la amenaza carece de motivación o capacidad y los controles existentes previenen o impiden de manera significativa la vulnerabilidad a ser ejercida. (Stoneburner et al, 2002, p.21.)
- El nivel de probabilidad es medio, cuando la amenaza está motivada y capacitada, pero los controles impiden el éxito de ejercer la vulnerabilidad. (Stoneburner et al, 2002, p.21.)
- El nivel de probabilidad es alto, cuando la amenaza está muy motivada y suficientemente capacitada y los controles son ineficientes para evitar el ejercer la vulnerabilidad. (Stoneburner et al, 2002, p.21.)

2.4.5.1.6. Análisis de Impacto.

En este paso se busca determinar las consecuencias resultantes de que una amenaza sea ejecutada con éxito. El análisis del impacto es importante para la medición del nivel de riesgo. Como resultado se obtiene la magnitud del impacto. (Stoneburner et al, 2002, p.21.)

El impacto se refiere a la magnitud del daño que podría ser causado al ser ejercida una amenaza a través de la vulnerabilidad del sistema. El impacto se puede describir en términos de pérdida o degradación de la integridad, disponibilidad y confidencialidad del sistema. (Stoneburner et al, 2002, p.22.)

La integridad se refiere a que la información debe ser protegida contra modificaciones incorrectas. Pierde la información integridad al ser modificada sin autorización. El uso de información corrompida da lugar a impresiones, fraude o decisiones erróneas. La violación a la integridad es el primer paso para un ataque exitoso. (Stoneburner et al, 2002, p.22.)

La disponibilidad se refiere a estar el sistema y los datos disponibles al usuario final. Es importante en cuanto a la funcionalidad del sistema y eficacia operativa. (Stoneburner et al, 2002, p.22.)

La confidencialidad se refiere a la protección de la información para no ser divulgada sin autorización. Es importante para la confianza del usuario en el sistema. (Stoneburner et al, 2002, p.22.)

Algunos impactos pueden medirse cuantitativamente como en costo de reparación, pérdida de ingresos, etc. Pero otros impactos no pueden ser calificados cuantitativamente como la pérdida de confianza del usuario, pérdida de credibilidad, etc. Por lo que se utiliza las medidas de alto, medio y bajo impacto. (Stoneburner et al, 2002, p.22.)

- El impacto es bajo, si el resultado es la pérdida de recursos o activos tangibles. O afectación notable a la organización en cuanto a su misión, reputación o interés. (Stoneburner et al, 2002, p.23.)

- El impacto es medio, si el resultado es la pérdida costosa de recursos o bienes materiales. O daños de la misión, reputación o interés de la organización. O resultan daños a las personas. (Stoneburner et al, 2002, p.23.)
- El impacto es alto, si el resultado es la pérdida altamente costosa de recursos y activos. O el daño es significativo y dificulta la misión, reputación o interés de la organización. O resulta la muerte o lesiones humanas graves. (Stoneburner et al, 2002, p.23.)

La ventaja de realizar un análisis de impacto cualitativo es que da prioridad a los riesgos y se realiza la mejora al tratamiento de las vulnerabilidades. Pero es complicado para realizar análisis de costo-beneficio de los controles. (Stoneburner et al, 2002, p.23.)

La ventaja de realizar un análisis cuantitativo del impacto es que se puede realizar un análisis costo-beneficio de los controles recomendados. La desventaja es que no proporciona mediciones específicas de la magnitud del impacto. (Stoneburner et al, 2002, p.23.)

2.4.5.1.7. Determinación del Riesgo.

En este paso se busca evaluar el nivel de riesgo. Para medir el riesgo, se necesita desarrollar la escala de riesgo y la matriz de riesgos. (Stoneburner et al, 2002, p.24.)

La escala de riesgo se representa en bajo, medio y alto. Las acciones necesarias a realizar en cada caso son las siguientes:

- Si el riesgo es bajo, se determina si es necesario tomar medidas correctoras o si llegó al nivel aceptable de riesgo. (Stoneburner et al, 2002, p.25.)
- Si el riesgo es medio, es necesario tomar acciones correctivas en un periodo razonable de tiempo con el desarrollo de un plan. (Stoneburner et al, 2002, p.25.)

- Si el riesgo es alto, es necesario tomar medidas correctivas lo más pronto posible. (Stoneburner et al, 2002, p.25.)

La matriz de riesgos es la determinación final del riesgo, la cual se obtiene multiplicando la probabilidad por el impacto de la amenaza. (Stoneburner et al, 2002, p.24.)

Tabla 37. Matriz – Nivel de riesgos.

Probabilidad	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alta (1.0)	Bajo $10 \times 1.0 = 10$	Medio $50 \times 1.0 = 50$	Alto $100 \times 1.0 = 100$
Media (0.5)	Bajo $10 \times 0.5 = 5$	Medio $50 \times 0.5 = 25$	Medio $100 \times 0.5 = 50$
Baja (0.1)	Bajo $10 \times 0.1 = 1$	Bajo $50 \times 0.1 = 5$	Bajo $100 \times 0.1 = 10$

Nota: La escala de riesgo es: Alto(>50 a 100), Medio(>10 a 50) y Bajo(1 a 10) Tomado de Stoneburner et al, 2002, p.25.

- El nivel de riesgo se obtiene de la multiplicación de los valores asignados a la probabilidad e impacto de la amenaza.
- El valor asignado para cada nivel de probabilidad es de 1.0 para alta, 0.5 para medio, 0.1 para baja y el valor asignado para cada nivel de impacto es de 100 para alta, 50 para medio y 10 para bajo.
- La matriz actual es de 3x3, dependiendo de los requisitos y granularidad del análisis puede ser de 4x4 o 5x5 obteniendo los niveles de Muy alto y Muy bajo.

2.4.5.1.8. Recomendaciones de Control.

En este paso se busca recomendar controles o soluciones alternativas que permitan eliminar o reducir los riesgos identificados. Como resultado se obtiene las recomendaciones de control y soluciones alternativas para la mitigación de riesgos. (Stoneburner et al, 2002, p.26.)

El objetivo de las recomendaciones de control es reducir el nivel de riesgo a un nivel aceptable. Las recomendaciones son el resultado del proceso de la

evaluación de riesgos, que son evaluados, priorizados e implementados en el proceso de mitigación de riesgos. (Stoneburner et al, 2002, p.26.)

Para las recomendaciones se tienen que tener en cuenta los factores de eficiencia, legislación y regulación, política de la organización, impacto operativo, seguridad y fiabilidad. (Stoneburner et al, 2002, p.26.)

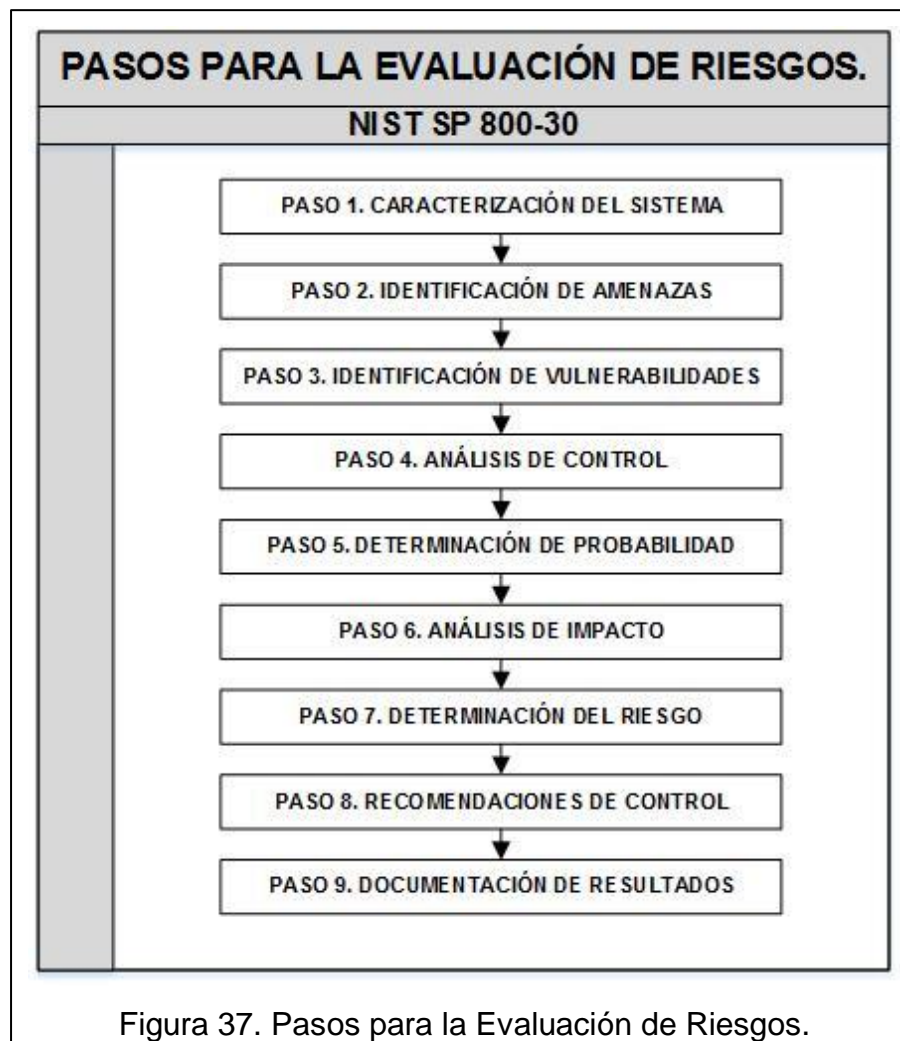
2.4.5.1.9. Documentación de Resultados.

En este paso se busca realizar el informe de la evaluación de riesgos, en el que se describen las amenazas, vulnerabilidades, medición del riesgo y las recomendaciones de control. (Stoneburner et al, 2002, p.26.)

El informe de evaluación de riesgos es para que los altos directivos entiendan los riesgos y asignen los recursos necesarios para la mitigación de riesgos existentes. La diferencia al informe de auditoría es que el informe de evaluación de riesgos no es presentado en forma acusadora, sino en forma sistemática y analítica. (Stoneburner et al, 2002, p.26.)

3. Capítulo III. Análisis de Riesgos.

En el capítulo anterior se realizó el análisis de las metodologías existentes para el análisis de riesgos obteniendo como resultado que la metodología NIST SP 800-30 es la más óptima para el siguiente análisis de riesgos de los usuarios en Facebook. En el presente capítulo se va aplicar la metodología elegida, la cual consta de nueve pasos.



3.1. Caracterización del Sistema.

La caracterización del sistema es la recopilación de los recursos e información del software en cuanto a sus procesos y controles de seguridad actuales. (Stoneburner et al, 2002, pp.10-12.)

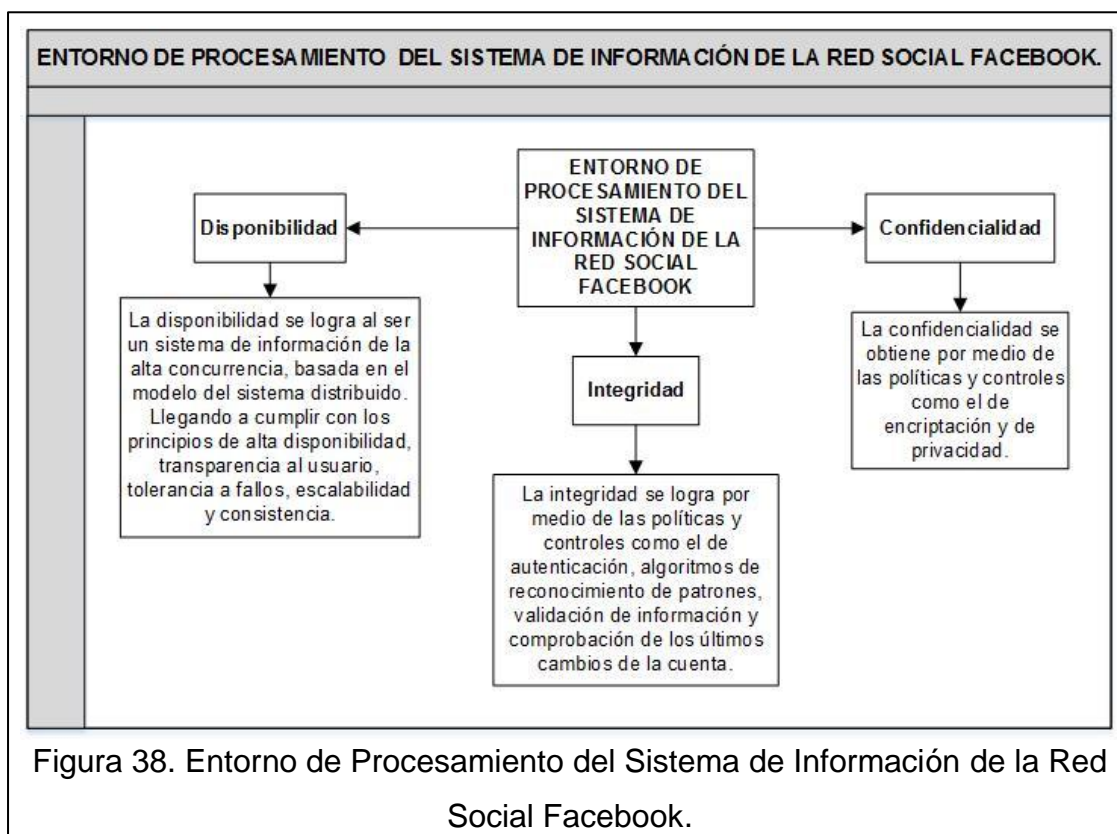
3.1.1. Alcance de la Evaluación de Riesgos.

En el alcance de la evaluación de riesgos del presente trabajo de titulación corresponde el análisis de la seguridad personal de los usuarios en la red social Facebook. Los recursos e información que serán identificados son los controles actuales de seguridad personal de los usuarios y los procesos actuales que utilizan los usuarios en la red social.

Lo que se encuentra fuera del alcance es el Hardware y tipologías internas de infraestructura por el motivo que es información confidencial de la empresa.

3.1.2. Entorno de Procesamiento del Sistema de Información de la Red Social Facebook.

Uno de los principales componentes de la red social es su sistema de información, el mismo que se apoya en los principios de seguridad que son disponibilidad, integridad y confidencialidad.



3.1.2.1. Software.

El software que constituye parte del sistema de información de la red social, permite a los usuarios relacionarse con la familia, amigos, compañeros, conocidos, colegas y desconocidos. Al ser una red social cuenta con los componentes principales que son los usuarios con su respectivo perfil que contiene la información personal del mismo, la relación de amistad entre los usuarios y sus respectivos muros.

El contenido que los usuarios comparten en sus muros son fotografías, videos, imágenes, ideas, estados, etc.

La red social proporciona al usuario la opción de controlar la privacidad del contenido que comparte, como seleccionar quien puede ver la publicación. También cuenta con aplicaciones asociadas, las cuales hacen que sea una herramienta más interactiva, por ejemplo los juegos que permiten ver la posición que tiene ante sus amigos.

3.1.2.2. Tecnologías que Utiliza el Software.

Facebook utiliza tecnologías como cookies, etiquetas pixel, identificador de dispositivos y almacenamiento local para la seguridad del usuario. (Facebook, s.f.)

Estas tecnologías son utilizadas en las autenticaciones para identificar el dispositivo y la IP de donde se inicia sesión cuando se usa la aprobación de inicio de sesión y para las notificaciones de inicio de sesión.

Con las etiquetas pixel se puede rastrear las acciones y recorrido de un usuario, saber la dirección IP del dispositivo, hora, fecha, tipo de navegador, etc. (Facebook, s.f.)

También son utilizadas para activar algunas funciones de seguridad que tiene Facebook como detectar las actividades que infringen las normas comunitarias

y la declaración de derechos y responsabilidades. Así mismo, sirven para evitar la creación masiva de cuentas falsas. (Facebook, s.f.)

Facebook se encuentra inmerso en la inteligencia artificial al utilizar algoritmos para el análisis y reconocimiento de patrones, dichos algoritmos se encuentran en sus equipos para cumplir con las políticas y detección de infracciones de las normas comunitarias de una forma rápida y uniforme. (Facebook, s.f.)

3.1.2.3. Datos e Información.

Los datos que proporcionan los usuarios en su perfil son en la mayoría de ocasiones reales y en otros falsos.

La información básica que va a contener un perfil es el nombre, apellido, dirección de correo electrónico, número de teléfono, fecha de nacimiento, género, foto de perfil. Otro tipo de información que es proporcionada por el usuario es la ciudad de origen, ciudad actual, idiomas, creencias religiosas, intereses, ideología política, estado civil, etc.

La red social además de la información personal de los usuarios, tiene el contenido que comparten entre ellos que son fotografías, videos, imágenes, ideas, estados, etc.

Para comprender de mejor manera lo importante que es la información proporcionada en la red social, se realizó el mapa de calor con la clasificación según la sensibilidad de la información.

Tabla 38. Sensibilidad de Información.

CATEGORÍA	DESCRIPCIÓN	VALOR
Sensibilidad Alta.	La información es muy importante y decisiva en los procesos de seguridad del usuario en el sistema.	Alto.
Sensibilidad Media.	La información es básica y en ciertos casos se utiliza en los procesos de seguridad del usuario en el sistema.	Medio.
Sensibilidad Baja.	La información es adicional y no se utiliza en los procesos de seguridad del usuario en el sistema.	Bajo.

Tabla 39. Mapa de Calor - Sensibilidad de información.

CLASIFICACIÓN DE LA SENSIBILIDAD DE INFORMACIÓN.				
NOMBRE	APELLIDO	AÑO DE NACIMIENTO	GÉNERO	NÚMERO DE TELÉFONO
CORREO ELÉCTRONICO	CONTRASEÑA	CIUDAD ACTUAL	CIUDAD DE ORIGEN	FORMACIÓN ACADÉMICA
TRABAJO	FECHA DE NACIMIENTO (DÍA Y MES)	FOTO DE PERFIL	FOTO DE PORTADA	DIRECCIÓN DE VIVIENDA
PUBLICACIONES	VIDEOS	FOTOS	VISITAS	AMIGOS
EVENTOS	CLAVE PÚBLICA	INTERESES	IDIOMAS	CREENCIAS RELIGIOSAS
IDEOLOGÍA POLÍTICA	SITUACIÓN SENTIMENTAL Y FAMILIAR	INFORMACIÓN ADICIONAL	OTROS NOMBRES (APODO)	CITAS FAVORITAS
ACONTECIMIENTOS IMPORTANTES	PROGRAMAS DE TV	PELÍCULAS	MÚSICA	LIBROS
DEPORTES	APLICACIONES Y JUEGOS	PÁGINAS QUE LE GUSTA	APTITUD PROFESIONAL	GRUPOS
OPINIONES	NOTAS	SITIOS WEB		

3.1.2.4. Usuarios del Sistema.

Las personas que interactúan en la red social Facebook es el personal administrativo y técnico de la red social, los administradores encargados de revisar los reportes de abusos para determinar si infringen las normas y políticas de la red social, los desarrolladores de las aplicaciones asociadas, usuarios que tienen cuenta en la red social y los usuarios de Internet que tienen acceso a la información pública de los usuarios.

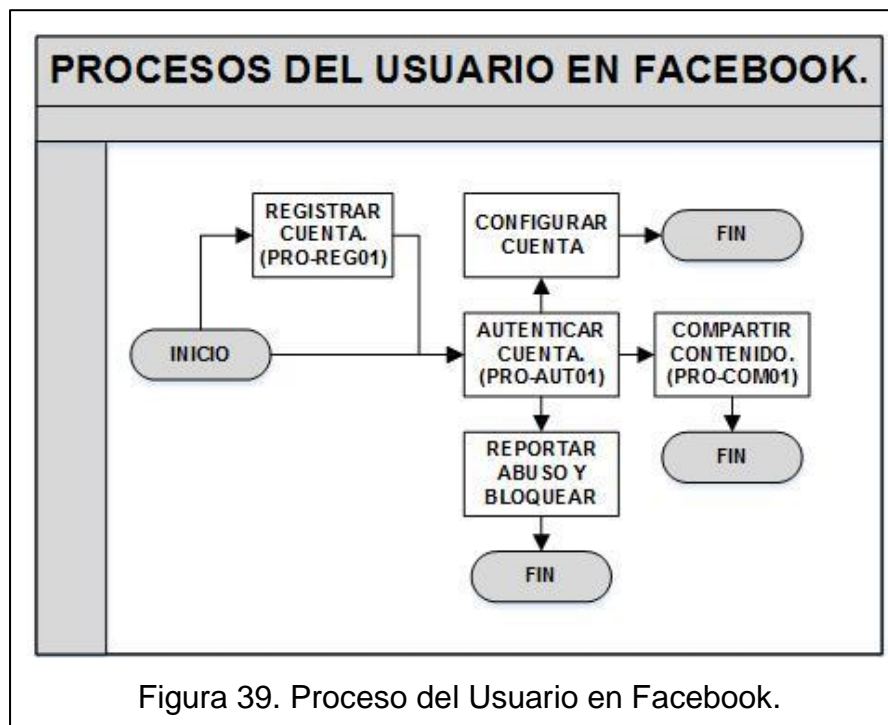
3.1.2.5. Procesos Actualmente Utilizados en el Software.

Los procesos que la red social proporciona a los usuarios son: registrar la cuenta, autenticar la cuenta, configurar la cuenta, compartir contenido, reportar abuso y bloquear.

El proceso de registrar la cuenta se realiza solo una vez, cuando el usuario crea la cuenta en Facebook. Los procesos se pueden realizar en cualquier orden después de autenticar la cuenta y es opcional su realización.

Los diagramas de flujos de los procesos técnicos del software se realizaron a base de los pasos que realiza el usuario en la red social Facebook, debido a que los procesos técnicos de Facebook no se encuentran disponibles al público.

Las nomenclaturas sirven para identificar de mejor manera cada proceso. Por ejemplo el proceso de Registrar cuenta en Facebook es identificada como PRO-REG01.



3.1.2.5.1. Registrar Cuenta en Facebook. ([PRO-REG01](#))

Para registrar una nueva cuenta en Facebook es necesario ir a la página oficial <https://www.facebook.com/> y llenar el formulario de registro. Los datos que requiere son nombre, apellido, dirección de correo electrónico o número de celular, confirmación de la dirección de correo electrónico o número de celular, contraseña, fecha de nacimiento y sexo.

Por seguridad se recomienda que la contraseña tenga mínimo 6 caracteres, entre la combinación compleja de números, signos de puntuación, letras mayúsculas y minúsculas. (Facebook, s.f.)

Al enviar el formulario, el sistema compara si ya es utilizado el número de teléfono o la dirección de correo electrónico en otra cuenta. Si es utilizado regresa el sistema a la página del formulario. En caso de no estar utilizado crea la cuenta, guarda la información proporcionada en el formulario de registro, genera y envía un enlace de confirmación a la dirección de correo electrónico o un código por medio de un mensaje de texto al número proporcionado en el formulario.

Por último el usuario confirma según el medio utilizado. En caso de no confirmar se puede usar la cuenta durante un día y será bloqueada hasta cumplir con el requisito de la confirmación.

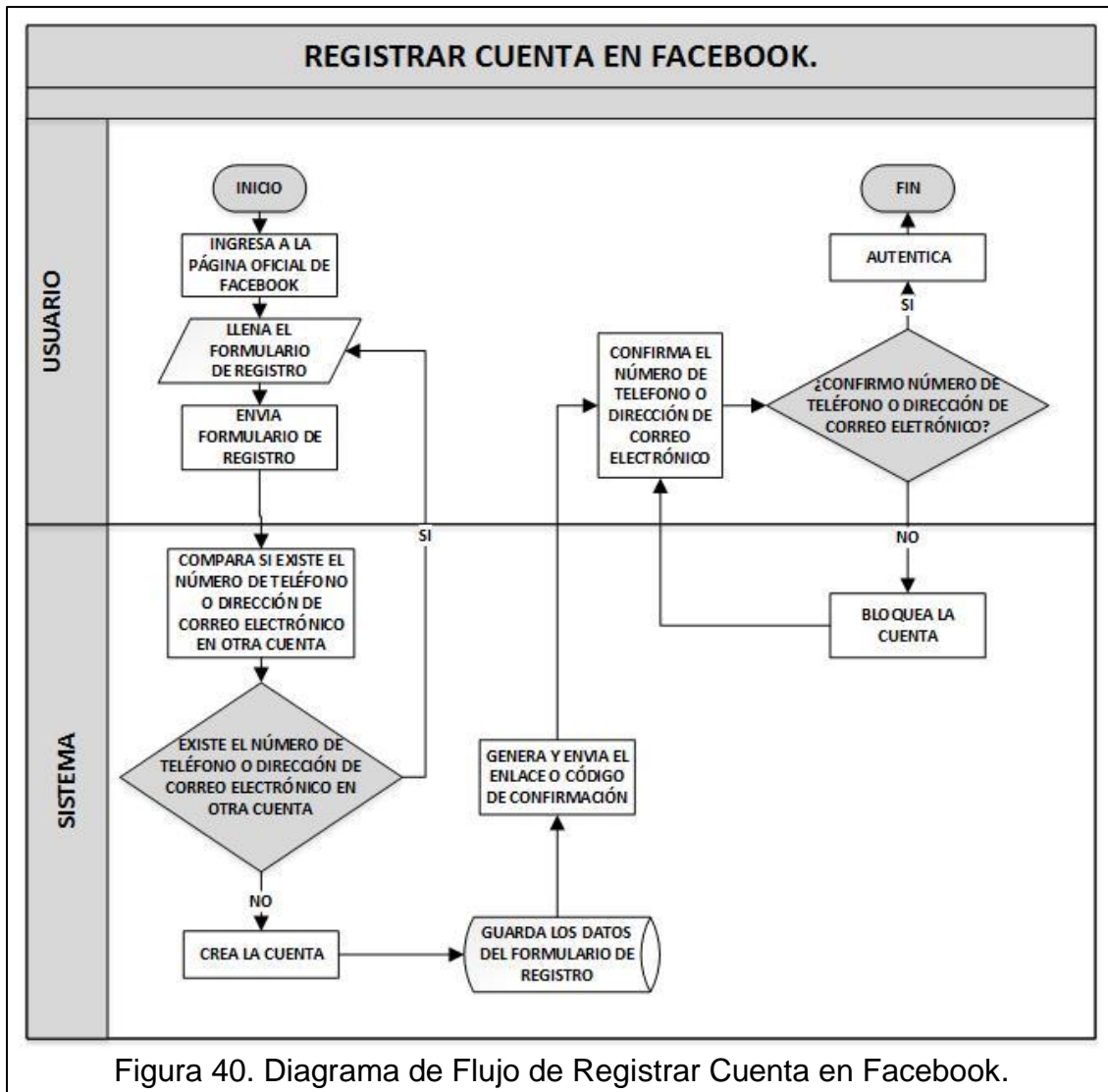


Figura 40. Diagrama de Flujo de Registrar Cuenta en Facebook.

Controles del proceso:

- Compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta.
- Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta.

3.1.2.5.2. Autenticar en Facebook. ([PRO-AUT01](#))

Para iniciar sesión en Facebook se ingresa en la parte superior de la página web o aplicación móvil los datos de dirección de correo electrónico, nombre de usuario o número de celular y contraseña. En caso de no recordar la contraseña, se restablece la misma.

Existe la opción para que el usuario guarde la sesión y se quede abierta, caso contrario al cerrar el navegador se cierra sesión automáticamente.

El sistema encripta la contraseña cuando se envían los datos de autenticación para validar el usuario y contraseña. Si es correcta inicia sesión y extrae todo el contenido relacionado al usuario de la base de datos, para posteriormente desplegar la información en la página de inicio de la red social. El usuario accede a su cuenta y navega por la misma.

Las funciones que la red social proporciona al usuario para el control de seguridad de autenticación es la alerta de inicio de sesión y aprobación de inicio de sesión. Estas funciones hacen variar el proceso de autenticación básico.

Otra opción de seguridad que tiene Facebook para los usuarios es generar contraseñas extras para proteger la contraseña de la cuenta de la red social. Las cuales son contraseña de un solo uso y la contraseña de aplicaciones.

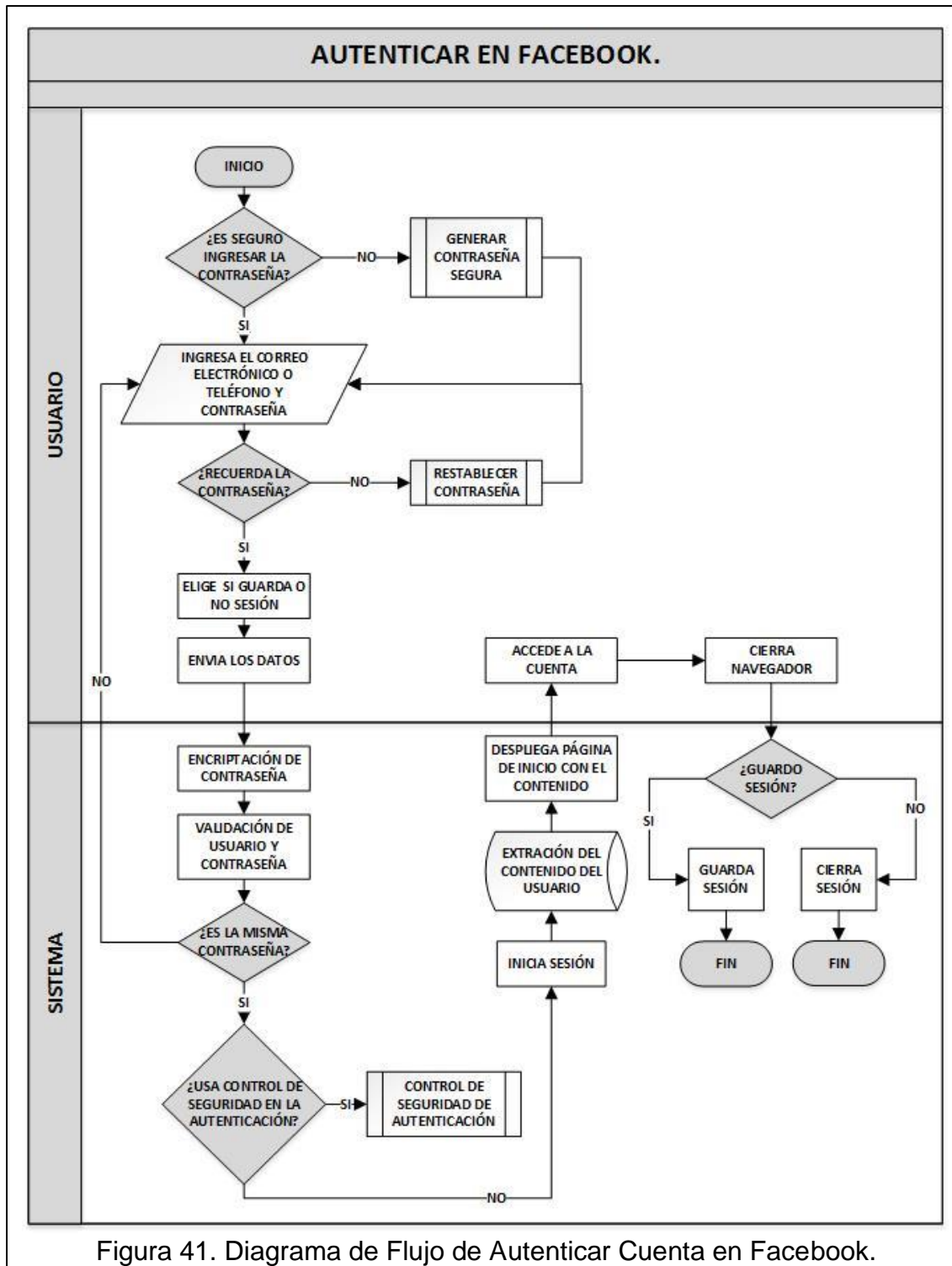


Figura 41. Diagrama de Flujo de Autenticar Cuenta en Facebook.

Controles del proceso:

- Encriptación de contraseña.
- Validación del usuario y contraseña.

Controles opcionales:

- [CON-AUT01](#). Contraseña de un solo uso. (Generar contraseña segura).
- [CON-AUT02](#). Contraseña de aplicaciones. (Generar contraseña segura).
- [CON-AUT03](#). Restablecer contraseña.
- [CON-AUT04](#). Restablecer contraseña por medio de la pregunta de seguridad.
- [CON-AUT05](#). Restablecer contraseña con ayuda de los amigos de confianza.
- [CON-AUT06](#). Alerta de inicio de sesión en Facebook.
- [CON-AUT07](#). Aprobación de inicio de sesión.
- [CON-AUT08](#). Protección de cuenta.

[CON-AUT01](#). Contraseña de un solo uso. (Generar contraseña segura)

La contraseña de un solo uso es para los casos en los que se inicie sesión en un lugar no seguro, por ejemplo en una biblioteca. Para solicitar la contraseña se envía un mensaje de texto con la palabra “otp” al número que le corresponde a la operadora del país del usuario, el sistema genera y envía la respuesta con una contraseña única de 8 caracteres. En caso de no tener configurado el número de teléfono en la cuenta, el sistema envía las indicaciones para realizarlo. (Facebook, s.f.)

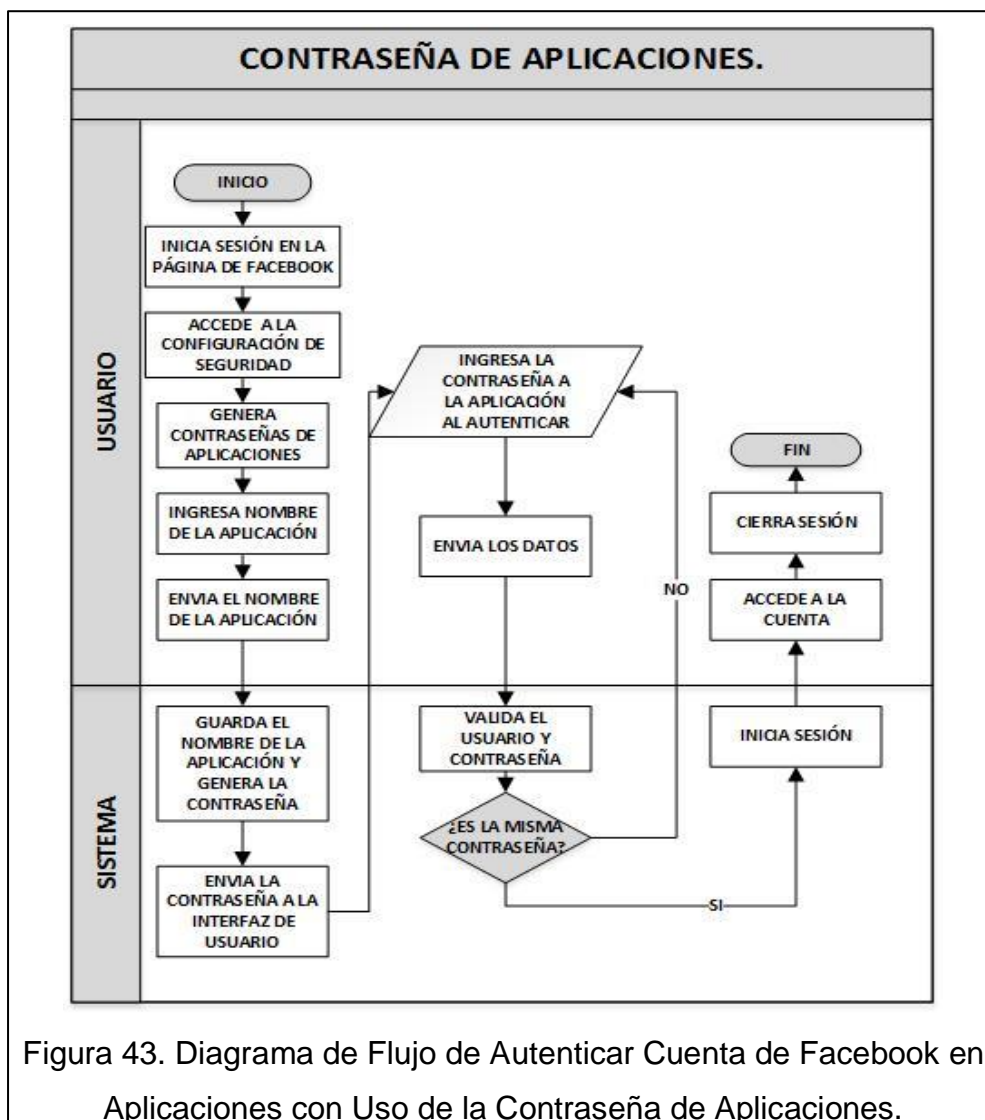
La contraseña es válida durante 20 minutos. Esta opción no está disponible si se tiene activadas las aprobaciones de inicio de sesión. (Facebook, s.f.)

CON-AUT02. Contraseña de aplicaciones. (Generar contraseña segura)

Las contraseñas de aplicaciones son para iniciar sesión en las aplicaciones ligadas a la red social, así se mantiene segura la contraseña de la cuenta.

Para configurar las contraseñas de aplicaciones el usuario inicia sesión y accede a la configuración de seguridad, solicita generar contraseña de aplicaciones e ingresa el nombre de la aplicación. El sistema guarda el nombre de la aplicación, genera la contraseña y despliega al usuario la contraseña. El usuario ingresa la contraseña en la aplicación, llegando a autenticar en la misma.

Facebook guarda la lista de aplicaciones, pero no las contraseñas. Por lo tanto si se cierra sesión en la aplicación, tiene que generar de nuevo la contraseña.



Controles:

- Guarda el nombre de la aplicación y genera la contraseña.
- Validación de usuario y contraseña.

[CON-AUT03](#). Restablecer contraseña.

Facebook solo permite restablecer contraseñas y nunca envía la contraseña pasada, ya que usa el mecanismo de encriptación de contraseñas para ser almacenadas como por ejemplo hash md5() y sha-2().

Si el usuario tiene problemas para iniciar sesión en su cuenta de Facebook puede restablecer la contraseña. Primero ingresa el correo electrónico, número de teléfono o nombre de usuario para que el sistema busque la cuenta correspondiente.

Se abrirá una ventana con tres opciones que son:

1. Usar la cuenta de Google para iniciar sesión y restablecer la contraseña de una forma rápida.
2. Enviar un enlace al correo electrónico para restablecer la contraseña.
3. Enviar un código por SMS al número de teléfono para restablecer la contraseña.

Para evitar confusiones se contiene la foto y nombres de usuario en el lado derecho de las opciones.

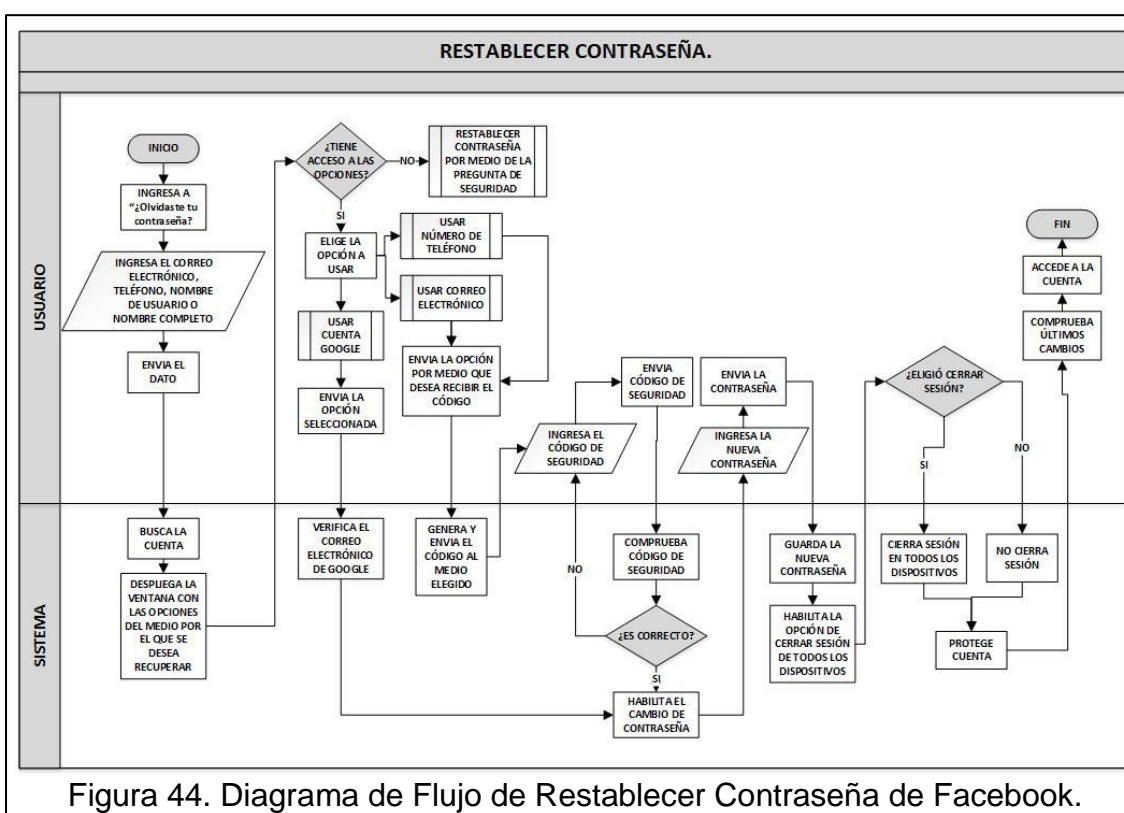
La opción de usar la cuenta de Google es la más rápida, el sistema verifica la cuenta automáticamente, permitiendo la comprobación de la misma. Una vez verificada habilita el ingreso de la nueva contraseña.

En caso de elegir la opción del correo electrónico o número de teléfono, el sistema envía un código de seguridad al mismo. El cual es ingresado para poder restablecer la contraseña.

Se ingresa la nueva contraseña y se guarda, desplegando el sistema la opción de cerrar sesión en todos los dispositivos que se encontraba abierta la cuenta del usuario. Por seguridad es preferible que si lo realice.

Por último el usuario revisa todos los últimos cambios realizados en la cuenta y accede a la misma.

Si el usuario no tiene acceso a la cuenta de Google, al correo electrónico y al número de teléfono, Facebook proporciona el restablecimiento de la contraseña por medio de la pregunta de seguridad.



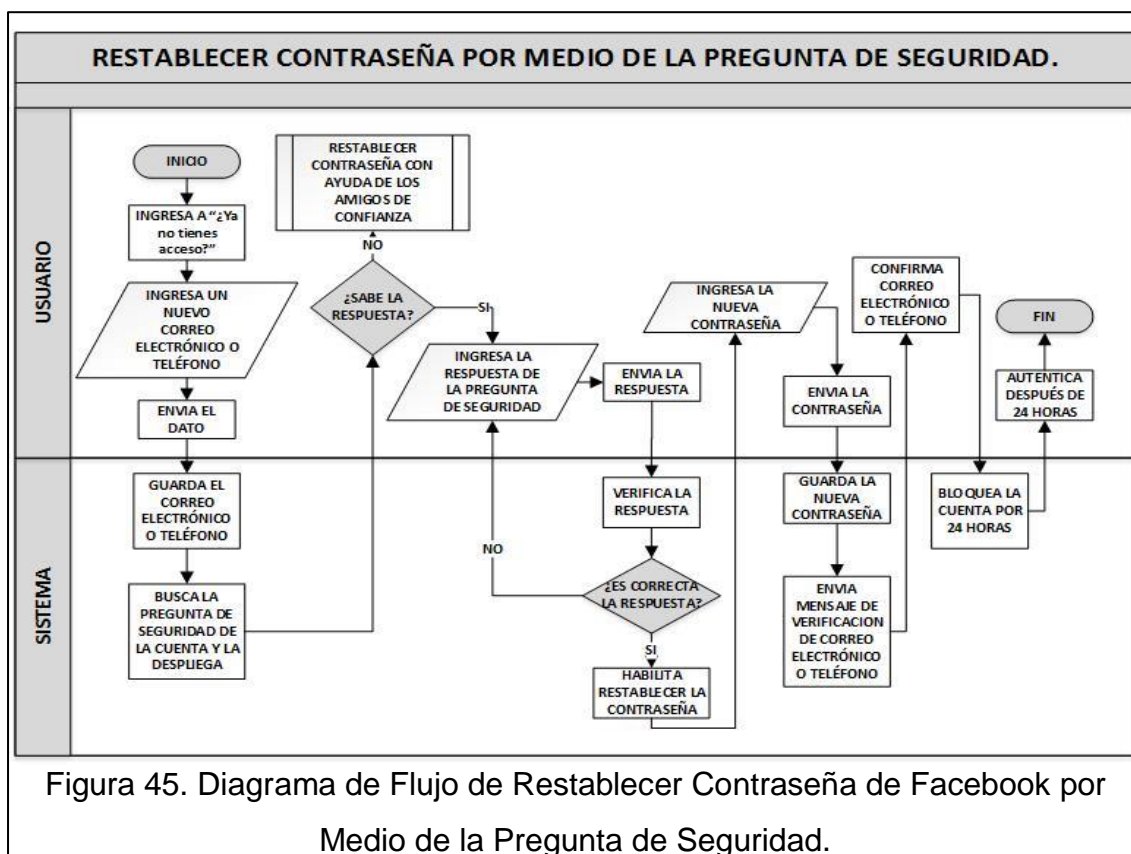
Controles:

- Verifica el correo electrónico de Google o el código de seguridad.
- Cerrar sesión en todos los dispositivos.
- Comprobación de los últimos cambios en la cuenta.

[CON-AUT04](#). Restablecer contraseña por medio de la pregunta de seguridad.

El usuario ingresa una nueva dirección de correo electrónico o número de teléfono al que tenga acceso. El sistema guarda el correo electrónico o teléfono, busca y despliega la pregunta de seguridad para que sea respondida por el usuario. En caso de ser correcta la respuesta, puede ingresar la nueva contraseña. El sistema envía el enlace para verificar el correo electrónico o el número de teléfono y una vez verificado bloquea la cuenta por 24 horas por motivos de seguridad del usuario.

Si no recuerda la respuesta de la pregunta de seguridad puede usar el restablecimiento de contraseña con ayuda de los amigos de confianza.

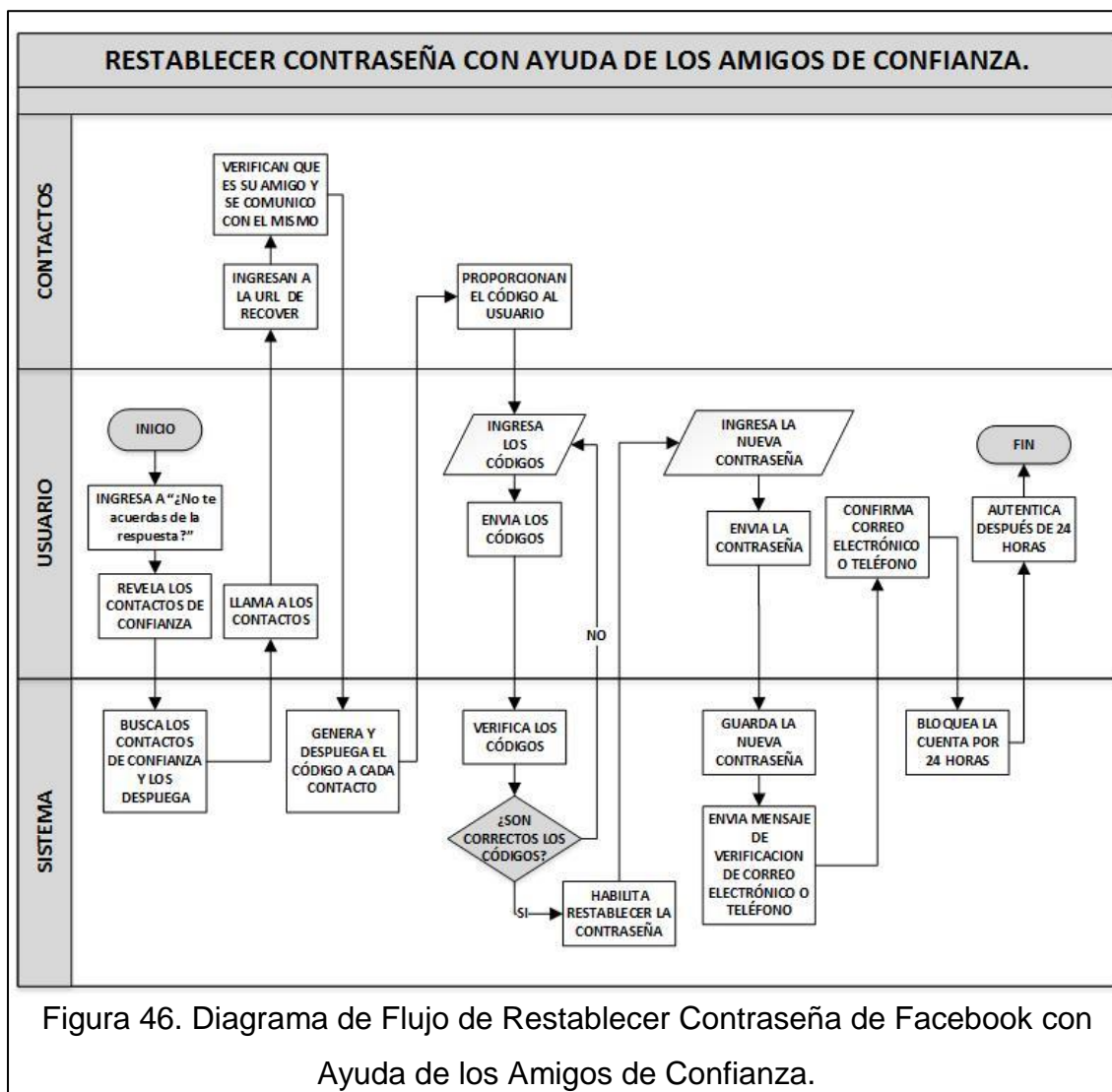


Controles:

- Verifica la respuesta de la pregunta de seguridad.
- Confirmación de la dirección del correo electrónico o teléfono.
- Bloquea la cuenta por 24 horas.

CON-AUT05. Restablecer contraseña con ayuda de los amigos de confianza.

Este proceso consta en revelar los amigos de confianza que son entre 3 a 5 contactos los cuales son configurados con anterioridad en la cuenta. Se localiza a los contactos y se les pide que accedan a la URL <https://www.facebook.com/recover>, en el cual sale una pantalla de confirmación de que le conocen al usuario y verifican que se comunicaron con el mismo. La herramienta genera y despliega un código a cada amigo de confianza, el cual debe ser ingresado por el usuario para poder proceder a cambiar la clave. El sistema envía el enlace para verificar el correo electrónico o el número de teléfono y una vez verificado bloquea la cuenta por 24 horas por motivos de seguridad del usuario.



Controles:

- Confirma el amigo de confianza que su amigo se comunicó.
- Verificación de los códigos de seguridad.
- Confirmación de la dirección del correo electrónico o teléfono.
- Bloquea la cuenta por 24 horas.

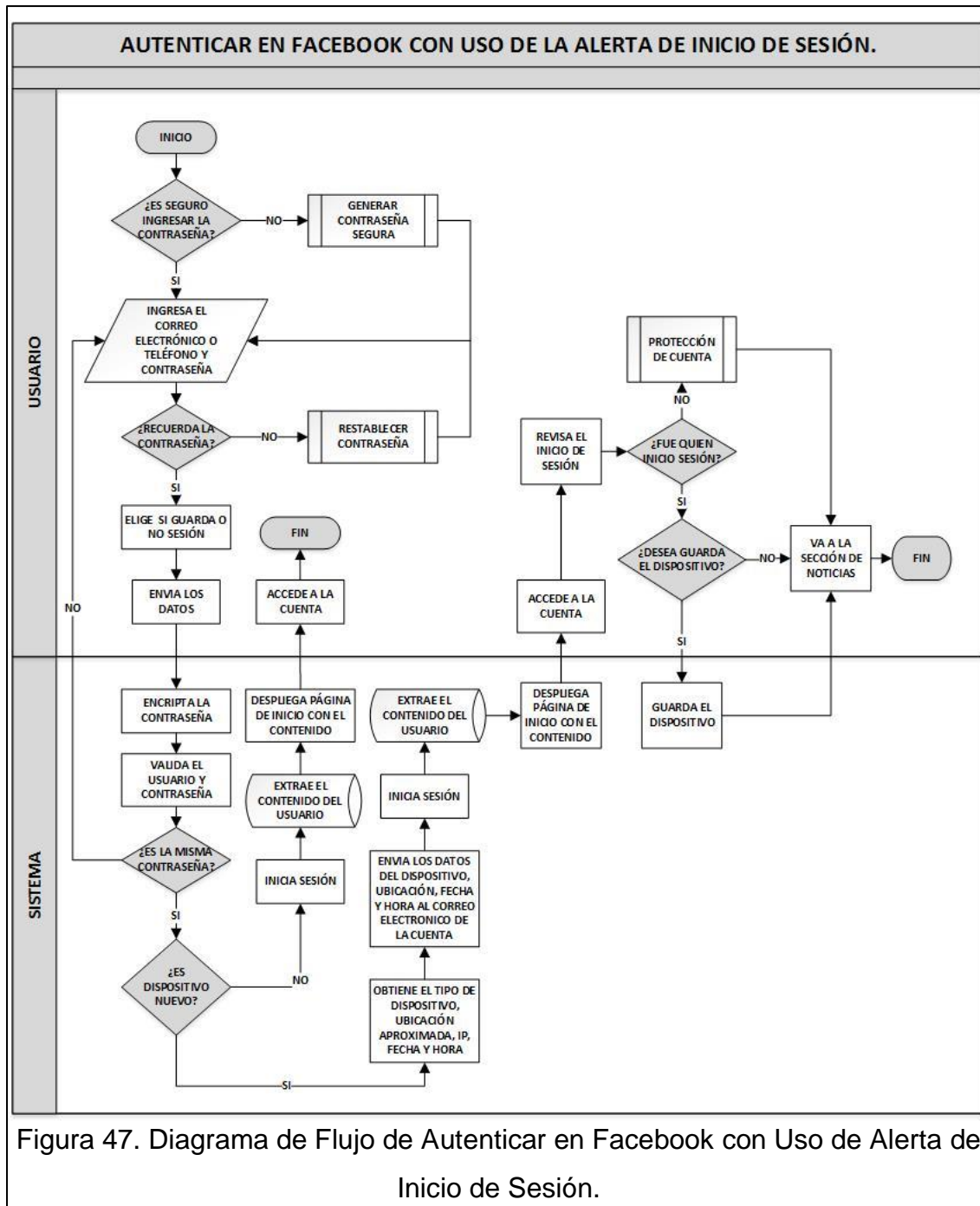
[CON-AUT06](#). Alerta de inicio de sesión en Facebook.

El fin es que el usuario tenga mayor control de seguridad al autenticar su cuenta. Es una forma más sencilla de descubrir si alguien extraño o sin autorización está accediendo a la cuenta.

El proceso de autenticación es el mismo, lo que tiene como función adicional es la verificación del dispositivo y en caso de ser nuevo obtiene los datos del dispositivo para posteriormente enviar la información como notificación a la cuenta del usuario y al correo electrónico.

La alerta despliega el dispositivo, la fecha, hora y ubicación aproximada del dispositivo en el que se ingresó a la cuenta de Facebook. Si el usuario identifica que no fue él quien inicio sesión, debe realizar la protección de cuenta.

Si es un dispositivo que se usa constantemente y es privado se guarda para que en próximas ocasiones no envíe dicha alerta.



Controles:

- Encriptación de contraseña.
- Validación de usuario y contraseña.
- Verifica si el dispositivo es nuevo, en caso de serlo obtiene y envía los datos del dispositivo como notificación y correo electrónico para ser revisado.
- Protección de cuenta. ([CON-AUT08](#))

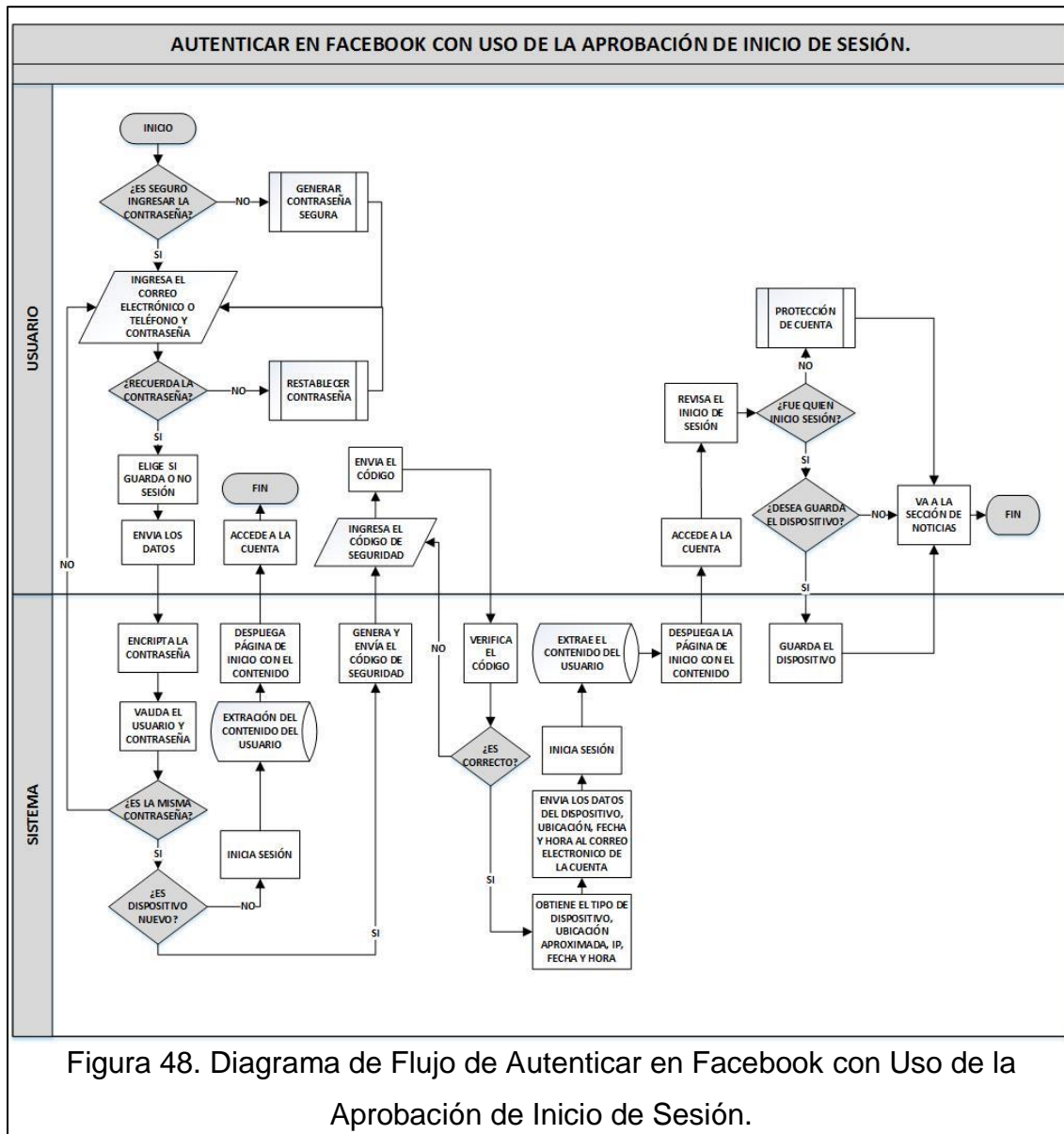
CON-AUT07. Aprobación de inicio de sesión.

Facebook tiene otra opción para controlar la seguridad en la autenticación y es al activar la aprobación de inicio de sesión. Esta función solicita un código de seguridad especial cada vez que se ingrese a la cuenta de Facebook desde un dispositivo nuevo.

Los códigos son enviados mediante mensajes de texto al número de teléfono, se obtienen 10 códigos y se guardan para cuando sea necesario o se utiliza el generador de códigos en caso de tener la aplicación de Facebook en el Smartphone. (Facebook, s.f.)

Esta opción tiene la alerta de inicio de sesión automáticamente activada. La alerta despliega el dispositivo, la fecha, hora y ubicación aproximada del dispositivo en el que se ingresó a la cuenta de Facebook. Si el usuario identifica que no fue él quien inicio sesión, debe realizar la protección de cuenta.

Si es un dispositivo que se usa constantemente y es privado se guarda para que en próximas ocasiones no envíe dicha alerta.



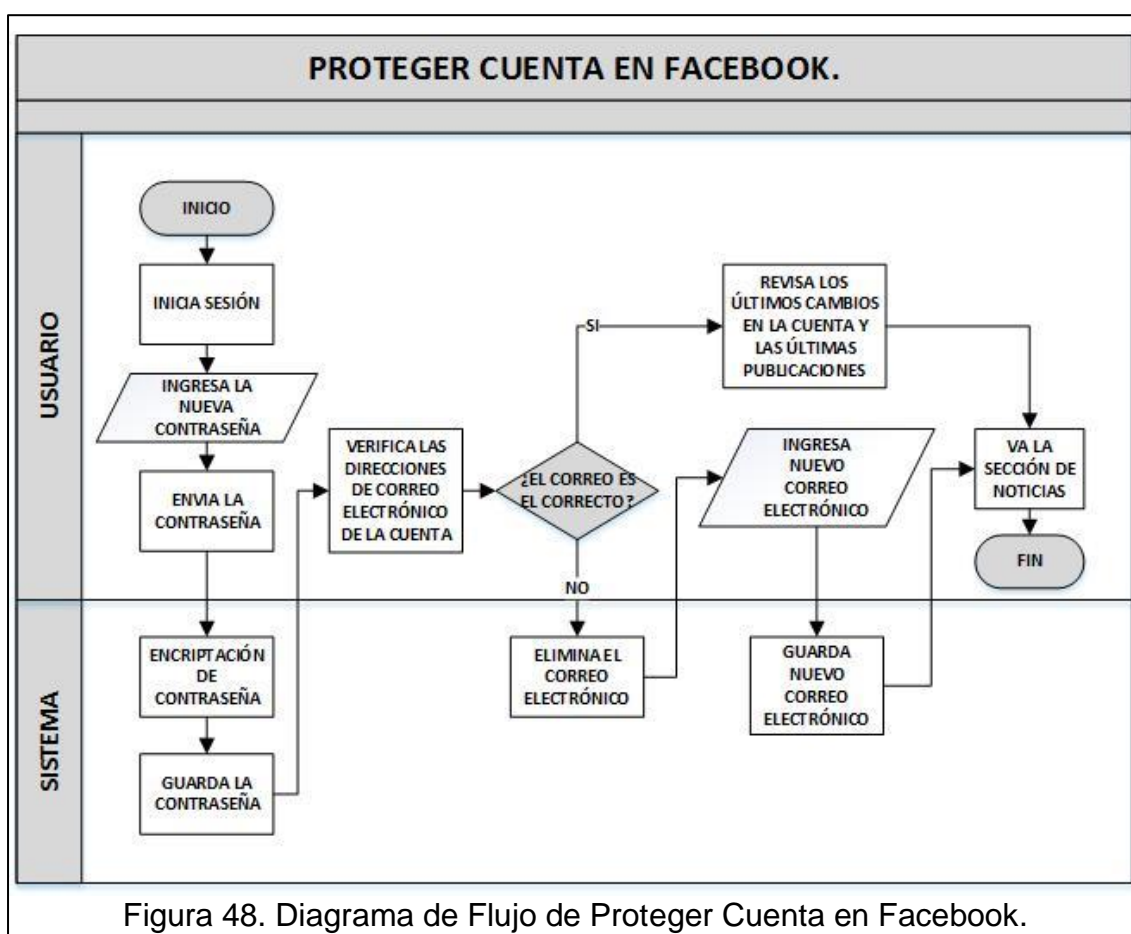
Controles:

- Encriptación de contraseña.
- Validación de usuario y contraseña.
- Verifica si el dispositivo es nuevo, en caso de serlo genera el código de seguridad.
- Verificación del código de seguridad.
- Revisión del inicio de sesión en la notificación y correo electrónico.
- Protección de cuenta. ([CON-AUT08](#))

CON-AUT08. Protección de cuenta.

En los casos que alguien está ingresando a la cuenta sin permiso o que el dispositivo se encuentra con virus o malware, se opta por la opción de protección de cuenta.

El proceso de proteger la cuenta se basa en cambiar la contraseña, verificar la o las direcciones de correos electrónicos de la cuenta, revisar las últimas acciones realizadas de la cuenta y en caso que no sean los correos electrónicos se eliminan e ingresa uno nuevo.



Controles:

- Encriptación de contraseña.
- Verificación de las direcciones de correo electrónico de la cuenta.
- Revisión de los últimos cambios de la cuenta y últimas publicaciones.

3.1.2.5.3. Configuración de la Cuenta.

La configuración de la cuenta se basa en la edición de los datos sensibles como nombre y fecha de nacimiento, la personalización de anuncios, desactivar y eliminar cuenta.

- [PRO-CONF01](#). Nombres en Facebook.
- [PRO-CONF02](#). Editar fecha de nacimiento.
- [PRO-CONF03](#). Editar pregunta de seguridad.
- [PRO-CONF04](#). Configurar anuncios.
- [PRO-CONF05](#). Desactivar cuenta.
- [PRO-CONF06](#). Eliminar cuenta.

Controles opcionales:

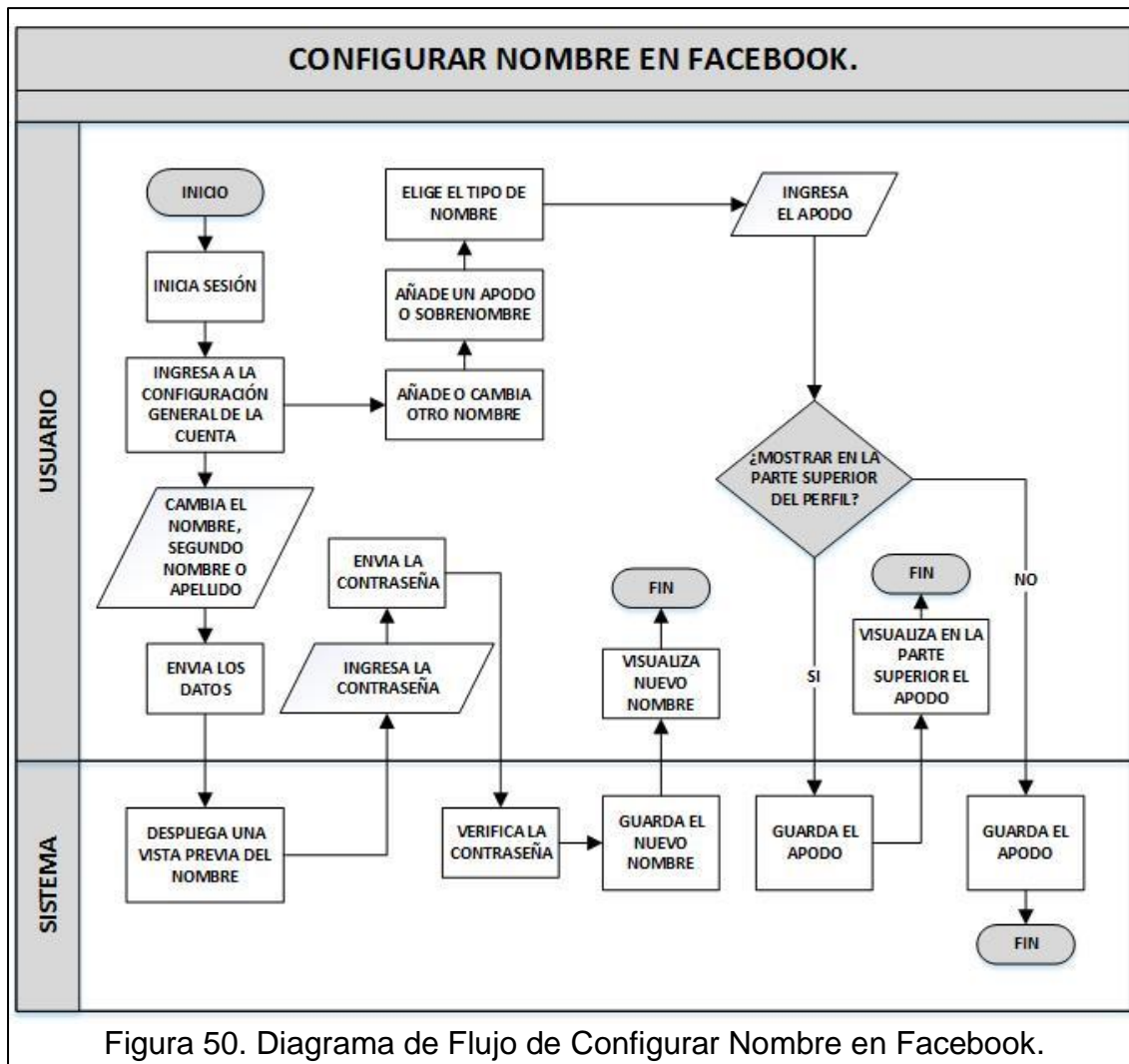
- [CON-PER01](#). Controles de privacidad en la información del perfil.
- [CON-PER02](#). Privacidad en la dirección electrónica.
- [CON-PER03](#). Privacidad en las secciones.
- [CON-PER04](#). Privacidad en la lista de amigos, solicitudes y búsqueda en Facebook.
- [CON-PER05](#). Control de privacidad de solicitud y búsqueda de usuario en Facebook.

[PRO-CONF01](#). Nombres en Facebook.

El nombre puede ser cambiado cada 60 días. Se cambia en la configuración general de la cuenta, en el que puede editar el nombre, segundo nombre o apellido. El sistema despliega una vista previa del nombre y solicita que el usuario ingrese la contraseña, una vez verificada la contraseña el sistema guarda el nuevo nombre y es visible para el usuario.

La red social permite agregar otro nombre en la cuenta para apodos, nombres profesionales, etc. Para añadir o cambiar ingresa a la configuración general de la cuenta, en añadir o cambiar otro nombre, elige el tipo de nombre e ingresa el

apodo. El usuario elige si muestra el apodo en la parte superior del perfil, el sistema guarda el apodo y lo hace visible para el usuario.



Controles:

- Verificación de contraseña.

[PRO-CONF02](#). Editar fecha de nacimiento.

En Facebook es posible cambiar la fecha de nacimiento, para lo que el usuario ingresa a la información general, en editar la información básica y de contacto, en el cual edita la fecha de nacimiento.

Ingresa la nueva fecha de nacimiento y edita el selector de público en el día, mes, y año. La fecha de nacimiento se puede indicar solo el día y mes o solo el año o completa. Cuando no se comparte el día y mes, los contactos no reciben la notificación de su cumpleaños.

El usuario confirma la edad para que el sistema guarde la fecha de nacimiento, aumente el contador de cambios y bloquee el cambio de fecha de nacimiento por unos días. Por último, el usuario visualiza la fecha de nacimiento actualizada.

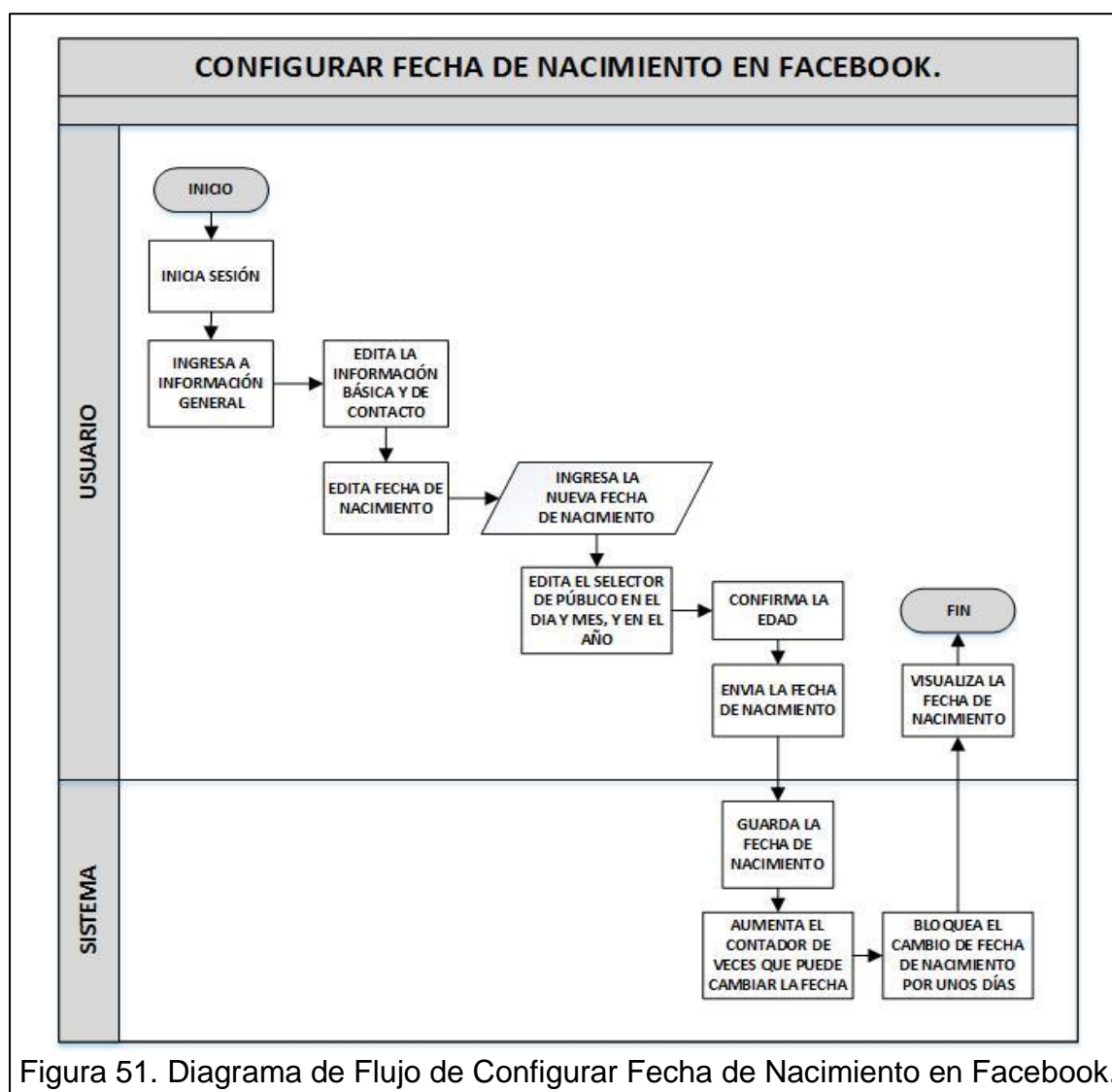


Figura 51. Diagrama de Flujo de Configurar Fecha de Nacimiento en Facebook.

Controles:

- Verificación de contraseña.

[PRO-CONF03](#). Editar pregunta de seguridad.

Facebook no permite editar la pregunta de seguridad una vez configurada.

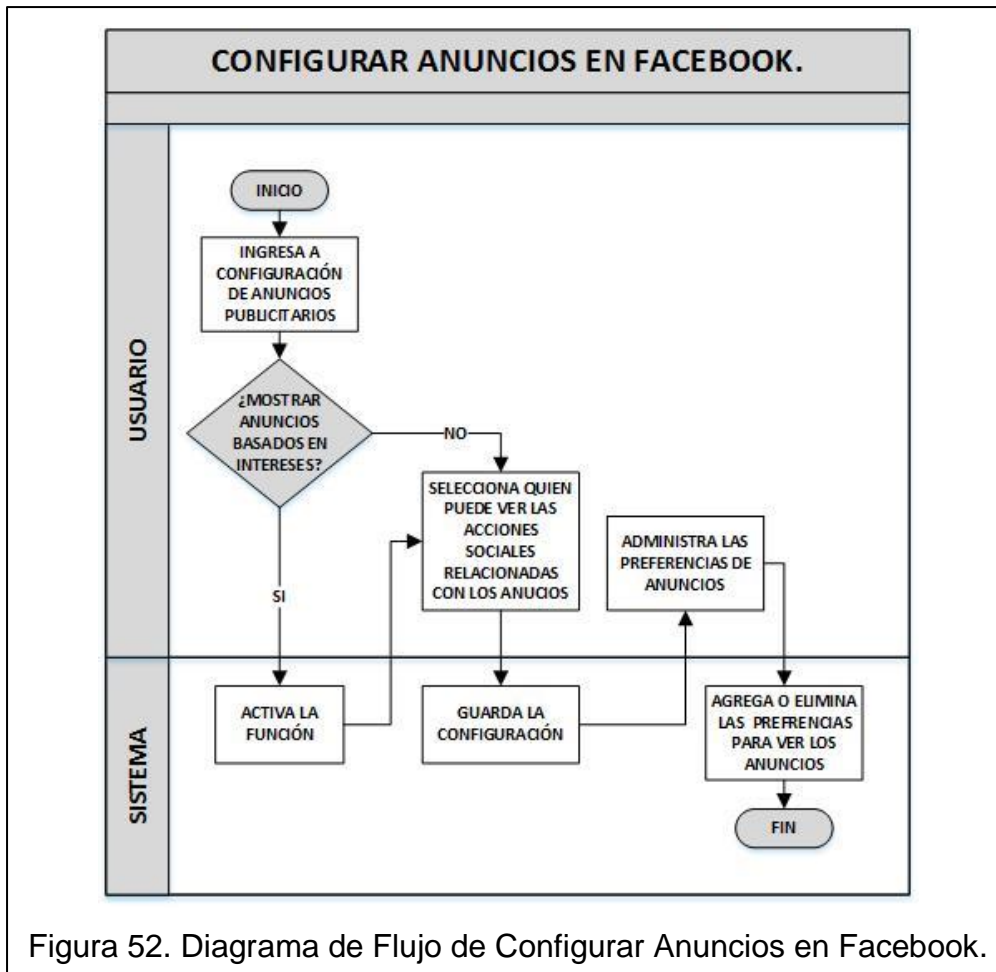
[PRO-CONF04](#). Configurar anuncios.

Los anuncios en Facebook son a base de los intereses de los usuarios, estos intereses se sacan a partir de las páginas que a un usuario le gustan, información que comparte, datos como edad, ubicación, sexo, etc. (Facebook, s.f.)

Los anuncios no se pueden ocultar por completo, ya que Facebook es gratuito por ellos. Pero permite personalizar que tipo de anuncios prefiere visualizar, en una lista que se puede modificar.

Para configurar los anuncios en Facebook, el usuario ingresa a la configuración de anuncios publicitarios y decide si desea mostrar anuncios basados en intereses, en caso de decidir que si se activa la función.

El usuario selecciona quien puede ver las acciones sociales relacionadas con los anuncios y se guarda la configuración. Así mismo, el usuario administra las preferencias de anuncios en el que agrega o elimina las preferencias para ver los anuncios.



PRO-CONF05. Desactivar cuenta.

Para desactivar la cuenta en Facebook el usuario ingresa a la configuración general de la cuenta y descarga la copia de información para la cual ingresa la contraseña, una vez verificada la contraseña el sistema recopila la información, crea el archivo, guarda la información en el archivo, crea y envía el correo electrónico con el enlace para descargar.

El usuario accede al correo electrónico y al enlace proporcionado y procede a descargar la información para el cual debe ingresar la contraseña de su cuenta, una vez verificada y descargada visualiza la carpeta con la información e ingresa a la configuración de seguridad, accede a desactivar cuenta, ingresa la razón por la que desactiva la cuenta y confirma que desea desactivar la cuenta. El sistema procede a inhabilitar la cuenta.

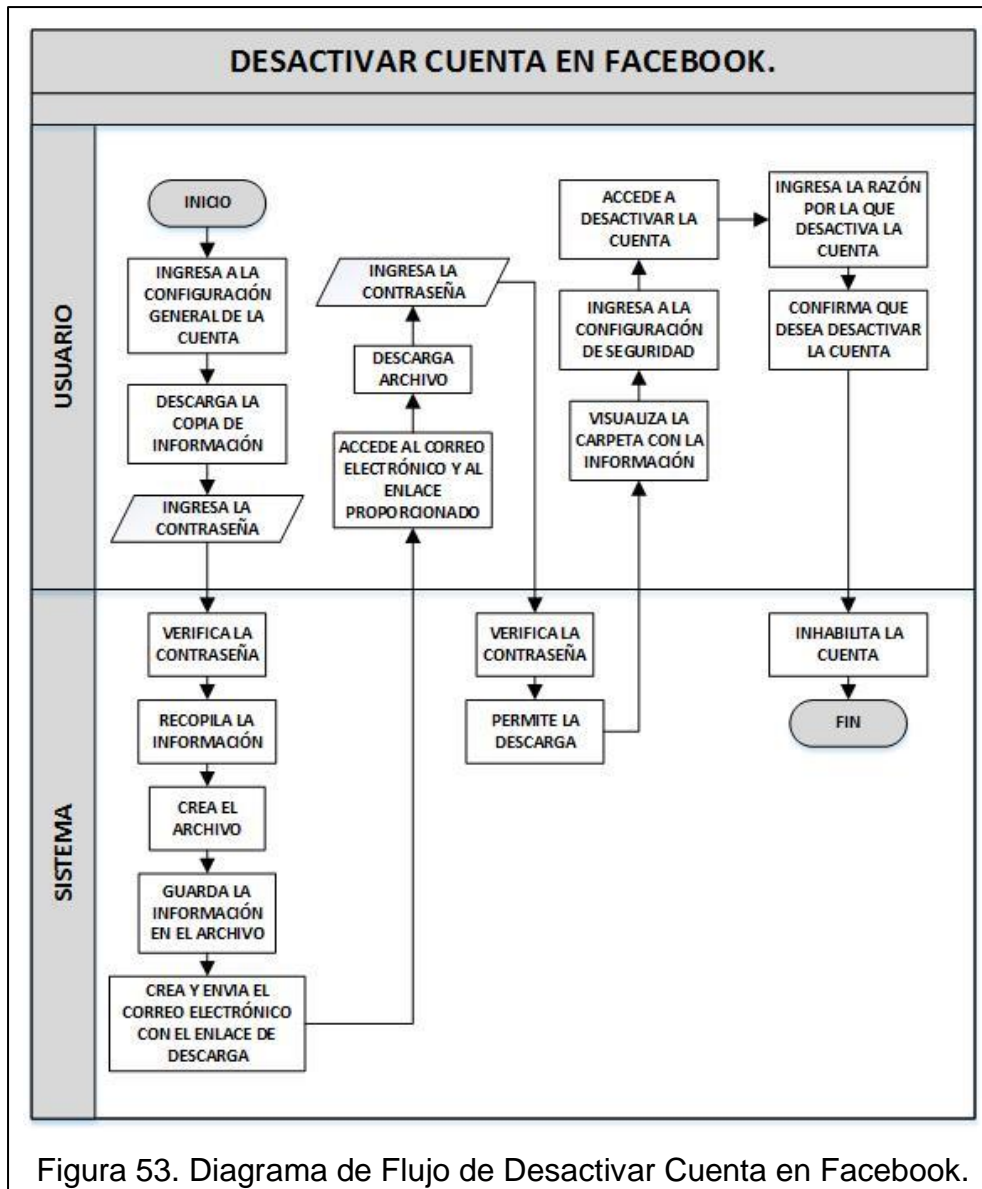


Figura 53. Diagrama de Flujo de Desactivar Cuenta en Facebook.

Controles:

- Verificación de contraseña.
- Copia de seguridad (información).
- Confirmación que desea desactivar la cuenta.

[PRO-CONF06](#). Eliminar cuenta.

Al eliminar definitivamente la cuenta se tiene que tener claro que no se podrá reactivar ni recuperar.

Cuando se elimina la cuenta la red social primero inhabilita 14 días por si el usuario quiere cancelar la solicitud. Una vez pasado el tiempo establecido procede a eliminar toda la información. Facebook se demora hasta 90 días para eliminar toda la información como publicaciones, fotos, estados, etc. En el transcurso de este tiempo los otros usuarios no pueden acceder a la misma. Los mensajes que tienen otros usuarios desde la cuenta no se borran. (Facebook, s.f.)

Se puede solicitar que se elimine la cuenta de una persona que se encuentra enferma, fallecida o condenado por delito sexual. (Facebook, s.f.)

Para eliminar la cuenta, el usuario ingresa a la configuración general de la cuenta y descarga la copia de información para la cual ingresa la contraseña, una vez verificada la contraseña el sistema recopila la información, crea el archivo, guarda la información en el archivo, crea y envía el correo electrónico con el enlace para descargar.

El usuario accede al correo electrónico y al enlace proporcionado y procede a descargar la información para el cual debe ingresar la contraseña de su cuenta, una vez verificada y descargada visualiza la carpeta con la información e ingresa a la URL [/HELP/DELETE_ACCOUNT](#), acepta eliminar la cuenta, ingresa la contraseña y selecciona todas las fotos que aparece el animal o planta indicada. Una vez enviada la información el sistema inhabilita la cuenta y después de 14 días elimina definitivamente la cuenta.

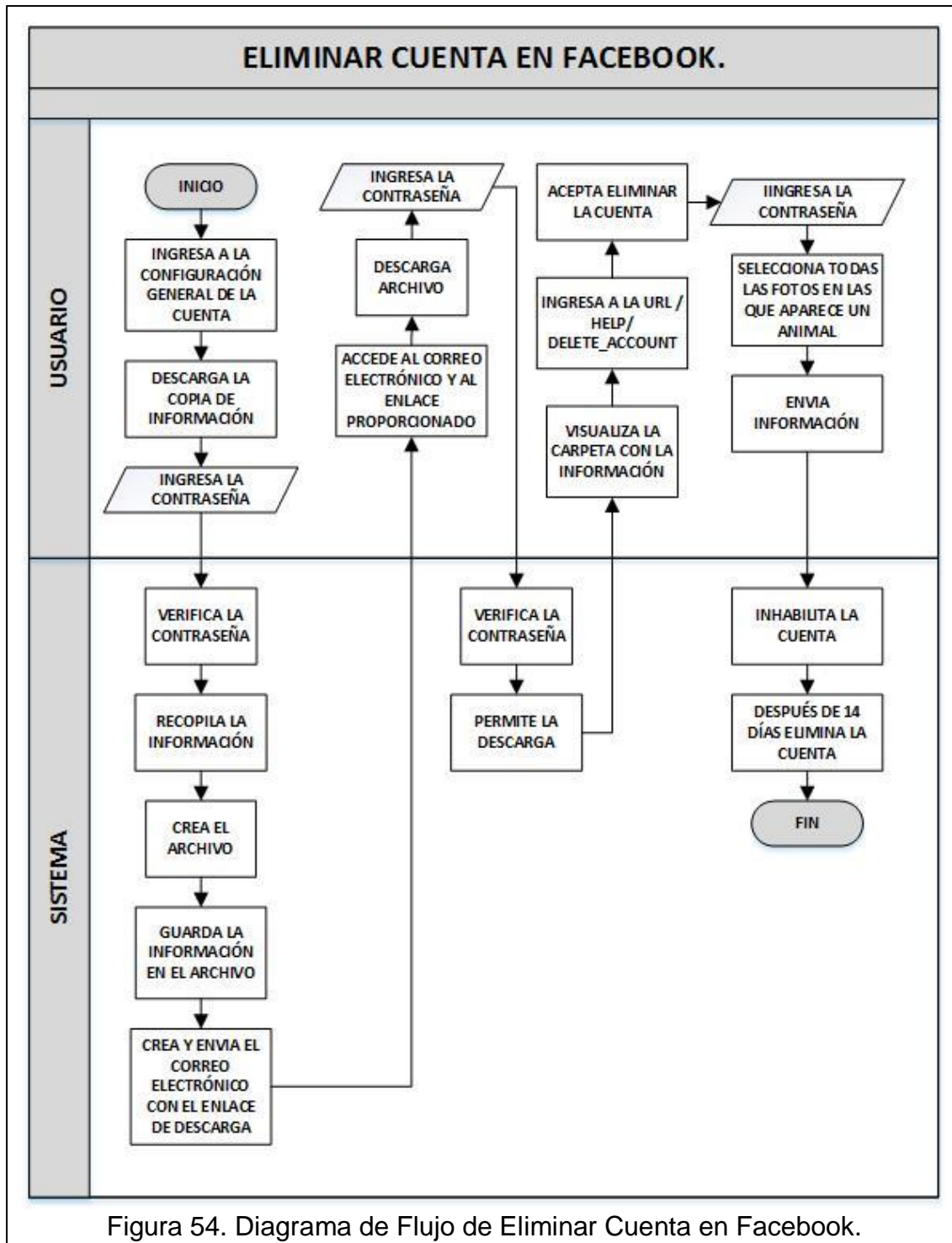


Figura 54. Diagrama de Flujo de Eliminar Cuenta en Facebook.

Controles:

- Verificación de contraseña.
- Copia de seguridad (información).
- Selecciona todas las fotos en las que aparece un animal.

CON-PER01. Controles de privacidad en la información del perfil.

Facebook permite controlar con quien se comparte la información del perfil y biografía. Solo la información pública del perfil, como el nombre, foto de perfil, foto de portada, género, edad, idioma, país, URL del perfil y redes, no se puede controlar su audiencia, siempre será visible. (Facebook, s.f.)

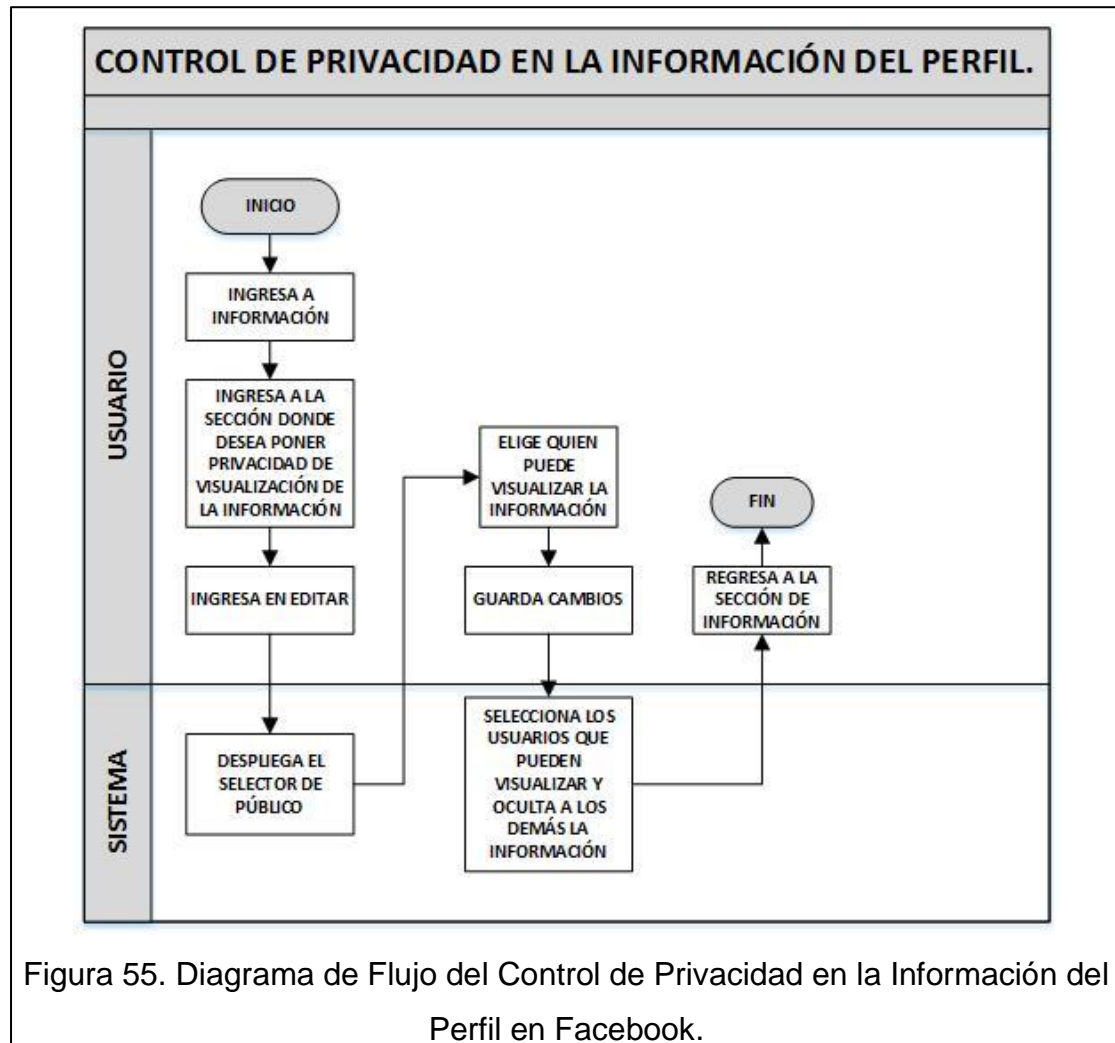
La información del perfil que se puede controlar la privacidad es la formación y empleo, lugares en los que vivió, información básica y de contacto, familia y relaciones e información adicional sobre el usuario.

Para hacer uso del control de privacidad de la información del perfil, el usuario ingresa en información, a la sección donde desea poner la privacidad de visualización de información, ingresa en editar y el sistema despliega el selector de público.

Existen cuatro opciones en el selector de público:

1. El "Público" permite a todos los usuarios de la web visualizar la publicación.
2. "Amigos" es para que solo los contactos del usuario puedan observar la publicación.
3. "Solo yo" es para publicaciones privadas que solo el usuario pueda ver.
4. "Personalizado" es para compartir las publicaciones con determinados contactos o para ocultar de ciertos usuarios.

El usuario elige quien puede visualizar la información y guarda los cambios, el sistema selecciona los usuarios que pueden visualizar y oculta a los demás la información.



Controles:

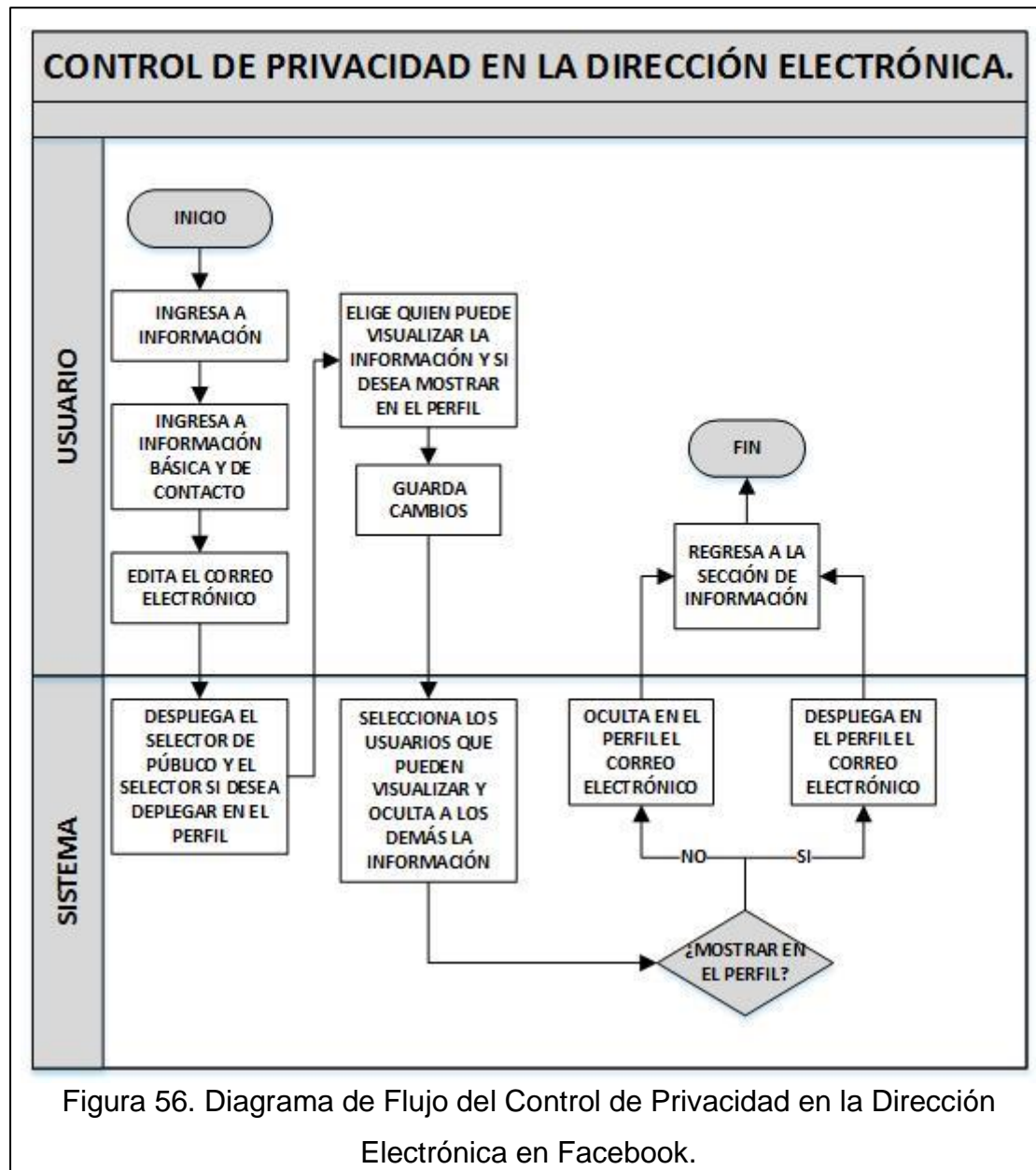
- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

[CON-PER02](#). Privacidad en la dirección electrónica.

Facebook permite ajustar la privacidad en la dirección del correo electrónico, en la cual elige con quien desea compartir y si desea mostrar en el perfil o no.

Para configurar la privacidad, el usuario ingresa a información en información básica y de contacto, en el cual edita el correo electrónico. El sistema despliega el selector de público y el selector si desea desplegar en el perfil, el usuario

elige quien puede visualizar la información y si desea mostrar en el perfil. El sistema selecciona los usuarios que pueden visualizar y oculta a los demás la información, en caso de elegir mostrar en el perfil se despliega o en caso contrario lo oculta.



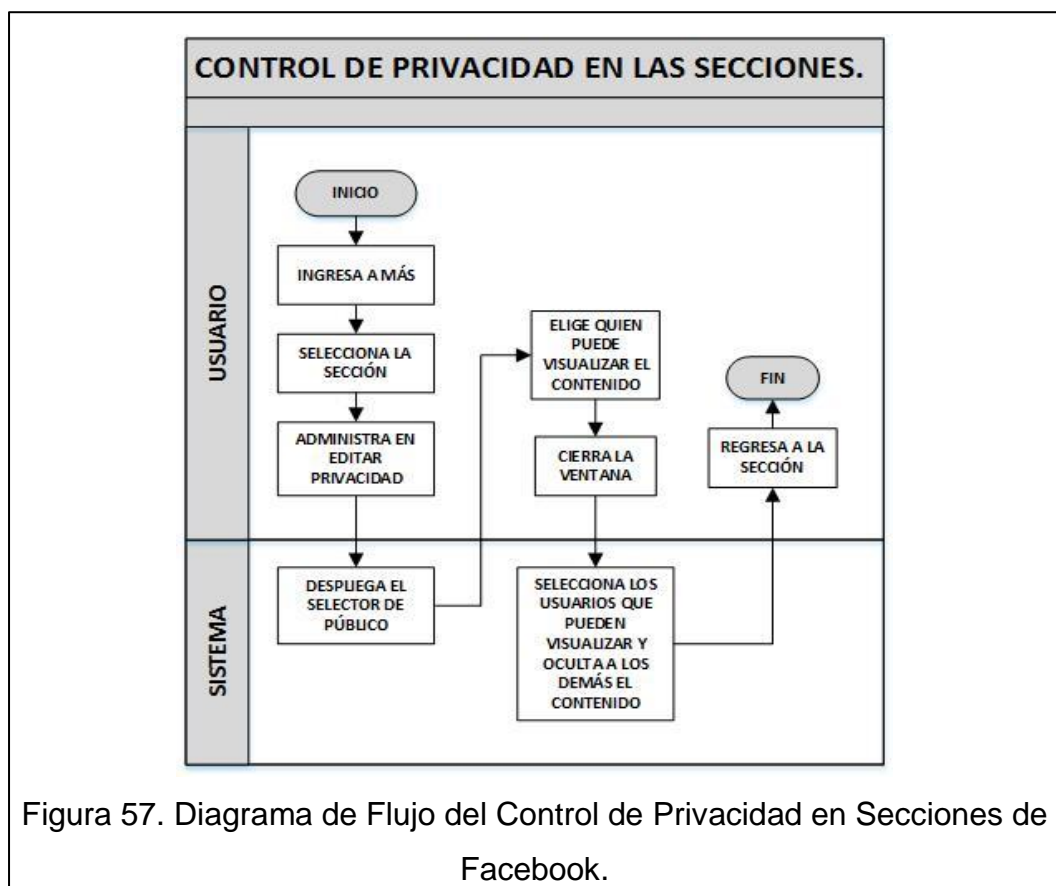
Controles:

- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

CON-PER03. Privacidad en las secciones.

También se puede controlar la privacidad en las secciones de la página, como películas, programas de TV, música, deportes, libros, páginas que le gusta al usuario, aplicaciones y juegos. Se da privacidad a las cosas que se añaden, que indican que les gusta e historias de aplicaciones y juegos. Se usa el selector de público como en los demás controles de privacidad.

El usuario ingresa a Más y selecciona la sección, administra en editar privacidad y el sistema despliega el selector de público para que el usuario elija quien puede visualizar el contenido. Una vez cerrada la ventana el sistema selecciona los usuarios que pueden visualizar y oculta a los demás el contenido.



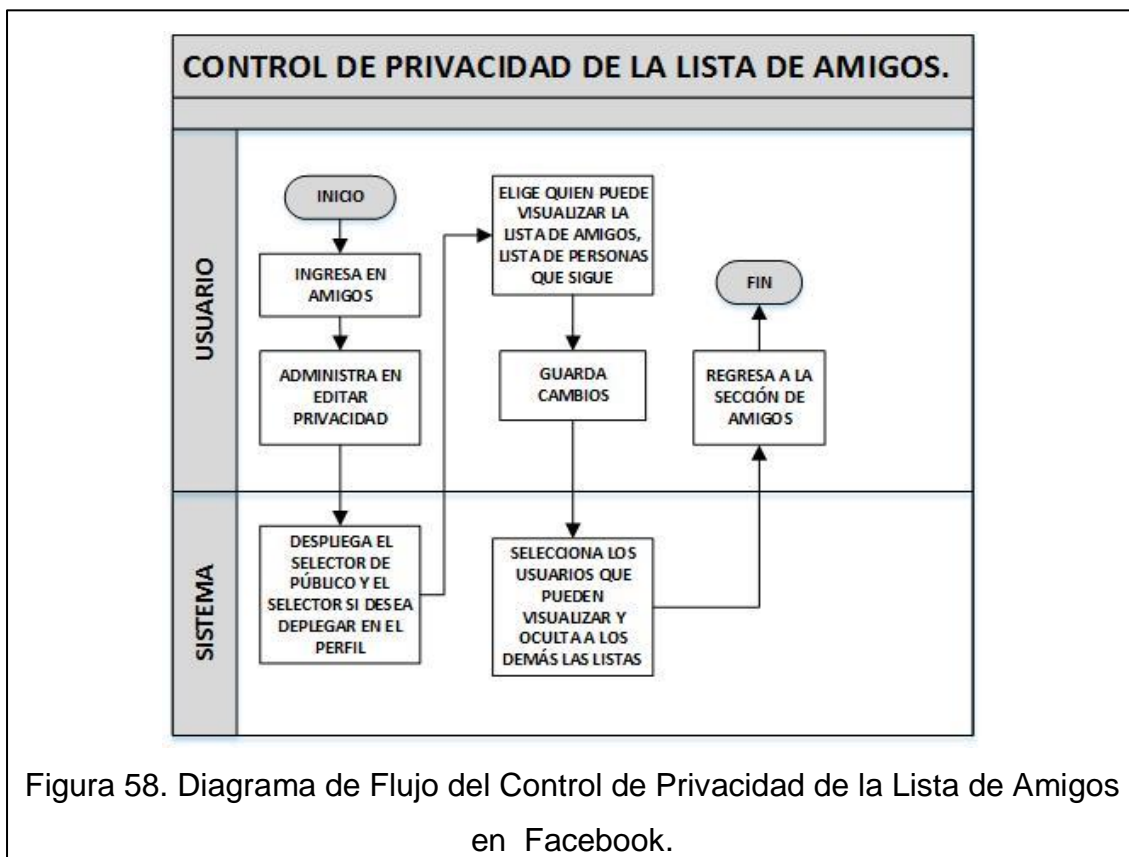
Controles:

- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

[CON-PER04](#). Privacidad en la lista de amigos, solicitudes y búsqueda en Facebook.

Facebook entre sus opciones para administrar la privacidad, permite también elegir quien puede visualizar a la lista de amigos y listas que sigue. Los amigos en común serán siempre visibles en la sección de amigos.

El usuario ingresa en amigos y administra en editar privacidad, el sistema despliega el selector de público y el selector si desea desplegar en el perfil. El usuario elige quien puede visualizar la lista de amigos y la lista de personas que sigue. Una vez guardados los cambios, el sistema selecciona los usuarios que pueden visualizar y oculta a los demás las listas.



Controles:

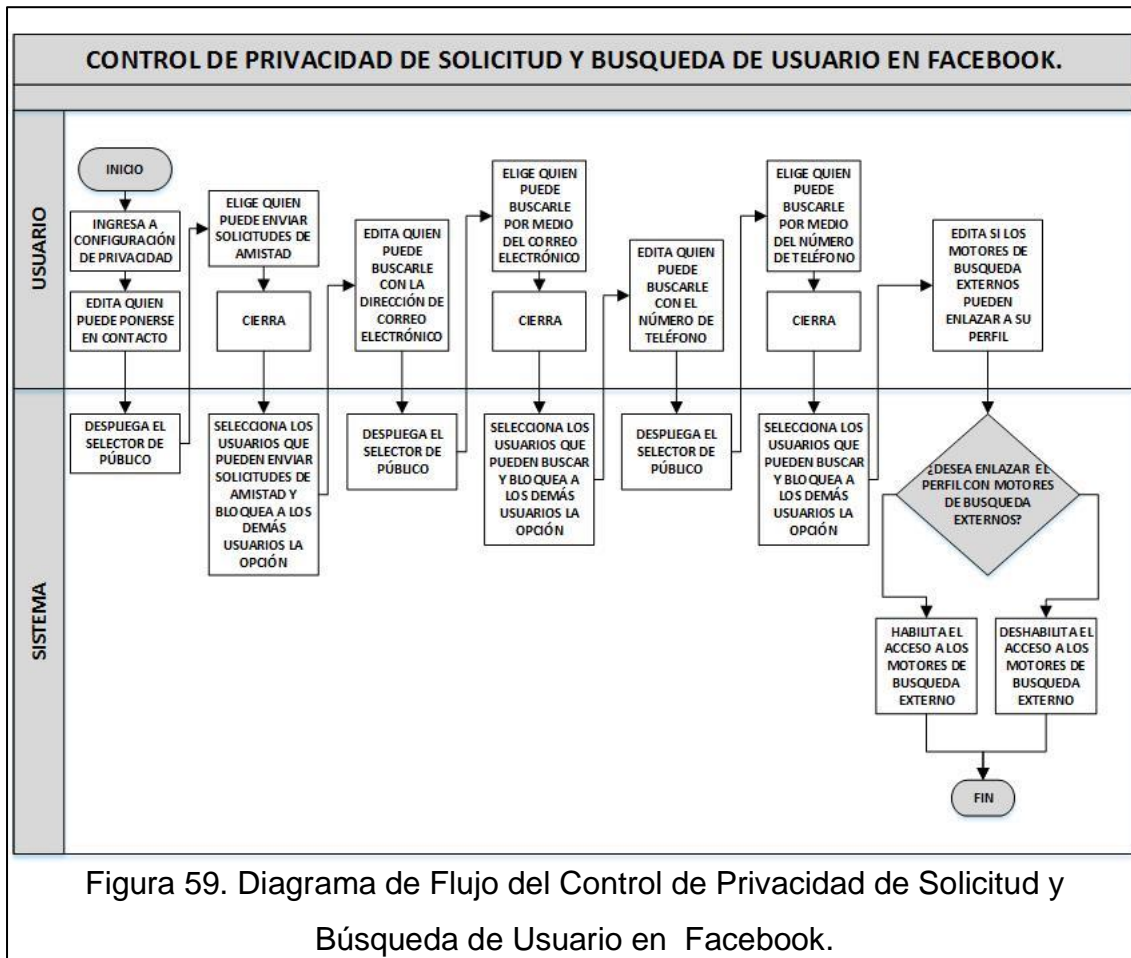
- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

[CON-PER05](#). Control de privacidad de solicitud y búsqueda de usuario en Facebook.

Se puede también configurar quien puede enviar solicitudes de amistad a un usuario. Solo existen dos opciones “Todos” o “Amigos de amigos”. Así mismo, es posible configurar quien puede buscarle al usuario, por medio de la dirección electrónica, número de teléfono o motor de búsqueda.

El usuario ingresa a configuración de privacidad y edita quien puede ponerse en contacto, el sistema despliega el selector de público para que el usuario elija quien puede enviar solicitudes de amistad. El sistema selecciona los usuarios que pueden enviar solicitudes de amistad y bloquea a los demás usuarios la opción.

Es el mismo proceso para elegir quien puede buscar por medio de la dirección de correo electrónico, elegir quien puede buscar por medio del número de teléfono y para elegir si los motores de búsqueda externos pueden enlazar al perfil del usuario para lo cual se habilita o deshabilita el acceso a los motores de búsqueda externa.



Controles:

- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

3.1.2.5.4. Compartir Contenido. ([PRO-COM01](#))

Para compartir contenido el usuario ingresa a la cuenta de Facebook y decide si el contenido es nuevo o desea compartir contenido ya publicado. Si decide compartir nuevo contenido, ingresa el contenido, etiqueta a las personas en la publicación, agrega que está haciendo o sintiendo, registra la ubicación, selecciona quien puede ver la publicación y envía el contenido. El sistema analiza la información automáticamente en sus equipos, guarda y despliega el contenido para que el usuario lo visualice.

En caso de compartir contenido ya publicado tiene tres opciones que es enviar por medio de mensaje, compartir la publicación directamente y compartir la publicación.

Para enviar por mensaje ingresa el usuario, comenta y envía el contenido, el sistema busca el usuario, envía y despliega el contenido por medio del mensaje.

Para compartir directamente la publicación solo envía el contenido, el sistema analiza la información, guarda y despliega el contenido para que el usuario lo visualice.

Para compartir la publicación normal, añade la etiqueta a las personas en la publicación, agrega que está haciendo o sintiendo, registra la ubicación, selecciona quien puede ver la publicación y envía el contenido. El sistema analiza la información en sus equipos, guarda y despliega el contenido para que el usuario lo visualice.

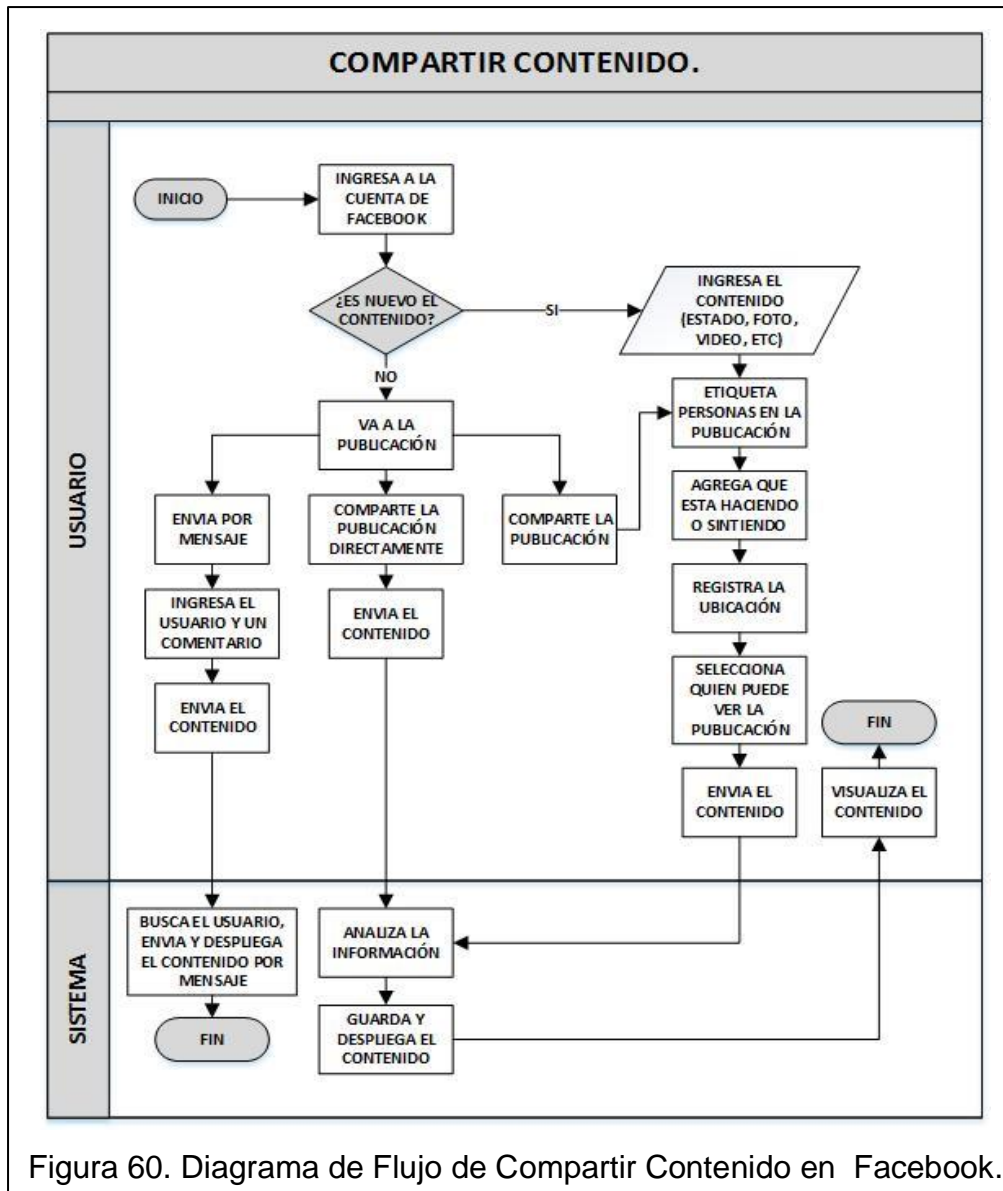


Figura 60. Diagrama de Flujo de Compartir Contenido en Facebook.

Controles:

- Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos.

Controles opcionales:

- [CON-PUB01](#). Controles de privacidad en publicaciones.
- [CON-PUB02](#). Control de privacidad en publicaciones que otros usuarios realizan en la biografía.
- [CON-PUB03](#). Revisión de la biografía.
- [CON-PUB04](#). Visualizar como otros usuarios ven la biografía.

CON-PUB01. Controles de privacidad en publicaciones

Facebook para la seguridad del usuario al publicar contenido tiene la opción de elegir con quien desea compartir dicha información.

Es parecido al control de privacidad de la información del perfil, se controla por medio de las mismas opciones de audiencia. La herramienta recuerda a que audiencia estuvo la última publicación, por lo que si no se cambia seguirá siendo la misma.

La audiencia se puede observar en el lado superior de la publicación compartida y se puede cambiar ahí mismo.

Para configurar el control de privacidad en publicaciones realizadas, el usuario ingresa a la configuración de privacidad y edita quien puede ver las publicaciones. El sistema despliega el selector de público para que el usuario elija quien puede visualizar. Una vez elegida la audiencia, el sistema selecciona los usuarios que pueden visualizar las publicaciones y oculta a los demás usuarios. El usuario puede limitar al público las publicaciones antiguas para que el sistema las oculte.

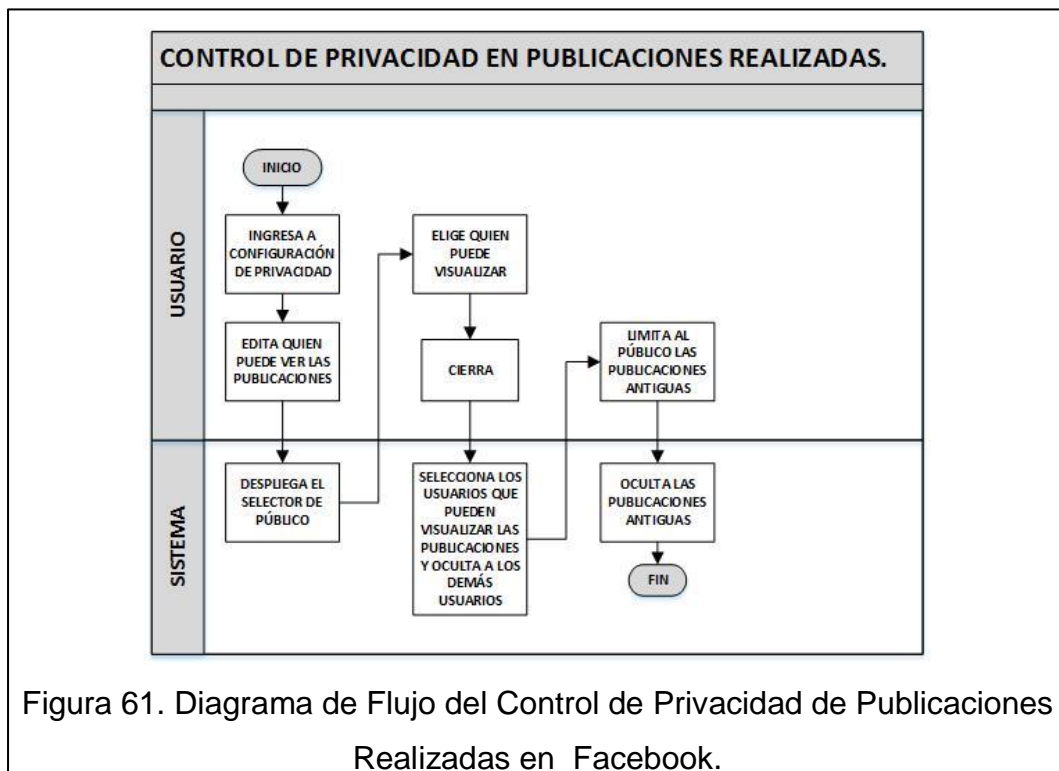


Figura 61. Diagrama de Flujo del Control de Privacidad de Publicaciones Realizadas en Facebook.

Controles:

- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

[CON-PUB02](#). Control de privacidad en publicaciones que otros usuarios realizan en la biografía.

Las publicaciones que se realizan en los muros de otros usuarios, no se pueden controlar, la decisión de que audiencia puede ver esa publicación será el dueño del muro.

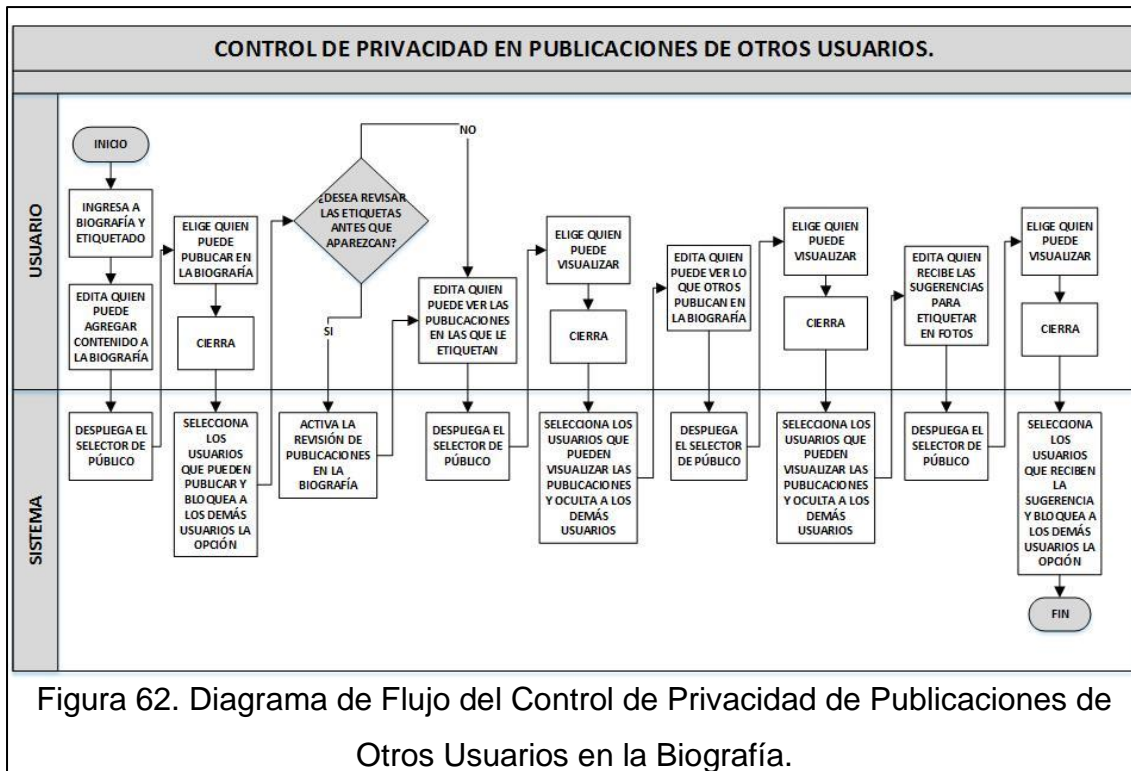
Toda publicación en la que se etiqueta a una persona es visual para ese usuario y sus contactos.

Se puede controlar quien puede ver el contenido en la biografía, tanto en publicaciones como en etiquetas. El selector de público tiene un extra que es la de "Amigos de amigos" el cual permite que sea visible hasta para los amigos de sus contactos.

El usuario ingresa a biografía y etiquetado para editar quien puede agregar contenido a la biografía, el sistema despliega el selector de público para que el usuario elija quien puede publicar en la biografía. Una vez seleccionado, el sistema selecciona los usuarios que pueden publicar y bloquea la opción a los demás usuarios.

El usuario elige si desea revisar las etiquetas antes que aparezcan en la biografía, en caso de ser afirmativo, el sistema activa la revisión de publicaciones en la biografía.

El proceso para elegir quien puede ver las publicaciones en las que se encuentra etiquetado el usuario, quien puede ver lo que otros publican en su biografía y quien recibe sugerencias para etiquetarle en fotos es la misma que para editar quien puede agregar contenido en la biografía.



Controles:

- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

CON-PUB03. Revisión de la biografía.

Facebook tiene la opción de “Revisión de la biografía” en la que el usuario revisa manualmente las publicaciones en las que fue etiquetado para permitir que aparezcan en su biografía. La etiqueta no aparece hasta que el usuario la aprueba.

El usuario ingresa a biografía y etiquetado para editar la revisión de las etiquetas antes que aparezcan, el sistema despliega el selector de activar o desactivar. Una vez seleccionado activar, se habilita la función de la revisión de publicaciones en la biografía.

El usuario edita quien puede ver las publicaciones que no se encuentran incluidas y el sistema despliega el selector de público para que el usuario elija

quien pueda visualizar. Una vez elegido, el sistema selecciona los usuarios que pueden visualizar y oculta a los demás las publicaciones.

El usuario ingresa a revisión de la biografía y revisa las publicaciones, agrega u oculta la publicación para que el sistema añada o no la publicación a la biografía.

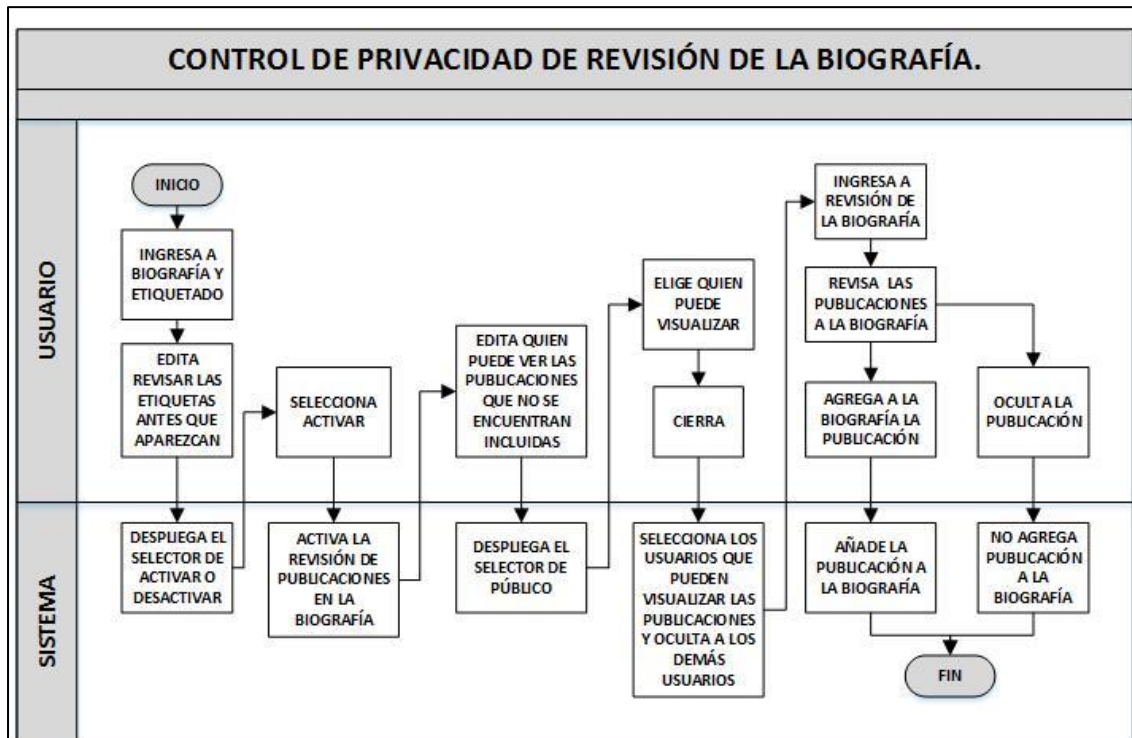


Figura 63. Diagrama de Flujo del Control de Privacidad de Revisión de la Biografía.

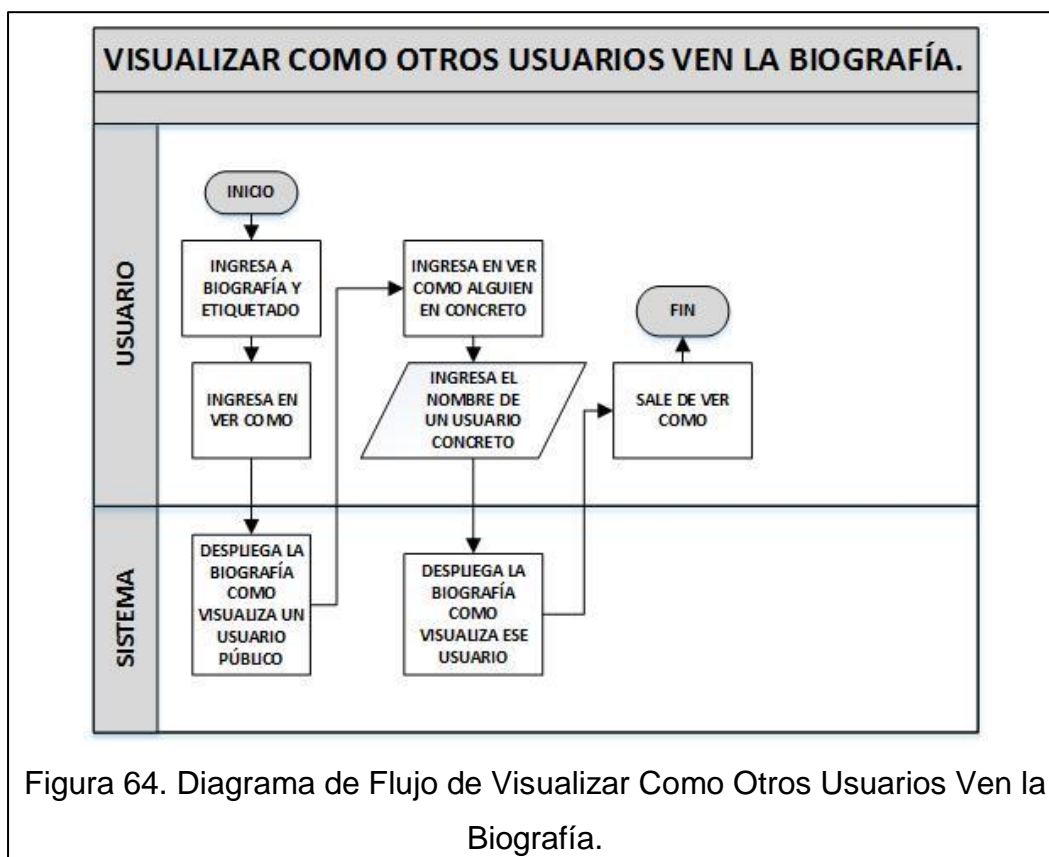
Controles:

- Revisión de etiquetas antes que aparezcan.
- Selecciona los usuarios que pueden visualizar y oculta a los demás la información.

[CON-PUB04](#). Visualizar como otros usuarios ven la biografía.

La opción “Ver como” permite observar el perfil desde el punto de vista de un usuario público. Y en caso de querer ver desde un usuario determinado, existe la opción “Ver como alguien en concreto”

El usuario ingresa a biografía y etiquetado y presiona la opción “Ver como...”, el sistema despliega la biografía como visualiza un usuario público. El usuario presiona la opción de “Ver como alguien en concreto” e ingresa el nombre del usuario que desea ver, el sistema despliega la biografía como visualiza ese usuario.



Controles:

- Desplegar la biografía como visualiza un usuario público o uno en concreto.

3.1.2.5.5. Reportar Abuso y Bloquear Usuarios, Paginas, Aplicaciones, etc.

Se puede denunciar perfiles, publicaciones, fotos, videos, mensajes, paginas, grupos, anuncios, eventos, aplicaciones, preguntas y comentarios.

- [PRO-REP01](#). Reportar abuso.
- [PRO-REP02](#). Reportar abuso por medio de formulario.
- [PRO-REP03](#). Reportar cuenta de menor de 13 años.
- [PRO-REP04](#). Bloquear en Facebook.

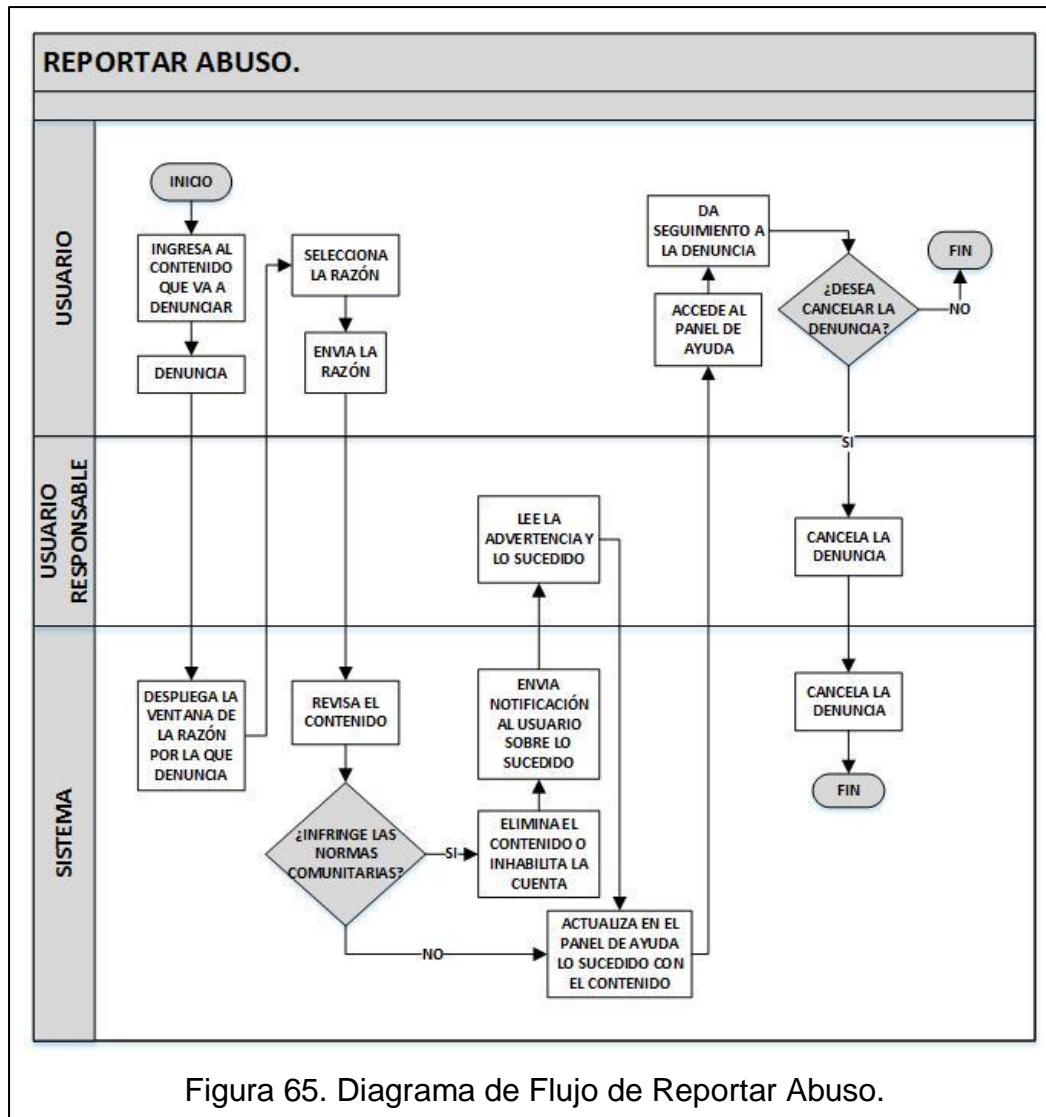
[PRO-REP01](#). Reportar abuso.

Para reportar, el usuario ingresa al contenido y presiona la opción de denunciar. El sistema despliega la ventana de la razón por la que denuncia. Una vez elegida y enviada, el sistema revisa el contenido.

Si infringe, elimina el contenido o inhabilita la cuenta y envía la notificación al responsable del contenido sobre lo sucedido.

En caso que infrinja o no, el sistema actualiza el panel de ayuda con información de lo sucedido con el contenido para que el usuario que reporto de seguimiento a la denuncia. El usuario puede decidir cancelar la denuncia en el panel de ayuda.

En caso de cuentas falsas, solo la persona que está siendo suplantada puede realizar la denuncia correspondiente. La revisión es realizada por un administrador bajo los parámetros de las normas comunitarias. El panel de ayuda es privado de cada usuario. Por este medio el usuario se comunica con las personas encargadas de administrar Facebook. (Facebook, s.f.)



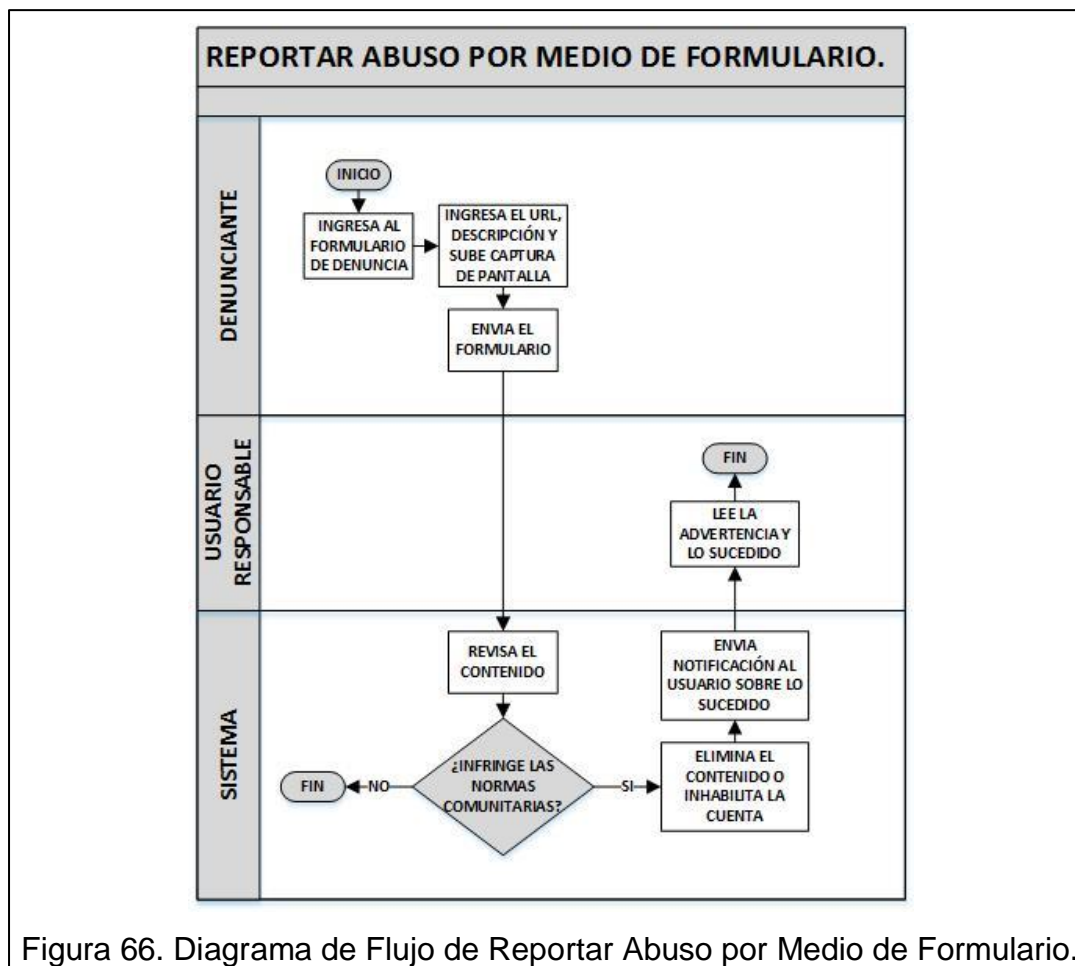
Controles:

- Revisión del contenido.
- Dar seguimiento de la denuncia por medio del panel de ayuda.

[PRO-REP02](#). Reportar abuso por medio de formulario.

En caso de no tener cuenta en Facebook, se puede denunciar llenando el formulario que proporciona la red social. La mejor forma para denunciar en estos casos, es con la URL del contenido o captura de pantalla del contenido, con el enlace de página, perfil o grupo, fecha y hora en el que fue publicado.

Para reportar por medio de formulario, el denunciante ingresa al formulario de denuncia e ingresa la URL, descripción y captura de pantalla. Una vez enviado el formulario, el sistema o el administrador revisa el contenido y si infringe las normas comunitarias elimina el contenido o inhabilita la cuenta. El sistema envía la notificación al usuario responsable sobre lo sucedido.



Controles:

- Revisión del contenido.

[PRO-REP03](#). Reportar cuenta de menor de 13 años.

En Facebook la edad mínima para crear una cuenta es de 13 años, por lo tanto se puede reportar el perfil de un menor que tenga falsa la fecha de nacimiento. (Facebook, s.f.)

Para reportar, se ingresa al formulario de denuncia, ingresa el URL, nombre completo, edad y otra información adicional. Una vez enviado el formulario el administrador revisa y si es menor de 13 años inhabilita la cuenta y envía la notificación al usuario responsable sobre lo sucedido.

El sistema actualiza el panel de ayuda con lo sucedido para que el usuario que realizo la denuncia pueda hacer seguimiento de la misma.

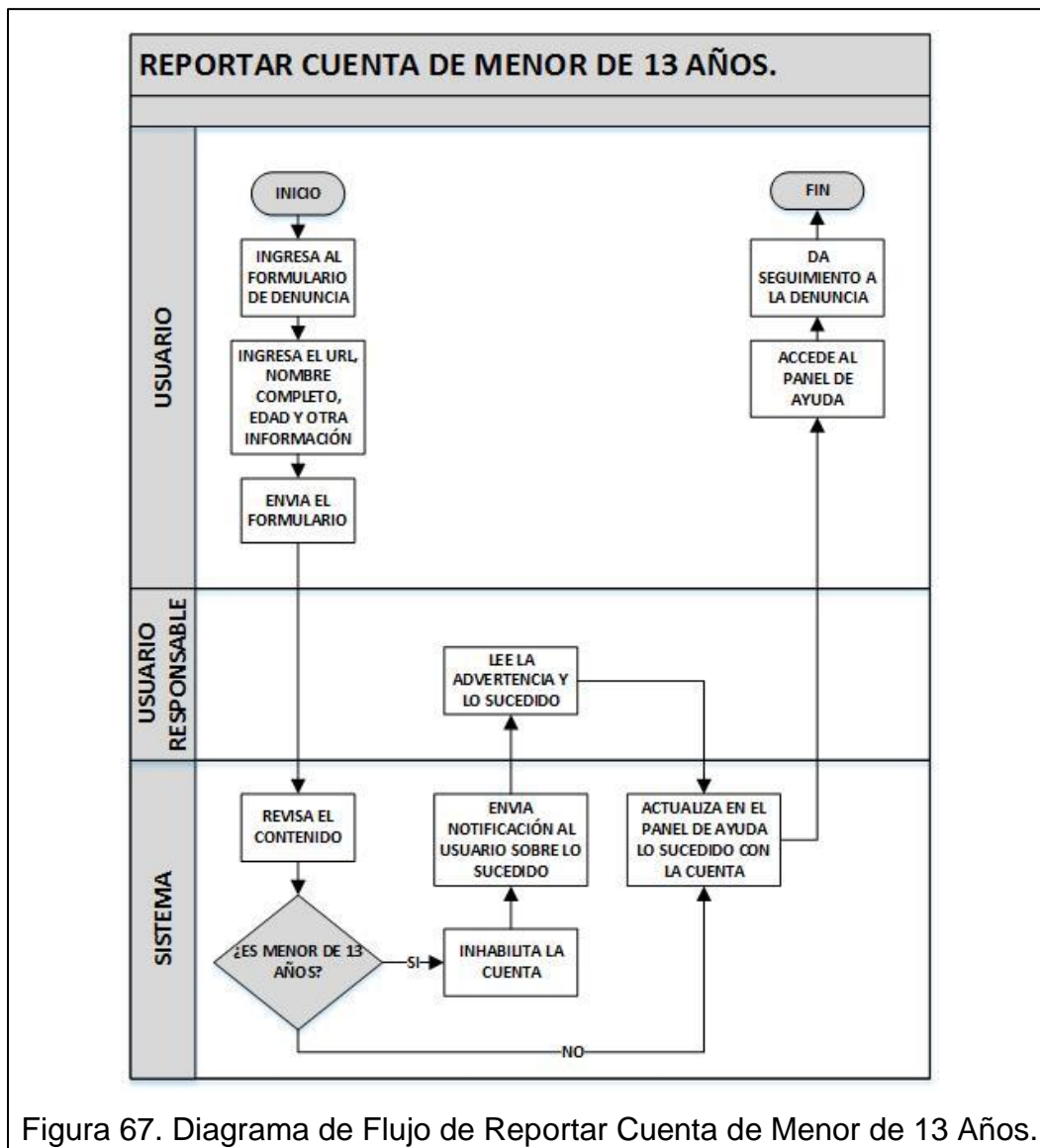


Figura 67. Diagrama de Flujo de Reportar Cuenta de Menor de 13 Años.

Controles:

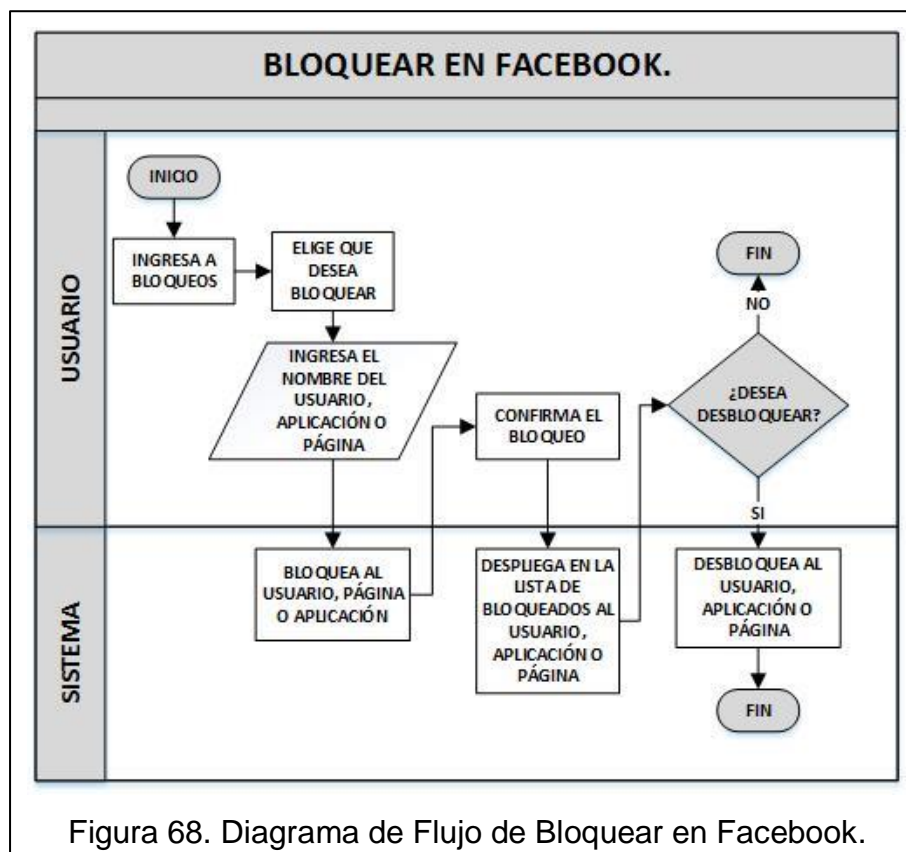
- Revisión del contenido.
- Dar seguimiento de la denuncia por medio del panel de ayuda.

PRO-REP04. Bloquear en Facebook.

Una de las opciones de mayor impacto que tiene Facebook en cuanto a seguridad es la de bloquear usuarios, mensajes, invitaciones a aplicaciones, invitaciones a eventos de una persona en concreto. También permite bloquear aplicaciones y páginas.

Esto se realiza cuando otro usuario acosa o molesta, el usuario bloqueado no recibe ninguna notificación del bloqueo.

El usuario ingresa a bloqueos, elige que desea bloquear e ingresa el nombre del usuario, aplicación o página. El sistema bloquea y espera la confirmación para desplegar en la lista de bloqueados. El usuario puede en cualquier momento desbloquear al usuario, aplicación o página.



Controles:

- Bloquear usuario, página o aplicación.

3.1.2.6. Controles de Gestión, Técnicos y Operacionales.

El sistema en cuanto a la protección de datos cuenta con los controles de gestión, controles técnicos y operacionales.

3.1.2.6.1. Controles de Gestión. ([CON-GES01](#))

Facebook cuenta con los controles de gestión, que asesora el consejo de seguridad de Facebook para la creación, actualización y ejecución. Las políticas de datos, la declaración de derechos y responsabilidades y las normas comunitarias son las principales en el mismo. (Facebook, s.f.)

La política de datos tiene el fin de que los usuarios comprendan de qué manera es usada, recopilada y compartida la información que proporcionan en la red social. Así mismo como el usuario puede administrar o eliminar su información, como responde la red social a los requerimientos legales y cómo funcionan sus servicios a nivel mundial. (Facebook, s.f.)

La declaración de derechos y responsabilidades es el documento en el que Facebook indica los principios y condiciones de servicio con relación a los usuarios y con todos los que interactúan con la red social. En dicho documento se pueden observar los compromisos que solicita Facebook por parte de los usuarios. (Facebook, s.f.)

Entre dichos compromisos se encuentra el no proporcionar información falsa, no falsificar identidad, no tener más de una cuenta personal, no utilizar la cuenta personal con fin comercial, no crear una cuenta de Facebook si es menor de 13 años, no compartir contraseña y no transferir la cuenta. (Facebook, s.f.)

Las normas comunitarias son políticas para saber que contenido no es apto en la red social Facebook, llegando a infringir sus políticas. El fin de dichas normas es ayudar a los usuarios a estar seguros, fomentar el respeto, proteger las cuentas e información personal y proteger la propiedad intelectual. (Facebook, s.f.)

Infringen las normas comunitarias las amenazas a otras personas, promoción de autolesiones, perfiles o apoyo a organizaciones peligrosas, acoso, actividades delictivas, todo contenido que amenace o promueva la explotación y violencia sexual, comercialización de armas de fuego o productos para adultos. (Facebook, s.f.)

La red social usa el marco establecido por Digital Advertising Alliance, que desarrolla estándares de privacidad para publicidades en internet. Facebook cuenta con proveedores de datos que son Acxiom, Datalogix, Epsilon, Experian y Merkle para ayudar a buscar a las personas adecuadas a las que se mostrara un anuncio. (Facebook, s.f.)

3.1.2.6.2. Algoritmos para Reconocimiento de Patrones. ([CON-TEC01](#))

Facebook utiliza algoritmos en sus equipos para el análisis de reconocimientos de patrones. Dichos algoritmos son utilizados para detectar las infracciones de las normas comunitarias de una forma automática cuando el usuario comparte contenido. (Facebook, s.f.)

La detección de patrones son utilizados para detectar si existe algo sospechoso, por ejemplo si el dispositivo tiene virus o malware. Cuando se activan sugiere al usuario analizar el computador. La red social cuenta con F-Secure y Trend Micro para analizar la computadora, aislar y eliminar los archivos infectados. (Facebook, s.f.)

3.1.2.6.3. Advertencias. ([CON-TEC02](#))

Facebook envía advertencias por crear contenido de acoso o ataque a un grupo o persona, cargar fotos y videos inapropiados o por cargar contenido no autorizado, por ejemplo una foto en la que se encuentra una menor de 13 años y se reporta el abuso a la publicación porque fue compartida sin autorización del representante del menor. (Facebook, s.f.)

Otras advertencias que emite la red social son por enviar demasiadas solicitudes de amistad, envió excesivo de mensajes a personas desconocidas o por el uso de automatización de aplicaciones no creadas por Facebook. (Facebook, s.f.)

Es considerado que se envió un Spam, si envía solicitudes y mensajes a personas desconocidas, publicación de una URL varias veces, envió de un mensaje reiteradamente, etiquetar a personas que no son contactos y contactar a una persona con fines comerciales sin su consentimiento. (Facebook, s.f.)

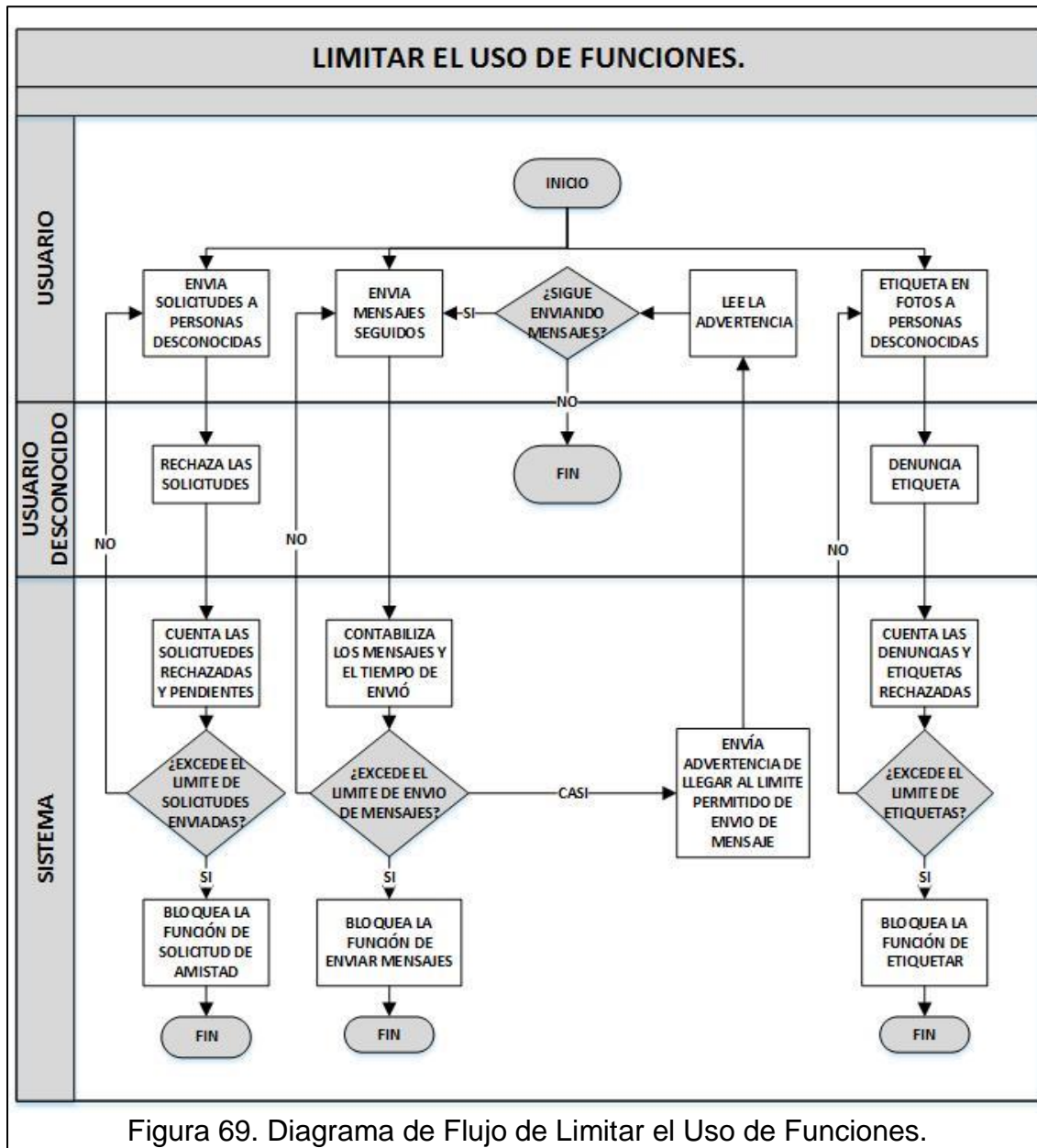
3.1.2.6.4. Limite en el Uso de Funciones. ([CON-TEC03](#))

Facebook limita el uso de algunas funciones por razones de seguridad, es una forma de proteger a los usuarios contra el acoso o correo no deseado. Los límites son basados en factores, como la velocidad y cantidad. El tiempo depende de la causa y no se anula la misma bajo ningún motivo. (Facebook, s.f.)

En caso de que un usuario envíe solicitudes de amistad a personas desconocidas y son rechazadas, el sistema contabiliza las solicitudes rechazadas y pendientes. Al momento que excede el límite de solicitudes enviadas, el sistema bloquea la función de solicitud de amistad.

Si el usuario envía mensajes seguidos, el sistema contabiliza los mensajes y el tiempo de envió. Si está a punto de exceder el límite, el sistema envía la advertencia de llegar al límite permitido de envío de mensajes. Al momento que excede el límite de envío de mensajes, el sistema bloquea la función de enviar mensajes.

Cuando se etiqueta en fotos a personas desconocidos y realizan la denuncia correspondiente, el sistema contabiliza las denuncias y etiquetas rechazadas para el momento en que excede el límite permitido, bloquear la función de etiquetar.



Controles:

- Bloquear la función al exceder el límite de intentos permitidos.
- Advertencias de llegar al límite permitido.

3.1.2.6.5. Controles de Seguridad en Menores de Edad. ([CON-TEC04](#))

El control de seguridad en menores de edad comienza cada que el usuario cumple años.

Si el usuario es menor de edad se inhabilita la visibilidad y motores de búsqueda la información delicada, se activa la revisión de etiquetas, se desactiva la ubicación, se activa la función que todo contenido público es visible solo para contactos y se desactiva la opción de enviar mensajes y etiquetar a desconocidos. (Facebook, s.f.)

Cuando el usuario se convierte en mayor de edad, se habilita la visibilidad y motores de búsqueda la información delicada, se cambia a visible todo el contenido que encuentra en público y se activa la opción de enviar mensajes y etiquetar a desconocidos.

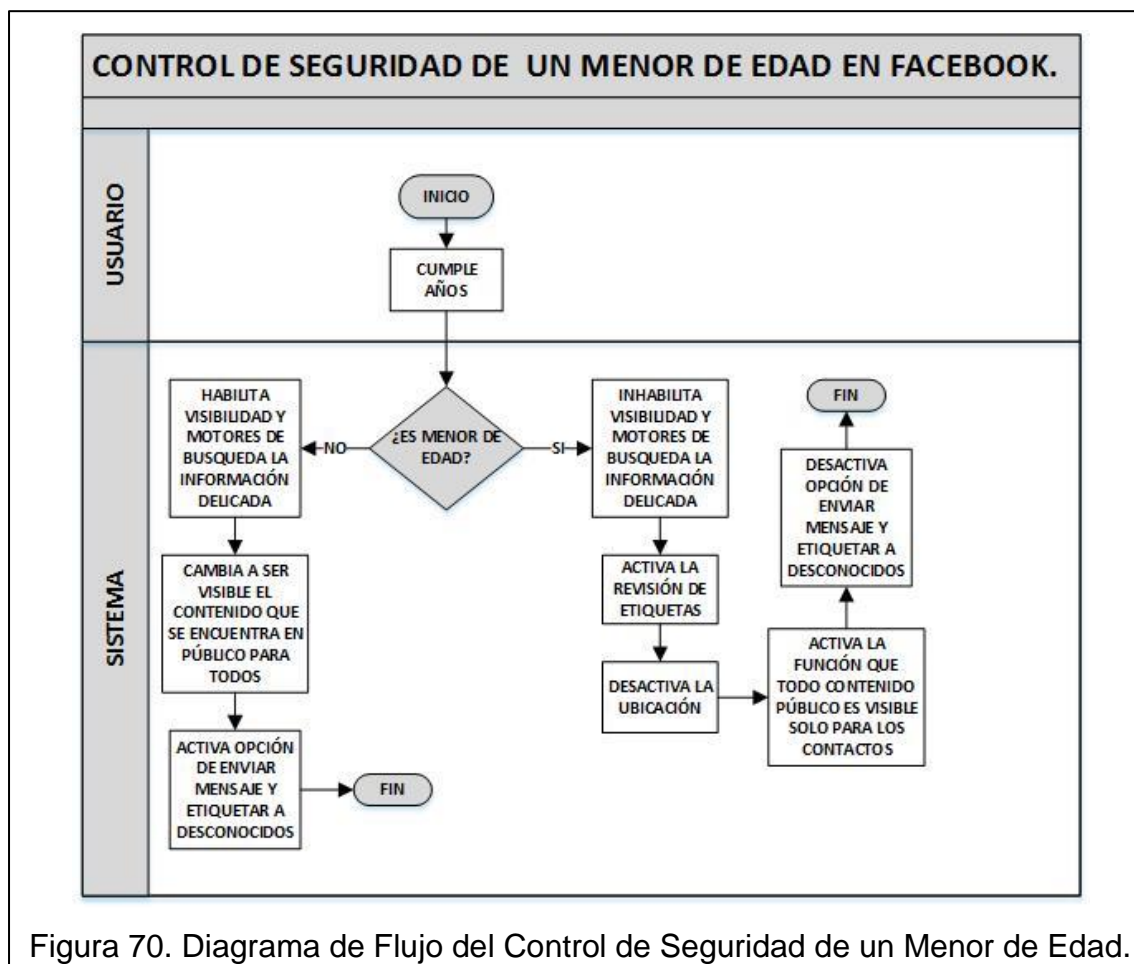


Figura 70. Diagrama de Flujo del Control de Seguridad de un Menor de Edad.

Controles:

- Inhabilita la visibilidad y motores de búsqueda de la información delicada.
- Activa la revisión de biografía.
- Desactiva la ubicación.

- Activar la función que todo contenido público es visible solo para los contactos.
- Desactivar la opción de enviar y recibir mensajes y etiquetas de desconocidos.

3.1.2.6.6. Inhabilitar Cuentas. ([CON-OPE01](#))

En Facebook se puede reportar cuando el contenido infringe las normas comunitarias de la red social. Los administradores de la red social analizan cada denuncia y si llegan a estar en contra de las normas comunitarias, localizan al responsable del contenido y eliminan el mismo. Toda denuncia es anónima para el responsable. (Facebook, s.f.)

Facebook inhabilita cuentas cuando proceden a no cumplir con las normas comunitarias, por lo que para cada caso proceden de manera diferente. Solo el titular de la cuenta puede enviar el reclamo para recuperar su usuario. (Facebook, s.f.)

3.1.2.6.7. Control Operativo en Caso de Falsificación de Información. ([CON-OPE02](#))

Facebook permite usar el nombre con el que más se identifica el usuario en su vida cotidiana. Por ejemplo, se llama “José” y sus amigos le llaman “Pepé”. (Facebook, s.f.)

En los casos que se solicitan documentos para confirmar el nombre, por denuncias de robo de identidad, robo de cuenta, etc. Se puede verificar por medio de un documento oficial o dos identificaciones no oficiales. (Facebook, s.f.)

- El documento oficial es en el que conste el nombre, fecha de nacimiento y foto de la persona por ejemplo el cedula de identidad, una vez verificada la información es eliminada. (Facebook, s.f.)

- Las identificaciones no oficiales, estos documentos tienen que coincidir en los nombres y uno de ellos debe contener la fecha de nacimiento o foto para confirmar con la información que se tiene en el perfil. El documento puede ser el carnet estudiantil, licencia, factura de un servicio básico, etc. (Facebook, s.f.)

3.2. Identificación de Amenaza.

La amenaza es la probabilidad de que suceda un problema de seguridad con la utilización de las vulnerabilidades del sistema. (Stoneburner et al, 2002, p.12.)

Tabla 40. Amenazas Humanas – Red Social Facebook.

AMENAZA-FUENTE	MOTIVACIÓN	ACCIÓN
Agresor	<ul style="list-style-type: none"> • Ego. • Manipulación. • Venganza. • Chantaje. • Divulgación de información. • Violación a la intimidad personal. • Envidia. 	<ul style="list-style-type: none"> • Acoso cibernético. • Grooming. • Crímenes contra el honor. • Suplantación de identidad. • Divulgación de contenido inapropiado.
Criminal	<ul style="list-style-type: none"> • Ganancia monetaria. • Espionaje. • Estafa. • Manipulación. • Venganza. • Soborno. • Secuestro y extorsión. • Violación a la intimidad personal. 	<ul style="list-style-type: none"> • Fraude informático. • Falsificación de identidad. • Acceso no autorizado. • Robo de información • Hurto de cuenta. • Ingeniería social.
Hacker.	<ul style="list-style-type: none"> • Curiosidad. • Ego. • Reto. • Divulgación de información. • Violación a la intimidad personal. 	<ul style="list-style-type: none"> • Robo de información. • Acceso no autorizado. • Ingeniería social. • Hurto de cuenta.
Usuario.	<ul style="list-style-type: none"> • Descuido. • Desconocimiento. • Error involuntario. • Evadir controles. 	<ul style="list-style-type: none"> • Falta de privacidad. • Divulgación de contenido inapropiado. • Falsificación de identidad. • Hurto de cuenta.

3.3. Identificación de Vulnerabilidad.

Las vulnerabilidades de un sistema son las circunstancias (fallas o debilidades) que hacen susceptibles a que sucedan las amenazas. (Stoneburner et al, 2002, p.15.)

El objetivo es elaborar una lista de las vulnerabilidades del sistema que pueden ser explotados para las posibles amenazas. (Stoneburner et al, 2002, p.15.)

Tabla 41. Pares de la Vulnerabilidad / Amenaza – Red Social Facebook.

VULNERABILIDAD	AMENAZA-FUENTE	ACCIÓN
<ul style="list-style-type: none"> Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Agresor. 	Acoso cibernético.
<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Criminal. Usuario. 	Falsificación de identidad.
<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser un adolescente. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Agresor. 	Grooming.
<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser una persona o empresa oficial. El sistema permite editar el nombre y la fecha de nacimiento. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de control del contenido publicado (Links de videos contaminados de malware). Falta de información de las configuraciones de privacidad a los usuarios. Falta de información de las configuraciones de seguridad de autenticación. 	<ul style="list-style-type: none"> Criminal. 	Fraude informático.
<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de control del contenido publicado (Links de videos contaminados de malware). 	<ul style="list-style-type: none"> Criminal. Hacker. 	Robo de información.
<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Agresor. 	Suplantación de identidad.

VULNERABILIDAD	AMENAZA-FUENTE	ACCIÓN
<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 		
<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • El sistema no permite editar la pregunta de seguridad. 	<ul style="list-style-type: none"> • Hacker • Criminal. 	Acceso no autorizado.
<ul style="list-style-type: none"> • Falta de prevención e información a los usuarios sobre las funciones disponibles para la privacidad en los datos de perfil y publicaciones, es opcional poner dichas seguridades. • Falta de información de las configuraciones de seguridad de autenticación. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> • Usuario 	Falta de privacidad.
<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control de la recepción de mensajes de desconocidos. 	<ul style="list-style-type: none"> • Agresor. 	Crímenes contra el honor.
<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone. • El sistema no permite editar la pregunta de seguridad. • El sistema permite que solo utilice el correo electrónico o número de teléfono. 	<ul style="list-style-type: none"> • Hacker. • Criminal. • Usuario. 	Hurto de cuenta.
<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control de la recepción de mensajes de desconocidos. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Agresor. • Usuario. 	Divulgación de contenido inapropiado.
<ul style="list-style-type: none"> • Falta de verificación de los datos ingresados al registrar la cuenta • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Criminal. • Hacker. 	Ingeniería social.

- Nota:* a. En el cuadro se encuentra el listado de las vulnerabilidades de la red social Facebook, clasificadas por la amenaza y por quien es posible que sea ejercida.
b. Una vulnerabilidad puede ser utilizada para diferentes amenazas.
c. Las amenazas son las identificadas en la tabla 40.

3.4. Análisis de Control.

Los controles que utiliza la red social para regularizar el sistema y minimizar los riesgos son de prevención, detección y corrección.

Para realizar un análisis más completo, se optó por calificar los controles que fueron identificados en los procesos de la red social Facebook. Para dar valor a cada control se tomó en cuenta el tipo de control (prevención, detección y corrección) y la automatización del control (automático, semi automático y manual).

La calificación del control es la multiplicación del tipo de control por la automatización del control.

Tabla 42. Tipo del Control – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Prevenir.	Control de alto nivel orientado a prevenir la causa del riesgo en una etapa muy temprana.	Alto.
Detectar	Control clave que actúa durante el proceso y permite corregir las deficiencias.	Medio.
Corregir.	Control menos frecuente y actúa una vez que el proceso ha terminado	Bajo.

Nota: a. Es preferible prevenir a detectar, por ese motivo el valor de prevenir es alto, detectar es medio y corregir es bajo.

Tabla 43. Automatización del Control – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Automatizado.	Control incorporado en el proceso de forma automática.	Alto.
Semi automatizado.	Control incorporado en el proceso de forma parcialmente automática.	Medio.
Manual.	Control incorporado en el proceso de forma manual.	Bajo.

Nota: a. Es preferible que un control se ejecute automáticamente que manualmente, por ese motivo el valor de automático es alto, semi automático es medio y manual es bajo.

Tabla 44. Escalas y Niveles de la Efectividad de Controles – Red Social Facebook.

DESDE	HASTA	NIVEL	CALIFICACIÓN
7	9	Óptimo.	Alto.
4	6	Regular.	Medio.
1	3	Deficiente.	Bajo.

Nota: a. La escala de efectividad del control es: Alto (>7 a 9), Medio (>4 a 6) y Bajo (1 a 3).

b. El nivel del control es: óptimo si la calificación es alta, regular si la calificación es media y deficiente si la calificación del control es baja.

Tabla 45. Mapa de Calor de la Efectividad de Controles – Red Social Facebook.

AUTOMATIZACIÓN	TIPO DE CONTROL		
	Bajo (1)	Medio (2)	Alto (3)
Alta (3)	3 (Bajo)	6 (Medio)	9 (Alto)
Media (2)	2 (Bajo)	4 (Medio)	6 (Medio)
Baja (1)	1 (Bajo)	2 (Bajo)	3 (Bajo)

Nota: a. El nivel del control se obtiene de la multiplicación de los valores asignados al tipo de control y a la automatización del control.

b. El valor asignado para cada nivel del tipo de control es 3 para alta, 2 para medio, 1 para baja y el valor asignado para cada nivel de automatización es 3 para alta, 2 para medio y 1 para bajo.

c. Para determinar la calificación final, si es Alto (amarillo), Medio (naranja) o Bajo (rojo) se utiliza la escala de efectividad del control en la tabla 44.

Tabla 46. Evaluación de Controles – Red Social Facebook.

CONTROL	TIPO	AUT.	VALOR
Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01)	Alto.	Alto.	Alto
Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01)	Alto.	Alto.	Alto
Validación del usuario y contraseña. (PRO-AUT01 , CON-AUT02 , CON-AUT06 , CON-AUT07 , PRO-CONF01 , PRO-CONF02 , PRO-CONF05 , PRO-CONF06)	Alto.	Alto.	Alto
Encriptación de contraseña. (PRO-AUT01 , CON-AUT01 , CON-AUT06 , CON-AUT07 , CON-AUT08)	Alto.	Alto.	Alto
Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01 , CON-AUT02)	Alto.	Medio.	Medio
Restablecer contraseña (por correo electrónico, pregunta de	Alto.	Medio.	Medio

CONTROL	TIPO	AUT.	VALOR
seguridad o amigos de confianza) (CON-AUT03 , CON-AUT04 , CON-AUT05)			
Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03 , CON-AUT04 , CON-AUT05 , CON-AUT07 , CON-AUT08)	Alto.	Alto.	Alto
Cerrar sesión en todos los dispositivos. (CON-AUT03)	Medio.	Medio.	Medio
Comprobación de los últimos cambios en la cuenta. (CON-AUT03)	Medio.	Medio.	Medio
Bloqueo de la cuenta por 24 horas. (CON-AUT04 , CON-AUT05)	Alto.	Alto.	Alto
Confirma el amigo de confianza que su amigo se comunicó. (CON-AUT05)	Alto.	Bajo.	Bajo
Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06 , CON-AUT07)	Alto.	Medio.	Medio
Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08)	Medio.	Medio.	Medio
Copia de información. (PRO-CONF05 , PRO-CONF06)	Alto.	Medio.	Medio
Confirmación que desea desactivar la cuenta. (PRO-CONF05)	Alto.	Bajo.	Bajo
Selecciona todas las fotos en las que aparece un animal. (PRO-CONF06)	Alto.	Medio.	Medio
Control de privacidad en la información del perfil. (CON-PER01 , CON-PER02 , CON-PER03 , CON-PER04 , CON-PER05)	Alto.	Medio.	Medio
Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01 , CON-TEC01)	Alto.	Alto.	Alto
Control de privacidad en publicaciones. (CON-PUB01 , CON-PUB02)	Alto.	Medio.	Medio
Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03)	Alto.	Medio.	Medio
Visualizar como otros usuarios ven la biografía. (CON-PUB04)	Alto.	Medio.	Medio
Reportar abuso. (PRO-REP01 , PRO-REP02 , PRO-REP03)	Medio.	Bajo.	Bajo
Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04)	Medio.	Medio.	Medio
Advertencias. (CON-TEC02 , CON-TEC03)	Alto.	Alto.	Alto
Limite en el uso de funciones. (CON-TEC03)	Medio.	Alto.	Medio
Control de seguridad en menores de edad. (CON-TEC04)	Alto.	Alto.	Alto
Inhabilitar cuentas. (CON-OPE01)	Bajo.	Bajo.	Bajo
Control operativo en caso de falsificación de información. (CON-OPE02)	Bajo.	Bajo.	Bajo

Nota: a. En el cuadro se encuentra el listado de los controles identificados en los procesos de la red social Facebook, con el valor asignado al tipo de control y el valor asignado a la automatización del control.

b. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar cuenta en Facebook es identificada como PRO-REG01.

c. Los parámetros para determinar la calificación en el tipo de control y automatización del control se encuentra en las tablas 42 y 43.

d. El valor final del control se obtiene de la multiplicación de los valores asignados al

tipo de control y a la automatización del control. Para determinar el valor final se utiliza la matriz que se encuentra en la tabla 45. Por ejemplo, si es tipo (Alto) y automatización (Medio) la multiplicación sería de $3 \times 2 = 6$ en la cual la escala indica que es Medio.

3.5. Determinación de Probabilidad. (PROB).

Las probabilidades para que se ejecute una amenaza por medio de las vulnerabilidades se miden en bajo, medio y alto. (Stoneburner et al, 2002, p.21.)

Tabla 47. Criterios de Evaluación de la Probabilidad – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Probable.	Cuando la amenaza está muy motivada y suficientemente capacitada y los controles son ineficientes para evitar el ejercer la vulnerabilidad.	Alto.
Moderado.	Cuando la amenaza está motivada y capacitada, pero los controles impiden el éxito de ejercer la vulnerabilidad.	Medio.
Improbable.	Cuando la amenaza carece de motivación o capacidad y los controles existentes previenen o impiden de manera significativa la vulnerabilidad a ser ejercida.	Bajo.

Nota: a. Para asignar un valor de probabilidad a que se ejecute una amenaza, se considera en los parámetros las vulnerabilidades y controles actuales de la red social Facebook. Si una amenaza se puede ejecutar por medio de varias vulnerabilidades del sistema y los controles no evitan que la vulnerabilidad sea utilizada, la motivación y capacidad de la amenaza va a ser más alta (es más probable a ser ejecutada).

Tabla 48. Determinación de Probabilidad – Red Social Facebook.

AMENAZA	VULNERABILIDAD	CONTROL	PROB
Acoso cibernético.	<ul style="list-style-type: none"> Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Limite en el uso de funciones. (CON-TEC03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	Alto
Falsificación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto
Grooming.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser un adolescente. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Control de seguridad en menores de edad. (CON-TEC04) Limite en el uso de funciones. (CON-TEC03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto
Fraude informático.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) 	Medio

AMENAZA	VULNERABILIDAD	CONTROL	PROB
	<p>registrar la cuenta, lo cual permite el engaño de ser una persona o empresa oficial.</p> <ul style="list-style-type: none"> • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control del contenido publicado (Links de videos contaminados de malware). • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de información de las configuraciones de seguridad de autenticación. 	<ul style="list-style-type: none"> • Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Limite en el uso de funciones. (CON-TEC03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Control operativo en caso de falsificación de información. (CON-OPE02) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	
Robo de información.	<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control en el contenido que otras personas pueden guardar 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) 	Medio

AMENAZA	VULNERABILIDAD	CONTROL	PROB
	<p>como fotografías, videos e información.</p> <ul style="list-style-type: none"> Falta de control del contenido publicado (Links de videos contaminados de malware). 	<ul style="list-style-type: none"> Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Control de seguridad en menores de edad. (CON-TEC04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	
Suplantación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto
Acceso no autorizado.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema no permite editar la pregunta de 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) 	Bajo

AMENAZA	VULNERABILIDAD	CONTROL	PROB
	seguridad.	<ul style="list-style-type: none"> • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) • Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Copia de información. (PRO-CONF05,PRO-CONF06) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	
Falta de privacidad.	<ul style="list-style-type: none"> • Falta de prevención e información a los usuarios sobre las funciones disponibles para la privacidad en los datos de perfil y publicaciones, es opcional poner dichas seguridades. • Falta de información de las configuraciones de seguridad de autenticación. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Control de seguridad en menores de edad. (CON-TEC04) 	Medio
Crímenes contra el honor.	<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar 	<ul style="list-style-type: none"> • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) 	Medio

AMENAZA	VULNERABILIDAD	CONTROL	PROB
	<p>como fotografías, videos e información.</p> <ul style="list-style-type: none"> • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control de la recepción de mensajes de desconocidos. 	<ul style="list-style-type: none"> • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Advertencias. (CON-TEC02,CON-TEC03) • Limite en el uso de funciones. (CON-TEC03) • Control de seguridad en menores de edad. (CON-TEC04) • Inhabilitar cuentas. (CON-OPE01) 	
Hurto de cuenta.	<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone. • El sistema no permite editar la pregunta de seguridad. • El sistema permite que solo utilice el correo electrónico o número de teléfono. 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Bloqueo de la cuenta por 24 minutos. (CON-AUT04,CON-AUT05) • Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Confirma el amigo de confianza que su amigo se comunicó. (CON-AUT05) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Copia de información. (PRO-CONF05,PRO-CONF06) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de 	Medio

AMENAZA	VULNERABILIDAD	CONTROL	PROB
		confianza) (CON-AUT03 , CON-AUT04 , CON-AUT05) <ul style="list-style-type: none"> • Selecciona todas las fotos en las que aparece un animal. (PRO-CONF06) 	
Divulgación de contenido inapropiado.	<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control de la recepción de mensajes de desconocidos. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Inhabilitar cuentas. (CON-OPE01) 	Medio
Ingeniería social.	<ul style="list-style-type: none"> • Falta de verificación de los datos ingresados al registrar la cuenta • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) • Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Limite en el uso de funciones. (CON-TEC03) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Bajo

Nota: a. En el cuadro se encuentran las amenazas identificadas en la tabla 40, las vulnerabilidades identificadas en la tabla 41 y los controles identificados en la tabla 46.

b. Los parámetros para determinar la probabilidad se encuentra en la tabla 47.

c. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar cuenta en Facebook es identificada como PRO-REG01.

3.6. Análisis de Impacto. (IMP)

El impacto se refiere a la magnitud del daño que podría ser causado al ser ejercida una amenaza a través de la vulnerabilidad del sistema. (Stoneburner et al, 2002, p.21.)

Tabla 49. Criterios de Evaluación del Impacto – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Catastrófico.	Si el resultado es la pérdida altamente costosa de recursos y activos. O el daño es significativo y dificulta la misión, reputación o interés de la organización. O resulta la muerte o lesiones humanas graves.	Alto.
Moderado.	Si el resultado es la pérdida costosa de recursos o bienes materiales. O daños de la misión, reputación o interés de la organización. O resultan daños a las personas.	Medio.
Insignificante.	Si el resultado es la pérdida de recursos o activos tangibles. O afectación notable a la organización en cuanto a su misión, reputación o interés.	Bajo.

Nota: a. Para medir el impacto en caso que se ejecute una amenaza, se considera en los parámetros la pérdida económica y daños directos a personas. Si existe muerte o lesiones graves de una persona o pérdidas económicas sumamente altas es catastrófica (Alta), si existen daños leves a una persona o pérdida costosa económicamente es moderado (Medio) y si es pérdida de recursos es insignificante (Bajo).

Tabla 50. Análisis de Impacto – Red Social Facebook.

AMENAZA	VULNERABILIDAD	CONTROL	IMP
Acoso cibernético.	<ul style="list-style-type: none"> Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Limite en el uso de funciones. (CON-TEC03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	Alto
Falsificación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Medio
Grooming.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser un adolescente. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Control de seguridad en menores de edad. (CON-TEC04) Limite en el uso de funciones. (CON-TEC03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto
Fraude informático.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser una persona o empresa oficial. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) 	Bajo

AMENAZA	VULNERABILIDAD	CONTROL	IMP
	<ul style="list-style-type: none"> • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control del contenido publicado (Links de videos contaminados de malware). • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de información de las configuraciones de seguridad de autenticación. 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Limite en el uso de funciones. (CON-TEC03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Control operativo en caso de falsificación de información. (CON-OPE02) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	
Robo de información.	<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación 	Bajo

AMENAZA	VULNERABILIDAD	CONTROL	IMP
	<ul style="list-style-type: none"> Falta de control del contenido publicado (Links de videos contaminados de malware). 	<ul style="list-style-type: none"> de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Control de seguridad en menores de edad. (CON-TEC04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	
Suplantación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Medio
Acceso no autorizado.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema no permite editar la pregunta de seguridad. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) 	Bajo

AMENAZA	VULNERABILIDAD	CONTROL	IMP
		<ul style="list-style-type: none"> Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Copia de información. (PRO-CONF05,PRO-CONF06) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Alto
Falta de privacidad.	<ul style="list-style-type: none"> Falta de prevención e información a los usuarios sobre las funciones disponibles para la privacidad en los datos de perfil y publicaciones, es opcional poner dichas seguridades. Falta de información de las configuraciones de seguridad de autenticación. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Control de seguridad en menores de edad. (CON-TEC04) 	Medio
Crímenes contra el	<ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar 	<ul style="list-style-type: none"> Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Control de privacidad en la información del perfil. (CON-PER01,CON- 	Alto

AMENAZA	VULNERABILIDAD	CONTROL	IMP
honor.	<p>como fotografías, videos e información.</p> <ul style="list-style-type: none"> Falta de información de las configuraciones de privacidad a los usuarios. Falta de control de la recepción de mensajes de desconocidos. 	<p>PER02,CON-PER03,CON-PER04,CON-PER05)</p> <ul style="list-style-type: none"> Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Limite en el uso de funciones. (CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	
Hurto de cuenta.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone. El sistema no permite editar la pregunta de seguridad. El sistema permite que solo utilice el correo electrónico o número de teléfono. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Bloqueo de la cuenta por 24 minutos. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Confirma el amigo de confianza que su amigo se comunicó. (CON-AUT05) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Copia de información. (PRO-CONF05,PRO-CONF06) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y 	Bajo

AMENAZA	VULNERABILIDAD	CONTROL	IMP
		<ul style="list-style-type: none"> eventos de una persona en concreto. (PRO-REP04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) Selecciona todas las fotos en las que aparece un animal. (PRO-CONF06) 	
Divulgación de contenido inapropiado.	<ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Inhabilitar cuentas. (CON-OPE01) 	Alto
Ingeniería social.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta El sistema permite editar el nombre y la fecha de nacimiento. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Cerrar sesión en todos los dispositivos. (CON-AUT03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Limite en el uso de funciones. (CON-TEC03) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Bajo

Nota: a. En el cuadro se encuentran las amenazas identificadas en la tabla 40, las vulnerabilidades identificadas en la tabla 41 y los controles identificados en la tabla 46.

b. Los parámetros para determinar el impacto se encuentra en la tabla 49.

c. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar cuenta en Facebook es identificada como PRO-REG01.

3.7. Determinación del Riesgo.

La matriz de riesgos es la determinación final del riesgo, la cual se obtiene multiplicando la probabilidad por el impacto de la amenaza. (Stoneburner et al, 2002, p.24.)

Tabla 51. Acciones a Realizar – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Riesgo Alto.	Es necesario tomar medidas correctivas lo más pronto posible.	Alto.
Riesgo Medio.	Es necesario tomar acciones correctivas en un periodo razonable de tiempo con el desarrollo de un plan.	Medio.
Riesgo Bajo.	Se determina si es necesario tomar medidas correctoras o si llego al nivel aceptable de riesgo.	Bajo.

Nota: a. Si la calificación final es riesgo alto, el control que se recomienda para minimizar el riesgo debe ser implementada inmediatamente. Si la calificación final es riesgo medio, el control recomendado debe ser implementado en un periodo moderado. Y si la calificación final es riesgo bajo, el control recomendado debe ser implementado en un periodo aceptable.

Tabla 52. Escalas y Niveles del Riesgo – Red Social Facebook.

DESDE	HASTA	NIVEL	CALIFICACIÓN
7	9	Extremo	Alto.
4	6	Moderado	Medio.
1	3	Bajo	Bajo.

Nota: a. La escala de efectividad del control es: Alto (>7 a 9), Medio (>4 a 6) y Bajo (1 a 3).

b. El nivel de riesgo es: extremo si la calificación es alta, moderado si la calificación es media y bajo si la calificación del riesgo es baja.

Tabla 53. Mapa de Calor del Riesgo – Red Social Facebook.

PROBABILIDAD	IMPACTO		
	Bajo (1)	Medio (2)	Alto (3)
Alta (3)	3 (Bajo)	6 (Medio)	9 (Alto)
Media (2)	2 (Bajo)	4 (Medio)	6 (Medio)
Baja (1)	1 (Bajo)	2 (Bajo)	3 (Bajo)

Nota: a. El nivel de riesgo se obtiene de la multiplicación de los valores asignados a la probabilidad e impacto de la amenaza.

- b. El valor asignado para cada nivel de probabilidad es de 3 para alta, 2 para medio, 1 para baja y el valor asignado para cada nivel de impacto es de 3 para alto, 2 para medio y 1 para bajo.
- c. Para determinar la calificación final, si es Alto (rojo), Medio (naranja) o Bajo (amarillo) se utiliza la escala de efectividad del control en la tabla 52.

Tabla 54. Matriz de Riesgos – Red Social Facebook.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
Acoso cibernético.	<ul style="list-style-type: none"> Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Limite en el uso de funciones. (CON-TEC03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	Alto.	Alto.	Alto.
Falsificación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto.	Medio.	Medio.
Grooming.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser un adolescente. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Control de seguridad en menores de edad. (CON-TEC04) Limite en el uso de funciones. (CON-TEC03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto.	Alto.	Alto.
Fraude	<ul style="list-style-type: none"> Falta de verificación de 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o 	Medio.	Bajo.	Bajo.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
informático.	<p>los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser una persona o empresa oficial.</p> <ul style="list-style-type: none"> • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control del contenido publicado (Links de videos contaminados de malware). • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de información de las configuraciones de seguridad de autenticación. 	<p>dirección de correo electrónico en otra cuenta. (PRO-REG01)</p> <ul style="list-style-type: none"> • Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Limite en el uso de funciones. (CON-TEC03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Control operativo en caso de falsificación de información. (CON-OPE02) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 			
Robo de información.	<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • Falta de información de 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) 	Medio.	Bajo.	Bajo.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
	<p>las configuraciones de privacidad a los usuarios.</p> <ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de control del contenido publicado (Links de videos contaminados de malware). 	<ul style="list-style-type: none"> Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Control de seguridad en menores de edad. (CON-TEC04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 			
Suplantación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto.	Medio.	Medio.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
	e información.				
Acceso no autorizado.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema no permite editar la pregunta de seguridad. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Copia de información. (PRO-CONF05,PRO-CONF06) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Bajo.	Bajo.	Bajo.
Falta de privacidad.	<ul style="list-style-type: none"> Falta de prevención e información a los usuarios sobre las funciones disponibles para la privacidad en los datos de perfil y publicaciones, es opcional poner dichas seguridades. Falta de información de las configuraciones de 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) 	Medio.	Medio.	Medio.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
	<p>seguridad de autenticación.</p> <ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Control de seguridad en menores de edad. (CON-TEC04) 			
Crímenes contra el honor.	<ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control de la recepción de mensajes de desconocidos. 	<ul style="list-style-type: none"> Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Limite en el uso de funciones. (CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	Medio.	Alto.	Medio.
Hurto de cuenta.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone. El sistema no permite editar la pregunta de 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Bloqueo de la cuenta por 24 minutos. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la 	Medio.	Bajo.	Bajo.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
	<p>seguridad.</p> <ul style="list-style-type: none"> El sistema permite que solo utilice el correo electrónico o número de teléfono. 	<p>pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08)</p> <ul style="list-style-type: none"> Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Confirma el amigo de confianza que su amigo se comunicó. (CON-AUT05) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Copia de información. (PRO-CONF05,PRO-CONF06) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) Selecciona todas las fotos en las que aparece un animal. (PRO-CONF06) 			
Divulgación de contenido inapropiado.	<ul style="list-style-type: none"> Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Inhabilitar cuentas. (CON-OPE01) 	Medio.	Alto.	Medio.
Ingeniería social.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta El sistema permite editar 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) 	Bajo.	Bajo.	Bajo.

AMENAZA	VULNERABILIDAD	CONTROLES	PROB	IMP	RIESGO
	el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios.	• Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de privacidad en la información del perfil. (CON-PER01 , CON-PER02 , CON-PER03 , CON-PER04 , CON-PER05) • Control de privacidad en publicaciones. (CON-PUB01 , CON-PUB02) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Limite en el uso de funciones. (CON-TEC03) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03 , CON-AUT04 , CON-AUT05)			

Nota: a. En el cuadro se encuentra el listado de las amenazas, vulnerabilidades, controles, valor asignado a la probabilidad y valor asignado al impacto. Se encuentra clasificado por amenaza (una amenaza tiene varias vulnerabilidades y controles).

b. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar Cuenta en Facebook es identificada como PRO-REG01.

c. Las calificaciones asignadas a la probabilidad por amenaza se encuentra en la tabla 48 y las calificaciones asignadas al impacto por amenaza se encuentra en la tabla 50.

d. El valor final del riesgo se obtiene de la multiplicación de los valores asignados a la probabilidad e impacto de la amenaza. Para determinar el valor final se utiliza la matriz que se encuentra en la tabla 53. Por ejemplo, si es probabilidad (Alta) e impacto (Medio) la multiplicación sería de $3 \times 2 = 6$ en la cual la escala indica que es Medio.

3.8. Recomendaciones de Control.

El objetivo de recomendar controles o soluciones alternativas es reducir el nivel de riesgo a un nivel aceptable. (Stoneburner et al, 2002, p.26.)

Para saber si es viable implementar los controles recomendados, se optó por realizar el análisis de los mismos. Para dar valor a cada control se tomó en cuenta el tipo de control (prevención, detección y corrección) y la automatización del control (automático, semi automático y manual).

La calificación del control es la multiplicación del tipo de control por la automatización del control.

Tabla 55. Tipo del Control – Recomendaciones de Control de la Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Prevenir.	Control de alto nivel orientado a prevenir la causa del riesgo en una etapa muy temprana.	Alto.
Detectar	Control clave que actúa durante el proceso y permite corregir las deficiencias.	Medio.
Corregir.	Control menos frecuente y actúa una vez que el proceso ha terminado.	Bajo.

Nota: a. Es preferible prevenir a detectar, por ese motivo el valor de prevenir es alto, detectar es medio y corregir es bajo.

Tabla 56. Automatización del Control – Recomendaciones de Control de la Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Automatizado.	Controles incorporados en el proceso de forma automática.	Alto.
Semi automatizado.	Controles incorporados en el proceso de forma parcialmente automática.	Medio.
Manual.	Controles incorporados en el proceso de forma manual.	Bajo.

Nota: a. Es preferible que un control se ejecute automáticamente que manualmente, por ese motivo el valor de automático es alto, semi automático es medio y manual es bajo.

Tabla 57. Escalas y Niveles de la Efectividad de Controles - Recomendaciones de Control de la Red Social Facebook.

DESDE	HASTA	NIVEL	CALIFICACIÓN
7	9	Óptimo.	Alto.
4	6	Regular.	Medio.
1	3	Deficiente.	Bajo.

Nota: a. La escala de efectividad del control es: Alto (>7 a 9), Medio (>4 a 6) y Bajo (1 a 3).

b. El nivel del control es: óptimo si la calificación es alta, regular si la calificación es media y deficiente si la calificación del control es baja.

Tabla 58. Mapa de Calor de la Efectividad de Controles – Recomendaciones de Control de la Red Social Facebook.

AUTOMATIZACIÓN	TIPO DE CONTROL		
	Bajo (1)	Medio (2)	Alto (3)
Alta (3)	3 (Bajo)	6 (Medio)	9 (Alto)
Media (2)	2 (Bajo)	4 (Medio)	6 (Medio)
Baja (1)	1 (Bajo)	2 (Bajo)	3 (Bajo)

Nota: a. El nivel del control se obtiene de la multiplicación de los valores asignados al tipo de control y a la automatización del control.

b. El valor asignado para cada nivel del tipo de control es de 3 para alta, 2 para medio, 1 para baja y el valor asignado para cada nivel de automatización es de 3 para alta, 2 para medio y 1 para bajo.

c. Para determinar la calificación final, si es Alto (amarillo), Medio (naranja) o Bajo (rojo) se utiliza la escala de efectividad del control en la tabla 57.

Tabla 59. Evaluación de Controles – Recomendaciones de Control de la Red Social Facebook.

CONTROL	AMENAZAS	TIPO	AUT.	VALOR
Compara la información de la cuenta con el documento oficial subido (Foto, nombre, apellido y fecha de nacimiento).	Falsificación de identidad, grooming, fraude informático, suplantación de identidad e ingeniería social.	Alto	Alto	Alto
Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar	Acoso cibernético, fraude informático, robo de información, suplantación de identidad, falta de privacidad, crímenes	Alto	Medio	Medio

la cuenta.	contra el honor, divulgación de contenido inapropiado e ingeniería social.			
Bloqueo de guardar fotografías, videos e información.	Acoso cibernético, fraude informático, robo de información, suplantación de identidad, falta de privacidad, crímenes contra el honor, divulgación de contenido inapropiado e ingeniería social.	Alto	Alto	Alto
La alerta de inicio de sesión es obligatoria y se activa automáticamente la función al crear la cuenta.	Acceso no autorizado y hurto de cuenta.	Alto	Alto	Alto
La revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.	Acoso cibernético, crímenes contra el honor y divulgación de contenido inapropiado.	Alto	Medio	Medio
El sistema permite editar la pregunta de seguridad.	Fraude informático, acceso no autorizado y hurto de cuenta.	Medio	Medio	Medio
El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualiza permanentemente). Como alternativa permite configurar un sobrenombre.	Falsificación de identidad, grooming, fraude informático, suplantación de identidad e ingeniería social.	Alto	Alto	Alto
Usar la pregunta de seguridad para poder eliminar la cuenta.	Acceso no autorizado y hurto de cuenta.	Alto	Medio	Medio

Nota: a. En el cuadro se encuentra el listado de los controles recomendados, las amenazas a las que contrarresta el riesgo, el valor asignado al tipo de control y el valor asignado a la automatización del control.

b. Los parámetros para determinar la calificación en el tipo de control y automatización del control se encuentra en las tablas 55 y 56.

c. El valor final del control se obtiene de la multiplicación de los valores asignados al tipo de control y a la automatización del control. Para determinar el valor final se utiliza la matriz que se encuentra en la tabla 58. Por ejemplo, si es tipo (Alto) y automatización (Medio) la multiplicación sería de $3 \times 2 = 6$ en la cual la escala indica que es Medio.

3.9. Documentación de Evaluación de Riesgos.

Las amenazas encontradas en el análisis de riesgos con respecto a los usuarios son de diferentes tipos, como los que están orientados a denigrar la integridad moral del usuario que son el acoso cibernético, grooming, divulgación de contenido inapropiado y crímenes contra el honor. Los que

están orientados a ingresar información falsa, suplantación de identidad y falsificación de identidad. Los que están orientados a sustraer contenido, que son fraude informático, robo de información, acceso no autorizado, ingeniería social, falta de privacidad y hurto de la cuenta.

Tabla 60. Acciones a Realizar – Red Social Facebook.

CATEGORÍA	DESCRIPCIÓN	VALOR
Riesgo Alto.	Es necesario tomar medidas correctivas lo más pronto posible.	Alto.
Riesgo Medio.	Es necesario tomar acciones correctivas en un periodo razonable de tiempo con el desarrollo de un plan.	Medio.
Riesgo Bajo.	Se determina si es necesario tomar medidas correctoras o si llego al nivel aceptable de riesgo.	Bajo.

Nota: a. Si la calificación final es riesgo alto, el control que se recomienda para minimizar el riesgo debe ser implementada inmediatamente. Si la calificación final es riesgo medio, el control recomendado debe ser implementado en un periodo moderado. Y si la calificación final es riesgo bajo, el control recomendado debe ser implementado en un periodo aceptable.

Los controles que se recomiendan implementar en el sistema de la red social Facebook pueden combatir diferentes riesgos al mismo tiempo.

Los controles recomendados son los siguientes:

- Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento.
- Bloqueo de guardar fotografías, videos e información.
- La alerta de inicio de sesión es obligatoria y se activa automáticamente la función al crear la cuenta.
- El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.
- Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta.
- La revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.

- El sistema permite editar la pregunta de seguridad.
- Usar la pregunta de seguridad para poder eliminar la cuenta.

Tabla 61. Resumen de la Evaluación de Riesgos – Red Social Facebook.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
Acoso cibernético.	<ul style="list-style-type: none"> Falta de control de la recepción de mensajes de desconocidos. Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> Limite en el uso de funciones. (CON-TEC03) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Advertencias. (CON-TEC02,CON-TEC03) Control de seguridad en menores de edad. (CON-TEC04) Inhabilitar cuentas. (CON-OPE01) 	Alto.	<ul style="list-style-type: none"> Configuración del control de seguridad (Opción para no receptor mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. Bloqueo de guardar fotografías, videos e información. La revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.
Grooming.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser un adolescente. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Control de seguridad en menores de edad. (CON-TEC04) Limite en el uso de funciones. (CON-TEC03) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Alto.	<ul style="list-style-type: none"> Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento. El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
Falsificación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Medio.	<ul style="list-style-type: none"> Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento. El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.
Suplantación de identidad.	<ul style="list-style-type: none"> Falta de verificación de los datos ingresados al registrar la cuenta. El sistema permite editar el nombre y la fecha de nacimiento. Falta de información de las configuraciones de privacidad a los usuarios. Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<ul style="list-style-type: none"> Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Visualizar como otros usuarios ven la biografía. (CON-PUB04) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Control operativo en caso de falsificación de información. (CON-OPE02) Inhabilitar cuentas. (CON-OPE01) 	Medio.	<ul style="list-style-type: none"> Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento. Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. Bloqueo de guardar fotografías, videos e información. El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.
Falta de privacidad.	<ul style="list-style-type: none"> Falta de prevención e información a los usuarios sobre las funciones disponibles para la privacidad en 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de 	Medio.	<ul style="list-style-type: none"> Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
	<p>los datos de perfil y publicaciones, es opcional poner dichas seguridades.</p> <ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. 	<p>solo un uso) (CON-AUT01,CON-AUT02)</p> <ul style="list-style-type: none"> • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Control de seguridad en menores de edad. (CON-TEC04) 		<ul style="list-style-type: none"> • Bloqueo de guardar fotografías, videos e información.
Crímenes contra el honor.	<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control de la 	<ul style="list-style-type: none"> • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) 	Medio.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Opción para no receptor mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. • Bloqueo de guardar fotografías, videos e información. • La revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
	recepción de mensajes de desconocidos.	<ul style="list-style-type: none"> • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Advertencias. (CON-TEC02,CON-TEC03) • Limite en el uso de funciones. (CON-TEC03) • Control de seguridad en menores de edad. (CON-TEC04) • Inhabilitar cuentas. (CON-OPE01) 		
Divulgación de contenido inapropiado.	<ul style="list-style-type: none"> • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control de la recepción de mensajes de desconocidos. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Revisión de la biografía (Etiquetas y publicaciones) (CON-PUB03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Inhabilitar cuentas. (CON-OPE01) 	Medio.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. • Bloqueo de guardar fotografías, videos e información. • La revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.
Fraude informático.	<ul style="list-style-type: none"> • Falta de verificación de los datos ingresados al registrar la cuenta, lo cual permite el engaño de ser una persona o empresa oficial. 	<ul style="list-style-type: none"> • Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) • Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) 	Bajo.	<ul style="list-style-type: none"> • Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento. • Configuración del control de seguridad

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
	<ul style="list-style-type: none"> • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control del contenido publicado (Links de videos contaminados de malware). • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de información de las configuraciones de seguridad de autenticación. 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Limite en el uso de funciones. (CON-TEC03) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Control operativo en caso de falsificación de información. (CON-OPE02) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) 		<p>(Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta.</p> <ul style="list-style-type: none"> • Bloqueo de guardar fotografías, videos e información. • El sistema permite editar la pregunta de seguridad. • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
		(CON-AUT03,CON-AUT04,CON-AUT05)		
Robo de información.	<ul style="list-style-type: none"> • Falta de información de las configuraciones de seguridad de autenticación. • Falta de información de las configuraciones de privacidad a los usuarios. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de control del contenido publicado (Links de videos contaminados de malware). 	<ul style="list-style-type: none"> • Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) • Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) • Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Comprobación de los últimos cambios en la cuenta. (CON-AUT03) • Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) • Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Análisis de información por medio de algoritmos de reconocimiento de patrones en los equipos. (PRO-COM01,CON-TEC01) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Control de seguridad en menores de edad. (CON- 	Bajo.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. • Bloqueo de guardar fotografías, videos e información.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
		<p>TEC04)</p> <ul style="list-style-type: none"> Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 		
Acceso no autorizado.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema no permite editar la pregunta de seguridad. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Comprobación de los últimos cambios en la cuenta. (CON-AUT03) Bloqueo de la cuenta por 24 horas. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Copia de información. (PRO-CONF05,PRO-CONF06) Reportar abuso. (PRO-REP01,PRO-REP02,PRO-REP03) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Bajo.	<ul style="list-style-type: none"> La alerta de inicio de sesión es obligatoria y se activa automáticamente la función al crear la cuenta. El sistema permite editar la pregunta de seguridad. Usar la pregunta de seguridad para poder eliminar la cuenta.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
Hurto de cuenta.	<ul style="list-style-type: none"> Falta de información de las configuraciones de seguridad de autenticación. El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone. El sistema no permite editar la pregunta de seguridad. El sistema permite que solo utilice el correo electrónico o número de teléfono. 	<ul style="list-style-type: none"> Validación del usuario y contraseña. (PRO-AUT01,CON-AUT02,CON-AUT06,CON-AUT07,PRO-CONF01,PRO-CONF02,PRO-CONF05,PRO-CONF06) Generar contraseña segura (para aplicaciones y de solo un uso) (CON-AUT01,CON-AUT02) Encriptación de contraseña. (PRO-AUT01,CON-AUT01,CON-AUT06,CON-AUT07,CON-AUT08) Cerrar sesión en todos los dispositivos. (CON-AUT03) Bloqueo de la cuenta por 24 minutos. (CON-AUT04,CON-AUT05) Verifica el correo electrónico, código de seguridad o respuesta de la pregunta de seguridad. (CON-AUT03,CON-AUT04,CON-AUT05,CON-AUT07,CON-AUT08) Control de seguridad de autenticación (alerta de inicio de sesión y la aprobación de inicio de sesión) (CON-AUT06,CON-AUT07) Protección de cuenta (cambiar contraseña, revisar últimas acciones en la cuenta) (CON-AUT08) Confirma el amigo de confianza que su amigo se comunicó. (CON-AUT05) Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) Copia de información. (PRO-CONF05,PRO-CONF06) Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) 	Bajo.	<ul style="list-style-type: none"> La alerta de inicio de sesión es obligatoria y se activa automáticamente la función al crear la cuenta. El sistema permite editar la pregunta de seguridad. Usar la pregunta de seguridad para poder eliminar la cuenta.

AMENAZA	VULNERABILIDAD	CONTROL ACTUAL.	RIESGO	RECOMENDACIÓN
		(CON-AUT03,CON-AUT04,CON-AUT05) • Selecciona todas las fotos en las que aparece un animal. (PRO-CONF06)		
Ingeniería social.	<ul style="list-style-type: none"> • Falta de verificación de los datos ingresados al registrar la cuenta • El sistema permite editar el nombre y la fecha de nacimiento. • Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información. • Falta de información de las configuraciones de privacidad a los usuarios. 	<ul style="list-style-type: none"> • Verifica al registrar la cuenta, si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (PRO-REG01) • Bloquea la cuenta en casos que no se confirme el número de teléfono o dirección de correo electrónico al crear la cuenta. (PRO-REG01) • Cerrar sesión en todos los dispositivos. (CON-AUT03) • Control de privacidad en la información del perfil. (CON-PER01,CON-PER02,CON-PER03,CON-PER04,CON-PER05) • Control de privacidad en publicaciones. (CON-PUB01,CON-PUB02) • Visualizar como otros usuarios ven la biografía. (CON-PUB04) • Bloquear usuarios, mensajes, páginas, aplicaciones, invitaciones a aplicaciones y eventos de una persona en concreto. (PRO-REP04) • Limite en el uso de funciones. (CON-TEC03) • Restablecer contraseña (por correo electrónico, pregunta de seguridad o amigos de confianza) (CON-AUT03,CON-AUT04,CON-AUT05) 	Bajo.	<ul style="list-style-type: none"> • Compara la información de la cuenta con el documento subido, el documento debe contener foto, nombre, apellido y fecha de nacimiento. • Configuración del control de seguridad (Opción para no recibir mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta. • Bloqueo de guardar fotografías, videos e información. • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.

Nota: a. En el cuadro se encuentra el listado de las amenazas, vulnerabilidades, controles actuales, nivel de riesgo y controles recomendados. Se encuentra clasificado por amenaza (una amenaza tiene varias vulnerabilidades, controles actuales y controles recomendados).

b. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar cuenta en Facebook es identificada como PRO-REG01.

4. Capitulo IV. Diseño de Controles Propuestos de Seguridad Personal en Redes Sociales.

En el presente capitulo se rediseña los procesos actuales del software de Facebook revisados en el capítulo anterior y se diseñan nuevos controles de seguridad personal en redes sociales.

El objetivo de este capítulo es proponer procesos estándar a las redes sociales, en las cuales se encuentran los controles necesarios para minimizar los riesgos existentes.

Tabla 62. Controles recomendados para minimizar los riesgos por amenaza.

AMENAZA	RIESGO	CONTROL
Acoso cibernético	Alto.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01) • Advertencias de información incorrecta o maliciosa. (DIS-COM01) • Revisión de publicaciones y comentarios antes que aparezcan (se activa automáticamente). (DIS-COM02) • Reportar contenido. (DIS-COM03) • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01) • Control de seguridad en un menor de edad. (DIS-MEN01)
Grooming.	Alto.	<ul style="list-style-type: none"> • Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01) • Reportar contenido. (DIS-COM03) • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01) • Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01) • Control de seguridad en un menor de edad. (DIS-MEN01)
Falsificación de identidad.	Medio.	<ul style="list-style-type: none"> • Compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (DIS-REG01) • Confirma el número de teléfono y dirección de correo electrónico, caso contrario se bloquea la cuenta. (DIS-REG01) • Compara la información de la cuenta (foto, nombre, apellido y

		<p>fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01)</p> <ul style="list-style-type: none"> • Reportar contenido. (DIS-COM03) • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01)
Suplantación de identidad.	Medio.	<ul style="list-style-type: none"> • Compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (DIS-REG01) • Confirma el número de teléfono y dirección de correo electrónico, caso contrario se bloquea la cuenta. (DIS-REG01) • Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01) • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Reportar contenido. (DIS-COM03) • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01) • El sistema permite editar la configuración de seguridad. (DIS-SEG01)
Falta de privacidad.	Medio.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Encriptación de contraseña. (DIS-REG02,DIS-AUT01) • Reportar contenido. (DIS-COM03) • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Control de seguridad en un menor de edad. (DIS-MEN01)
Crímenes contra el honor.	Medio.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01) • Advertencias de información incorrecta o maliciosa. (DIS-COM01) • Revisión de publicaciones y comentarios antes que aparezcan (se activa automáticamente). (DIS-COM02) • Reportar contenido. (DIS-COM03)

		<ul style="list-style-type: none"> • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01) • Control de seguridad en un menor de edad. (DIS-MEN01)
Divulgación de contenido inapropiado.	Medio.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01) • Advertencias de información incorrecta o maliciosa. (DIS-COM01) • Revisión de publicaciones y comentarios antes que aparezcan (se activa automáticamente). (DIS-COM02) • Reportar contenido. (DIS-COM03) • El sistema permite editar la configuración de seguridad. (DIS-SEG01)
Fraude informático.	Bajo.	<ul style="list-style-type: none"> • Compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (DIS-REG01) • Confirma el número de teléfono y dirección de correo electrónico, caso contrario se bloquea la cuenta. (DIS-REG01) • Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01) • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Encriptación de contraseña. (DIS-REG02,DIS-AUT01) • Validación del usuario y contraseña (autenticación). (DIS-REG02,DIS-AUT01) • Restablecer contraseña (DIS-AUT02) • Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02) • Cerrar sesión en todos los dispositivos. (DIS-AUT02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01) • Advertencias de información incorrecta o maliciosa. (DIS-COM01) • Reportar contenido. (DIS-COM03) • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01) • El sistema permite editar la pregunta de seguridad. (DIS-

		<p>CON02)</p> <ul style="list-style-type: none"> • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01)
Robo de información.	Bajo.	<ul style="list-style-type: none"> • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Encriptación de contraseña. (DIS-REG02,DIS-AUT01) • Validación del usuario y contraseña (autenticación). (DIS-REG02,DIS-AUT01) • Restablecer contraseña (DIS-AUT02) • Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02) • Cerrar sesión en todos los dispositivos. (DIS-AUT02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01) • Reportar contenido. (DIS-COM03) • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Control de seguridad en un menor de edad. (DIS-MEN01)
Acceso no autorizado.	Bajo.	<ul style="list-style-type: none"> • Encriptación de contraseña. (DIS-REG02,DIS-AUT01) • Validación del usuario y contraseña (autenticación). (DIS-REG02,DIS-AUT01) • Alerta de inicio de sesión (se activa automáticamente). (DIS-AUT01) • Restablecer contraseña (DIS-AUT02) • Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02) • Cerrar sesión en todos los dispositivos. (DIS-AUT02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • El sistema permite editar la pregunta de seguridad. (DIS-CON02) • Copia de Seguridad. (DIS-ELI01) • Verificación de la respuesta de la pregunta de seguridad y contraseña. (DIS-ELI01)
Hurto de cuenta.	Bajo.	<ul style="list-style-type: none"> • Encriptación de contraseña. (DIS-REG02,DIS-AUT01) • Validación del usuario y contraseña (autenticación). (DIS-REG02,DIS-AUT01) • Alerta de inicio de sesión (se activa automáticamente). (DIS-AUT01) • Restablecer contraseña (DIS-AUT02) • Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02) • Cerrar sesión en todos los dispositivos. (DIS-AUT02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • El sistema permite editar la pregunta de seguridad. (DIS-CON02) • Copia de Seguridad. (DIS-ELI01) • Verificación de la respuesta de la pregunta de seguridad y

		contraseña. (DIS-ELI01)
Ingeniería social.	Bajo.	<ul style="list-style-type: none"> • Compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta. (DIS-REG01) • Confirma el número de teléfono y dirección de correo electrónico, caso contrario se bloquea la cuenta. (DIS-REG01) • Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01) • Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02) • Bloqueo de guardar fotografías, videos e información. (DIS-REG02) • Restablecer contraseña (DIS-AUT02) • Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02) • Cerrar sesión en todos los dispositivos. (DIS-AUT02) • Comprobar los últimos cambios de la cuenta. (DIS-AUT02) • El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01) • El sistema permite editar la configuración de seguridad. (DIS-SEG01) • Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01)

Nota: a. En el cuadro se encuentra el listado de las amenazas con su respectivo nivel de riesgo y los controles propuestos que contrarrestan dicho riesgo.

b. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar Cuenta es identificada como DIS-REG01.

En general una red social debe proporcionar a los usuarios los siguientes procesos: registrar la cuenta, autenticar la cuenta, compartir contenido y los controles automáticos del sistema.

El proceso de registrar la cuenta se realiza solo una vez, cuando el usuario crea la cuenta en la red social. Los procesos compartir contenido y configurar cuenta se pueden realizar en cualquier orden después de autenticar la cuenta y es opcional su realización.

Los recuadros de color rojo corresponden a los nuevos procesos recomendados, los de color azul corresponden a los procesos rediseñados del capítulo anterior y los de color negro son los procesos originales revisados en el capítulo III.

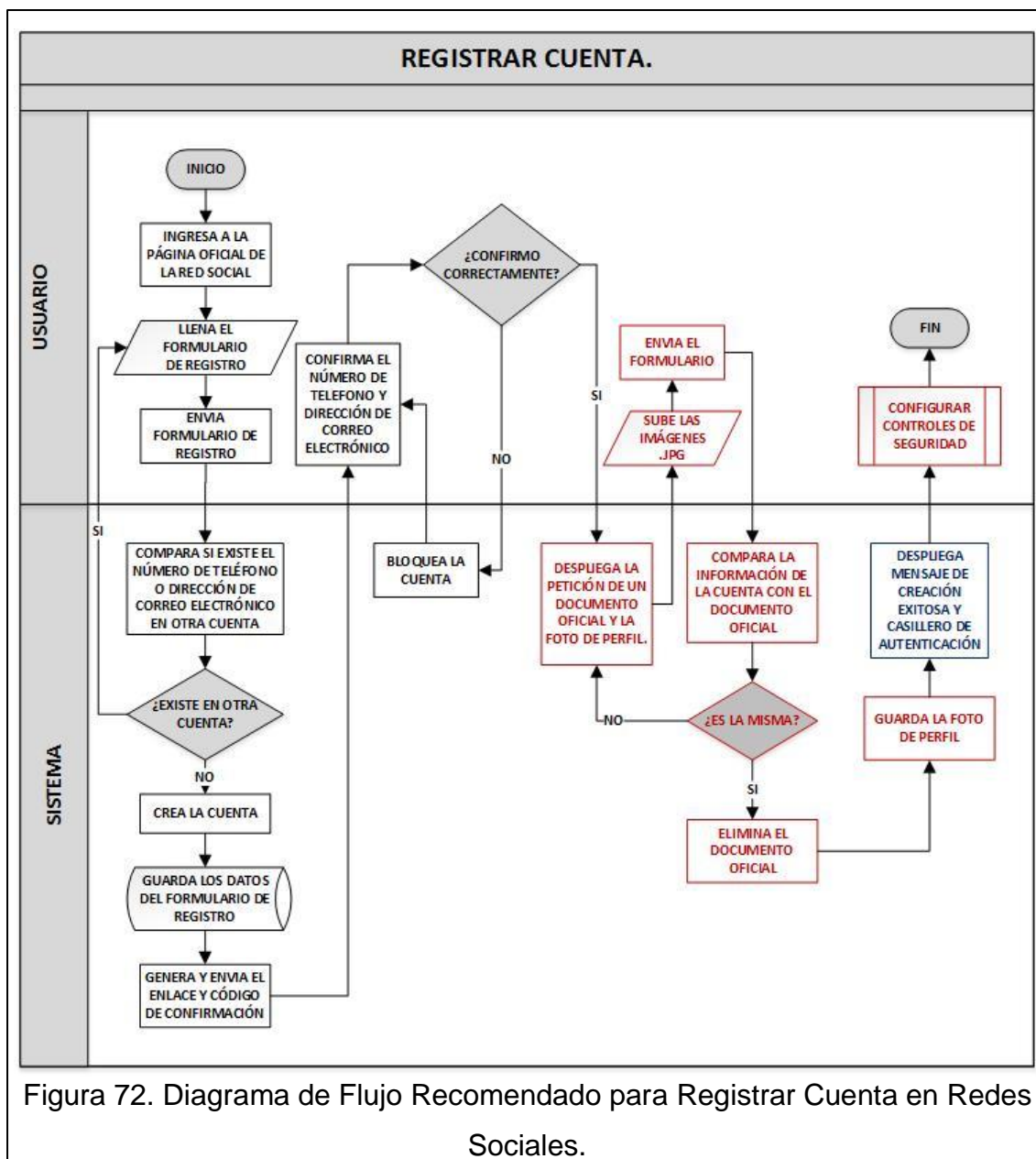
regresa el sistema a la página del formulario. En caso de no estar utilizado crea la cuenta, guarda la información proporcionada en el formulario de registro, genera y envía un enlace de confirmación a la dirección de correo electrónico y un código por medio de mensaje de texto al número proporcionado en el formulario.

El usuario confirma el número de teléfono y la dirección de correo electrónico. En caso de no confirmar la cuenta es bloqueada hasta cumplir con el requisito de la confirmación.

Cuando se realiza la confirmación, el sistema despliega el formulario con la petición de la foto de perfil y un documento en el que conste el nombre, apellido, fecha de nacimiento y foto de la persona (por ejemplo la cédula de identidad). El usuario sube las imágenes en formato .JPG y envía. El sistema compara la información de la cuenta con el documento por medio de algoritmos de reconocimiento de patrones.

Si es la misma información, elimina el documento y guarda la foto de perfil para desplegar el mensaje de creación exitosa en conjunto con el casillero de autenticación. Automáticamente comienza el subproceso de configurar controles de seguridad.

En caso que no sea la misma información, despliega el formulario solicitando el documento (foto, nombre, apellido y fecha de nacimiento) en formato .JPG nuevamente.



Controles:

- El sistema compara si existe el número de teléfono o dirección de correo electrónico en otra cuenta.
- El usuario confirma el número de teléfono y la dirección de correo electrónico, caso contrario la cuenta es bloqueada hasta cumplir con el requisito de la confirmación.

- El sistema compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones.

Objetivo de los controles:

El objetivo es minimizar la falsificación y suplantación de identidad en las redes sociales para evitar delitos cibernéticos como el grooming, fraudes informáticos, ingeniería social, etc.

Parámetros de medición:

- Número de reportes de abuso por falsificación y suplantación de identidad.
- Encuesta de seguridad personal.

4.1.1. Proceso Recomendado para Configurar Controles de Seguridad. ([DIS-REG02](#))

Se ingresa en los casilleros de autenticación los datos de dirección de correo electrónico o número de celular y contraseña. En caso de no recordar la contraseña, se restablece la misma.

Existe la opción para que el usuario guarde la sesión y se quede abierta, caso contrario al cerrar el navegador se cierra sesión automáticamente.

El sistema encripta la contraseña cuando se envían los datos de autenticación para validar el usuario y contraseña. Si es correcta inicia sesión y extrae todo el contenido relacionado al usuario de la base de datos, para posteriormente desplegar la página de configuración de seguridad.

El usuario ingresa la respuesta a la pregunta de seguridad, selecciona la audiencia que puede publicar en la biografía, ver las publicaciones, la información del perfil, las secciones, la lista de amigos, enviar solicitudes de amistad y elige si activa la función de recepción de mensajes de desconocidos para guardar los cambios.

Si activo la recepción de mensajes, el sistema activa la función y selecciona los usuarios que pueden visualizar y oculta a los demás la información. En caso de no activar, el sistema solo selecciona los usuarios que pueden visualizar y oculta a los demás la información.

El sistema activa automáticamente los controles de alerta de inicio de sesión que enviara notificaciones a la cuenta y al correo electrónico cada vez que se ingrese a la cuenta desde un dispositivo nuevo, la revisión de la biografía para revisar las publicaciones de otras personas antes que aparezcan en la biografía, activa el bloqueo de guardar fotografías, videos e información de la cuenta y por ultimo despliega el video indicando las opciones de seguridad y privacidad del usuario.

El usuario reproduce el video y automáticamente al terminar la reproducción el sistema despliega la página de inicio.

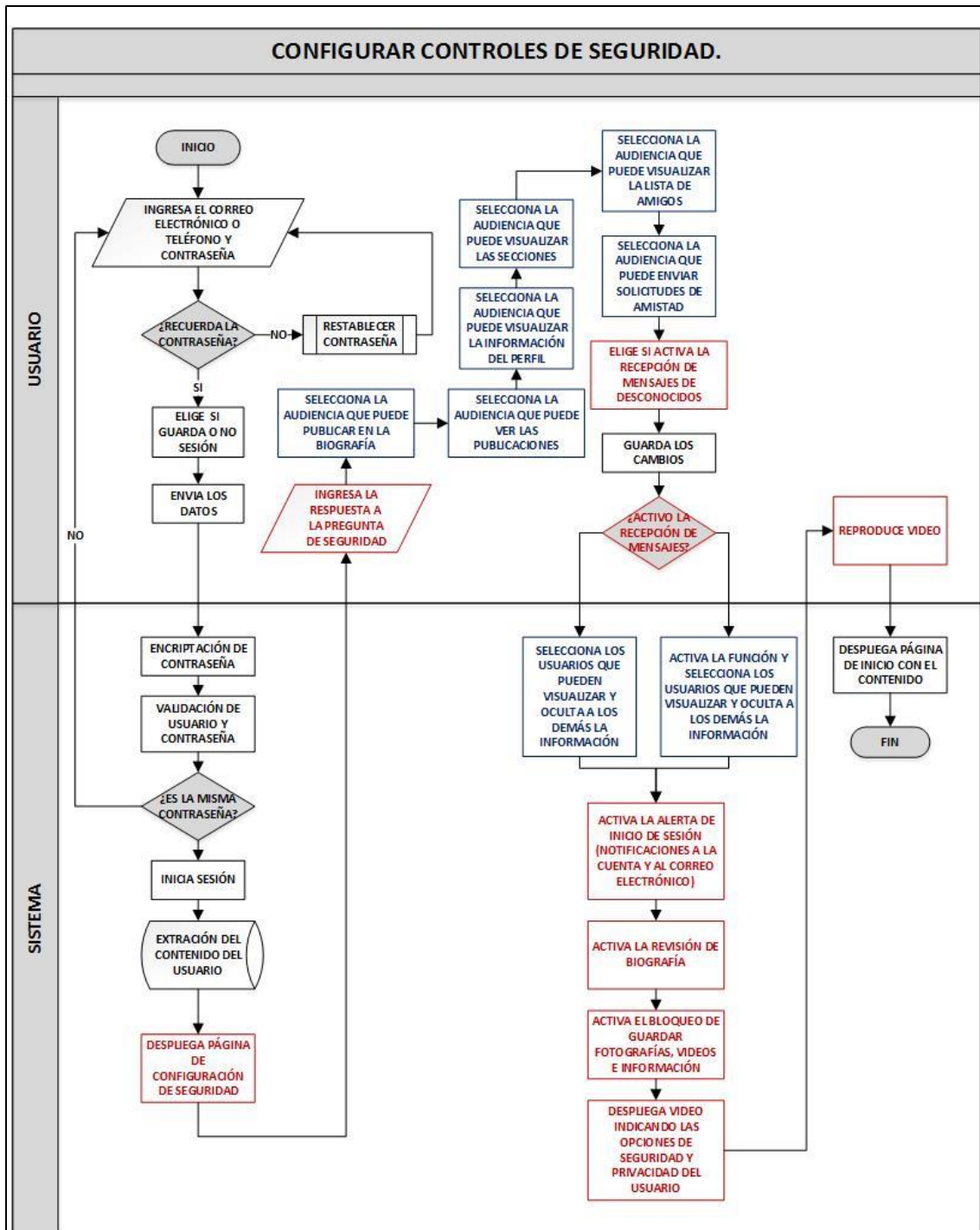


Figura 73. Diagrama de Flujo Recomendado para Configurar Controles de Seguridad en Redes Sociales.

Controles:

- Encriptación de contraseña.
- Validación del usuario y contraseña (autenticación).

- Configuración del control de seguridad (quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos).
- Bloqueo de guardar fotografías, videos e información.

Objetivo de los controles:

El objetivo es dar niveles de seguridad personal eficaces a los usuarios para prevenir el acoso cibernético, robo de información, divulgación de contenido inapropiado, fraude informático, suplantación de identidad, falta de privacidad, etc.

Parámetros de medición:

- Número de reportes de abuso por falta de privacidad y acoso.
- Cuentas eliminadas por razones de seguridad.
- Encuesta de seguridad personal.

4.2. Proceso Recomendado para Autenticar en Redes Sociales. ([DIS-AUT01](#))

Para iniciar sesión se ingresan los datos de dirección de correo electrónico, nombre de usuario o número de celular y contraseña. En caso de no recordar la contraseña, se restablece la misma.

Existe la opción para que el usuario guarde la sesión y se quede abierta, caso contrario al cerrar el navegador se cierra sesión automáticamente.

El sistema encripta la contraseña cuando se envían los datos de autenticación para validar el usuario y contraseña. Si es incorrecta regresa a la página de autenticación.

En caso de ser correcta, verifica si el dispositivo se encuentra guardado. Si es un dispositivo antiguo, inicia sesión y extrae todo el contenido relacionado al

usuario de la base de datos, para posteriormente desplegar la información en la página de inicio de la red social. El usuario accede a su cuenta y navega por la misma.

Si es un dispositivo nuevo, el sistema obtiene los datos del dispositivo para posteriormente enviar la información como notificación a la cuenta del usuario y al correo electrónico. La alerta despliega el dispositivo, la fecha, hora y ubicación aproximada del dispositivo en el que se ingresó a la cuenta.

El sistema inicia sesión y extrae todo el contenido relacionado al usuario de la base de datos, para posteriormente desplegar la información en la página de inicio de la red social y la notificación correspondiente.

El usuario accede a la cuenta y revisa la notificación. Si el usuario identifica que no fue él quien inicio sesión, debe restablecer la contraseña.

Caso contrario, si es un dispositivo que se usa constantemente y es privado se guarda para que en próximas ocasiones no envíe dicha alerta. Al final el usuario va acceder a la página de inicio.

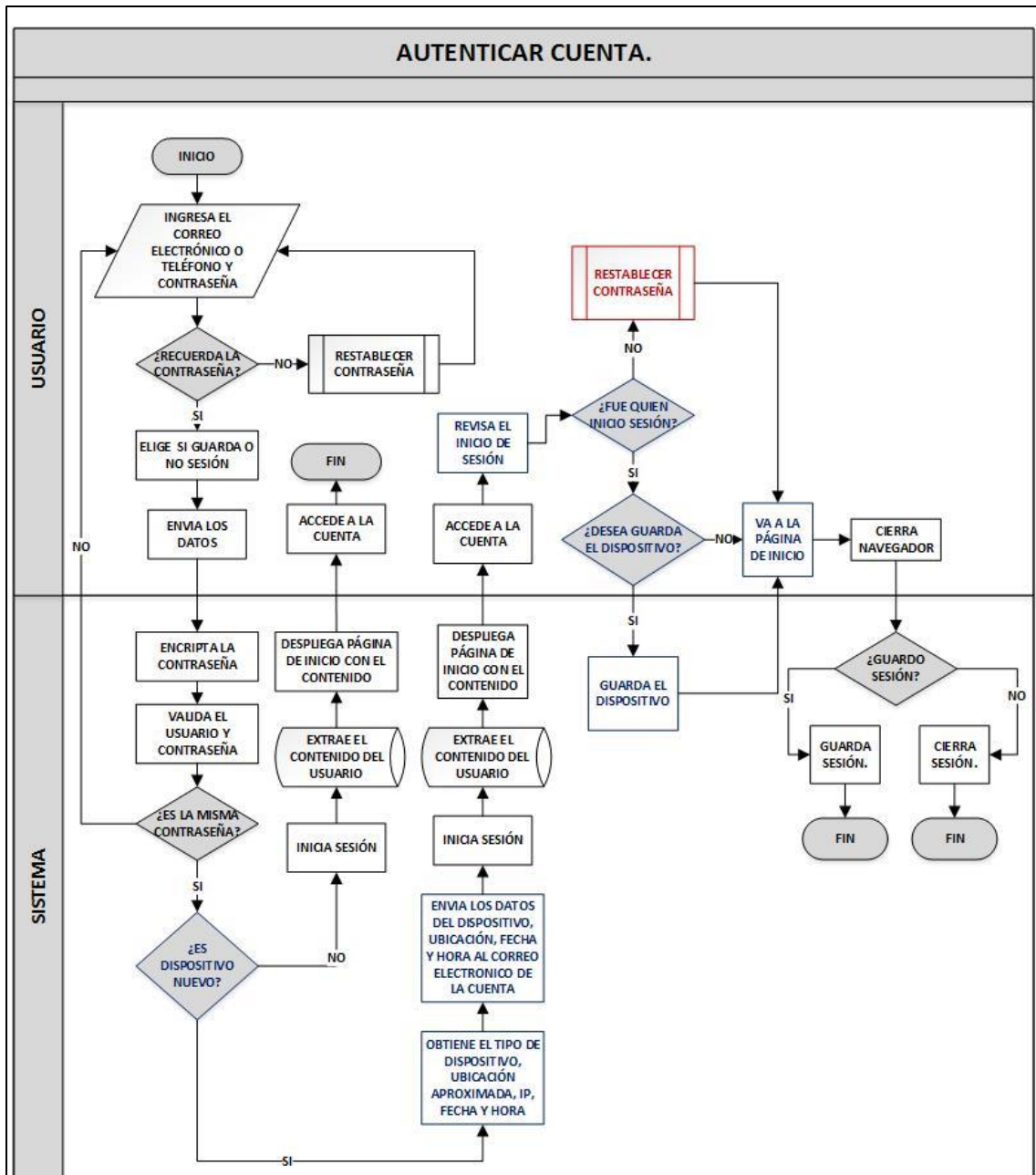


Figura 74. Diagrama de Flujo Recomendado para Autenticar en Redes Sociales.

Controles:

- Encriptación de contraseña.
- Validación del usuario y contraseña (autenticación).
- Verifica si el dispositivo es nuevo, en caso de serlo obtiene y envía los datos del dispositivo como notificación y correo electrónico para ser revisado el inicio de sesión (alerta de inicio de sesión).

Objetivo de los controles:

El objetivo es impedir el acceso no autorizado a la cuenta del usuario para prevenir y detectar el hurto de la cuenta, robo de información, fraude informático, falta de privacidad, etc.

Parámetros de medición:

- Número de reportes de abuso por acceso no autorizado.
- Número de veces de restablecimiento de contraseña.
- Encuesta de seguridad personal.

4.2.1. Proceso Recomendado para Restablecer Cuenta en Redes Sociales. ([DIS-AUT02](#))

Por seguridad del usuario, la red social solo permite restablecer contraseñas y nunca envía la contraseña pasada, ya que usa el mecanismo de encriptación de contraseñas para ser almacenadas como por ejemplo hash md5() y sha-2().

Si el usuario tiene problemas para iniciar sesión en su cuenta puede restablecer la contraseña. Primero ingresa el correo electrónico o número de teléfono para que el sistema busque la cuenta correspondiente.

El sistema despliega las opciones por el medio que se puede recuperar:

1. Responder la pregunta de seguridad.
2. Enviar un enlace al correo electrónico para restablecer la contraseña.
3. Enviar un código por SMS al número de teléfono para restablecer la contraseña.

La opción de usar la pregunta de seguridad, consiste en que el sistema busca la pregunta de seguridad de la cuenta y la despliega, el usuario responde y envía para que el sistema verifique la respuesta.

En caso de elegir la opción del correo electrónico o número de teléfono, el sistema envía un código de seguridad al mismo. El cual es ingresado para que el sistema verifique el mismo.

Si es correcto el sistema habilita el cambio de contraseña. El usuario ingresa la nueva contraseña y se guarda, desplegando el sistema la opción de cerrar sesión en todos los dispositivos que se encontraba abierta la cuenta del usuario. Por seguridad es preferible que si lo realice.

Por último el usuario revisa todos los últimos cambios realizados en la cuenta y accede a la misma.

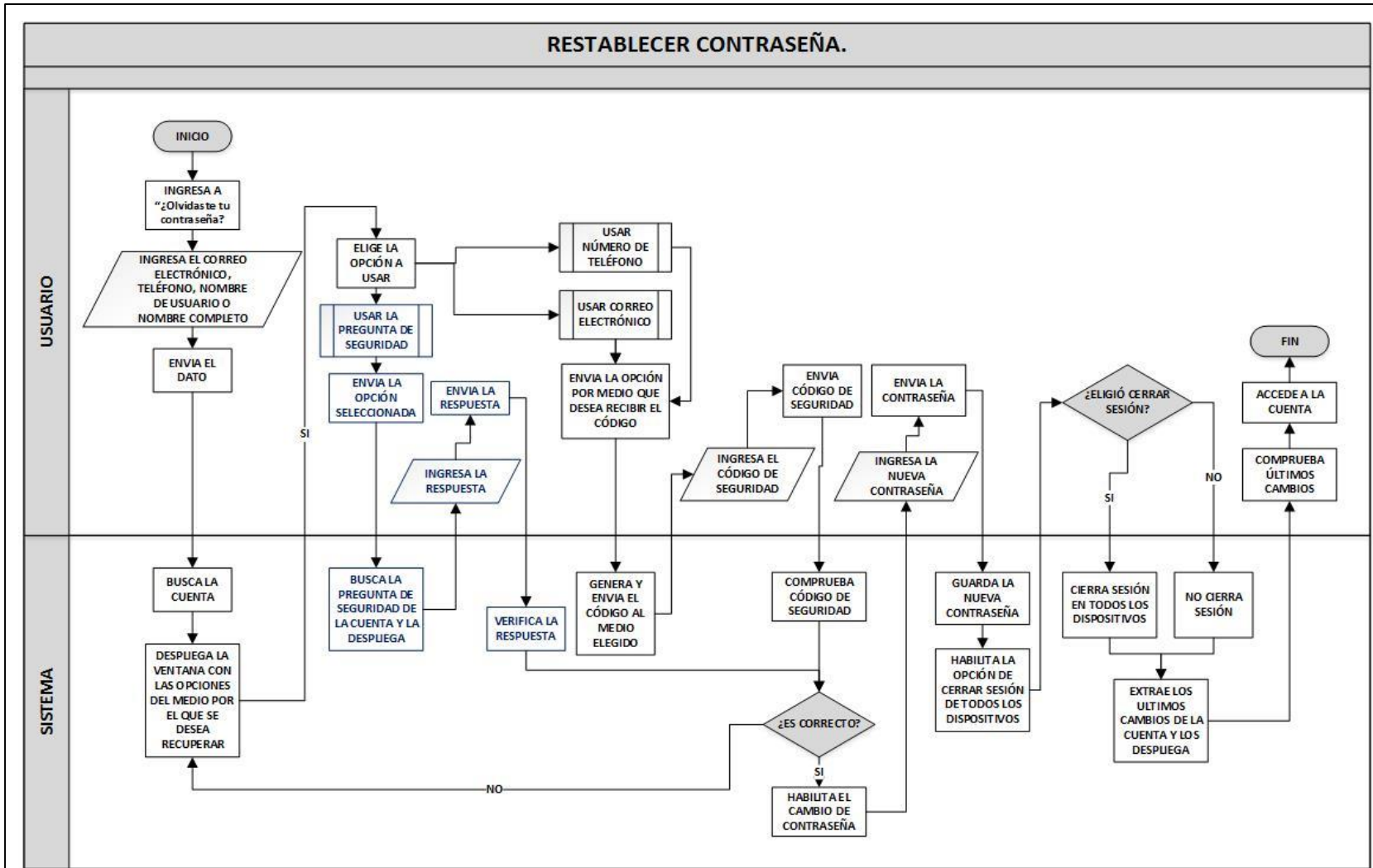


Figura 75. Diagrama de Flujo Recomendado para Restablecer Contraseña en Redes Sociales.

Controles:

- Verifica el código de seguridad o respuesta de la pregunta de seguridad.
- Restablecer contraseña.
- Cerrar sesión en todos los dispositivos.
- Comprobar los últimos cambios de la cuenta.

Objetivo de los controles:

El objetivo es proteger la cuenta del usuario en caso que se de hurto de la cuenta, acceso no autorizado, fraude informático, ingeniería social, etc.

Parámetros de medición:

- Número de contraseñas cambiadas.
- Número de sesiones cerradas en los dispositivos.
- Número de reportes de abuso por cambios en la cuenta no autorizados.
- Encuesta de seguridad personal.

4.3. Proceso Recomendado para Compartir Información. ([DIS-COM01](#))

Para compartir contenido el usuario ingresa a la página inicial de la red social y decide si el contenido es nuevo o desea compartir contenido ya publicado.

Si decide compartir nuevo contenido, ingresa el contenido (estado, foto, video, etc.), registra la ubicación y envía el contenido. El sistema analiza la información automáticamente por medio de los algoritmos de reconocimiento de patrones en sus equipos. Si es segura la información, guarda y despliega el contenido para que el usuario lo visualice. Si no es segura la información, el sistema despliega la advertencia y envía a la página principal.

Cuando envía por mensaje, va la publicación, ingresa en enviar por mensaje, ingresa el usuario y el comentario para posteriormente enviar el contenido. El sistema analiza la información automáticamente por medio de los algoritmos de reconocimiento de patrones en sus equipos. Si es segura la información, busca

el usuario, envía y despliega el contenido por medio del mensaje. Si no es segura la información, el sistema despliega la advertencia y envía a la página principal.

Para compartir la publicación en la biografía, va a la publicación, ingresa en compartir, ingresa un comentario y envía el contenido. El sistema analiza la información automáticamente por medio de los algoritmos de reconocimiento de patrones en sus equipos. Si es segura la información, guarda y despliega el contenido para que el usuario lo visualice. Si no es segura la información, el sistema despliega la advertencia y envía a la página principal.

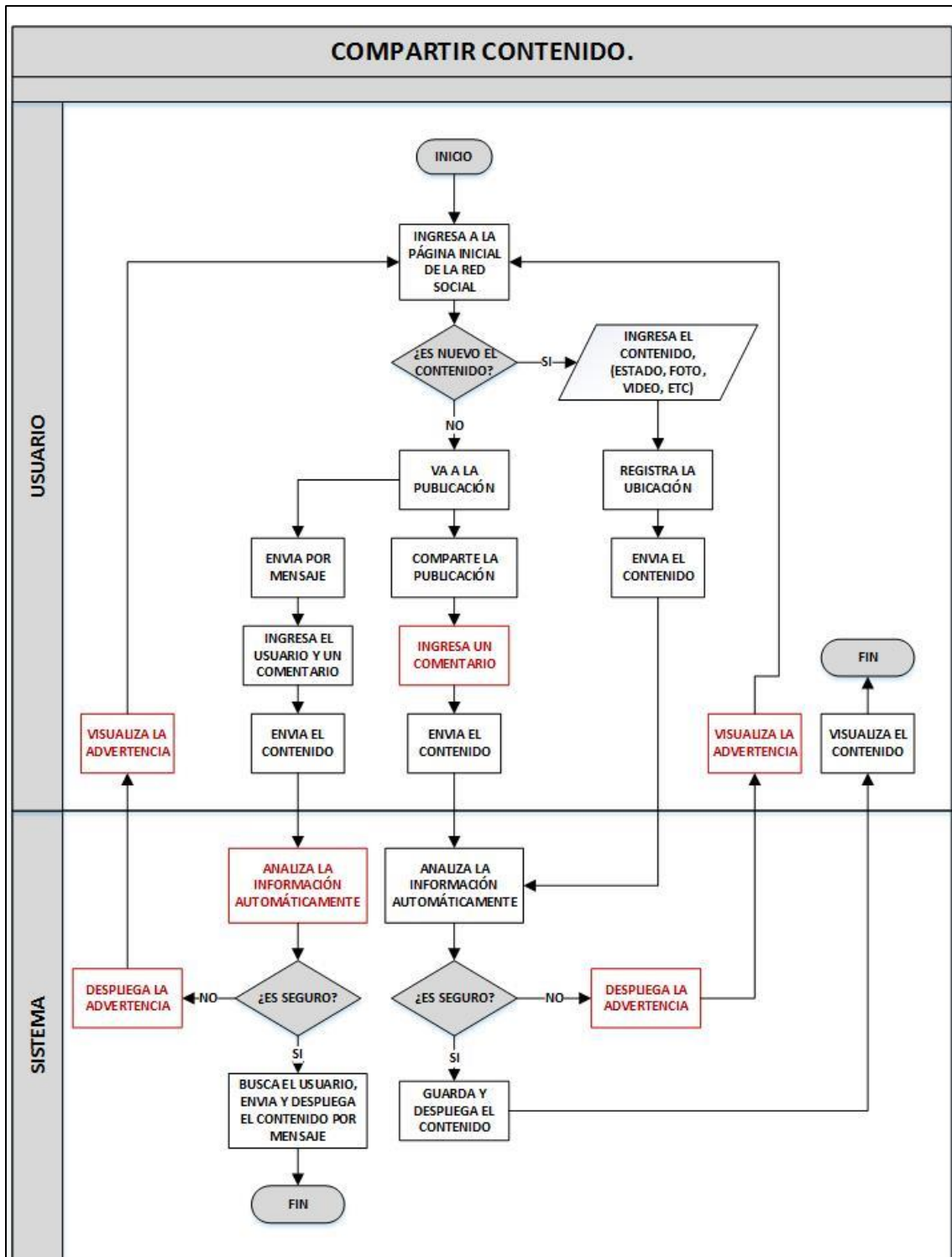


Figura 76. Diagrama de Flujo Recomendado para Compartir Contenido en Redes Sociales.

Controles:

- Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos.
- Advertencias de información incorrecta o maliciosa.

Objetivo de los controles:

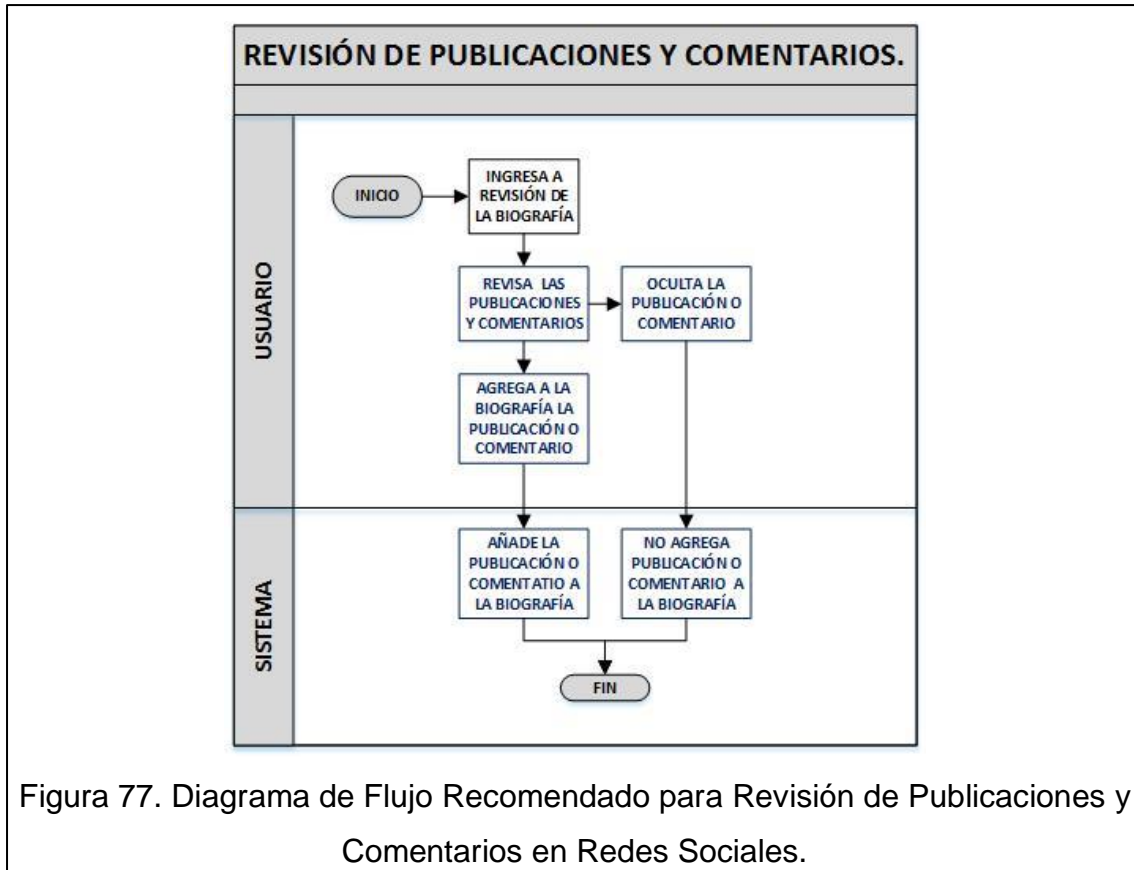
El objetivo es prevenir y proteger al usuario de la divulgación de contenido inapropiado, crímenes contra el honor, contaminación de malware, acoso cibernético, etc.

Parámetros de medición:

- Número de reportes de abuso por contenido inapropiado y malware.
- Número de advertencias emitidas.
- Encuesta de seguridad personal.

4.3.1. Proceso Recomendado para Revisión de Publicaciones y Comentarios. ([DIS-COM02](#))

El usuario ingresa a revisión de la biografía, revisa las publicaciones y comentarios, agrega u oculta la publicación o comentarios para que el sistema añada o no la a la biografía.



Controles:

- Revisión de publicaciones y comentarios antes que aparezcan.

Objetivo de los controles:

El objetivo es prevenir al usuario de la divulgación de contenido inapropiado, crímenes contra el honor, acoso cibernético, falta de privacidad, etc.

Parámetros de medición:

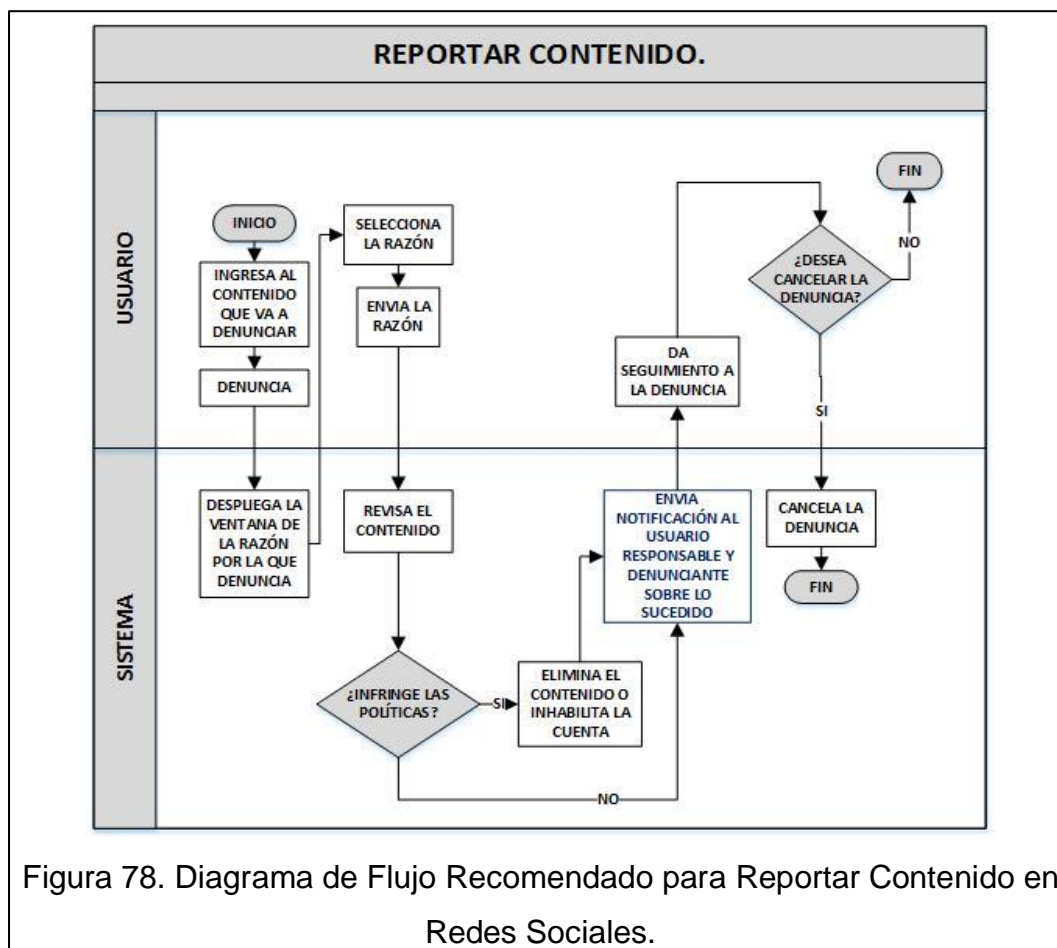
- Número de reportes de abuso por publicaciones o comentarios inapropiados.
- Encuesta de seguridad personal.

4.3.2. Proceso Recomendado para Reportar Contenido. (DIS-COM03)

Para reportar, el usuario ingresa al contenido y presiona la opción de denunciar. El sistema despliega la ventana de la razón por la que denuncia. Una vez elegida y enviada, el sistema revisa el contenido.

Si infringe, elimina el contenido o inhabilita la cuenta.

En caso que infrinja o no, envía la notificación al responsable y al denunciante sobre lo sucedido. El usuario denunciante da seguimiento a la denuncia llegando a decidir si cancela la denuncia o no.



Controles:

- Reportar contenido.
- Revisión del contenido.
- Dar seguimiento de la denuncia.

Objetivo de los controles:

El objetivo es eliminar el contenido o inhabilitar la cuenta en caso de ser necesario cuando existe divulgación de contenido inapropiado, suplantación de identidad, fraude informático, etc.

Parámetros de medición:

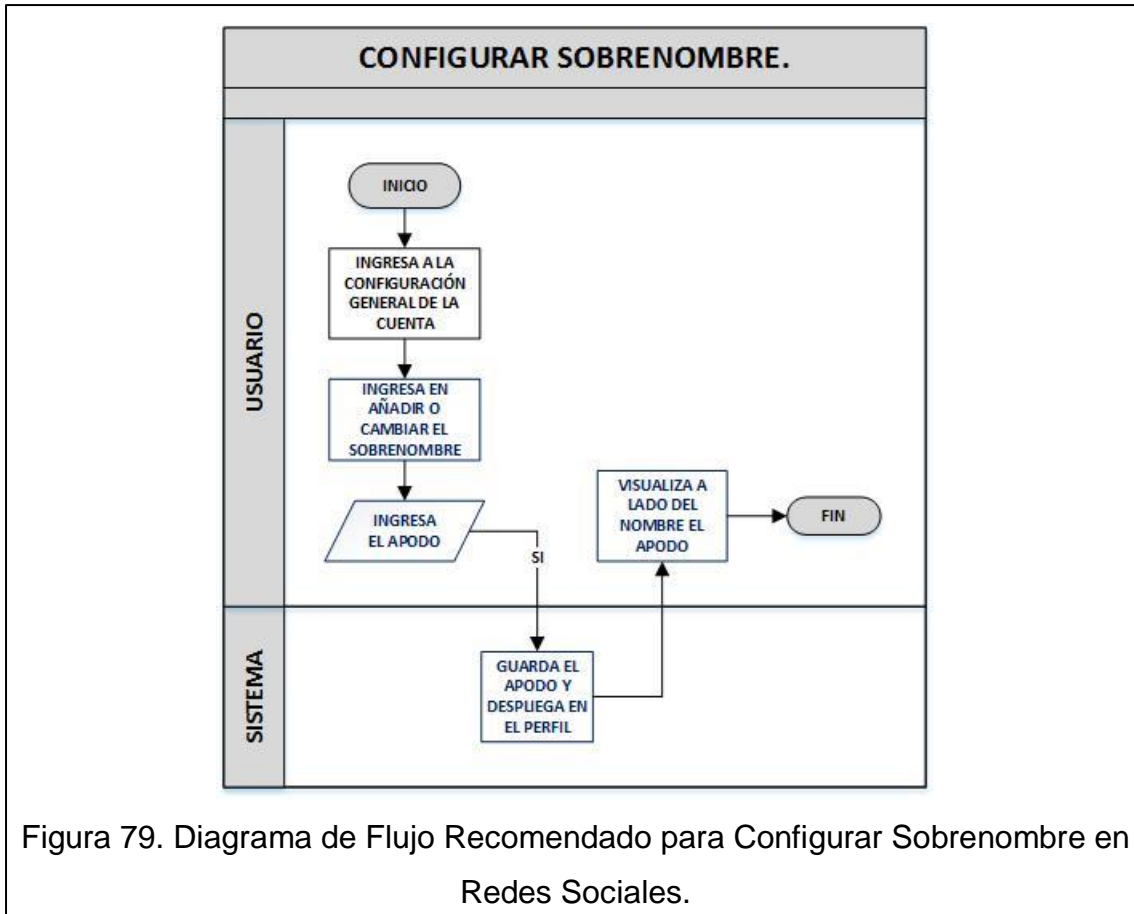
- Número de reportes de abuso.
- Tiempo de respuesta del reporte.
- Número de contenido y cuentas eliminadas.
- Número de cancelación de denuncias.
- Encuesta de seguridad personal.

4.4. Proceso Recomendado para Configurar Cuenta.

Es importante que en la configuración de la cuenta permita configurar un sobrenombre con el que los amigos identifican a la persona, ya que el nombre es el registrado oficialmente y no se puede cambiar. Permitir editar la pregunta de seguridad porque se usan en varios procesos y en el caso que alguien lo descubra puede ser un riesgo. Editar la configuración de seguridad en caso de querer hacer más privada o visible la información. Y al eliminar la cuenta, es importante tener en cuenta los controles de seguridad correspondientes.

4.4.1. Proceso Recomendado para Configurar Sobrenombre. ([DIS-CON01](#))

El usuario ingresa a la configuración general de la cuenta, en añadir o cambiar el sobrenombre e ingresa el apodo. El sistema guarda el sobrenombre y lo despliega en el perfil para que el usuario lo visualice a lado del nombre.



Controles:

- El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre.

Objetivo de los controles:

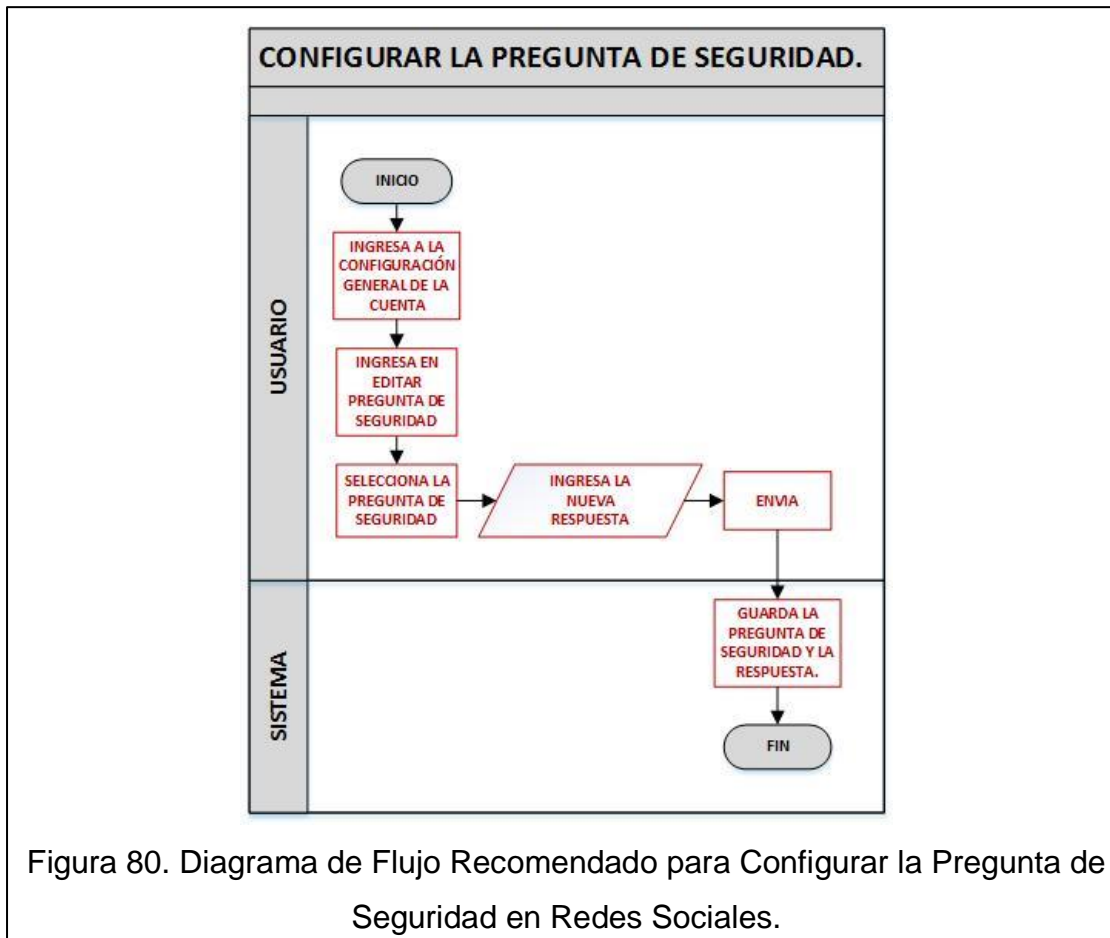
El objetivo es que el nombre oficial de los usuarios siempre se encuentre visible para brindar seguridad y fiabilidad de que el usuario no es falso.

Parámetros de medición:

- Número de cuentas denunciadas por falsificación o suplantación de identidad.
- Encuesta de seguridad personal.

4.4.2. Proceso Recomendado para Configurar la Pregunta de Seguridad. (DIS- CON02)

El usuario ingresa a la configuración general de la cuenta, en editar la pregunta de seguridad. Selecciona la pregunta de seguridad e ingresa la nueva respuesta para posteriormente enviar. El sistema guarda la pregunta de seguridad y la respuesta.



Controles:

- El sistema permite editar la pregunta de seguridad.

Objetivo de los controles:

El objetivo es que en caso que alguien adivine o sepa la respuesta de la pregunta de seguridad se pueda editar y así lograr un control más óptimo de la seguridad de la cuenta.

Parámetros de medición:

- Número de preguntas de seguridad cambiadas.
- Número de reportes de abuso por acceso no autorizado o eliminación de la cuenta sin autorización.
- Encuesta de seguridad personal.

4.4.3. Proceso Recomendado para Editar la Configuración de Seguridad. ([DIS-SEG01](#))

El usuario ingresa a la configuración general de la cuenta, en configuración de seguridad. Selecciona la audiencia que puede publicar en la biografía, ver las publicaciones, la información del perfil, las secciones, la lista de amigos, enviar solicitudes de amistad y elige si activa la función de recepción de mensajes de desconocidos para guardar los cambios.

Si activo la recepción de mensajes, el sistema activa la función y selecciona los usuarios que pueden visualizar y oculta a los demás la información. En caso de no activar, el sistema solo selecciona los usuarios que pueden visualizar y oculta a los demás la información. Y por último, despliega la página de inicio.

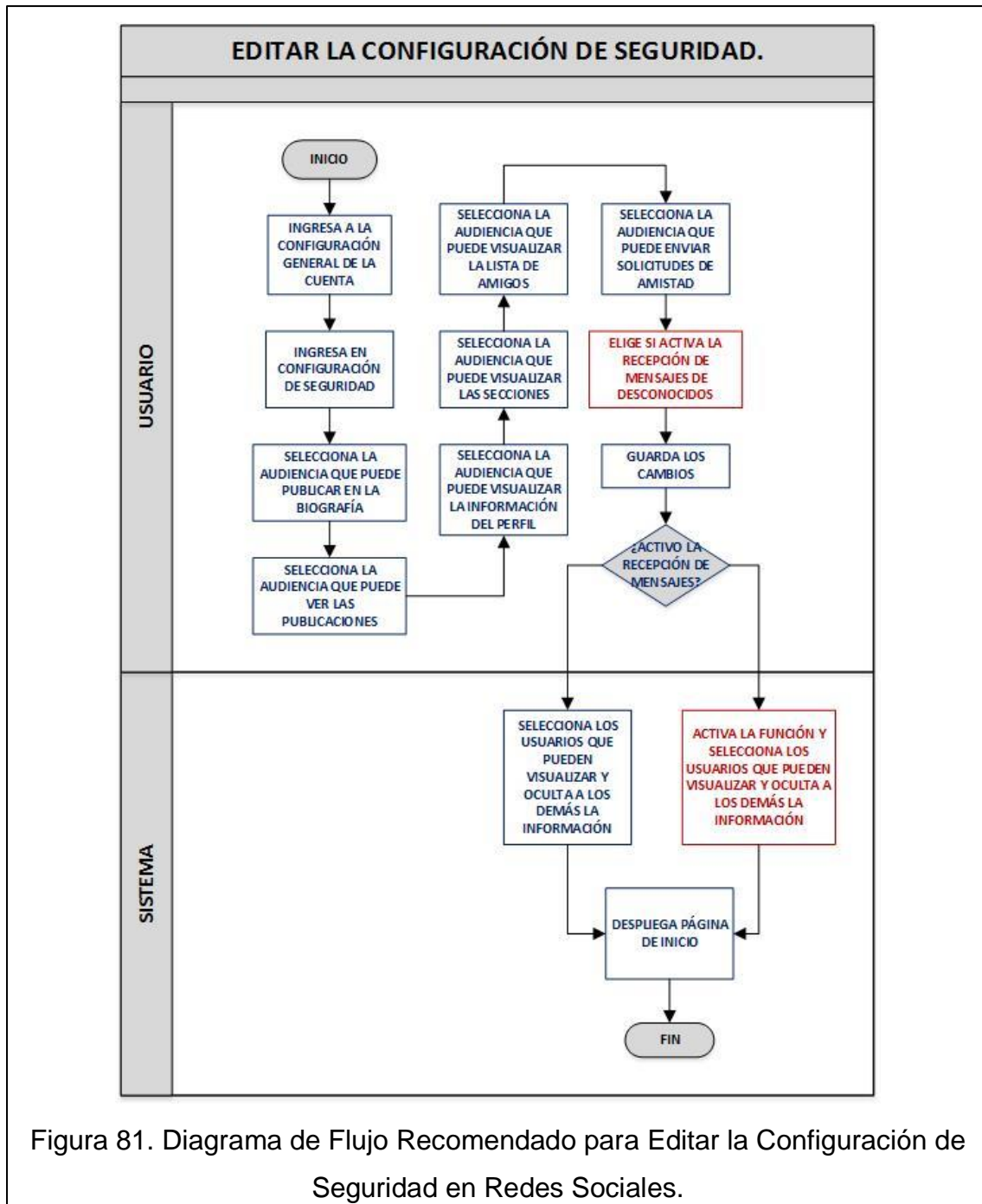


Figura 81. Diagrama de Flujo Recomendado para Editar la Configuración de Seguridad en Redes Sociales.

Controles:

- El sistema permite editar la configuración de seguridad. (quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos).

Objetivo de los controles:

El objetivo es brindar seguridad a los usuarios y que ellos pueden controlar la privacidad de su información.

Parámetros de medición:

- Número de reportes de abuso por falta de privacidad y acoso.
- Cuentas eliminadas por razones de seguridad.
- Encuesta de seguridad personal.

4.4.4. Proceso Recomendado para Eliminar Cuenta. ([DIS-ELI01](#))

Para eliminar la cuenta, el usuario ingresa a la configuración general de la cuenta y descarga la copia de información para la cual ingresa la contraseña. Una vez verificada la contraseña, el sistema crea el archivo, recopila la información, guarda la información en el archivo, crea y envía el correo electrónico con el enlace para descargar.

El usuario accede al correo electrónico y al enlace proporcionado, procede a descargar la información para lo que debe ingresar la contraseña de su cuenta. Una vez verificada la contraseña, el sistema permite la descarga para que el usuario visualice la carpeta con la información. El usuario acepta eliminar la cuenta y el sistema despliega la pregunta de seguridad y solicita de nuevo la contraseña. El usuario ingresa la contraseña y la respuesta de la pregunta de seguridad. Una vez enviada la información el sistema inhabilita la cuenta y después de 30 días elimina definitivamente la cuenta.

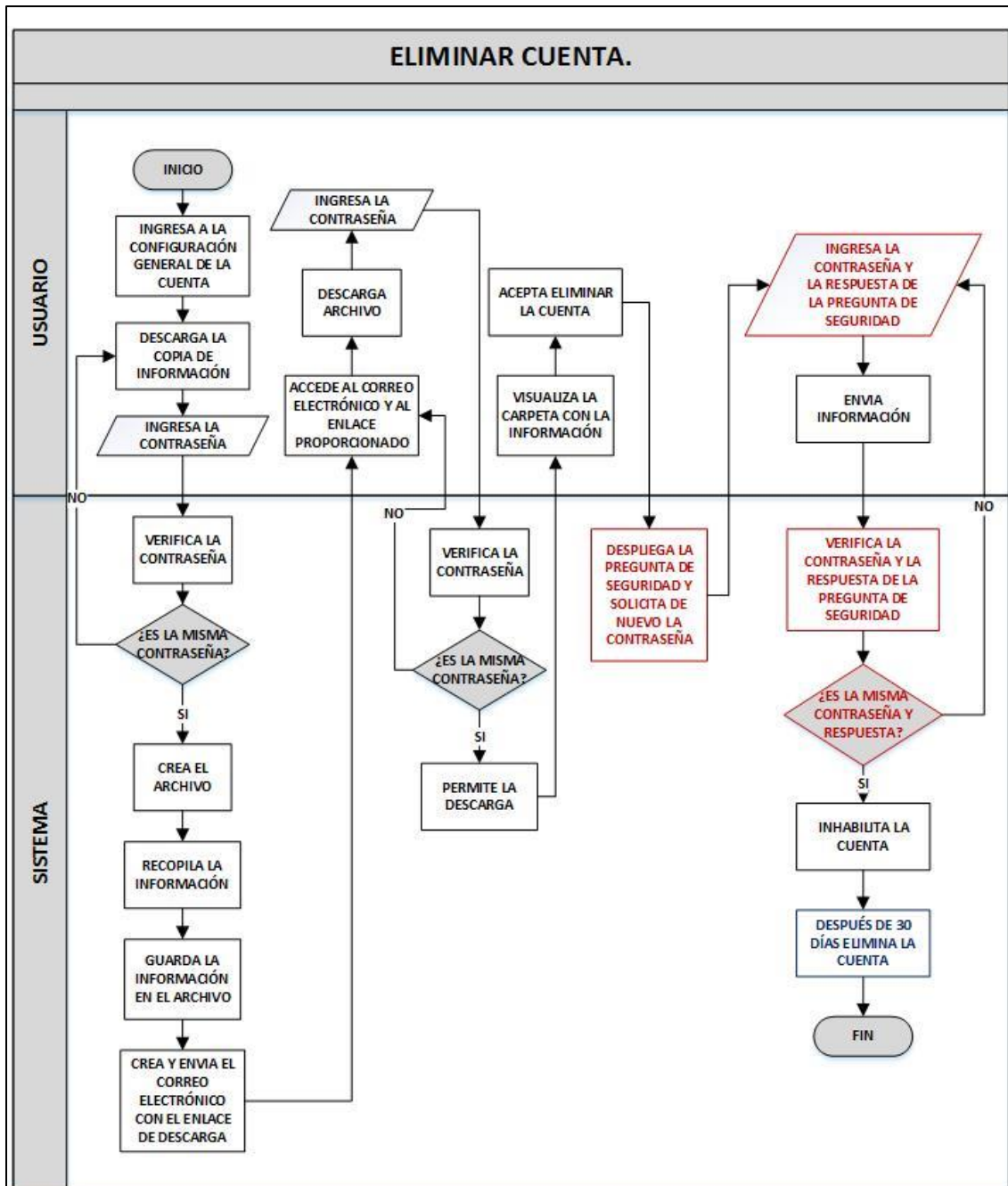


Figura 82. Diagrama de Flujo Recomendado para Eliminar Cuenta en Redes Sociales.

Controles:

- Copia de seguridad (información).
- Verificación de contraseña (autenticación).
- Verificación de la respuesta de la pregunta de seguridad y contraseña para eliminar la cuenta.

Objetivo de los controles:

El objetivo es brindar seguridad a los usuarios al eliminar su cuenta, contando con un backup de su información y asegurar que el dueño de la cuenta es quien se encuentra eliminando la misma.

Parámetros de medición:

- Número de copias de seguridad realizadas.
- Número de cuentas eliminadas satisfactoriamente e insatisfactoriamente.
- Encuesta de seguridad personal.

4.5. Proceso Recomendado para Controles Automáticos del Sistema.

Los controles de seguridad del usuario que el sistema lo realiza automáticamente es el límite en el uso de funciones y el control de seguridad en menores de edad.

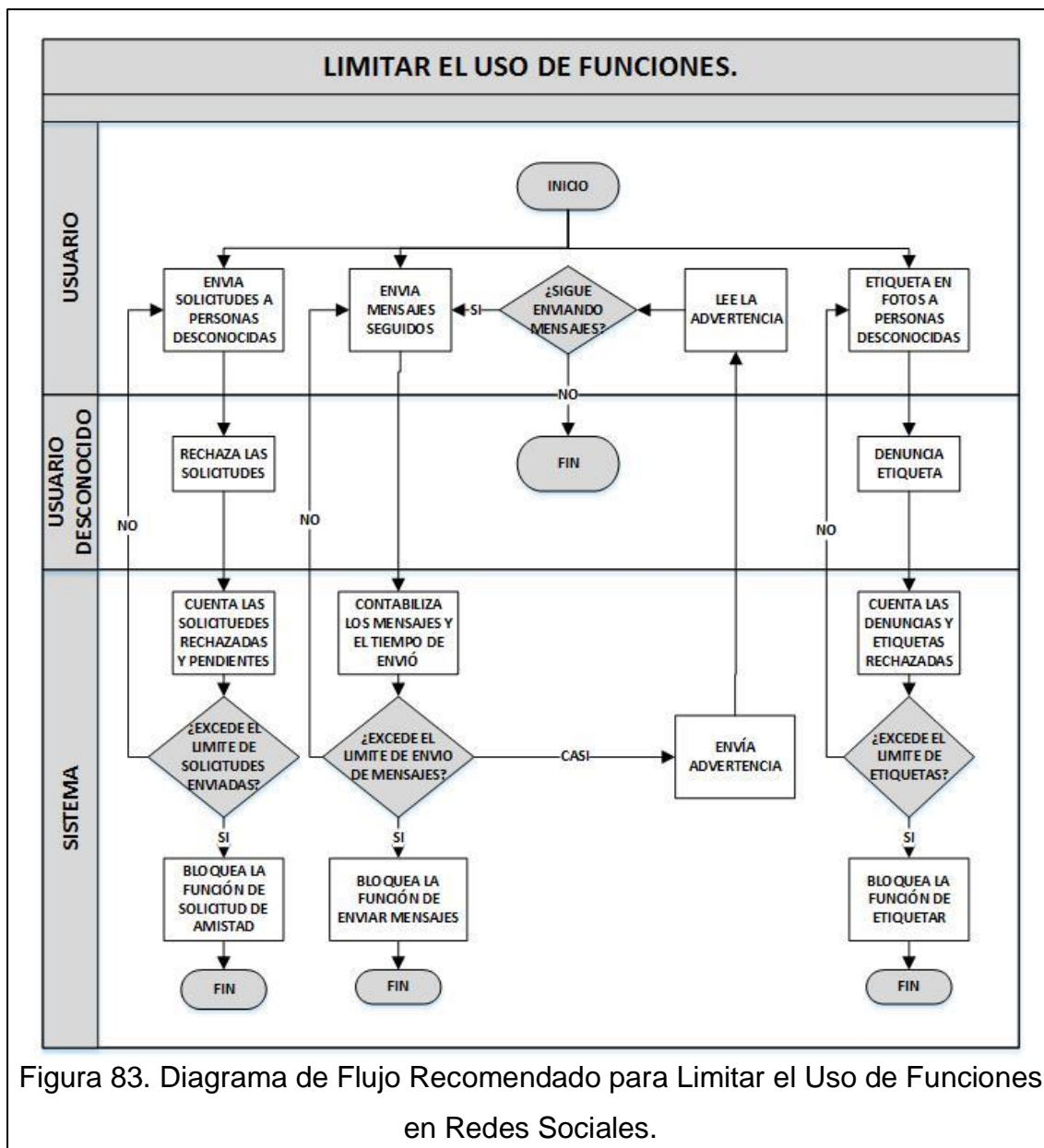
4.5.1. Proceso Recomendado para Limitar el Uso de Funciones. ([DIS-LIM01](#))

El límite en el uso de algunas funciones, es una forma de proteger a los usuarios contra el acoso o correo no deseado.

En caso de que un usuario envíe solicitudes de amistad a personas desconocidas y son rechazadas, el sistema contabiliza las solicitudes rechazadas y pendientes. Al momento que excede el límite de solicitudes enviadas, el sistema bloquea la función de solicitud de amistad.

Si el usuario envía mensajes seguidos, el sistema contabiliza los mensajes y el tiempo de envío. Si está a punto de exceder el límite, el sistema envía la advertencia de llegar al límite permitido de envío de mensajes. Al momento que excede el límite de envío de mensajes, el sistema bloquea la función de enviar mensajes.

Cuando se etiqueta en fotos a personas desconocidas y realizan la denuncia correspondiente, el sistema contabiliza las denuncias y etiquetas rechazadas para el momento en que excede el límite permitido, bloquear la función de etiquetar.



Controles:

- Bloquear la función al exceder el límite de intentos permitidos.
- Advertencias de llegar al límite permitido.

Objetivo de los controles:

El objetivo es detectar el uso excesivo de las funciones principales para prevenir el spam, acoso, etc.

Parámetros de medición:

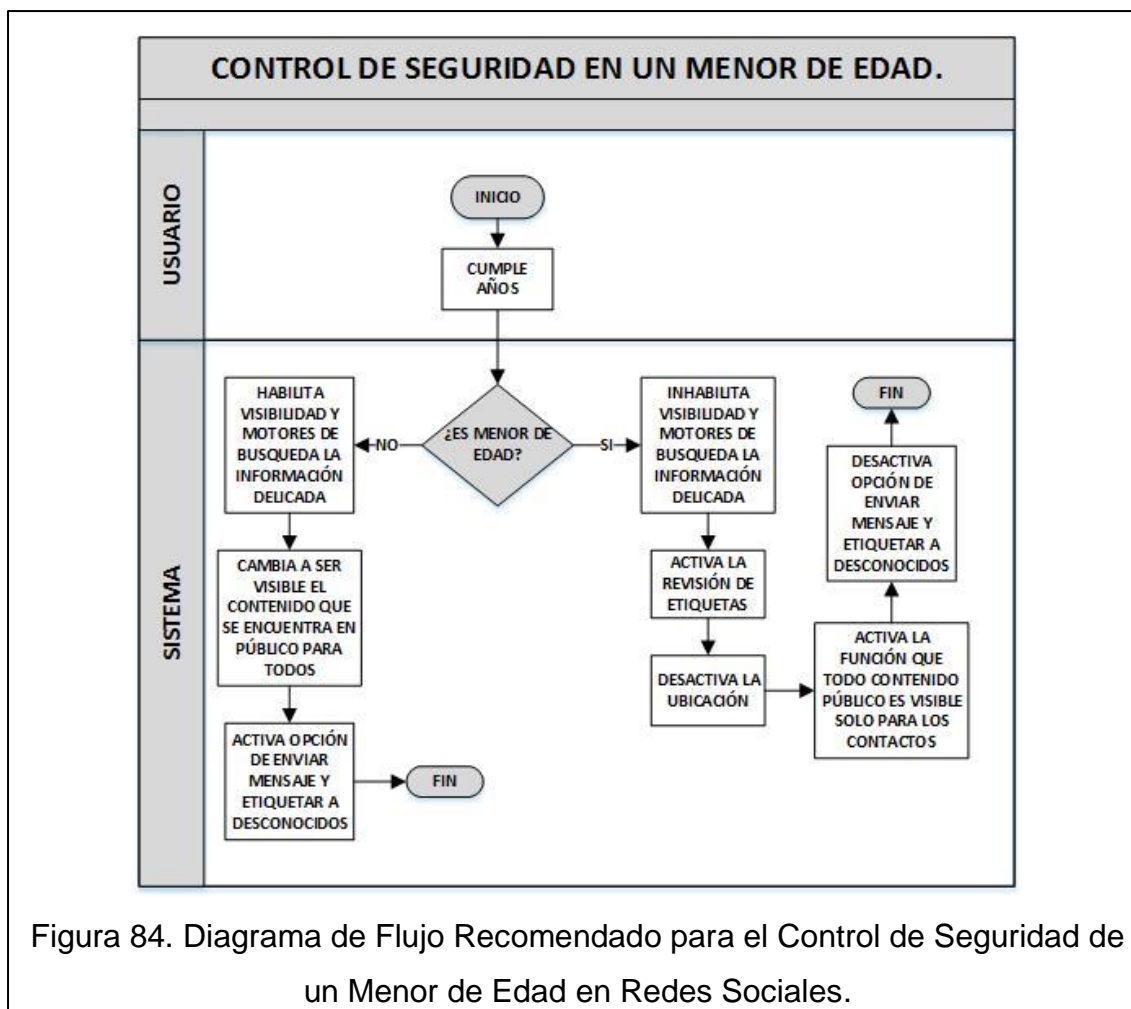
- Número de bloqueos de una función.
- Tiempo de bloqueos de una función.
- Número de advertencias emitidas.
- Encuesta de seguridad personal.

4.5.2. Proceso Recomendado para Control de Seguridad en un Menor de Edad. ([DIS-MEN01](#))

El control de seguridad en menores de edad comienza cada que el usuario cumple años.

Si el usuario es menor de edad se inhabilita la visibilidad y motores de búsqueda de la información delicada, se activa la revisión de etiquetas, se desactiva la ubicación, se activa la función que todo contenido público es visible solo para contactos y se desactiva la opción de enviar mensajes y etiquetar a desconocidos.

Cuando el usuario se convierte en mayor de edad, se habilita la visibilidad y motores de búsqueda de la información delicada, se cambia a visible todo el contenido que se encuentra en público y se activa la opción de enviar mensajes y etiquetar a desconocidos.



Controles:

- Inhabilita la visibilidad y motores de búsqueda de la información delicada.
- Activa la revisión de biografía.
- Desactiva la ubicación.
- Activar la función que todo contenido público es visible solo para los contactos.
- Desactivar la opción de enviar y recibir mensajes y etiquetas de desconocidos.

Objetivo de los controles:

El objetivo es proteger a los menores de edad en las redes sociales para evitar que sean acosados, desconocimiento de configuraciones de privacidad,

contacto con desconocidos al ser los más vulnerables a los delitos informáticos como el grooming.

Parámetros de medición:

- Número de reportes de abuso por grooming o falta de privacidad.
- Cuentas eliminadas por razones de inseguridad.
- Encuesta de seguridad personal.

4.6. Análisis de Control.

Los controles de seguridad personal que se diseñaron en los procesos de las redes sociales para regularizar el sistema y minimizar los riesgos son preventivos, de detección y correctivos.

Para asegurar que los controles son óptimos para implementar en una red social, se optó por calificar los controles propuestos de seguridad personal que se encuentran en los procesos recomendados para las redes sociales. Para dar valor a cada control se tomó en cuenta el tipo de control (prevención, detección y corrección) y la automatización del control (automático, semi automático y manual).

La calificación del control es la multiplicación del tipo de control por la automatización del control.

Tabla 63. Tipo del Control – Diseño de Controles.

CATEGORÍA	DESCRIPCIÓN	VALOR
Prevenir	Control de alto nivel orientado a prevenir la causa del riesgo en una etapa muy temprana.	Alto.
Detectar.	Control clave que actúa durante el proceso y permite corregir las deficiencias.	Medio.
Corregir	Control menos frecuente y actúa una vez que el proceso ha terminado	Bajo.

Nota: a. Es preferible prevenir a detectar, por ese motivo el valor de prevenir es alto, detectar es medio y corregir es bajo.

Tabla 64. Automatización del Control – Diseño de Controles.

CATEGORÍA	DESCRIPCIÓN	VALOR
Automatizado.	Control incorporado en el proceso de forma automática.	Alto.
Semi automatizado.	Control incorporado en el proceso de forma parcialmente automática.	Medio.
Manual.	Control incorporado en el proceso de forma manual.	Bajo.

Nota: a. Es preferible que un control se ejecute automáticamente que manualmente, por ese motivo el valor de automático es alto, semi automático es medio y manual es bajo.

Tabla 65. Escalas y Niveles de la Efectividad de Controles – Diseño de Controles.

DESDE	HASTA	NIVEL	CALIFICACIÓN
7	9	Óptimo.	Alto.
4	6	Regular.	Medio.
1	3	Deficiente.	Bajo.

Nota: a. La escala de efectividad del control es: Alto (>7 a 9), Medio (>4 a 6) y Bajo (1 a 3).

b. El nivel del control es: óptimo si la calificación es alta, regular si la calificación es media y deficiente si la calificación del control es baja.

Tabla 66. Mapa de Calor de la Efectividad de Controles – Diseño de Controles.

AUTOMATIZACIÓN	TIPO DE CONTROL		
	Bajo (1)	Medio (2)	Alto (3)
Alta (3)	3 (Bajo)	6 (Medio)	9 (Alto)
Media (2)	2 (Bajo)	4 (Medio)	6 (Medio)
Baja (1)	1 (Bajo)	2 (Bajo)	3 (Bajo)

Nota: a. El nivel del control se obtiene de la multiplicación de los valores asignados al tipo de control y a la automatización del control.

b. El valor asignado para cada nivel del tipo de control es 3 para alta, 2 para medio, 1 para baja y el valor asignado para cada nivel de automatización es 3 para alta, 2 para medio y 1 para bajo.

c. Para determinar la calificación final, si es Alto (amarillo), Medio (naranja) o Bajo (rojo) se utiliza la escala de efectividad del control en la tabla 65.

Tabla 67. Evaluación de Controles – Diseño de Controles.

CONTROL	TIPO	AUT.	VALOR
Compara si existe el número de teléfono y dirección de correo electrónico en otra cuenta. (DIS-REG01)	Alto.	Alto.	Alto.
Confirma el número de teléfono y dirección de correo electrónico, caso contrario se bloquea la cuenta. (DIS-REG01)	Alto.	Alto.	Alto.
Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones. (DIS-REG01)	Alto.	Alto.	Alto.
Configuración del control de seguridad (Quien puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver la secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos). (DIS-REG02)	Alto.	Medio.	Medio.
Bloqueo de guardar fotografías, videos e información. (DIS-REG02)	Alto.	Alto.	Alto.
Encriptación de contraseña. (DIS-REG02,DIS-AUT01)	Alto.	Alto.	Alto.
Validación del usuario y contraseña (autenticación). (DIS-REG02,DIS-AUT01)	Alto.	Alto.	Alto.
Alerta de inicio de sesión (se activa automáticamente). (DIS-AUT01)	Alto.	Alto.	Alto.
Restablecer contraseña (DIS-AUT02)	Medio.	Medio.	Medio
Verifica el código de seguridad o respuesta de la pregunta de seguridad. (DIS-AUT02)	Alto.	Alto.	Alto.
Cerrar sesión en todos los dispositivos. (DIS-AUT02)	Medio.	Medio.	Medio
Comprobar los últimos cambios de la cuenta. (DIS-AUT02)	Medio.	Medio.	Medio.
Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos. (DIS-COM01)	Alto.	Alto.	Alto.
Advertencias de información incorrecta o maliciosa. (DIS-COM01)	Medio.	Alto.	Medio.
Revisión de publicaciones y comentarios antes que aparezcan (se activa automáticamente). (DIS-COM02)	Alto.	Medio.	Medio.
Reportar contenido. (DIS-COM03)	Medio.	Bajo.	Bajo.
El sistema no permite cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permite configurar un sobrenombre. (DIS-CON01)	Alto.	Alto.	Alto.
El sistema permite editar la pregunta de seguridad. (DIS-CON02)	Medio.	Medio.	Medio.
El sistema permite editar la configuración de seguridad. (DIS-SEG01)	Medio.	Medio.	Medio.
Copia de Seguridad. (DIS-ELI01)	Alto.	Medio.	Medio.
Verificación de la respuesta de la pregunta de seguridad y contraseña. (DIS-ELI01)	Alto.	Medio.	Medio.
Limite en el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos). (DIS-LIM01)	Medio.	Alto.	Medio.
Control de seguridad en un menor de edad. (DIS-MEN01)	Alto.	Alto.	Alto.

Nota: a. En el cuadro se encuentra el listado de los controles, con el valor asignado al tipo de control y el valor asignado a la automatización del control.

b. Las nomenclaturas que se encuentran a lado derecho de los controles sirven para identificar el proceso al que pertenecen. Por ejemplo el proceso de Registrar Cuenta es identificada como DIS-REG01.

c. Los parámetros para determinar la calificación en el tipo de control y automatización

del control se encuentra en las tablas 63 y 64.

d. El valor final del control se obtiene de la multiplicación de los valores asignados al tipo de control y a la automatización del control. Para determinar el valor final se utiliza la matriz que se encuentra en la tabla 66. Por ejemplo, si es tipo (Alto) y automatización (Medio) la multiplicación sería de $3 \times 2 = 6$ en la cual la escala indica que es Medio.

5. Conclusiones y Recomendaciones.

Existe poca información sobre la problemática de los crímenes cibernéticos en las redes sociales.

En la investigación realizada, no se encontraron estadísticas y análisis de una entidad oficial sobre crímenes cibernéticos en las redes sociales en el Ecuador.

Los diagramas de flujos de los procesos técnicos del software se realizaron a base de los pasos que realiza el usuario en la red social Facebook, debido a que los procesos técnicos de Facebook no se encuentran disponibles al público.

Tabla 68. Conclusiones de la encuesta “SEGURIDAD PERSONAL EN REDES SOCIALES” por rangos de edad.

Rango de Edad.	10-12.	13-18.	19-55.
¿Qué red social mas utiliza?	YouTube.	Facebook.	Facebook.
¿Qué tipo de verificación tuvo al crear la cuenta?	Código al e-mail.	Código al e-mail.	Código al e-mail.
¿Los datos publicados en su red social son falsos?	76,2%	18,9%	32,3%
¿Considera su contraseña es segura?	83%	83,2%	73,1%
¿Con que frecuencia acostumbra cambiar su contraseña?	Nunca.	Nunca.	Cada 6 meses.
¿Qué configuración de privacidad contiene su red social?	No sabe.	Visible solo para amigos.	Visible solo para amigos.
¿Ha sido amenazado o insultado a través de su red social?	8,2%	25,4%	20%
¿Ha aceptado invitaciones de amistad de desconocidos?	6,8%	51,9%	37,7%
¿Qué le preocupa de las redes sociales?	Robo de información.	Robo de información.	Robo de información.

Nota: a. Los rangos de las encuestas se basan de 10 a 12 años porque son pre-adolescentes que comienzan a evadir los controles de seguridad para poder ingresar a las redes sociales. Muchas de las redes sociales son creadas en Estados Unidos, por lo que la edad mínima es de 13 años para crear un perfil.

b. El rango de 13 a 18 años es porque en la adolescencia son más vulnerables a las amenazas de las redes sociales por el comportamiento que tienen a esa edad.

c. El rango de 19 a 55 años es porque a partir de los 55 disminuye la cantidad de usuarios que utilizan las redes sociales, ya que se les dificulta su uso.

Facebook, es de las redes sociales más utilizadas a nivel mundial y siempre se mantiene en los primeros puestos en los rankings de los sitios webs. Es una de las redes sociales más completas en cuanto a funciones integradas.

Las normas que utiliza Facebook son reactivas, ya que espera que suceda el evento para reportar o tomar medidas. Por ejemplo, una suplantación de identidad es reportada después de que se creó el perfil.

De las metodologías de análisis de riesgo, la más óptima para realizar el análisis de seguridad personal en redes sociales fue NIST SP 800-30, porque es una metodología que da prioridad a los controles actuales de los procesos con el fin de recomendar mejoras en los mismos.

Las amenazas encontradas en la red social Facebook para los usuarios son: acoso cibernético, falsificación de identidad, grooming, fraude informático, robo de información, suplantación de identidad, acceso no autorizado, falta de privacidad, crímenes contra el honor, hurto de cuenta, divulgación de contenido inapropiado e ingeniería social.

En la política de datos se recomienda que la información de las cuentas inhabilitadas por incumplir las condiciones se pongan en backups de cintas.

Se recomienda que la empresa Facebook en la declaración y responsabilidades se haga responsable de la privacidad y el contenido de los usuarios, ya que en sus políticas manifiesta que se cede a Facebook los derechos sobre las fotos, videos y otro tipo de información cargada a la página, de esta forma la empresa puede manejar y gestionar la información que se ha subido a la misma. Es importante que las empresas pongan énfasis en la seguridad social para que los usuarios se encuentren en un ambiente confiable.

Es preferible que los controles de seguridad sean proactivos y no reactivos. Si se previene el evento antes que suceda, el impacto y la probabilidad bajan su nivel.

De las vulnerabilidades encontradas en el análisis de riesgos de la red social Facebook, se recomiendan los siguientes controles para minimizar la probabilidad o impacto en caso que se ejecute la amenaza.

Tabla 69. Conclusión y Recomendación – Vulnerabilidades y Controles Recomendados a la Red Social Facebook.

Vulnerabilidades.	Amenazas.	Controles.
Falta de verificación de los datos ingresados al registrar la cuenta.	Falsificación de identidad, grooming, fraude informático, suplantación de identidad e ingeniería social	Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones.
El sistema permite editar el nombre y la fecha de nacimiento.	Falsificación de identidad, grooming, fraude informático, suplantación de identidad e ingeniería social	El sistema no permite cambiar el nombre, apellido y fecha de nacimiento (Dicha información se visualizara permanentemente). Como alternativa permite configurar un sobrenombre.
Falta de control en el contenido que otras personas pueden guardar como fotografías, videos e información.	Fraude informático, robo de información, suplantación de identidad, falta de privacidad, crímenes contra el honor, divulgación de contenido inapropiado e ingeniería social	Bloquear la opción de guardar fotografías, videos e información.
Falta de información de las configuraciones de seguridad de autenticación.	Fraude informático, robo de información, acceso no autorizado, falta de privacidad, hurto de cuenta	La alerta de inicio de sesión es obligatoria y se activa automáticamente la función al crear la cuenta.
Falta de control del contenido publicado (Links de videos contaminados de malware).	Fraude informático y robo de información	Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos.
Falta de información de las configuraciones de privacidad y seguridad a los usuarios.	Acoso cibernético, fraude informático, robo de información, suplantación de identidad, falta de privacidad, crímenes contra el honor, divulgación de contenido inapropiado e ingeniería social	Configuración del control de seguridad (Opción para no receptar mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al registrar la cuenta.
Falta de control de la recepción de mensajes de desconocidos.	Acoso cibernético, fraude informático, robo de información, suplantación de identidad, falta de privacidad, crímenes contra el honor,	Configuración del control de seguridad (Opción para no receptar mensajes de desconocidos, control de privacidad en la información del perfil y publicaciones) al

Vulnerabilidades.	Amenazas.	Controles.
	divulgación de contenido inapropiado e ingeniería social.	registrar la cuenta.
El sistema no permite editar la pregunta de seguridad.	Acceso no autorizado y hurto de cuenta	El sistema permite editar la pregunta de seguridad y usar la pregunta de seguridad para poder eliminar la cuenta.
El sistema deja automáticamente abierta la sesión de las cuentas en celulares Smartphone.	Hurto de cuenta	Cerrar sesión en todos los dispositivos y la revisión de publicaciones y comentarios es obligatoria y se activa automáticamente la función al crear la cuenta.
El sistema permite que solo utilice el correo electrónico o número de teléfono.	Hurto de cuenta	Al registrar la cuenta, es obligatorio el ingreso de un correo electrónico y un número de celular.

Nota: a. En la presente tabla, se encuentran las vulnerabilidades con las amenazas identificadas en el análisis de riesgos de la red social Facebook y los controles recomendados a ser implementados en la misma.

b. El orden de los controles se encuentran por el valor que adquirieron en el análisis de la tabla 59 y por el nivel de riesgos de las amenazas a las que contrarresta. Por ejemplo, “Compara la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones.” Es un control categorizado como óptimo (Nivel Alto) y contrarresta a la amenaza grooming que tiene un nivel de riesgo alto.

Los controles de seguridad personal estándar que se recomienda a una red social implementar son:

- Comparar si existe el número de teléfono o dirección de correo electrónico en otra cuenta, al registrar la cuenta.
- Confirmar el número de teléfono y dirección de correo electrónico al registrar la cuenta, caso contrario bloquear la cuenta hasta cumplir con el requisito.
- Comparar la información de la cuenta (foto, nombre, apellido y fecha de nacimiento) con el documento subido (por ejemplo la cédula de identidad) por medio de algoritmos de reconocimiento de patrones al registrar la cuenta.
- Bloquear la opción de guardar fotografías, videos e información automáticamente.
- Encriptación de contraseña al autenticar.
- Validación de usuario y contraseña (autenticación).

- Alerta de inicio de sesión (se activa automáticamente).
- Verificar el código de seguridad o respuesta de la pregunta de seguridad al restablecer la cuenta.
- Analizar la información automáticamente por medio de algoritmos de reconocimiento de patrones en los equipos.
- No permitir cambiar el nombre, apellido y fecha de nacimiento. Como alternativa permitir configurar un sobrenombre.
- Control de seguridad en un menor de edad.
- Configuración del control de seguridad (Quién puede publicar en la biografía, ver las publicaciones, ver la información de perfil, ver las secciones, ver la lista de amigos, enviar solicitudes de amistad y activar la función de recepción de mensajes de desconocidos) al registrar la cuenta.
- Restablecer contraseña.
- Cerrar sesión en todos los dispositivos.
- Comprobar los últimos cambios de la cuenta.
- Advertencias de información incorrecta o maliciosa.
- Revisión de publicaciones y comentarios antes que aparezcan (se activa automáticamente).
- Permitir editar la pregunta de seguridad.
- Permitir editar la configuración de seguridad.
- Permitir hacer al usuario una copia de seguridad (información del perfil).
- Verificar la respuesta de la pregunta de seguridad y contraseña al eliminar la cuenta.
- Limitar el uso de funciones (advertencias y bloqueo de la función al exceder el límite de intentos permitidos).
- Reportar contenido.

Referencias.

About, (s.f.). A qué edad se pueden usar Facebook y otras redes sociales populares. Recuperado el 31 de Julio del 2016, de <http://redessociales.about.com/od/redessocialesmaspopulares/a/A-Que-Edad-Se-Pueden-Usar-Facebook-Y-Otras-Redes-Sociales-Populares.htm>

Agencia Europea de Red y Seguridad de la Información (s.f.). CRAMM. Recuperado el 03 de Agosto del 2016, de https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

Alexa Internet, Inc. (s.f.). How popular is facebook.com?. Recuperado el 22 de Febrero del 2016, de <http://www.alexa.com/siteinfo/facebook.com>

Alexa Internet, Inc. (s.f.). How popular is youtube.com?. Recuperado el 22 de Febrero del 2016, de <http://www.alexa.com/siteinfo/youtube.com>

Barzallo, J., Téllez, J., Reyes, P. y Amoroso, Y. (2012). *XVI Congreso Iberoamericano de Derecho e Informática, Tomo II*. Quito, Ecuador: Moreno.

CID, R. (2013). Metodologías de Análisis de Riesgo. Recuperado el 02 de Agosto del 2016, de <http://es.slideshare.net/RamiroCid/anlisis-de-riesgos-26199990>

Facebook. (s.f.). ¿Qué es el Facebook Safety Advisory Board (consejo asesor de seguridad de Facebook) y a qué se dedica?. Recuperado el 13 de Enero del 2016, de <https://www.facebook.com/help/222332597793306>

Facebook. (s.f.). Cookies, píxeles y otras tecnologías similares. Recuperado el 18 de Enero del 2016, de <https://www.facebook.com/help/cookies/>

Facebook. (s.f.). Fomentar un comportamiento respetuoso. Recuperado el 21 de Diciembre del 2015, de <https://www.facebook.com/communitystandards>

Facebook. (s.f.). Our history. Recuperado el 22 de Enero del 2016, de <https://newsroom.fb.com/company-info/>

Facebook. (s.f.). Política de datos. Recuperado el 03 de Febrero del 2016, de <https://www.facebook.com/about/privacy/>

Facebook. (s.f.). Proteger tu cuenta e información personal. Recuperado el 21 de Diciembre del 2015, de <https://www.facebook.com/communitystandards>

Facebook. (s.f.). Proteger tu propiedad intelectual. Recuperado el 21 de Diciembre del 2015, de <https://www.facebook.com/communitystandards>

Facebook. (s.f.). Seguridad de la cuenta y registro. Recuperado el 11 de Enero del 2016, de <https://www.facebook.com/legal/terms>

Facebook. (s.f.). Te ayudamos a estar seguro. Recuperado el 21 de Diciembre del 2015, de <https://www.facebook.com/communitystandards>

Facebook. (s.f.). ¿Cuál es la seguridad mínima de la contraseña y qué puedo hacer para que mi contraseña sea segura?. Recuperado el 18 de Enero del 2016, de <https://www.facebook.com/help/124904560921566>

Formación Gerencial Internacional, (s.f.). Estadísticas Facebook Ecuador. Recuperado el 31 de Julio del 2016, de <http://blog.formaciongerencial.com/2016/02/01/estadisticasfacebookecuador/>

García, R. (2015). *IV. Actividad académica y tecno-científica sobre ciberseguridad, ciberdelincuencia y protección de los menores*. Recuperado el 9 de Mayo del 2015 de <http://revistas.unam.mx/index.php/derecho/article/view/47035>

Gomez, F. (2010). *El Pequeño Libro de las Redes Sociales*. Barcelona, España: Parangona Realización Editorial, S.L.

Instituto Nacional de Estadística y Geografía (s.f.). Metodología de la investigación. Recuperado el 01 de Agosto del 2016, de <http://www.inegi.org.mx/inegi/spc/doc/INTERNET/22->

%20CURSO%20DE%20METODOLOG%C3%8DA%20DE%20LA%20INVESTIGACI%C3%93N.pdf

Matalobos, M. (2009). Análisis de Riesgos de Seguridad de la Información. Recuperado el 03 de Agosto del 2016, de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Modelo Estándar de Control Interno del Paraguay (s.f.). Controles. Recuperado el 01 de Agosto del 2016, de <http://www.mecip.gov.py/mecip/?q=node/176>

Naciones Unidas. (s.f.). Delito Cibernético. Recuperado el 18 de Febrero del 2016, de <http://www.un.org/es/events/crimecongress2015/cibercrime.shtml>

Portal de Administración Electrónica (s.f.). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 03 de Agosto del 2016, de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V6FgJrjhDIU

Rodriguez, J. (2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Recuperado el 01 de Agosto del 2016, de <http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf>

SEGOB, CNS y Policía Federal (2014). *Impacto y Gravedad de los ciberdelitos. Taller: Legislación en materia de Ciberdelincuencia en América Latina*. Recuperado el 11 de Mayo del 2015 de <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/31March/Impacto-y-gravedad-de-los-delitos.pdf>

Shanthamurthy, D. (s.f.). NIST SP 800-30 standard for technical risk assessment: An evaluation. Recuperado el 03 de Agosto del 2016, de <http://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation>

Statista. (s.f.). Número de ciberdelitos ocurridos en España en 2014, por tipo de delito. Recuperado el 23 de Febrero del 2016, de <http://es.statista.com/estadisticas/472655/cifras-tipo-ciberdelito-espana/>

Stoneburner, G., Goguen, A. y Feringa, A. (2002). NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. Recuperado el 25 de Enero del 2016, de <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

Stopbullying.gov, (s.f.). What is Cyberbullying. Recuperado el 01 de Agosto del 2016, de <https://www.stopbullying.gov/cyberbullying/what-is-it/index.html>

Temperini, M (2013). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte*. Recuperado el 10 de Mayo del 2015 de <http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf>

○ Sub referencias:

- “Internet, libertad y sociedad: una perspectiva analítica”, Conferencia inaugural del curso académico 2001-2002 de la UOC.

Torres, D. (2008). Mark Zuckerberg, fundador de Facebook, en la Universidad de Navarra. La historia de Facebook. Recuperado el 22 de Diciembre del 2015, de http://eprints.rclis.org/13896/1/Torres-Salinas%2C_Daniel-Mark_Zuckerberg%2C_fundador_de_Facebook%2C_en_la_Universidad_de_Navarra.pdf

Trend Micro Incorporated, (s.f.). Seguridad cibernética: protección frente a los ciberataques. Recuperado el 31 de Julio del 2016, de <http://www.trendmicro.es/tecnologia-innovacion/seguridad-cibernetica/>

Tu abogado defensor, (s.f.). Abusos y delitos en las redes sociales. Recuperado el 01 de Agosto del 2016, de <http://www.tuabogadodefensor.com/proteccion-redes-sociales/#uso>

Urrutia, J. (2014). Metodologías de Análisis de Riesgos. Recuperado el 03 de Agosto del 2016, de <http://metodologia-y-evaluacion-de-riesgos.blogspot.com/2014/03/seguridad-informatica-la-seguridad.html>

Urueña, A., Ferrari, A., Blanco, D., Valdecasa, E. (2011). Definición de Red Social. Recuperado el 6 de Noviembre del 2015, de http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf

Anexos.

Anexo A. Encuesta “Seguridad Personal en Redes Sociales”.

ENCUESTA “Seguridad Personal en Redes Sociales.”

*Obligatorio

Edad *

Seleccione el rango de edad a la que pertenece.

- 10-12
- 13-18
- 19-55

Seleccione las redes sociales que utiliza. *

- Facebook
- Youtube
- Wikipedia
- Twitter
- LinkedIn
- Instagram
- Otro:

Seleccione el tipo de verificación que tuvo al crear su cuenta. *

- Código al e-mail
- Código al celular
- Ninguno
- Otro:

¿Todos los datos publicados en su Red Social son reales? *

- Si
- No

¿Considera que su contraseña es segura al tener mínimo 8 caracteres entre mayúsculas, minúsculas, números y símbolos? *

- Si
- No

¿Con que frecuencia acostumbra cambiar su contraseña? *

- Cada 6 meses
- Cada año
- Nunca

¿Qué configuración de privacidad contiene su Red Social? *

Visibilidad de su perfil para otros usuarios.

- Es visible para todos
- Es visible solo para amigos
- Es visible solo para amigos específicos
- No lo sé

¿Sabía que al usar aplicaciones en las Redes Sociales proporciona su información personal a los propietarios de la aplicación? *

- Si
- No

¿Ha sido amenazado o insultado a través de su Red Social? *

- Si
- No

¿Ha aceptado invitaciones de amistad de desconocidos? *

- Si
- No

¿Qué le preocupa de las Redes Sociales? *

- Falsificación de Identidad
- Acceso sin autorización
- Falta de privacidad
- Crímenes contra el honor
- Grooming (Pornografía Infantil)
- Acoso.
- Robo de información (Fotos, datos,etc.)
- Nada
- Otro:

Enviar

100%: has terminado.

Nunca envíes contraseñas a través de Formularios de Google.

Anexo B. Glosario de Términos.

- **Coacciones:** Violencia física, psíquica o moral para obligar a una persona a decir o hacer algo contra su voluntad. (Enciclopedia Jurídica, 2014)
- **Geeks:** Persona fanática por la tecnología.
- **IRC:** Internet Relay Chat, es un protocolo de comunicación en tiempo real.
- **Inteligencia artificial:** Es el área dedicada a simular la inteligencia humana en sistemas para que sean capaces de resolver problemas por sí mismos.
- **Microblogging:** Es un servicio que permite publicar mensajes pequeños con límite de caracteres.
- **Timeline:** Es utilizado en las redes sociales para enseñar las publicaciones en orden cronológico.
- **Retweet:** Es la acción de compartir una publicación de otro usuario en la red social Twitter
- **Hashtag:** Es una forma de abreviar lo que se desea escribir.
- **Cortadores de url:** Es la publicación de un hipervínculo sin toda su extensión.
- **Like:** Es la acción en la que el usuario indica que le gusta una publicación.
- **Friending:** Es la acción de agregar a un usuario a la lista de amigos en la red social.
- **Following:** Es la acción de seguir a un usuario o empresa en la red social.
- **Delito cibernético:** es la acción que daña o perjudica a una persona o empresa por medio de las vías informáticas.
- **Ingeniería social:** Es la acción de obtener información confidencial por medio de la manipulación.
- **Malware:** Es el software que tiene como fin dañar o infiltrarse a los sistemas de información sin autorización.
- **Pedófilo:** Es una persona adulta con atracción sexual hacia niños, niñas y adolescentes.
- **News feeds:** Es la sección de las últimas noticias, que presenta las publicaciones de los amigos en la red social Facebook.

- **Amenaza:** Es la probabilidad de que suceda un problema de seguridad con la utilización de las vulnerabilidades del sistema.
- **Vulnerabilidades:** son las circunstancias que hacen susceptibles a que sucedan las amenazas.
- **SDLC:** Es el ciclo de vida del desarrollo de software.
- **Sistema informático:** Es el conjunto de hardware, software y personal informático interrelacionados entre sí.
- **Software:** Es un programa o conjunto de programas informáticos que permiten realizar diferentes tareas en un sistema informático.
- **Encriptación:** Es el proceso que transforma la información importante a información incomprensible.
- **Backup:** Es la copia de la información original con el fin de recuperar dicha información en caso de pérdida.

Enciclopedia Jurídica. (2014). Copy of Derecho Penal. Delito de Coacciones. Recuperado el 01 de Junio del 2016, de <http://www.encyclopedia-juridica.biz14.com/d/delito-de-coacciones/delito-de-coacciones.htm>