Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de proyecto de investigación aplicada 2

Propuesta de un marco de trabajo para mejorar la seguridad en Internet para personas en edad laboral madura y personas adultas mayores de la asociación gerontológica costarricense que cuentan con alfabetización digital

Solórzano Jiménez, Eric

Monge Montoya, Luis Diego

Julio, 2022

Declaratoria derechos de autor

El presente documento cuenta con la autorización por parte de los autores, para la consulta y uso solamente con fines académicos.

Agradecimiento, Eric Solórzano Jiménez

En primer término, a Dios, por la oportunidad de alcanzar esta meta y la salud para hacerlo.

A mi esposa e hijas, de quienes he tomado tiempo prestado, en este camino de esfuerzo y aprendizaje que al llegar a esta etapa son quienes han estado a mi lado en todo este proceso.

A mi madre quien, sin su ejemplo, no estaría siguiendo su camino de esfuerzo y trabajo.

A mi compañero de propuesta, por todo el trabajo en equipo realizado, en el entregable que hoy compartimos.

Al profesor guía, por su apoyo y valiosos consejos que nos permitieron enrumbar el trabajo.

A los profesionales que nos brindaron su valioso aporte en diferentes maneras, para llevar adelante esta propuesta.

A todo el grupo de personas colaboradoras de la Asociación Gerontológica Costarricense, sin quienes la propuesta no tendría el componente de contexto fundamental para el aporte propuesto.

A todas aquellas personas con las que tuve la oportunidad de compartir clase, sean profesores o compañeras y compañeros de estudio, con quienes tuve la oportunidad de vivir esta experiencia.

Agradecimiento, Luis Diego Monge Montoya

Quiero agradecer primero a Dios, por darme fortaleza, salud y capacidad para concluir este reto.

A mi familia, por estar siempre presente ofreciéndome su apoyo y colaboración a lo largo de la maestría.

A mi compañero de trabajo final de graduación por el apoyo, compromiso y dedicación en cada etapa de la elaboración de la propuesta.

Al profesor tutor por el apoyo brindado y por todos los consejos y recomendaciones recibidas a lo largo de este proyecto final de graduación.

A la Asociación Gerontológica Costarricense por abrirnos las puertas y permitirnos desarrollar la propuesta en ellos.

A todas las personas expertas que colaboraron en brindarnos información valiosa para el desarrollo de la propuesta.

A todas las personas que fueron parte de la propuesta y que gracias a este proyecto final de graduación pudimos conocerlas.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para los estudiantes: **Monge Montoya Luis Diego** y **Solórzano Jiménez Eric**

ROY VALENCIANO GONZALEZ (FIRMA)
Digitally signed by ROY VALENCIANO GONZALEZ (FIRMA)
Date: 2022.07.08 20:42:07 -06'00'

M. Sc. Roy Valenciano González
Tutor

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Digitally signed by DENNIS ALONSO DURAN CESPEDES (FIRMA)
DN: SERIALNUMBER=CPF-01-1029-0075, SN=DURAN CESPEDES, G=DENNIS ALONSO, C=CR, O=PERSONA FISICA, OU=CIUDADANO, CN=DENNIS ALONSO DURAN CESPEDES (FIRMA)
Reason: I am the author of this document
Location:
Date: 2022.07.11 14:41:39-06'00'
Foxit PDF Reader Version: 12.0.0

M. Sc. Dennis Durán Céspedes
Lector 1

JASON ULLOA HERNANDEZ (FIRMA)
Firmado digitalmente por JASON ULLOA HERNANDEZ (FIRMA)
Fecha: 2022.07.12 20:11:44 -06'00'

MTEL. Jason Ulloa Hernández
Lector 2

San José, Costa Rica, 08 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de contenido

Capítulo I. Introducción 1

1.1. Generalidades 1

1.2. Antecedentes del problema 1

1.3. Definición y descripción del problema 4

1.4. Justificación 4

1.5. Viabilidad 5

1.5.1. Punto de vista técnico. 5

1.5.2. Punto de vista operativo. 5

1.5.3. Punto de vista económico. 5

1.6. Objetivos 5

1.6.1. Objetivo general. 5

1.6.2. Objetivos específicos. 6

1.7. Alcances y limitaciones 6

1.7.1. Alcances. 6

1.7.2. Limitaciones. 7

1.8. Marco de deferencia organizacional y socioeconómico 7

1.8.1. Historia. 7

1.8.2. Tipo de negocio y mercado meta. 8

1.8.3. Misión, visión y valores. 8

1.8.3.1. Misión. 8
1.8.3.2. Visión. 9
1.8.3.3. Valores. 9
1.8.4. Políticas institucionales. 9
1.8.4.1. Eje 1: Transformación. 9
1.8.4.2. Eje 2: Sostenibilidad. 9
1.8.4.3. Eje 3: Posicionamiento. 9
1.8.4.4. Eje 4: Gestión. 9
1.9. Estado de la cuestión 10
1.9.1. Planificación de la revisión. 10
1.9.1.1. Formulación de la pregunta. 10
1.9.1.1.1. Foco de la pregunta. 10
1.9.1.1.2. Amplitud y calidad de la pregunta. 11
1.9.1.1.2.1. Problema. 11
1.9.1.1.2.2. Pregunta. 11
1.9.1.1.2.3. Palabras clave y sinónimos. 11
1.9.1.1.2.4. Intervención. 12
1.9.1.1.2.5. Control. 12
1.9.1.1.2.6. Efectos. 12
1.9.1.1.2.7. Medida de salida. 13

1.9.1.1.2.8. Población. 13

1.9.1.1.2.9. Aplicación. 13

1.9.1.1.3. Selección de fuentes. 13

1.9.1.1.3.1. Definición del criterio de selección de fuentes. 13

1.9.1.1.3.2. Idioma de estudio. 13

1.9.1.1.4. Identificación de fuentes. 13

1.9.1.1.4.1. Método de selección de fuentes:. 13

1.9.1.1.4.2. Cadena de búsqueda. 14

1.9.1.1.4.3. Lista de fuentes. 14

1.9.1.1.4.4. Selección de fuentes después de la evaluación. 14

1.9.1.1.5. Comprobación de las fuentes. 14

1.9.1.1.5.1. Selección de los estudios. 14

1.9.1.2. Definición del criterio de inclusión y exclusión de estudios. 14

1.9.1.2.1. Procedimiento para la selección de los estudios. 15

1.9.2. Ejecución de la revisión. 15

1.9.2.1. Ejecución de la selección en la fuente utilizando el motor Google Scholar. 15

1.9.2.1.1. Selección de estudios iniciales. 16

1.9.2.1.2. Revisión de la selección. 19

1.9.2.1.3. Extracción de información. 19

1.9.2.1. Ejecución de la selección en la fuente IEEE. 37

1.9.2.1.1. Selección de estudios iniciales. 37

1.9.2.1.1. Extracción de información. 38

1.9.2.2. Ejecución de la selección en la fuente utilizando el motor ACM digital Library. 48

1.9.2.2.1. Selección de estudios iniciales. 48

1.9.2.2.2. Extracción de información. 48

1.9.3. Resumen de los resultados. 51

Capítulo II. Marco conceptual 52

2.1. Conceptos sobre contenido 53

2.1.1. Ciberseguridad. 54

2.1.2. Adulto mayor. 54

2.1.3. Usuarios. 55

2.1.4. Jubilación. 55

2.1.5. Internet. 55

2.1.6. En línea (on-line) 56

2.1.7. Ciberataque. 56

2.1.8. Redes sociales. 56

2.1.9. Ciberamenaza. 57

2.1.10. Vulnerabilidad. 57

2.1.11. Alfabetización digital. 57
2.1.12. Marco de trabajo (Framework). 58
2.1.13. Sistema financiero. 58
2.1.14. Suplantación de identidad. 58
2.1.15. Estafa informática. 59
2.1.16. Edad laboral madura. 59
Capítulo III. Marco metodológico 60
3.1. Tipo de investigación 60
3.2. Alcance investigativo 60
3.2.1. Exploratorio 60
3.2.2. Descriptivo. 60
3.3. Enfoque 60
3.3.1. Dimensión ontológica o conceptualización. 61
3.3.2. Dimensión epistemológica. 61
3.3.3. Dimensión axiológica. 61
3.4. Diseño 64
3.4.1. Contexto de aplicación. 65
3.4.2. Construcción y evaluación de artefactos. 65
3.4.3. Revisión sistemática de la base de conocimiento. 66
3.5. Población y muestreo 66

3.6. Instrumentos de recolección de datos 66

3.6.1. Entrevistas. 67

3.6.2. Encuestas. 76

3.7. Técnicas de análisis de información 80

3.8. Estrategia de desarrollo de la propuesta 81

Capítulo IV. Análisis del diagnóstico 83

4.1. Aplicación de entrevistas a expertos 83

4.1.1. Aplicación de entrevistas a representantes del Organismo de Investigación Judicial. 83

4.1.1.1. Entrevista aplicada a Genivieve Segura Robles. 83

4.1.1.2. Primera entrevista aplicada a Yorkssan Carvajal. 85

4.1.1.3. Segunda entrevista aplicada a Yorkssan Carvajal. 90

4.1.2. Entrevista con experto en ciberseguridad. 91

4.1.3. Entrevista al representante del Registro Nacional de Costa Rica. 94

4.1.4. Entrevista a representante de la Oficina del Consumidor Financiero. 96

4.1.5. Entrevista a docentes de la Asociación Gerontológica Costarricense. 97

4.1.6. Solicitud de información vía correo electrónico a Banco Nacional de Costa Rica y Banco de Costa Rica, como ejemplos de entidades financieras. 100

4.2. Análisis de entrevistas a expertos 101

4.2.1. Análisis de entrevistas representantes Organismo de Investigación

Judicial. 101

4.2.1.1. Análisis de entrevista con Genevieve Segura Robles de la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial. 101

4.2.1.2. Análisis de entrevista con Yorkssan Carvajal jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos de suplantación de identidad y estafa informática. 102

4.2.1.3. Análisis de entrevista con Yorkssan Carvajal jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles. 104

4.2.2. Análisis de entrevista experto en ciberseguridad. 104

4.2.3. Análisis de entrevista representante Registro Nacional de Costa Rica. 105

4.2.4. Análisis de entrevista representante Oficina del Consumidor Financiero. 106

4.2.5. Análisis de entrevista a docentes de la Asociación Gerontológica Costarricense. 106

4.3. Análisis y resultados de entrevistas a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense 108

4.4. Aplicación de cuestionarios 118

4.4.1. Pregunta 1. 118

4.4.2. Pregunta 2. 119

4.4.3. Pregunta 3. 120

4.4.4. Pregunta 4. 121

4.4.5. Pregunta 5. 122

4.4.6. Pregunta 6. 123

4.4.7. Pregunta 7. 124

4.4.8. Pregunta 8. 125

4.4.9. Pregunta 9. 126

4.4.10. Pregunta 10. 127

4.4.11. Pregunta 11. 128

4.4.12. Pregunta 12. 129

4.4.13. Pregunta 13. 130

4.4.14. Pregunta 14. 131

4.4.15. Pregunta 15. 132

4.4.16. Pregunta 16. 133

4.4.17. Pregunta 17. 134

4.4.18. Pregunta 18. 135

4.4.19. Pregunta 19. 136

4.4.20. Pregunta 20. 137

4.4.21. Pregunta 21. 138

4.4.22. Pregunta 22. 139

4.4.23. Pregunta 23. 140

Capítulo V. Propuesta de solución 141

5.1. Definición del marco de trabajo para mejorar la navegación en Internet de personas en edad laboral madura y persona adulta mayor 141

5.1.1. Justificación de la elaboración y propuesta. 141

5.1.2. Comprensión de la población. 141

5.1.2.1. Vulnerabilidades que se identificaron en la población en edad laboral madura y adulta mayor de la Asociación Gerontológica Costarricense. 142

5.1.2.1. Resultados evaluación de criterios para mejorar la seguridad en Internet, aplicada a población de muestra atendida por Ageco. 144

5.1.2.2. Resultados evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco. 149

5.1.2.3. Resultados de la evaluación de criterios de protección de identidad digital, aplicada a la población de muestra atendida por Ageco. 153

5.2. Lógica del marco de trabajo 156

5.2.1. Referencia para la construcción. 156

5.2.2. Etapas del marco de trabajo. 156

5.2.2.1. Función identificar. 157

5.2.2.2. Función proteger. 157

5.2.2.3. Función detectar. 158

5.2.2.4. Función responder. 158

5.2.2.5. Función recuperar. 159

5.3. Desarrollo del marco 159

5.3.1. Propuesta función identificar. 159

5.3.1.1. Concepto de delitos. 167

5.3.1.1.1. Estafa informática. 167

5.3.1.1.2. Suplantación de identidad. 167

5.3.1.2. Afectación financiera. 167

5.3.1.2.1. Información que proteger. 168

5.3.1.2.1.1. Datos personales de acceso irrestricto según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. 168

5.3.1.2.1.2. Datos sensibles según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. 168

5.3.1.2.1.3. Datos personales de acceso restringido según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. 169

5.3.1.2.2. Métodos que utilizan los delincuentes. 169

5.3.1.2.2.1. Ingeniería social. 169

5.3.1.2.2.2. Sitios web falsos de entidades financieras. 170

5.3.1.2.2.3. Vishing. 171

5.3.1.2.2.4. Instalación de remote desktop. 171

5.3.1.2.2.5. Enmascarado número telefónico origen. 171

5.3.1.2.2.6. Suplantación de funcionarios de instituciones o empresas. 172

5.3.1.2.2.7. Depósito bancario falso producto de gestión en Internet. 172

5.3.1.2.2.8. Ventanas emergentes en el navegador al acceder en sitios web (redirecciona a sitios maliciosos). 172

5.3.1.3. Afectación por bienes inmuebles. 172

5.3.1.3.1. Información que proteger. 172

5.3.1.3.1.1. Datos de acceso irrestricto. 173

5.3.1.3.2. Métodos que utilizan los delincuentes. 173

5.3.1.3.2.1. Participación de notarios. 173

5.3.1.3.2.2. Consulta de información de acceso irrestricto del Registro Nacional. 173

5.3.2. Propuesta función proteger. 173

5.3.2.1. Concientización. 184

5.3.2.1.1. Medios de información. 184

5.3.2.1.1.1. Información de recomendaciones en temas de seguridad a partir de redes sociales como fuente de información. 184

5.3.2.1.1.2. Personas de confianza para consulta. 184

5.3.2.1.1.3. Medios oficiales del gobierno. 185

5.3.2.1.2. Cursos de capacitación. 185

5.3.2.2. Afectación financiera..... 185

5.3.2.2.1. Protección a datos bancarios..... 185

5.3.2.2.1.1. Institución bancaria en la cual se tiene servicios..... 185

5.3.2.2.1.2. Productos bancarios con que se cuenta. 185

5.3.2.2.1.3. Número de cuenta. 186

5.3.2.2.1.4. Seguro de tarjetas. 186

5.3.2.2.1.5. Estados de cuenta..... 186

5.3.2.2.2. Protección a credenciales de acceso para asegurar la identidad digital. 186

5.3.2.2.2.1. Usuario..... 186

5.3.2.2.2.2. Contraseña..... 187

5.3.2.2.2.3. Firma digital..... 187

5.3.2.2.3. Protección a métodos de múltiple factor de autenticación entregado por entidad financiera. 187

5.3.2.2.3.1. OTP (one time password). 188

5.3.2.2.3.2. Tarjeta dinámica. 188

5.3.2.2.3.3. Métodos de autenticación biométricos. 188

5.3.2.2.3.4. Aplicaciones en dispositivos móviles. 188

5.3.2.2.4. Protección a métodos de acceso a servicios bancarios. 188

5.3.2.2.4.1. Navegadores en equipos de escritorio, equipos portátiles y dispositivos móviles..... 189

5.3.2.2.4.2. 2. Aplicaciones de dispositivos móviles. 190

5.3.2.2.5. Protección y seguridad en dispositivos de acceso. 190

5.3.2.2.5.1. Equipo de escritorio o portátil. 191

5.3.2.2.5.2. Dispositivo móvil. 192

5.3.2.2.6. Protección en servicios de seguridad que brinda la entidad financiera. 193

5.3.2.2.7. Protección en la información de huella digital del usuario en Internet. 193

5.3.2.2.7.1. Publicación en redes sociales. 193

5.3.2.2.7.2. Identificación de cuenta de correo asociada con notificaciones por parte de la entidad bancaria que brinda los servicios. 194

5.3.2.3. Afectación por bienes inmuebles. 194

5.3.2.3.1. Datos que se relacionan con bienes inmuebles y muebles. 194

5.3.2.3.1.1. Información disponible en el Registro Nacional. 194

5.3.2.3.1.2. Información de planos o certificaciones que se tengan en físico. 194

5.3.2.3.2. Información de huella digital del usuario en Internet. 195

5.3.3. Propuesta función detectar. 195

5.3.3.1. Afectación financiera. 204

5.3.3.1.1. Métodos de acceso a servicios bancarios. 204

5.3.3.1.1.1. Ingeniería social. 204

5.3.3.1.1.1.1. Vishing. 204

5.3.3.1.1.1.2. Phishing. 204

5.3.3.1.1.2. Instalación de remote desktop. 205

5.3.3.2. Afectación por bienes inmuebles. 206

5.3.3.2.1. Métodos que utilizan delincuentes. 206

5.3.3.2.1.1. Información de bienes muebles o inmuebles. 206

5.3.3.2.1.2. 2. Vishing. 206

5.3.4. Propuesta función responder. 206

5.3.4.1. Afectación financiera. 214

5.3.4.1.1. Respuesta de ataques a los métodos de acceso a servicios bancarios. 214

5.3.4.1.1.1. Ingeniería social. 214

5.3.4.1.1.1.1. Vishing. 214

5.3.4.1.1.1.2. Phising. 214

5.3.4.1.1.1.3. Enmascarado número telefónico origen. 215

5.3.4.1.1.1.4. Suplantación de funcionarios de instituciones o empresas. 215

5.3.4.1.1.1.5. Aplicar recomendación, detente, piensa y actúa.. 216

5.3.4.1.1.2. Instalación de remote desktop. 216

5.3.4.2. Afectación de bienes inmuebles. 216

5.3.4.2.1. Métodos que utilizan los delincuentes. 216

5.3.4.2.1.1. Información de bienes muebles o inmuebles. 216
5.3.4.2.1.2. Vishing..... 217
5.3.5. Propuesta función recuperar. 217
5.3.5.1. Afectación financiera..... 219
5.3.5.2. Afectación de bienes inmuebles. 219
5.4. Guía de aplicación rápida 219
5.4.1. Función identificar. 220
5.4.2. Función proteger. 220
5.4.3. Función detectar. 222
5.4.4. Función responder. 222
5.4.5. Función recuperar. 223
Capítulo VI. Conclusiones y recomendaciones 225
6.1. Conclusiones 225
6.1.1. Conclusiones del objetivo n.º 1. 225
6.1.2. Conclusiones del objetivo n.º 2. 225
6.1.3. Conclusiones del objetivo n.º 3. 226
6.1.4. Conclusiones del objetivo n.º 4. 226
6.1.5. Conclusiones del objetivo n.º 5. 226
6.1.6. Conclusiones del objetivo general. 227
6.2. Recomendaciones 227

Referencias 229

Bibliografía 233

Índice de tablas

Tabla 1 Población total por años quinquenales, según grupos quinquenales de edad, 2011-2050 2

Tabla 2 Casos registrados en el ámbito nacional por delitos informáticos, en el periodo 01/01/2016 al 30/01/2022, según año y rango de edad 3

Tabla 3 Casos registrados en el ámbito nacional por delitos informáticos, en el periodo 01/01/2016 al 30/01/2022, según delito y año 3

Tabla 4 Casos registrados en el ámbito nacional por delito de estafa según víctima y año, en el periodo 01/01/2016 al 30/01/2022 4

Tabla 5 Listado de palabras 12

Tabla 6 Criterio de escogencia de estudios 15

Tabla 7 Estudios que se encontraron con Google Scholar 17

Tabla 8 Extracción fuente 1 20

Tabla 9 Extracción fuente 2 22

Tabla 10 Extracción fuente 3 24

Tabla 11 Extracción fuente 4 26

Tabla 12 Extracción fuente 5 29

Tabla 13 Extracción fuente 6 31

Tabla 14 Extracción fuente 7 34

Tabla 15 Estudios que se encontraron IEEE 38

Tabla 16 Extracción fuente 8 39

Tabla 17 Extracción fuente 9 42

Tabla 18 Extracción fuente 10 45

Tabla 19 Estudios que se encontraron ACM digital library 48

Tabla 20 Extracción fuente 10 49

Tabla 21 Análisis de resultados 51

Tabla 22 Evaluación de criterios para mejorar la seguridad en Internet, aplicada a población atendida por Ageco 62

Tabla 23 Evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco 63

Tabla 24 Evaluación de criterios protección de identidad digital, aplicada a población de muestra atendida por Ageco 64

Tabla 25 Entrevista para aplicar a representantes del Organismo de Investigación Judicial, relacionada con delitos de suplantación de identidad y estafa informática 67

Tabla 26 Entrevista para aplicar a representante del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles 69

Tabla 27 Entrevista para aplicar a experto en ciberseguridad, con experiencia en los temas que se relacionan con delitos de suplantación de identidad y estafa informática 70

Tabla 28 Entrevista para aplicar al representante del Registro Nacional de Costa Rica, relacionada con delitos a patrimonio o bienes 71

Tabla 29 Entrevista para aplicar al representante de la Oficina del consumidor financiero, relacionada con delito estafa informática 72

Tabla 30 Entrevista para aplicar a docentes de la Asociación Gerontológica Costarricense 73

Tabla 31 Entrevista para aplicar a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense 74

Tabla 32 Cuestionario para aplicar a adultos en edad laboral madura y personas

adultas mayores con alfabetización digital 76

Tabla 33 Estrategia de desarrollo de la propuesta según objetivos específicos... 81

Tabla 34 Respuestas a entrevista con Genivieve Segura de la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial 83

Tabla 35 Respuestas a entrevista con Yorkssan Carvajal de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos de suplantación de identidad y estafa informática..... 86

Tabla 36 Respuestas de entrevista a Yorkssan Carvajal Aguilar jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles..... 90

Tabla 37 Respuestas de entrevista para aplicar a experto en ciberseguridad, con experiencia en los temas que se relacionan con delitos de suplantación de identidad y estafa informática..... 92

Tabla 38 Respuestas de entrevista para aplicar a representante del Registro Nacional de Costa Rica, relacionado con delitos a patrimonio o bienes..... 94

Tabla 39 Respuestas de entrevista a representante de la Oficina del Consumidor Financiero, relacionado con delito de estafa informática..... 96

Tabla 40 Respuestas de entrevista a docentes Asociación Gerontológica Costarricense..... 98

Tabla 41 Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función identificar la propuesta marco de trabajo 109

Tabla 42 Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función proteger, propuesta marco de trabajo..... 111

Tabla 43 Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense,

función proteger, propuesta marco de trabajo 113

Tabla 44 Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función responder, propuesta marco de trabajo 115

Tabla 45 Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función recuperar, propuesta marco de trabajo 117

Tabla 46 Identificación de vulnerabilidades según instrumentos a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense 143

Tabla 47 Resultados evaluación de criterios para mejorar la seguridad en Internet, aplicada a población de muestra atendida por Ageco 145

Tabla 48 Resultados evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco 150

Tabla 49 Resultados evaluación de criterios protección de identidad digital, aplicada a población de muestra atendida por Ageco 154

Tabla 50 Función identificar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital 160

Tabla 51 Función proteger, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuenta con alfabetización digital 174

Tabla 52 Función detectar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital 196

Tabla 53 Función responder, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas

adultas mayores que cuenta con alfabetización digital 207

Tabla 54 Función recuperar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital 218

Índice de figuras

Figura 1 Nube de palabras generada 52

Figura 2 Mapa conceptual de ciberseguridad en adultos en edad laboral madura y personas adultas mayores 53

Figura 3 Mapa conceptual 61

Figura 4 Esquema de ciencia de diseño 65

Figura 5 Mapa conceptual que explica la metodología que se utiliza para la recolección y análisis de datos 81

Abstract

El uso de Internet para realizar trámites y acceder a servicios que se relacionan con instituciones públicas y sistema financiero, entre otros servicios, ha generado en los usuarios la necesidad de adaptación. No obstante, también implica una serie de riesgos que llama a los usuarios a identificarlos y desarrollar una visión analítica y preventiva, para que sus acciones no los expongan a ser objetivo de delitos informáticos tipificados en el Código Penal de Costa Rica, como suplantación de identidad y la estafa informática.

En esta población Costa Rica muestra un comportamiento creciente y sostenido, como se planteó en el desarrollo de antecedentes y, a la vez, es importante considerar el origen histórico y retos en la adaptación a la tecnología. Se identificó a las personas en edad laboral madura y las personas adultas mayores como la población objetivo de esta propuesta, que cuentan con el apoyo de la Asociación Gerontológica Costarricense. A partir de la colaboración de las personas participantes designadas se reflejó la realidad que enfrentan en un entorno dinámico y ante el cual se propone aportar por medio de un marco de trabajo, como herramienta que permita mejorar la seguridad en el uso de Internet, a partir de la base de que son personas que tienen algún grado de alfabetización digital.

Este estudio tiene una primera etapa de contextualización, en la que se recabó información del estado de situación actual, entrevistas con representantes de instituciones públicas de Costa Rica, profesionales con amplia experiencia en temas de ciberseguridad, entre otras fuentes.

En una segunda etapa de trabajo se utilizaron instrumentos con la valiosa colaboración de personas dentro del segmento de edad objetivo de esta investigación. Lo anterior permitió conocer la realidad que enfrentan, mediante evaluaciones para aspectos como identificación de vulnerabilidades, criterios para mejorar la seguridad en Internet, criterios para medir la alfabetización digital y criterios para protección de la identidad digital.

En la tercera etapa, a partir de lo anterior, se materializaron estos insumos con la propuesta del marco de trabajo para mejorar la seguridad en Internet para personas en edad laboral madura y personas adultas mayores que participan en la Asociación Gerontológica Costarricense y que cuentan con alfabetización digital.

Como propuesta de vigencia en un entorno altamente cambiante, como la tecnología de información, el trabajo propuso un enfoque en protección de la identidad digital, considerando que las herramientas son cambiantes en el tiempo, mientras que la identidad digital del usuario es uno de los aspectos base y fundamentales para el uso de trámites y servicios disponibles. La Gobernanza Digital del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, establece la identificación y autenticación ciudadana en el Código Nacional de Tecnologías Digitales.

Palabras clave: personas adultas mayores, personas en edad laboral madura, seguridad en Internet, navegación en Internet, identidad digital, alfabetización digital, vulnerabilidades, riesgos de seguridad de la información, gobernanza digital, suplantación de la identidad, estafa informática.

Capítulo I. Introducción

1.1. Generalidades

La presente propuesta busca aportar un marco de trabajo para mejorar la seguridad en Internet de una población que ha tenido un crecimiento. Según la información del Instituto Nacional de Estadística y Censos de Costa Rica, se proyecta con este comportamiento como la población adulta mayor (mayores de 65 años) y la población en edad laboral madura (mayores de 50 años y menores de 65 años). Esta población corresponde a personas nacidas antes de 1970, lo que los incluye entre los grupos que no son nativos digitales y que han tenido la necesidad de adaptación a las herramientas que las tecnologías de información han entregado a las sociedades costarricenses.

En ambos casos según la información de referencia consultada al Organismo de Investigación Judicial, son segmentos que, a partir de las denuncias registradas, cuentan con la necesidad que busca atender la presente propuesta.

1.2. Antecedentes del problema

Según la información del Instituto Nacional de Estadísticas y Censos y los datos que se muestran en la Tabla 1, los habitantes comprendidos entre 50 años y más representaban en el año 2015 un 22 % de la población; en el año 2020 representaban un 24 %, para el año 2025 representa un 26 %; para el año 2030 representarán un 29 %; para el año 2035 representarán un 32 %; para el año 2040 representarán un 36 %; para el año 2045 representarán un 39 % y para el año 2050 representarán un 41 % de la población proyectada. Con lo anterior es claro el crecimiento que este segmento poblacional ha tenido y tiene en Costa Rica.

Tabla 1

Población total por años quinquenales, según grupos quinquenales de edad, 2011-2050

Edades	2011	2015	2020	2025	2030	2035	2040	2045	2050
Total	**4 592 149**	**4 832 234**	**5 111 238**	**5 355 592**	**5 563 906**	**5 742 091**	**5 892 491**	**6 009 490**	**6 093 068**
0-4	364 292	366 604	365 797	350 425	335 248	325 366	320 269	316 553	312 188
5-9	364 396	370 486	371 673	370 186	354 245	338 620	328 272	322 910	318 978
10-14	400 791	375 601	374 598	375 228	373 283	357 005	341 115	330 552	325 017
15-19	426 482	411 183	381 333	379 519	379 652	377 424	361 006	345 024	334 406
20-24	439 870	435 527	419 690	388 671	386 071	385 776	383 341	366 836	350 833
25-29	426 286	451 539	442 156	425 180	393 606	390 630	390 125	387 578	371 060
30-34	369 480	412 875	454 188	444 255	427 074	395 500	392 494	391 991	389 481
35-39	314 575	356 449	411 543	452 642	442 950	426 106	394 907	392 124	391 819
40-44	299 107	306 286	352 809	407 919	449 178	440 020	423 715	393 013	390 547
45-49	290 789	293 970	300 292	347 117	402 348	443 898	435 441	419 750	389 665
50-54	252 145	279 933	286 517	293 605	340 497	395 733	437 484	429 673	414 650
55-59	199 572	235 341	271 597	278 779	286 401	333 147	388 140	429 761	422 632
60-64	140 053	180 803	225 969	261 725	269 382	277 636	323 983	378 222	419 480
65-69	102 760	124 379	170 166	213 630	248 375	256 737	265 759	311 054	364 005
70-74	76 880	88 849	112 996	155 744	196 607	230 075	239 269	248 723	292 289
75-79	55 300	63 484	76 250	97 853	136 040	173 390	204 796	214 109	223 839
80-84	38 368	41 643	49 527	60 168	78 002	110 115	142 254	169 205	178 085
85-89	20 063	24 357	27 618	33 356	41 125	54 476	78 668	102 557	123 039
90-94	7 941	9 781	12 597	14 505	17 828	22 696	31 022	45 452	59 850
95-99	2 581	2 632	3 402	4 447	5 187	6 658	8 882	12 317	18 317
100 y más	418	512	521	640	807	1 084	1 549	2 086	2 886

Fuente: INEC Costa Rica. Estadísticas demográficas 2011 – 2050. Proyecciones nacionales. Población total por años quinquenales, según sexo y grupos quinquenales de edades.

Aunado a lo anterior, a partir de la consulta al Organismo de Investigación Judicial de Costa Rica se presentan los datos en la Tabla 2, Tabla 3 y Tabla 4, que resumen las denuncias presentadas en el periodo 01/01/2016 al 30/01/2022. La información obtenida permite identificar el crecimiento en denuncias por delitos informáticos, el comportamiento de denuncias según los delitos informáticos y las denuncias por delito de estafa de acuerdo con víctimas bienes muebles e inmuebles.

Tabla 2

Casos registrados en el ámbito nacional por delitos informáticos, en el periodo 01/01/2016 al 30/01/2022, según año y rango de edad

Rango Edad	2016	2017	2018	2019	2020	2021	2022	Totales
0-11	11	17	13	20	17	16		94
12-17	73	93	96	106	92	122	3	585
18-29	219	311	358	496	591	792	62	2829
30-39	216	358	441	561	595	692	58	2921
40-49	145	220	308	384	466	507	47	2077
50-64	94	242	294	347	400	399	39	1815
65-200	24	58	74	106	125	157	16	560
DESCONOCIDO	36	25	28	36	45	42	5	217
Totales	818	1324	1612	2056	2331	2727	230	11098

Fuente: Organismo de Investigación Judicial, Oficina de Planes y Operaciones Unidad Análisis Criminal. Datos estadísticos delitos informáticos adultos mayores de 65 años ID-51875.

Tabla 3

Casos registrados en el ámbito nacional por delitos informáticos, en el periodo 01/01/2016 al 30/01/2022, según delito y año

Delito	2016	2017	2018	2019	2020	2021	2022	Totales
SUPLANTACION DE IDENTIDAD	**287**	**346**	**373**	**608**	**755**	**949**	**27**	**3345**
ESTAFA INFORMATICA	**113**	**234**	**394**	**639**	**913**	**876**	**76**	**3245**
OTRO O INDETERMINADO	206	386	495	464	130	210	67	1958
DIFUSION DE INFORMACION FALSA	73	39	48	101	117	148	6	532
SUPLANTACION DE PAGINAS ELECTRONICAS	59	112	82	29	31	93	18	424
ESPIONAJE INFORMATICO	13	25	29	48	115	126	5	361
SEDUCCION O ENCUENTRO CON MENORES POR MEDIOS ELECTRONICOS	43	75	54	54	52	63	2	343
FACILITACION DE DELITO INFORMATICO	2	52	67	47	49	99	8	324
INSTALACION O PROPAGACION DE PROGRAMAS INFORMATICOS MALICIOSOS	2		4	4	82	70	3	165
SABOTAJE INFORMATICO	12	18	12	11	29	23		105
DAÑO INFORMATICO	6	11	10	9	17	15		68
Totales	816	1298	1568	2014	2290	2672	212	10870

Fuente: Organismo de Investigación Judicial, Oficina de Planes y Operaciones Unidad Análisis Criminal. Datos estadísticos delitos informáticos adultos mayores de 65 años ID-51875.

Tabla 4

Casos registrados en el ámbito nacional por delito de estafa según víctima y año, en el periodo 01/01/2016 al 30/01/2022

	año							
Delito / víctima	2016	2017	2018	2019	2020	2021	2022	Totales
ESTAFA	**350**	**234**	**290**	**254**	**224**	**240**	**12**	**1604**
EDIFICACION	115	94	99	84	56	51	1	500
VEHICULO	234	135	191	166	166	185	10	1087
VIVIENDA	1	5		4	2	4	1	17
ESTAFA INFORMATICA	**8**	**4**	**4**	**7**	**8**	**1**	**1**	**33**
EDIFICACION	8	4	4	7	6	1	1	31
VIVIENDA					2			2
Totales	358	238	294	261	232	241	13	1637

Fuente: Organismo de Investigación Judicial, Oficina de Planes y Operaciones Unidad Análisis Criminal. Datos estadísticos delitos informáticos adultos mayores de 65 años ID-51875.

1.3. Definición y descripción del problema

La vulnerabilidad en la población en edad laboral madura y adulta mayor, reflejada en los delitos denunciados en el Organismo de Investigación Judicial, da lugar a la identificación de la necesidad para la cual se plantea el marco de trabajo para mejorar la seguridad en Internet. Lo anterior para evitar la afectación patrimonial y económica.

1.4. Justificación

Con el acelerado crecimiento del uso de las herramientas digitales en los diferentes aspectos de la sociedad costarricense y el aumento de la población objeto de la presente propuesta, se propone un marco de trabajo para mejorar la seguridad en Internet para personas en edad laboral madura y personas adultas mayores. La propuesta se enfoca en los delitos informáticos con mayor cantidad de denuncias presentadas ante el Organismo de Investigación Judicial de Costa Rica, en el periodo consultado.

Para lo anterior, al contar con el cliente Asociación Gerontológica Costarricense, se realiza una investigación aplicada. Para dar vida útil tecnológica a la propuesta, el enfoque se basa en la protección de identidad, esto en el marco de un área que continuamente está en actualización y evolución, como las tecnologías de información y comunicación (TIC).

1.5. Viabilidad

La viabilidad de esta investigación se relaciona con atender una necesidad de vulnerabilidad de una población que se enfrenta a los retos de seguridad en la protección de su identidad. Lo anterior relacionado con su interacción con las herramientas digitales que están a disposición en la sociedad costarricense.

1.5.1. Punto de vista técnico. A partir de la formación recibida en los cursos del programa de Maestría en Ciberseguridad los autores de la presente investigación han adquirido las bases técnicas que les permiten desarrollar la propuesta.

1.5.2. Punto de vista operativo. Desde el punto de vista operativo se plantea trabajar con el apoyo de la Asociación Gerontológica Costarricense, que trabajan con la población adulta en edad laboral madura y población adulta mayor.

1.5.3. Punto de vista económico. El recurso económico involucrado corresponde a las horas de trabajo aportadas por los investigadores autores de la presente propuesta, así como los costos de los cursos asignados por la universidad para el desarrollo del trabajo final de graduación.

1.6. Objetivos

Como referencia de taxonomía se utiliza Bloom (1956), debido a su amplio uso en la academia.

1.6.1. Objetivo general. Proponer un marco de trabajo que mejore la seguridad en Internet para personas en edad laboral madura y personas adultas mayores costarricenses que cuentan con alfabetización digital.

1.6.2. Objetivos específicos. Los objetivos específicos de la investigación son los siguientes:

1. Definir las características de la población adulta en edad laboral madura y adulta mayor, atendida por la Asociación Gerontológica Costarricense.
2. Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad.
3. Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital.
4. Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad.
5. Elaborar una propuesta de un marco de trabajo que mejore la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital.

1.7. Alcances y limitaciones

1.7.1. Alcances. Los alcances del estudio son los siguientes:

- Tabla de resultados de evaluación de criterios para mejorar la seguridad en Internet, aplicada a población de muestra atendida por Ageco.
- Tabla de resultados de evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco.
- Tabla de resultados de evaluación de criterios de protección de identidad digital, aplicada a población de muestra atendida por Ageco.
- Propuesta de marco de trabajo para mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, que cuenta con alfabetización digital.

1.7.2. Limitaciones. Las limitaciones de la investigación son las siguientes:

- Según información identificada de los delitos informáticos con mayor cantidad de denuncias que se plantearon ante el Organismo de Investigación Judicial de Costa Rica, se consideran solamente delitos que se relacionan con estafa informática y con suplantación de identidad.
- Se consideran solamente los riesgos de afectación patrimonial en bienes inmuebles y afectación económica, producto de acceso a sitios en línea de servicios financieros en Costa Rica.
- Se trabaja solamente con recomendaciones generales de sistemas operativos en equipos de escritorio, portátiles y dispositivos móviles.
- Se excluye el proceso de capacitación para la población atendida por Ageco, para la propuesta de marco de trabajo para mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital.

1.8. Marco de deferencia organizacional y socioeconómico

1.8.1. Historia. La Asociación Gerontológica Costarricense (Ageco) se fundó el 14 de octubre de 1980. El fin de su fundación era estudiar las condiciones, las necesidades y las demandas de las personas adultas mayores.

En 1986 comenzó un proceso de contextualización, exploración, diagnóstico y proposición de programas y actividades para obtener recursos para la asociación. Además, ese mismo año inició la promoción de trabajo voluntario y la formación de clubes de las personas adultas mayores, con el fin de proporcionar una línea de autocuidado, que es lo que ahora se denomina en todos los documentos internacionales como envejecimiento activo.

Desde el 2008, tras unos años de incertidumbre sobre cómo obtener fondos para operar, Ageco logró que se le asignara un porcentaje de las utilidades netas de la Junta de Protección Social y pasar a ser una de las organizaciones sociales beneficiarias de la Junta. Desde entonces se ha propiciado la diversificación de las formas de financiamiento, programas y esfuerzos que le permiten a la asociación promover y crear nuevos espacios para las personas adultas mayores.

Ageco ha experimentado un importante crecimiento en cuanto a las acciones que realiza con la población mayor, pero también en la forma de abordar las temáticas que se relacionan con las personas mayores, ahora desde un enfoque de derechos humanos como eje transversal del quehacer de la organización.

1.8.2. Tipo de negocio y mercado meta. Ageco participa activamente en la formulación y seguimiento de las políticas públicas para la promoción de un envejecimiento activo, así como el respeto y el pleno ejercicio de los derechos humanos en la vejez. Los principales temas en los que trabaja Ageco son:

- Sensibilización acerca de la vejez y el envejecimiento.
- Promoción de una vejez digna, un envejecimiento activo.
- Defensa de los derechos humanos de las personas adultas mayores.
- Desarrollo de habilidades y nuevos conocimientos para personas mayores.
- Estos temas se abordan desde tres grandes procesos organizacionales, a saber, participación social y redes, gestión del aprendizaje y conocimiento, derechos humanos y proyección social.

1.8.3. Misión, visión y valores. La misión, visión y valores de Ageco son:

1.8.3.1. Misión. Somos una organización no gubernamental que desarrolla programas sociales y servicios para las personas mayores promovemos la incidencia política y la sensibilización acerca de la vejez y el envejecimiento.

1.8.3.2. Visión. Ser la organización no gubernamental líder en la promoción de una vejez con dignidad, un envejecimiento activo y con calidad a lo largo de la vida y en la defensa de los derechos humanos de las personas mayores.

1.8.3.3. Valores. Los valores son los siguientes:

- Respeto.
- Calidez.
- Solidaridad.
- Compromiso.
- Integridad.

1.8.4. Políticas institucionales. A continuación, se detallan los objetivos estratégicos:

1.8.4.1. Eje 1: Transformación. Innovar el quehacer institucional por medio de estrategias de fortalecimiento permanente de los programas y servicios dirigidos a la atención del proceso de envejecimiento y etapa de la vejez.

1.8.4.2. Eje 2: Sostenibilidad. Integrar estrategias para la sostenibilidad financiera, administrativa y programática de la organización.

1.8.4.3. Eje 3: Posicionamiento. Posicionar a Ageco como organización líder en los ámbitos nacional y regional en temas como derechos humanos de las personas mayores, vejez y envejecimiento activo, mediante una mayor proyección del liderazgo, la incidencia nacional e internacional y el fortalecimiento de la comunicación en todos sus niveles.

1.8.4.4. Eje 4: Gestión. Mejorar la gestión organizacional potenciando el talento humano y la modernización digital.

1.9. Estado de la cuestión

Se han realizado estudios en el ámbito internacional sobre las vulnerabilidades que enfrentan las personas en edad laboral madura y personas adultas mayores en internet y cómo son muy propensas a recibir ataques cibernéticos cuando usan diferentes servicios como banca en línea o las mismas redes sociales. Sin embargo, no se ha concretado alguna propuesta para mejorar esta situación, los estudios que se encontraron son pocos y en el ámbito nacional no existe algún tipo de propuesta similar.

1.9.1. Planificación de la revisión. Se formula una pregunta clara sobre la investigación. Además, se buscan documentos existentes sobre la ciberseguridad en personas en edad laboral madura y personas adultas mayores con alfabetización digital para comprender los desarrollos académicos, posibles áreas débiles que se pueden ampliar y verificar que no haya duplicación de investigaciones realizadas en otras encuestas.

1.9.1.1. Formulación de la pregunta. Se lleva a cabo una formulación de la pregunta para ayudar a definir la búsqueda de información en los diferentes repositorios de artículos. El objetivo es encontrar respuestas que demuestren el aporte de este trabajo al campo de la investigación y la relación entre ideas, teoría y aplicaciones prácticas en lo relacionado con la ciberseguridad de los adultos en edad laboral madura y personas adultas mayores.

1.9.1.1.1. Foco de la pregunta. Para la búsqueda de documentos se enfatizó en técnicas o medidas que se realizan para mejorar la ciberseguridad de las personas en edad laboral madura y personas adultas mayores, además de identificar qué es lo que utilizan más al navegar en Internet.

1.9.1.1.2. Amplitud y calidad de la pregunta. En función del problema que se pretende resolver se establece una pregunta de investigación por responder de forma clara y definida con la búsqueda de artículos que se relacionan con la ciberseguridad en adultos en edad laboral madura y personas adultas mayores. Se enumeran los términos clave relevantes para buscar información y se consideran componentes clave como poblaciones específicas, exposiciones y eventos de interés. Las medidas que se utilizan para medir la eficacia se definen en términos de la pregunta por responder y el diseño de la investigación que se aplica.

1.9.1.1.2.1. Problema. El incremento de la tecnología facilitó la vida cotidiana en muchos aspectos, este cambio tecnológico propició la alfabetización tecnológica o digital de varias personas que no utilizaban algún dispositivo tecnológico para realizar diversas funciones. Muchas de las personas que han experimentado este cambio son las personas en edad laboral madura y las personas adultas mayores que cada vez más utilizan servicios en Internet para llevar a cabo diferentes actividades como banca en línea o las mismas redes sociales.

A pesar de que lo anterior es un gran avance para esta población también implica una serie de peligros que se relacionan con ciberdelitos y ataques informáticos hacia ellos. Los adultos mayores son muy propensos a recibir este tipo de ataques y poner en peligro tanto datos personales como sus propios ahorros que han alcanzado en su vida laboral.

1.9.1.1.2.2. Pregunta. Al definir previamente el problema se establece la pregunta de la siguiente manera.

¿Cuáles estudios se realizan para mejorar la ciberseguridad de las personas en edad laboral madura y personas adultas mayores?

1.9.1.1.2.3. Palabras clave y sinónimos. Se creó una lista de palabras clave para buscar e identificar documentos y trabajos que se relacionan con la investigación por realizar. Algunas de estas palabras están escritas en inglés porque una gran cantidad de publicaciones están escritas en este idioma. En la Tabla 5 se presenta un listado de estas palabras.

Tabla 5

Listado de palabras

Palabra	Equivalente en inglés
Ciberseguridad	*Cyber security*
Ciberataque	*Cyber attack*
Adultos mayores	*Older adults, Older persons, Senior citizens*
Seguridad en Internet	*Internet safety*
Recomendaciones	*Recommendations*
Ciberdelitos	*Cybercrime*
Técnicas	*Techniques*
Navegación	*Internet surfing*
Clasificación	*Classification*
Concientización	*Awareness*
Alfabetización digital	*Digital literacy*

1.9.1.1.2.4. Intervención. Extraer los artículos y documentos de mayor relevancia para la investigación y analizar los resultados.

1.9.1.1.2.5. Control. Al iniciar la investigación se lleva a cabo una búsqueda desde cero, ya que no existe algún tipo de base para el inicio.

1.9.1.1.2.6. Efectos. Con la búsqueda exhaustiva se espera obtener la información suficiente para comprender qué se ha hecho, tanto en el ámbito nacional como internacional, para mejorar la ciberseguridad de las personas en edad laboral madura y personas adultas mayores usuarias de Internet.

1.9.1.1.2.7. Medida de salida. Para los documentos que se encontraron se lleva a cabo una revisión de calidad en un sitio *web* dedicado a este fin.

1.9.1.1.2.8. Población. La población que se quiere identificar en este estudio son los adultos en edad laboral madura y personas adultas mayores con algún nivel de alfabetización tecnológica o digital en Costa Rica.

1.9.1.1.2.9. Aplicación. Este tipo de investigación puede resultar de utilidad para personas en el área de la ciberseguridad.

1.9.1.1.3. Selección de fuentes. Para la selección de fuentes se utiliza la página Scimago Journal & Country Rank para verificar la calidad de los artículos buscados y seleccionados.

1.9.1.1.3.1. Definición del criterio de selección de fuentes. En general, se han tenido en cuenta varios aspectos en el momento de seleccionar una fuente, como la popularidad de las personas investigadoras y el soporte teórico disponible de la fuente. Además, se consideran fuentes con diversos documentos y relevancia actual. Asimismo, se considera importante tener fácil acceso a la información y la capacidad de tener credenciales para acceder a los documentos.

1.9.1.1.3.2. Idioma de estudio. Se utilizan artículos tanto en inglés como en español, ya que en inglés aumenta el rango de resultados posibles.

1.9.1.1.4. Identificación de fuentes. En este apartado se describe la selección de fuentes para la documentación primaria, se hace una descripción sobre cómo se ejecutan las búsquedas y se provee una lista de fuentes.

1.9.1.1.4.1. Método de selección de fuentes:. El método de selección de fuentes se basa principalmente en el respaldo con el que cuenta la fuente en el área de tecnología con respecto a la publicación de estudios y documentos investigativos. Además, se considera la facilidad de acceso al sitio y para hacer las búsquedas.

1.9.1.1.4.2. Cadena de búsqueda. Las cadenas de búsqueda que se utilizan tienen combinación, como *cybersecurity* y *older adults*, *cybersecurity* y *older persons*, cyber *attacks* y *older adults*, *senior citizens* y *cybersecurity.*

1.9.1.1.4.3. Lista de fuentes. Debido a la calidad de los artículos académicos y cantidad de artículos recientes, de acuerdo con el tema investigado, se considera el uso de las siguientes fuentes:

1. Google Scholar.
2. IEEE Digital Library.
3. ACM Digital Library.

1.9.1.1.4.4. Selección de fuentes después de la evaluación. Los elementos para refinar la lista de fuentes dependen de la facilidad de aplicación de las cadenas de búsqueda y la calidad de los documentos que se brindan. Un aspecto que se toma en cuenta es la facilidad que se tiene para acceder al material.

1.9.1.1.5. Comprobación de las fuentes. En este momento no se cuenta con criterio experto para la selección de las fuentes, sin embargo, se escogieron las que más se utilizan para obtener documentación relacionada con tecnología, entre otras ramas. Se espera obtener un criterio experto para refinar la lista o agregar más, según sea necesario.

1.9.1.1.5.1. Selección de los estudios. Después de definir las fuentes se establece cuáles trabajos recuperados en las búsquedas se incluyen en el análisis final.

1.9.1.2. Definición del criterio de inclusión y exclusión de estudios. Se utilizan los criterios detallados en la Tabla 6 para incluir o excluir un documento. Los artículos que cumplan los requisitos son candidatos por incluir.

Tabla 6

Criterio de escogencia de estudios

Pregunta de investigación	Término principal para criterio de inclusión	Criterio de exclusión
¿Cuáles estudios se realizan para mejorar la ciberseguridad de las personas en edad laboral madura y personas adultas mayores?	*Cybersecurity, older adults, older persons, senior citizens, cyber-attacks, Internet security, awareness*	Documentos muy antiguos. Documentos que no profundicen en la ciberseguridad de los adultos mayores.

1.9.1.2.1. Procedimiento para la selección de los estudios. Se llevó a cabo el siguiente proceso para seleccionar en cada fuente los artículos más importantes o relevantes:

1. En cada una de las fuentes se utilizaron diferentes criterios de búsqueda, ya sea búsqueda avanzada o general. En cada una se tapizaron los criterios de búsqueda o cadenas de búsqueda establecidas.
2. Según el número de resultados y utilizando las cadenas de búsqueda aplicables se lleva a cabo el proceso de escoger y excluir los artículos.
3. Se evalúan los resultados y se aplican los criterios de exclusión que se basan en palabras clave y el Abstract del artículo.
4. Se seleccionan los resultados más importantes que se encontraron para la fuente consultada y se lleva a cabo el mismo proceso con las otras fuentes.

1.9.2. Ejecución de la revisión. A continuación, se presenta el proceso de selección que se lleva a cabo para las diferentes fuentes.

1.9.2.1. Ejecución de la selección en la fuente utilizando el motor Google Scholar. A continuación, se presenta el proceso de selección que se lleva a cabo utilizando el motor Google Scholar.

1.9.2.1.1. Selección de estudios iniciales. Siguiendo las recomendaciones provistas por Blanco *et al.* (2007) se lleva a cabo la búsqueda de estudios iniciales de la siguiente manera. Búsqueda basada en los siguientes parámetros:

- Cybersecurity.
- Older Adults.
- Senior Citizens.
- Older Persons.
- Cyber Attacks.

Después de realizar las búsquedas con los parámetros anteriores se encontraron 15 resultados, de los cuales 7 se seleccionaron después de aplicar los métodos de exclusión sugeridos, principalmente porque no prestaron la atención a las alternativas o no profundizaron en los problemas de seguridad en Internet de las personas mayores, además de todos aquellos que sean muy antiguos. A continuación, se presenta su detalle.

Tabla 7

Estudios que se encontraron con Google Scholar

#	Titulo	Autores	Año	URL
1	“If It Important It Will Be A Headline”: Cybersecurity Information Seeking in Older Adults	James Nicholson Lynne Coventry Pamela Briggs	2019	https://dl.acm.org/doi/abs/10.1145/3290605.3300579#pill-authors__contentcon
2	Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults	Benjamin A. Morrison Lynne Coventry Pam Briggs	2020	https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00623/full?luicode=10000011&lfid=231522type%3D1%26t%3D10%26q%3D%23075%23&featurecode=newtitle&u=https:%2F%2Fwww.frontiersin.org%2Farticles%2F10.3389%2Ffpsyg.2020.00623%2Fabstract
3	The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers	Helena M. Mentis Galina Madjaroff Aaron Massey Zoya Trendafilova	2020	

4	A Mixed Methods Approach to Understanding Cyber-Security Vulnerability in the Baby Boomer Population	Morrison, Benjamín Alan.	2020	https://www.proquest.com/openview/20fbce6b1822faa8476310bf40c68f4b/1?pq-origsite=gscholar&cbl=44156
5	Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia	Rossanne Gale Vergara Nasreen Khan Shereen Khan	2020	http://myjms.mohe.gov.my/index.php/ajress/article/view/9697
6	Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective	Yair Levy John D'Archy Carlene Blackwood Brown	2019	https://www.tandfonline.com/doi/abs/10.1080/08874417.2019.1579076

1.9.2.1.2. Revisión de la selección. Después de revisar el Abstract y el contenido de cada artículo se llevó a cabo una selección para considerarlos como materia prima para la investigación. Los comentarios sobre estos artículos se ordenan según su relevancia.

1.9.2.1.3. Extracción de información. De acuerdo con los artículos seleccionados, se extrae una serie de información para ayudar en el desarrollo de la investigación y de la propuesta que se planteó. Los elementos considerados son los siguientes:

Tabla 8

Extracción fuente 1

Motor de búsqueda de artículos	**Google Scholar**
Titulo	“If It Important It Will Be A Headline”: Cybersecurity Information Seeking in Older Adults
Publicación	CHI ‘19: Proceedings of the 2019 CHI Conference on Human Factors in Computing SystemsMay 2019 Paper No.: 349 Pages 1–11 https://doi.org/10.1145/3290605.3300579
Autores	James Nicholson, Lynne Coventry, Pamela Briggs
Referencia	Nicholson, J., Coventry, L. y Briggs, P. (2019, May). *If It Important It Will Be A Headline* Cybersecurity Information Seeking in Older Adults. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-11)
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	Los adultos mayores son cada vez más vulnerables a los ataques y estafas de ciberseguridad. Sin embargo, sabemos poco sobre su conocimiento de la ciberseguridad, sus comportamientos de búsqueda de información y sus fuentes de confianza de información y asesoramiento en este ámbito. Hemos realizado 22 entrevistas semiestructuradas a adultos mayores que viven en la comunidad para explorar sus comportamientos de búsqueda de información sobre ciberseguridad. Tras un análisis temático de estas entrevistas, desarrollamos un marco de acceso a la información sobre ciberseguridad que pone de manifiesto las deficiencias en la

	elección de recursos de información por parte de los adultos mayores. En concreto, descubrimos que los usuarios mayores dan prioridad a los recursos sociales en función de su disponibilidad, más que a los conocimientos sobre ciberseguridad y que evitan utilizar Internet para buscar información sobre ciberseguridad a pesar de utilizarlo para otros ámbitos. Por último, analizamos el diseño de estrategias de difusión de información sobre ciberseguridad para usuarios de edad avanzada, incorporando fuentes favoritas como los anuncios de televisión y los programas de radio.

Aspectos por destacar

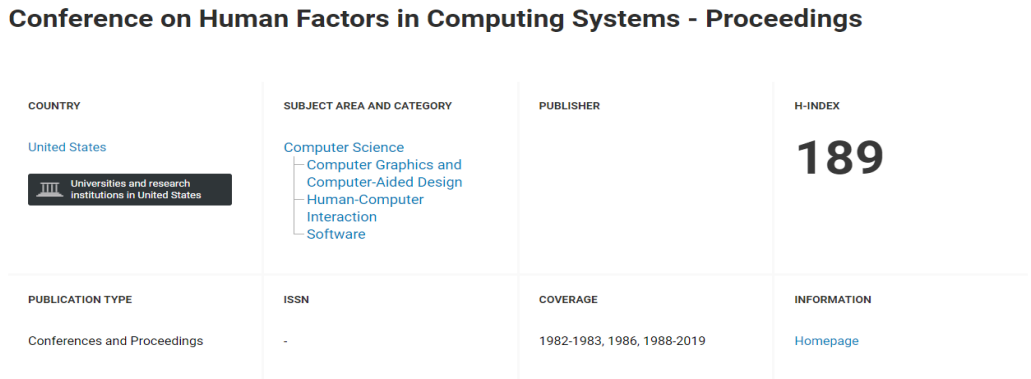
Interés de los adultos mayores por búsqueda de información de ciberseguridad.

Problemática de vulnerabilidades hacia esta población.

Alfabetización digital fundamental para prevenir este tipo de ataques.

Marco de acceso a temas de seguridad a personas mayores.

Calidad del estudio según revista publicada



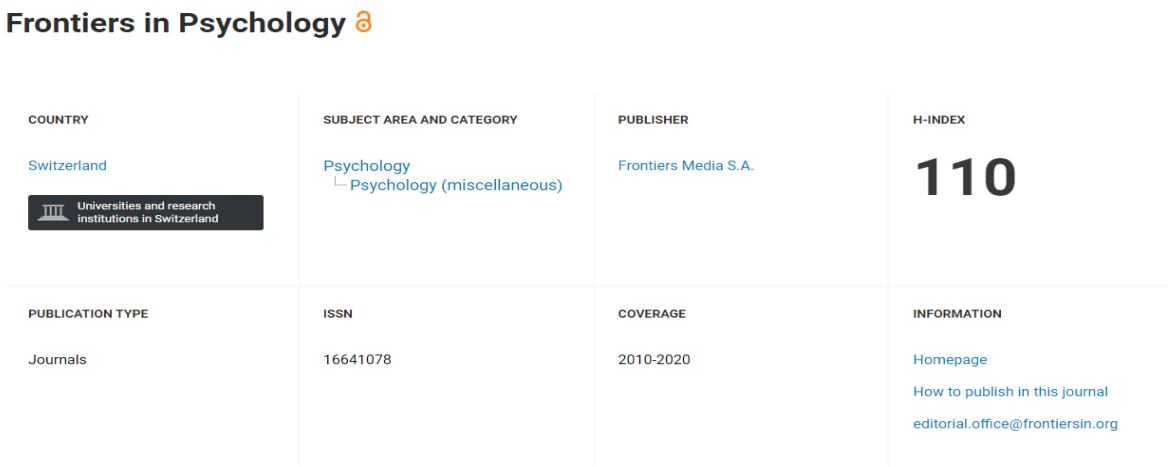
Validación de fuente

Tabla 9

Extracción fuente 2

Motor de búsqueda de artículos	**Google Scholar**
Titulo	Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults
Publicación	Front. Psychol., 30 April 2020 | https://doi.org/10.3389/fpsyg.2020.00623
Autores	Benjamin A. Morrison; Lynne Coventry; Pam Briggs
Referencia	Morrison, B. A., Coventry, L. y Briggs, P. (2020). Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. Frontiers in psychology, 11, 623.
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	La jubilación es una transición vital importante que conlleva cambios sustanciales en casi todos los aspectos de la vida cotidiana. Aunque esta transición se ha considerado hasta ahora como el marcador normativo de la entrada en la edad adulta, su influencia en la vida posterior no se ha estudiado en términos de uso de la tecnología y comportamientos de ciberseguridad. Esto es problemático, ya que los adultos mayores corren un riesgo especial de convertirse en víctimas de la ciberdelincuencia. El objetivo de este estudio era investigar qué factores asociados a la transición a la jubilación podían aumentar la vulnerabilidad a los ciberataques en una muestra

	de 12 adultos mayores residentes en el Reino Unido, todos ellos jubilados en los últimos 5 años. Se realizaron entrevistas semiestructuradas, uno a uno, y posteriormente se analizaron mediante un análisis temático. Se identificaron seis temas referidos a áreas de pérdida en: interacción social, finanzas, rutina diaria, sentimientos de competencia, sentido de propósito y estructuras de apoyo tecnológico. Se discuten las implicaciones de estas pérdidas para la construcción de la ciber-resiliencia en los jubilados, con sugerencias para futuras investigaciones.
Aspectos por destacar	
	Se identifican como mayores usos de navegación la banca en línea y redes sociales. La tecnología puede generar desafíos a las personas jubiladas y, por ende, ser propensas a ataques cibernéticos
Calidad del estudio según revista publicada	



Validación de fuente

Tabla 10

Extracción fuente 3

Motor de búsqueda de artículos	Google Scholar
Título	The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers
Publicación	Proceedings of the ACM on Human-Computer InteractionVolume 4 Issue CSCW2October 2020 Article No.: 164pp 1–19 https://doi.org/10.1145/3415235
Autores	Helena M. Mentis; Galina Madjaroff; Aaron Massey; Zoya Trendafilova
Referencia	Mentis, H. M., Madjaroff, G., Massey, A. y Trendafilova, Z. (2020). The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-19
Descripción	
Área	Ciberseguridad, aspectos humanos y sociales de la seguridad y la privacidad
Resumen	Aunque la continua interacción en línea es beneficiosa para un adulto mayor con deterioro cognitivo leve, los riesgos de ciberseguridad pueden acentuarse. En trabajos anteriores se ha destacado el beneficio de la toma de decisiones compartida entre los receptores de cuidados y los cuidadores que pueden querer inculcar salvaguardias de ciberseguridad, en particular en el ámbito de la seguridad en línea. En este estudio investigamos las prácticas actuales de toma de decisiones sobre seguridad en línea de los receptores de cuidados con deterioro cognitivo leve

	y sus cuidadores conyugales. Identificamos una brecha entre la toma de decisiones optativa y la real: mientras que las parejas expresaban su deseo de participar en la toma de decisiones compartida, la realidad era que la mayoría de los cuidadores se veían obligados a actuar en solitario. Además, determinamos que la toma de decisiones compartida no era factible, ya que no había opciones de protección adecuadas a lo largo de un espectro de cuidados para que la pareja pudiera elegir. Relacionamos estos hallazgos con trabajos anteriores que ponen de manifiesto retos similares y debatimos cómo es necesario ofrecer algo más que una simple ilusión de elección.
Aspectos por destacar	
	Se analiza cómo la pérdida del nivel cognitivo hace propensos a los adultos mayores a recibir ataques cibernéticos
Calidad del estudio según revista publicada	

Proceedings of the ACM on Human-Computer Interaction

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Computer Science Computer Networks and Communications Human-Computer Interaction Social Sciences Social Sciences (miscellaneous)	Association for Computing Machinery (ACM)	27

PUBLICATION TYPE	ISSN	COVERAGE	INFORMATION
Journals	25730142	2017-2020	Homepage How to publish in this journal jeff@jeffreynichols.com

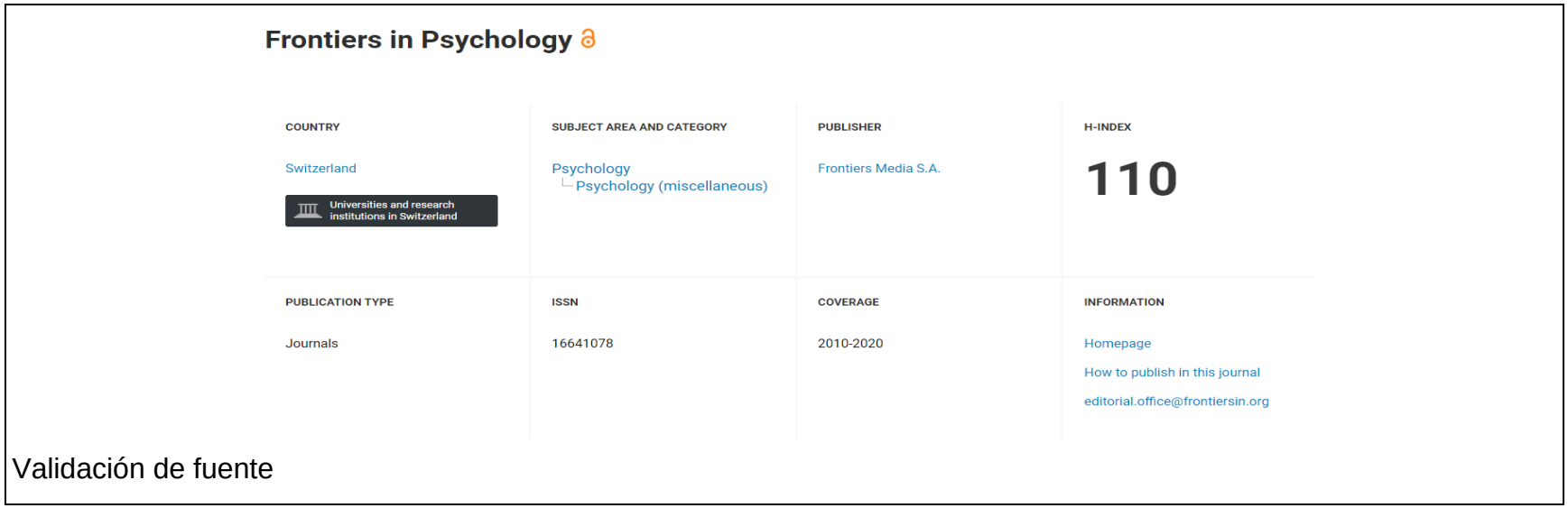
Validación de fuente

Tabla 11

Extracción fuente 4

Motor de búsqueda de artículos	Google Scholar
Título	A Mixed Methods Approach to Understanding Cyber-Security Vulnerability in the Baby Boomer Population
Publicación	University of Northumbria at Newcastle (United Kingdom). ProQuest Dissertations Publishing, 2020. 28302962.
Autores	Benjamin A. Morrison
Referencia	Morrison, B. A. (2020). A mixed methods approach to understanding cyber-security vulnerability in the baby boomer population. University of Northumbria at Newcastle (United Kingdom).
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	La pandemia de la enfermedad del Coronavirus 2019 (COVID-19) sigue causando problemas y riesgos frecuentes relacionados con la ciberseguridad y la privacidad de los datos en Malasia, que deben ser considerados meticulosamente y abordados de forma adecuada. Además, el envejecimiento de la población de Malasia está limitado en cuanto a la consciencia de ciberseguridad. El objetivo de esta investigación es explorar la mentalidad de ciberseguridad de la población mayor de Malasia y su impacto en su bienestar. Para ello, este estudio utilizó una metodología cualitativa destinada a comprender la mentalidad de ciberseguridad de la

	población que envejece y a desarrollar un marco político de apoyo. Las cuestiones que preocupan van desde los ciberdelincuentes que se dirigen a una mano de obra novata que trabaja desde casa (WFH) con ingeniosas estafas de *phishing* que se aprovechan de las víctimas en un entorno de incertidumbre. Las sociedades vulnerables, como las personas mayores de 60 años, se encuentran entre los objetivos del ciberfraude. Durante la pandemia de COVID-19, las personas mayores en Malasia no están seguras de si pueden o no compartir su información personal, financiera o médica según las leyes de privacidad aplicables. Además, las personas mayores siguen estando perplejas a la hora de abordar cuestiones de ciberseguridad como el *phishing* y el *malware*. Los investigadores realizaron entrevistas cara a cara en línea y encuestas con formularios de Google a encuestados de 60 años o más, basándose en una metodología de investigación cualitativa. Los resultados indican que muchos de los encuestados de la administración pública son conscientes de la ciberseguridad, pero siguen sin estar seguros y sin conocer el *modus operandi* real de los ciberdelincuentes.
Aspectos por destacar	
	Se identifica la generación llamada Baby Boomer nacidos de 1946 a 1964 como la generación que está recibiendo más impacto tecnológico, además sobre cómo la jubilación puede afectar en vulnerabilidades cibernéticas en sus usos en Internet. También se establece el estrés que puede causar la ciberseguridad en los adultos mayores.
Calidad del estudio según revista publicada	



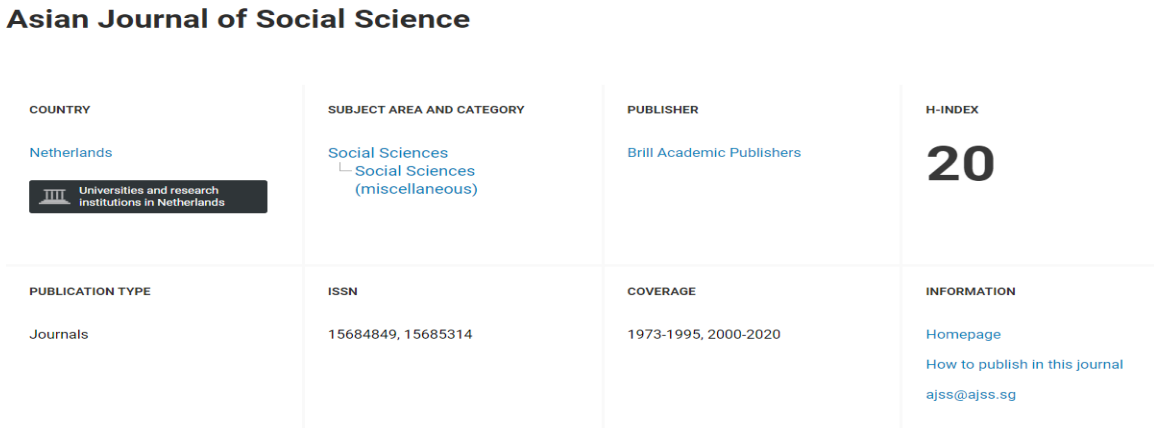
Validación de fuente

Tabla 12

Extracción fuente 5

Motor de búsqueda de artículos	Google Scholar
Titulo	Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia
Publicación	Asian Journal of Research in Education and Social Sciences
Autores	Rossanne Gale Vergara; Nasreen Khan; Shereen Khan
Referencia	Tan, S. L., Vergara, R. G., Khan, N. y Khan, S. (2020). Cybersecurity and privacy impact on older persons amid COVID-19: a socio-legal study in Malaysia. Asian Journal of Research in Education and Social Sciences, 2(2), 72-76.
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	La pandemia de la enfermedad del Coronavirus 2019 (COVID-19) sigue causando problemas y riesgos frecuentes relacionados con la ciberseguridad y la privacidad de los datos en Malasia, que deben ser considerados meticulosamente y abordados de forma adecuada. Además, el envejecimiento de la población de Malasia está limitado en cuanto a la conciencia de ciberseguridad. El objetivo de esta investigación es explorar la mentalidad de ciberseguridad de la población mayor de Malasia y su impacto en su bienestar. Para ello, este estudio utilizó una metodología cualitativa destinada a comprender la mentalidad de ciberseguridad de la

	población que envejece y a desarrollar un marco político de apoyo. Las cuestiones que preocupan van desde los ciberdelincuentes que se dirigen a una mano de obra novata que trabaja desde casa (WFH) con ingeniosas estafas de *phishing* que se aprovechan de las víctimas en un entorno de incertidumbre. Las sociedades vulnerables, como las personas mayores de 60 años, se encuentran entre los objetivos del ciberfraude. Durante la pandemia de COVID-19, las personas mayores en Malasia no están seguras de sí pueden o no compartir su información personal, financiera o médica según las leyes de privacidad aplicables. Además, las personas mayores siguen estando perplejas a la hora de abordar cuestiones de ciberseguridad como el *phishing* y el *malware*. Los investigadores realizaron entrevistas cara a cara en línea y encuestas con formularios de Google a encuestados de 60 años o más, basándose en una metodología de investigación cualitativa. Los resultados indican que muchos de los encuestados de la administración pública son conscientes de la ciberseguridad, pero siguen sin estar seguros y sin conocer el *modus operandi* real de los ciberdelincuentes.
Aspectos por destacar	
	Aspectos como la pandemia de la COVID-19 han hecho que se acreciente el número de adultos mayores ciberatacados. Hay mucha desinformación por parte de los adultos mayores en temas de *phishing* y *malware*.
Calidad del estudio según revista publicada	



Validación de fuente

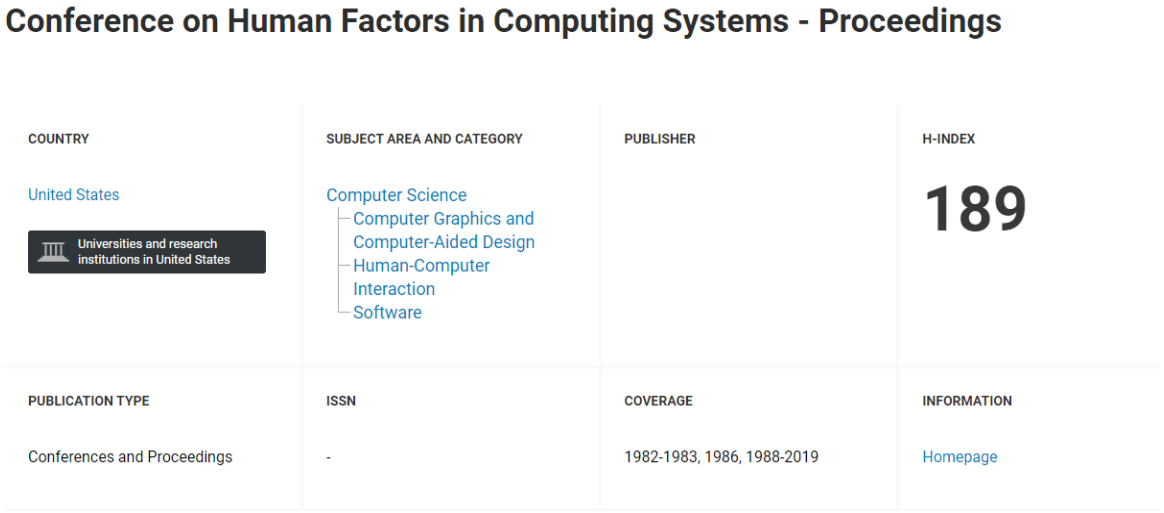
Tabla 13

Extracción fuente 6

Motor de búsqueda de artículos	**Google Scholar**
Título	Training and Embedding Cybersecurity Guardians in Older Communities.
Publicación	University of Northumbria at Newcastle (United Kingdom). ProQuest Dissertations Publishing, 2020. 28302962.
Autores	James Nicholson; Ben Morrison; Matt Dixon; Lynne Coventry; Jill McGlasson.
Referencia	Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L. y McGlasson, J. (2021, May).

	Training and Embedding Cybersecurity Guardians in Older Communities. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-15).
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	Los adultos mayores pueden tener dificultades para acceder a los conocimientos pertinentes de la comunidad cuando se enfrentan a situaciones nuevas. Una de esas situaciones es el número de ciberataques a los que pueden enfrentarse cuando interactúan en línea. Este artículo informa sobre una iniciativa que reclutó, formó y apoyó a los adultos mayores para que se convirtieran en educadores de ciberseguridad de la comunidad (ciberguardianes), encargados de promover las mejores prácticas de ciberseguridad en sus comunidades para evitar que los adultos mayores fueran víctimas de ciberataques oportunistas. Esta iniciativa utilizó una estrategia de difusión de información entre iguales, en lugar de entre expertos, lo que facilitó la inclusión de personas que usualmente no buscarían información sobre ciberseguridad y, por lo tanto, pueden ser vulnerables a los ciberataques. Informamos sobre el modo en que los ciberguardianes utilizaron métodos informales para crear comunidades más conscientes, sirvieron de modelos para el cambio de comportamiento y mejoraron indirectamente su bienestar personal. Discutimos las consideraciones para apoyar a los Ciber Guardianes, incluyendo las implicaciones para la sostenibilidad y para replicar este modelo en otros contextos digitales, por ejemplo, reconociendo la desinformación o mejorando la salud mental.
Aspectos por destacar	
	Cómo se idean planes para reclutar, capacitar y apoyar a las personas mayores para que se conviertan en educadores comunitarios de ciberseguridad. Estos adultos mayores son responsables de promover las mejores prácticas de ciberseguridad en sus comunidades para evitar que otras personas mayores se conviertan en víctimas de ciberataques oportunistas.

Calidad del estudio según revista publicada



Conference on Human Factors in Computing Systems - Proceedings

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Computer Science Computer Graphics and Computer-Aided Design Human-Computer Interaction Software		189

PUBLICATION TYPE	ISSN	COVERAGE	INFORMATION
Conferences and Proceedings	-	1982-1983, 1986, 1988-2019	Homepage

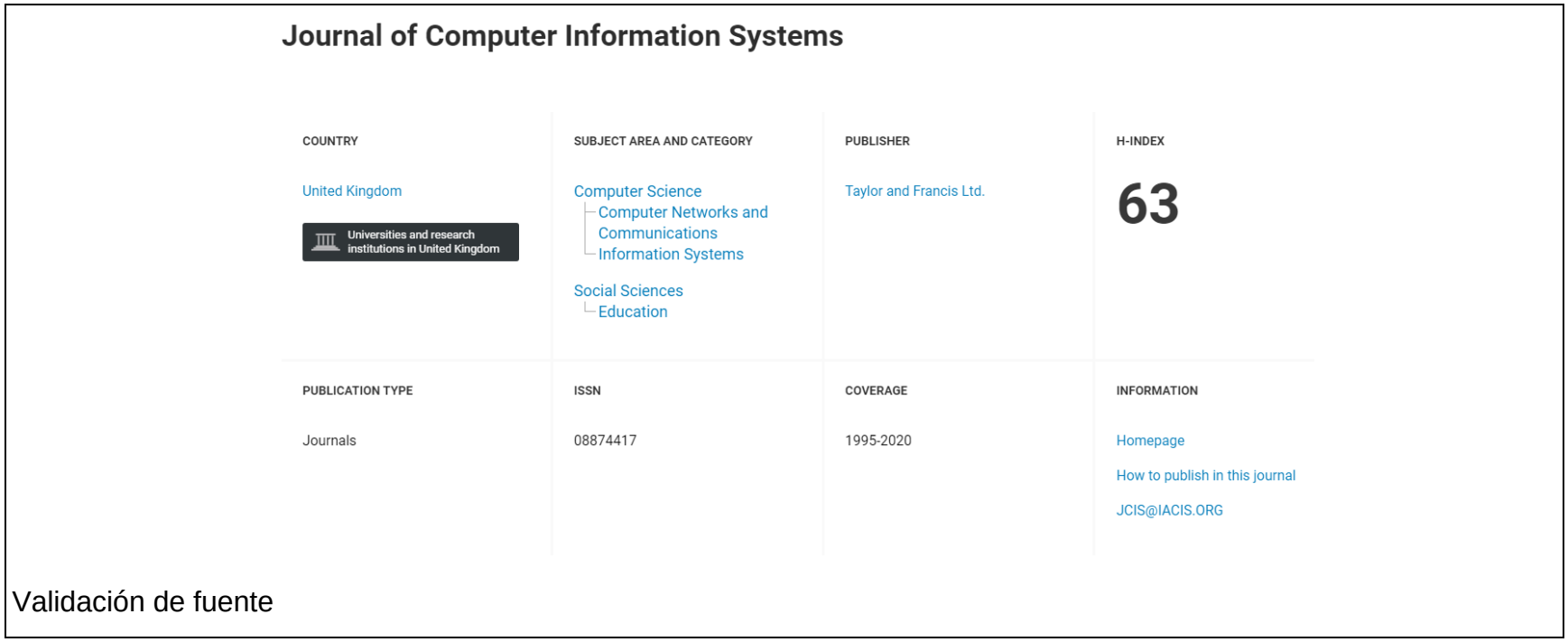
Validación de fuente

Tabla 14

Extracción fuente 7

Motor de búsqueda de artículos	**Google Scholar**
Título	**Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective**
Publicación	Journal of Computer Information Systems
Autores	Yair Levy; Ben Morrison; John Dárchy; Carlene Blackwood-Brown
Referencia	Blackwood-Brown, C. G. (2018). An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills (Doctoral dissertation, Nova Southeastern University).
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	Las personas mayores son uno de los grupos de usuarios de Internet más vulnerables y propensos a los ciberataques. Por lo tanto, evaluar la motivación de los ciudadanos mayores para adquirir conocimientos de ciberseguridad es fundamental para ayudarles a comprender los riesgos de los ciberataques. Este estudio investigó un conjunto de constructos que contribuyen a la motivación de los ciudadanos mayores para adquirir habilidades de ciberseguridad y evaluó el nivel real de habilidades de ciberseguridad de estas personas. Utilizando una encuesta basada en la *web* y una aplicación basada en escenarios prácticos llamada MyCyberSkills™, este estudio de investigación midió los constructos de interés antes y después de la formación

	en ciberseguridad. Los participantes en el estudio fueron 254 personas mayores con una edad media de aproximadamente 70 años. Los resultados indicaron que la formación de concienciación sobre ciberseguridad fue eficaz para aumentar el nivel de habilidades de ciberseguridad de los ciudadanos de edad avanzada y los dotó de pequeñas pero significativas mejoras en las habilidades requeridas para tomar acciones de mitigación contra los ciberataques. Se discuten las implicaciones teóricas y prácticas
Aspectos por destacar	
	Cómo se idean planes para reclutar, capacitar y apoyar a las personas mayores para que se interesen en la ciberseguridad y que esa motivación las ayude a integrarse más en este mundo.
Calidad del estudio según revista publicada	



Validación de fuente

1.9.2.1. Ejecución de la selección en la fuente IEEE. En el siguiente apartado se detalla la información.

1.9.2.1.1. Selección de estudios iniciales. Se lleva a cabo la búsqueda de estudios iniciales de la siguiente manera. Búsqueda basada en los siguientes parámetros:

- Cybersecurity.
- Older adults.
- Senior citizens.
- Older persons.
- Cyber attacks.

Tras realizar la búsqueda utilizando los parámetros anteriores se encontraron siete resultados, de los cuales solo se escogieron tres para utilizar.

Tabla 15

Estudios que se encontraron IEEE

#	Titulo	Autores	Año	URL
7	Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and phishing Attacks.	Premankit Sannd. David M. Cook	2018	
8	Biometrics: Password replacement for elderly?	Eiman Ahmed. Brandon DeLuca. Emily Hirowski. Connor Magee. Ivan Tang. Jean F. Coppola	2017	https://ieeexplore.ieee.org/document/8001958
9	Establishing a Cybersecurity Home Monitoring System for the Elderly	Mu-Yen Chen	2021	https://ieeexplore.ieee.org/document/9543573/authors#authors

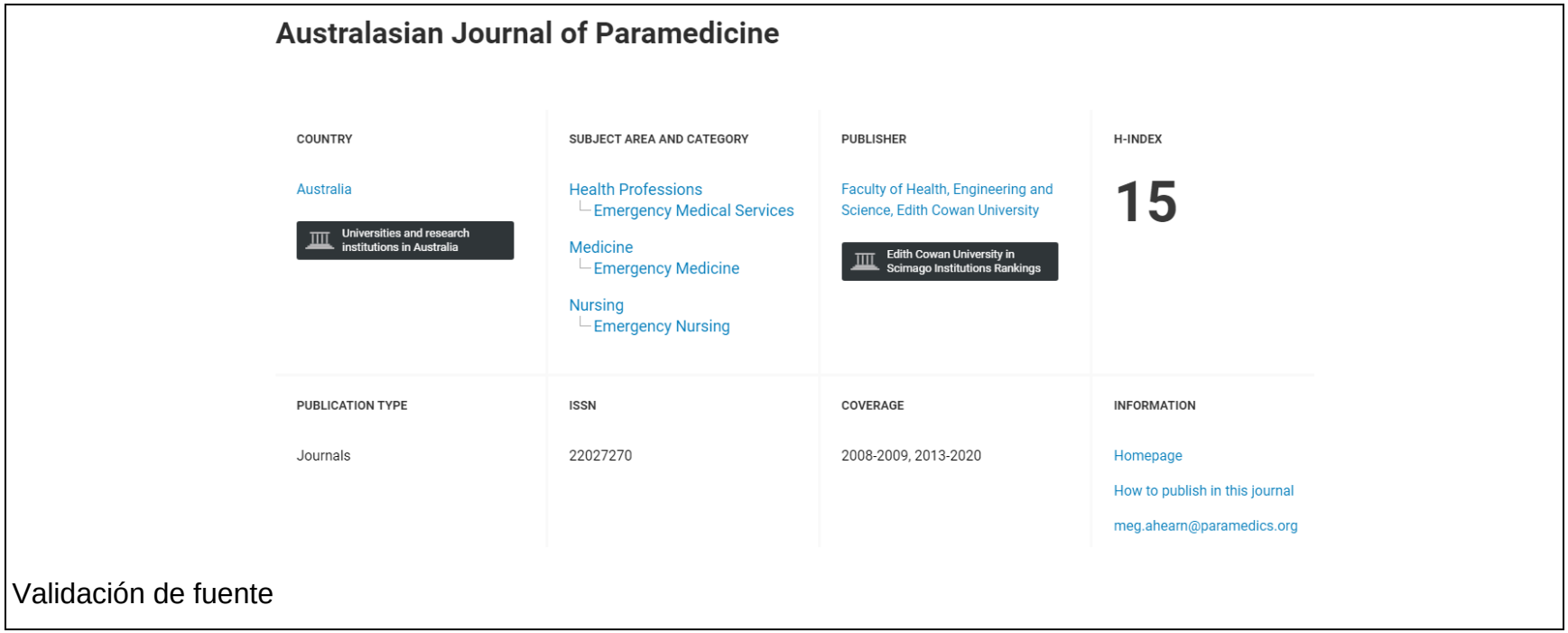
1.9.2.1.1. Extracción de información. Para extraer la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación se consideran los siguientes elementos:

Tabla 16

Extracción fuente 8

Motor de búsqueda de artículos	IEEE DIGITAL LIBRARY
Título	Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and phishing Attacks.
Publicación	2018 Fourteenth International Conference on Information Processing (ICINPRO)
Autores	Premankit Sannd. David M. Cook
Referencia	P. Sannd and D. M. Cook, “Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and phishing Attacks” 2018 Fourteenth International Conference on Information Processing (ICINPRO), 2018, pp. 1-5, DOI: 10.1109/ICINPRO43533.2018.9096878
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	A pesar de la variedad de investigaciones a nivel mundial sobre la identificación y proliferación del *ransomware* y otras estafas en línea, sigue existiendo un relativo vacío de investigación con respecto al problema del engaño digital y social en forma de *ransomware* sobre un individuo. Esto es especialmente problemático en el caso de las cohortes de mayor edad, en las que la experiencia vital en muchas actividades coexiste con la comprensión y la experiencia novatas

	en el uso de la tecnología en línea. Este artículo examina los indicadores que caracterizan la autenticidad y el engaño en el *ransomware* y el *phishing*. Una encuesta realizada a personas mayores australianas de más de 65 años revela marcadores y patrones que ayudan al usuario a determinar el probable engaño utilizando habilidades no cibernéticas. El artículo esboza un marco derivado de la gramática y la sintaxis para ayudar a los usuarios mayores en la capacidad y la conciencia de reconocer los correos electrónicos fraudulentos.
Aspectos por destacar	
	Los adultos mayores cada vez más son blancos para ataques de *phishing* y *ransomware*. Cada vez más se trata de que los adultos mayores identifiquen correos maliciosos.
Calidad del estudio según revista publicada	



Validación de fuente

Tabla 17

Extracción fuente 9

Motor de búsqueda de artículos	IEEE DIGITAL LIBRARY
Título	Biometrics: Password replacement for elderly?
Publicación	2017 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2017
Autores	Eiman Ahmed; Brandon DeLuca; Emily Hirowski; Connor Magee; Ivan Tang; Jean F. Coppola
Referencia	E. Ahmed, B. DeLuca, E. Hirowski, C. Magee, I. Tang and J. F. Coppola, “Biometrics: Password replacement for elderly?” 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2017, pp. 1-6, DOI: 10.1109/LISAT.2017.8001958.
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	A medida que la tecnología sigue creciendo y avanzando a un ritmo rápido, la mayoría de los productores y empresas están descuidando un grupo demográfico bastante grande: las personas mayores. Las personas mayores, acostumbradas a medios de comunicación más tradicionales que utilizan el lápiz y el papel tienen dificultades para seguir el ritmo de la tecnología en la era moderna. La ciberseguridad, uno de los aspectos más vitales de la tecnología es un área del ciberespacio en la que las personas mayores tienen dificultades para adaptarse. Aunque entienden la necesidad de tener contraseñas para mantener segura su información privada, a menudo se frustran al recordar sus contraseñas, que pueden variar de

	un sitio *web* a otro y a menudo son extenuantes de recordar debido a los procedimientos reglamentarios de las contraseñas. El objetivo de este proyecto es investigar cómo puede abordarse este problema de forma sencilla utilizando la biometría. La biometría es la forma de autenticación más segura hasta la fecha, independientemente de la edad. En este estudio, se evalúa a los adultos mayores de los centros geriátricos con preguntas respecto a cómo gestionan actualmente las distintas contraseñas que crean para sus cuentas, cómo se sienten con sus métodos de gestión actuales y los métodos con los que creen que se puede mejorar su experiencia más de lo que ya es. Además, se comparan diferentes tecnologías biométricas, por ejemplo, la retina, la huella dactilar, el reconocimiento facial, etc. y se propone una solución del marco que sería gratuita para los adultos mayores.
Aspectos por destacar	
	Cómo proteger la identidad de las personas adultas mayores utilizando la biometría remplazando las contraseñas tradicionales.
Calidad del estudio según revista publicada	

2017 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2017

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Computer Science Artificial Intelligence Computer Science Applications Software Energy Renewable Energy, Sustainability and the Environment Physics and Astronomy Instrumentation		5

PUBLICATION TYPE	ISSN	COVERAGE
Conferences and Proceedings	-	2017

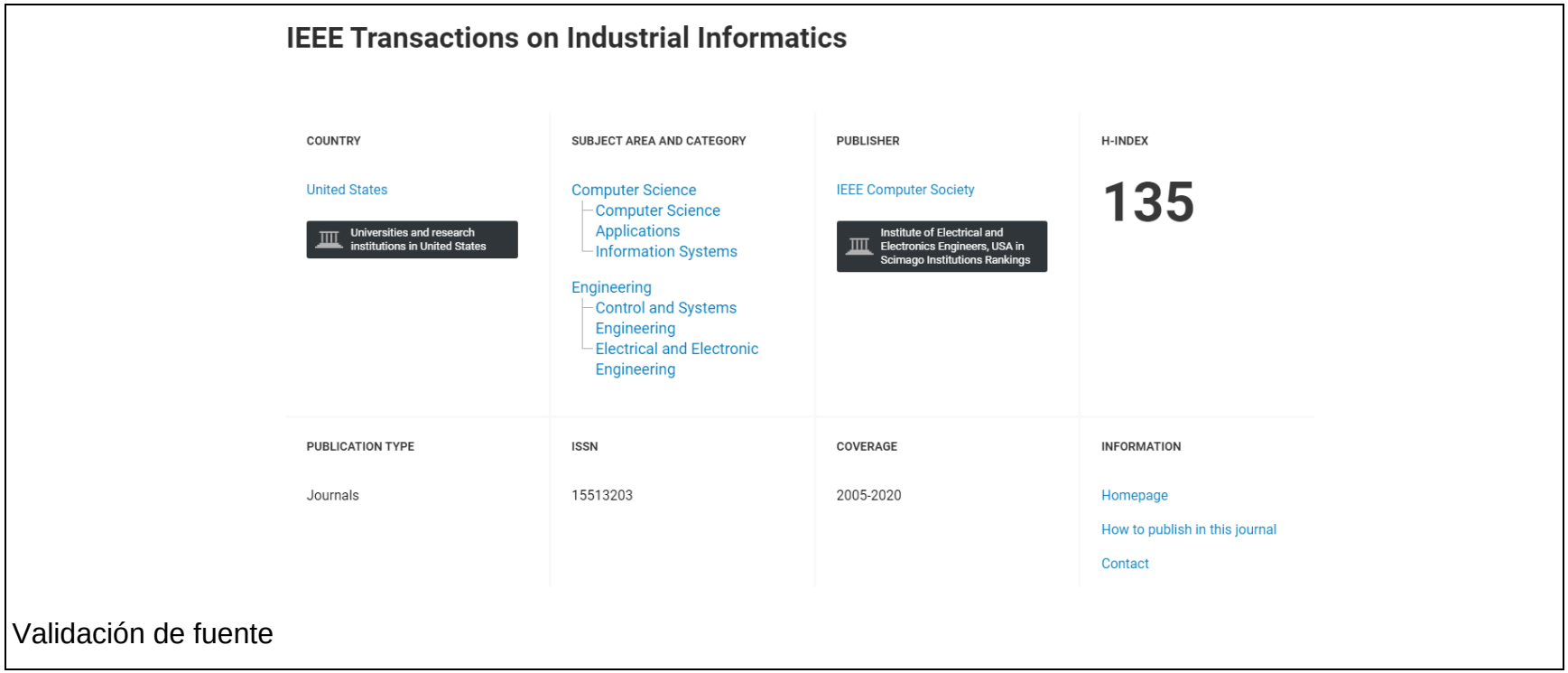
Validación de fuente

Tabla 18

Extracción fuente 10

Motor de búsqueda de artículos	**IEEE DIGITAL LIBRARY**
Título	Establishing a Cybersecurity Home Monitoring System for the Elderly
Publicación	IEEE Transactions on Industrial Informatics
Autores	Eiman Ahmed; Brandon DeLuca; Emily Hirowski; Connor Magee; Ivan Tang; Jean F. Coppola
Referencia	M. -Y. Chen, *Establishing a Cybersecurity Home Monitoring System for the Elderly,* in IEEE Transactions on Industrial Informatics, DOI: 10.1109/TII.2021.3114296.
Descripción	
Área	Ciberseguridad, Aspectos humanos y sociales de la seguridad y la privacidad
Resumen	Muchos países tienen poblaciones cada vez más envejecidas. Muchos de estos ancianos viven solos y de forma independiente, pero los que padecen enfermedades crónicas o discapacidades corren el riesgo de sufrir accidentes que requieran asistencia. Muchos de los sistemas de asistencia domiciliaria disponibles en el mercado ofrecen funciones de supervisión a distancia, pero estos sistemas requieren que alguien al otro lado de la conexión remota esté prestando atención. Esto plantea la necesidad de contar con sistemas inteligentes de monitorización del hogar que garanticen la vigilancia continua de la seguridad del usuario. Este artículo propone un sistema que utiliza la tecnología de balizas para evaluar el bienestar del sujeto basándose en la falta de movimiento, y que activa automáticamente las cámaras pre

	posicionadas y envía una alerta a los familiares o cuidadores en respuesta a una actividad potencialmente de alto riesgo, como la activación de determinados aparatos de cocina. Sin embargo, el uso de estas cámaras plantea problemas de privacidad. Para mejorar la legibilidad de los objetos y la privacidad, nuestra investigación utiliza el aprendizaje federado para mejorar la legibilidad de las RCNN rápidas. El enfoque presentado almacena la información personal de los ancianos en el servidor local, lo que evita revelar la información de su hogar y garantiza la seguridad de la transmisión de datos mediante la protección de la privacidad. El artículo ha demostrado su viabilidad y practicidad mediante la realización de un experimento; el sistema puede funcionar en la asistencia sanitaria a domicilio.
Aspectos por destacar	
	Cómo proteger la identidad de las personas adultas mayores mediante la biometría al reemplazar las contraseñas tradicionales
Calidad del estudio según revista publicada	



Validación de fuente

1.9.2.2. Ejecución de la selección en la fuente utilizando el motor ACM digital Library. En el siguiente apartado se detalla la información.

1.9.2.2.1. Selección de estudios iniciales. Siguiendo las recomendaciones provistas por Blanco *et al.* (2007) se lleva a cabo la búsqueda de estudios iniciales de la siguiente manera. Búsqueda basada en los siguientes parámetros:

- Cybersecurity.
- Older Adults.
- Senior Citizens.
- Older Persons.
- Cyber Attacks.

Después de realizar las búsquedas con los parámetros anteriores se encontraron dos resultados, de los cuales uno se seleccionó después de aplicar los métodos de exclusión sugeridos, principalmente porque no prestaron la atención a las alternativas o no profundizaron en los problemas de seguridad en Internet de las personas mayores, además de todos aquellos que sean muy antiguos. A continuación, se presenta su detalle.

Tabla 19

Estudios que se encontraron ACM digital library

#	Título	Autores	Año	URL
11	“Citizens Too”: Safety Setting Collaboration Among Older Adults with Memory Concerns	Nora Macdonald Helena M. Mentis	2021	https://dl.acm.org/doi/10.1145/3465217

1.9.2.2.2. Extracción de información. Para extraer la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación se consideran los siguientes elementos:

Tabla 20

Extracción fuente 10

Motor de búsqueda de artículos	ACM DIGITAL LIBRARY
Título	“Citizens Too”: Safety Setting Collaboration Among Older Adults with Memory Concerns
Publicación	ACM Transactions on Computer-Human Interaction
Autores	Nora Macdonald; Helena M. Mentis
Referencia	ACM Transactions on Computer-Human InteractionVolume 28 Issue 5 October 2021 Article No.: 31pp 1–32 https://doi.org/10.1145/3465217
Descripción	
Área	Ciberseguridad, aspectos humanos y sociales de la seguridad y la privacidad
Resumen	El diseño de tecnologías que apoyen la ciberseguridad de los adultos mayores con problemas de memoria implica luchar con una incómoda paradoja entre la vigilancia y la independencia y la estrecha colaboración de las parejas. Esta investigación capta las interacciones entre parejas de adultos mayores en las que uno o ambos tienen problemas de memoria -característica principal del declive cognitivo-a medida que toman decisiones sobre cómo salvaguardar sus actividades en línea utilizando una sonda de configuración de seguridad que diseñamos, y en el transcurso de varias entrevistas informales y un estudio de diario. En todo momento, las parejas demostraron una mentalidad de colaboración a la que aplicamos un marco de ciudadanía en la colaboración de código abierto, concretamente(a) historias de participación (b), menores

	barreras a la participación y (c) mantenimiento de la contribución continua. En esta metáfora de empresa colaborativa, un socio (o miembro de la pareja) puede ser el proveedor de servicios y el otro puede ser el participante, pero en distintos momentos, pueden cambiar los papeles sin dejar de mantener un enfoque colaborativo para preservar los activos compartidos y la libertad en Internet. Concluimos con un debate sobre lo que esta mentalidad de proveedor de servicios-contribuyente significa para el empoderamiento a través de la ciudadanía, y las implicaciones para la ciberseguridad de las poblaciones vulnerables.
Aspectos por destacar	
	Cómo proteger a los adultos mayores con problemas de memoria que pueden tener grandes implicaciones en delitos informáticos
Calidad del estudio según revista publicada	

ACM Transactions on Computer-Human Interaction

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Computer Science └ Human-Computer Interaction	Association for Computing Machinery (ACM)	90

PUBLICATION TYPE	ISSN	COVERAGE	INFORMATION
Journals	10730516, 15577325	1994-1995, 1997-2020	Homepage How to publish in this journal Contact

Validación de fuente

1.9.3. Resumen de los resultados. Como parte del proceso de selección de resultados, como se muestra en la Tabla 17, se analizaron 27 estudios, de los cuales 14 se identificaron como relevantes, con base en su contenido, número de referencias, año de publicación y calidad. Después de un proceso de refinamiento se seleccionaron 11 artículos, para los cuales se siguió el proceso de ejecución de la selección que se detalló en el apartado anterior.

Tabla 21

Análisis de resultados

Fuente	Encontrados	Filtrados	Seleccionados
Google Scholar	15	8	7
IEEE	7	3	3
ACM	5	2	1
Total	27	14	11

Capítulo II. Marco conceptual

Con el objetivo de identificar los conceptos más relevantes mencionados en cada uno de los artículos que se encontraron en la sección 1.9 Estado de la cuestión, se genera una nube de conceptos representados en la Figura 7. Esta nube se elaboró al unir todos los artículos y procesarlos con la herramienta nube de palabras.

Figura 1

Nube de palabras generada

Fuente: https://www.nubedepalabras.es

A continuación, se presentan las definiciones de la mayoría de los conceptos mencionados y más relevantes para la investigación. Cabe señalar que, para comprender mejor el tema en discusión, el orden de los conceptos presentados va desde aspectos generales hasta específicos para entender diversos elementos que se relacionan con la ciberseguridad para las personas adultas en edad laboral madura y personas adultas mayores con alfabetización digital.

2.1. Conceptos sobre contenido

A partir de los conceptos que se encontraron se lleva a cabo un mapa conceptual para dar sentido a cada una de las palabras encontradas que se relacionan con el objetivo central del trabajo.

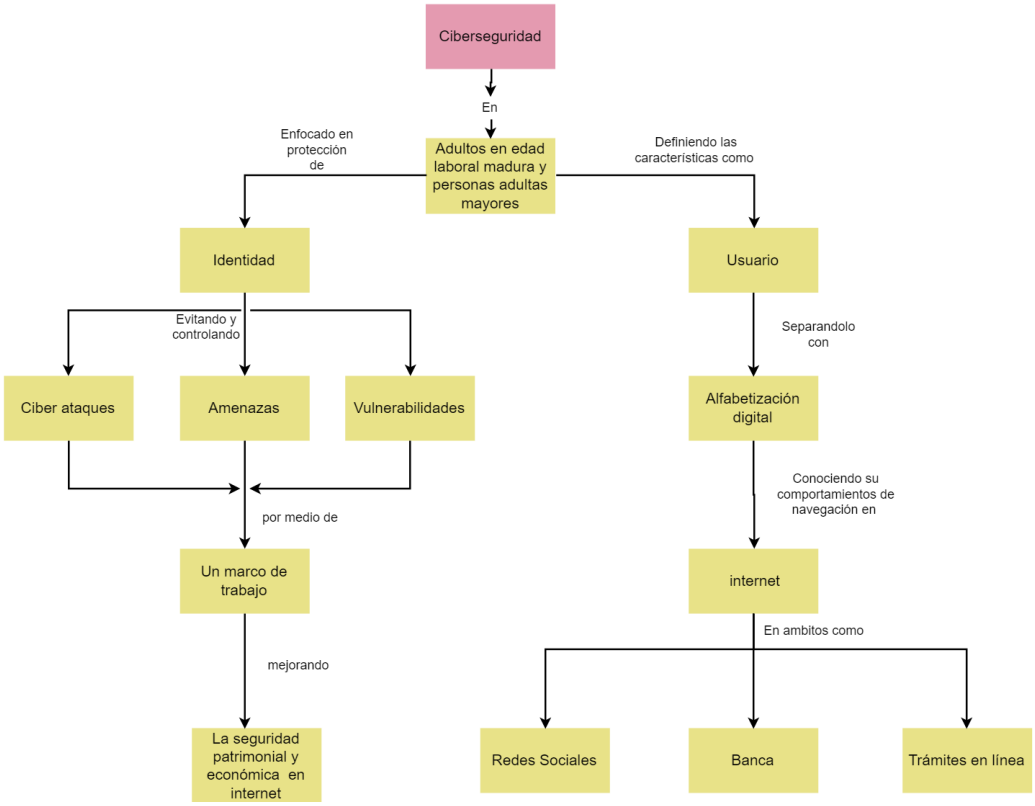


Figura 2

Mapa conceptual de ciberseguridad en adultos en edad laboral madura y personas adultas mayores

2.1.1. Ciberseguridad. La ciberseguridad se define como la: “Práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o interrumpir la continuidad del negocio” (Cisco, 2020, s. p.). La ciberseguridad, además, incluye una serie de metodologías, estrategias y tecnologías para proteger a las personas de amenazas actuales y es un punto de partida para lo que vendrá en el futuro. Según el estudio de Kaspersky (2021), la seguridad informática puede dividirse en algunas categorías comunes, las cuales son:

- La seguridad de red.
- La seguridad de aplicaciones.
- La seguridad de la información.
- La seguridad operativa.
- La recuperación de desastres y la continuidad del negocio.
- La capacitación del usuario final.

2.1.2. Adulto mayor. Según la Organización Mundial de la Salud (OMS), los adultos mayores son todas las personas que sobrepasen los 60 años de vida, es decir, que están en la etapa de la vejez. De acuerdo con el II informe del estado de la situación de la persona adulta mayor (2018):

> En Costa Rica, la legislación señala los 65 años como la edad a partir de la cual una persona se considera adulta mayor y la edad de la jubilación en el sistema que comprende la mayor cantidad de personas es de 65 años. Además de lo legal, hay distintas medidas que pueden tomarse en cuenta para trazar esta línea divisoria entre las edades. Algunas de las más usadas son la esperanza de vida, la edad promedio de jubilación y los cambios de las posibilidades de vida autónoma (s. p.).

2.1.3. Usuarios. Un usuario es cualquier persona que utilice un producto o un servicio de forma habitual. En el caso de la informática los usuarios habitualmente utilizan determinados programas, aplicaciones y sistemas del dispositivo, ya sea una computadora o un teléfono inteligente. Los usuarios de Internet pueden crear y acceder a cuentas de correo electrónico y plataformas de redes sociales mediante la creación de las cuentas de usuario.

2.1.4. Jubilación. La Real Academia Española (2021) define jubilación como: “Derecho de descanso de quien, alcanzada una determinada edad y después de trabajar un cierto número de años, abandona su vida laboral activa y pasa a asumir la condición de pensionado, previo cumplimiento de los requisitos legalmente” (s. p.).

En Costa Rica, según la Ley Nacional de Pensiones 7302, para recibir una pensión por invalidez, vejez y muerte (IVM), los trabajadores deben realizar al menos 300 aportes y tener 65 años. Para las mujeres, si tienen 59 años y 11 meses y han pagado 450 cuotas, los hombres deben tener 61 años y 11 meses y tener 462 cotizaciones. Si una persona no cumple con los requisitos de 300 cuotas, siempre que haya pagado al menos 180 cuotas puede optar por una pensión proporcional. Los fondos de pensiones también pueden posponerse. La pensión depende de la duración del periodo total de cotización y de los ingresos medios.

2.1.5. Internet. El concepto de Internet se puede definir como:

> A globally connected network system facilitating worldwide communication and access to data resources through a vast collection of private, public, business, academic and government networks. [Sistema de red conectado globalmente que facilita la comunicación mundial y el acceso a recursos de datos a través de una vasta colección de redes privadas, públicas, empresariales, académicas y gubernamentales] (Techopedia, 2021, s. p.).

El Internet se administra por instituciones como la Agencia de Asignación de Número de Internet (o IANA) que establece un protocolo común. Los términos Internet y *world wide web* a menudo se usan indistintamente, pero no son lo mismo; Internet se refiere al sistema de comunicación global, incluidos el *hardware* y la infraestructura y la *web* es uno de los servicios que se comunican a través de Internet.

2.1.6. En línea (on-line). El concepto se utiliza en el ámbito de la informática para nombrar a algo que está conectado o a alguien que usa una red, generalmente, Internet. Por otro lado, las personas que están en línea son personas a las que se puede contactar a través de la *Web* o personas que desarrollan tareas virtuales.

2.1.7. Ciberataque. Ciberataque se define como: “A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks” [Un ciberataque es la utilización no autorizada y deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología]” (Techopedia, 2021, s. p.). Los ataques cibernéticos o ciberataques pueden utilizar código malicioso para cambiar el código informático, la lógica o los datos de la computadora. Esto puede tener consecuencias devastadoras, poner en peligro los datos y provocar delitos informáticos, como el robo de información y de identidad.

2.1.8. Redes sociales. Las redes sociales se definen como: “Lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos” (Celaya, 2008, s. p.). En las redes sociales, ya sea por razones personales o comerciales, las conexiones de las personas con otras se expanden. Al principio, el propósito de usar las redes sociales era hacer amigos, conectarse con personas desconectadas a largo plazo y reuniones de escuelas, colegios y universidades. En la actualidad, las redes sociales tienen un papel más amplio, son otra forma de comunicación y, lo más importante, una manera de hacer negocios.

2.1.9. Ciberamenaza. Las ciberamenazas o amenaza digital se puede definir como: “Un acto malicioso que busca hacer daño a datos, robar datos, o afecta la vida digital en general. Los ciberataques incluyen amenazas cómo virus, brechas de datos, ataques DDoS, entre otros” (Poggi, 2018, s. p.). Poggi (2018) indica que las amenazas se pueden dividir en tres categorías principales, las cuales son:

- Ganancia financiera.
- Disrupción digital.
- Espionaje.

2.1.10. Vulnerabilidad. Una vulnerabilidad puede referirse a la incapacidad de resistir cuando ocurre una amenaza o la incapacidad de recuperarse después de un desastre. En el mundo informático una vulnerabilidad se define como:

> Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack [Vulnerabilidad es un término de ciberseguridad que hace referencia a un fallo en un sistema que puede dejarlo expuesto a un ataque] (Techopedia, 2021, s. p.).

Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema informático, en un conjunto de procedimientos o en cualquier elemento que deje la seguridad de la información expuesta a una amenaza.

2.1.11. Alfabetización digital. La alfabetización digital se define como:

Un camino que implica adquirir una serie de destrezas básicas de manejo de equipos y programas, lenguas y nuevas formas de comunicación, y que si bien es una parte sustantiva, no equivale a la idea de ciudadanía digital, la cual significa contemplar, además, desde una visión más macro, que este tipo de aprendizaje se encuentra en permanente construcción y que incorpora a nuestros comportamientos y actitudes respecto a las nuevas tecnologías y, al mismo tiempo, a nuestros derechos y obligaciones (Unesco, 2020, s. p.).

Es posible indicar entonces que la alfabetización digital permite tener la capacidad para realizar diferentes tareas en un entorno digital. Esta definición general incluye muchos matices, como la capacidad de utilizar la tecnología para localizar, investigar, analizar información y desarrollar contenidos como soluciones a través de medios digitales.

2.1.12. Marco de trabajo (Framework). Un marco de trabajo o *framework* se define como: “Un conjunto de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar” (Pérez, 2021, s. p.). Por lo tanto, es posible establecer que un marco de trabajo sirve de base para tratar tipos específicos de problemas, utilizando un conjunto de buenas prácticas, conceptos y criterios para resolverlos.

2.1.13. Sistema financiero. Un sistema financiero se define como: “Conjunto de instituciones (entidades financieras y gubernamentales), medios (activos financieros) y mercados que hacen posible que el ahorro (dinero ocioso) de unos agentes económicos vaya a parar a manos de los demandantes de crédito” (Economipedia, 2021, s. p.).

2.1.14. Suplantación de identidad. Según el Diccionario de la Real Academia Española (2021) se define suplantar como: “Falsificar un escrito con palabras o cláusulas que alteren el sentido que antes tenían u Ocupar con malas artes el lugar de alguien, defraudando el derecho, empleo o favor que disfrutaba” (s. p.). La suplantación de identidad es una actividad malintencionada que consiste en hacerse pasar por otra persona para diferentes motivos, por ejemplo, cometer algún tipo de fraude u obtener datos ilegalmente. El Código Penal costarricense en la sección VIII, en el artículo 230 establece que: “Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información”.

2.1.15. Estafa informática. La Real Academia Española (2021) define estafa informática como un: “Delito de estafa que se comete por medios informáticos” (s. p.). Es decir, una estafa informática es una manipulación ilegal de información, con el fin de obtener ganancias indebidas mediante la creación de datos falsos o la modificación de los datos en procesos contenidos dentro de sistemas informáticos. En el Código Penal costarricense en la Sección IV, artículo 217 bis indica que:

> Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule e influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

2.1.16. Edad laboral madura. Para efectos de la presente investigación, se define adulto en edad laboral madura como todas aquellas personas mayores de 50 años y menores de 65 que están en su recta final laboral, cerca de su jubilación. Aunque no hay una definición de este rango poblacional en Costa Rica, se utiliza como referencia los rangos de edades que usa el Organismo de Investigación Judicial, el cual es una fuente principal de información presente en el trabajo.

Capítulo III. Marco metodológico

3.1. Tipo de investigación

La presente propuesta plantea objetivos que son de interés para la Asociación Gerontológica Costarricense, lo cual genera que la investigación corresponda al tipo aplicada.

3.2. Alcance investigativo

La presente propuesta considera el alcance investigativo exploratorio y descriptivo, según se justifica a continuación.

3.2.1. Exploratorio. Se toma como referencia la definición de Vargas (2004) sobre investigación con alcance investigativo exploratorio, quien indica: “Tiene por objetivo esencial familiarizar al investigador con un tema no abordado antes, novedoso o escasamente” (s. p.). Para el tema seleccionado y a partir de la información identificada en el apartado 1.9 Estado de la cuestión, se identifica que, para el caso de Costa Rica, no se encuentra información de referencia de investigaciones previas, por lo tanto, es un tema novedoso o estudiado escasamente.

3.2.2. Descriptivo. Se toma como referencia la definición de Vargas (2004), quien define una investigación con alcance investigativo descriptivo como: “Este tipo de estudio busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis” (s. p.). En el apartado 1.6 Objetivos, se identifican caracterizaciones y perfiles de personas como parte del análisis que se plantea en la presente investigación.

3.3. Enfoque

Se trabaja con un abordaje con enfoque alternativo. Al respecto se pueden mencionar las dimensiones fundamentales de la investigación para el presente estudio.

3.3.1. Dimensión ontológica o conceptualización. Esta se define a continuación.

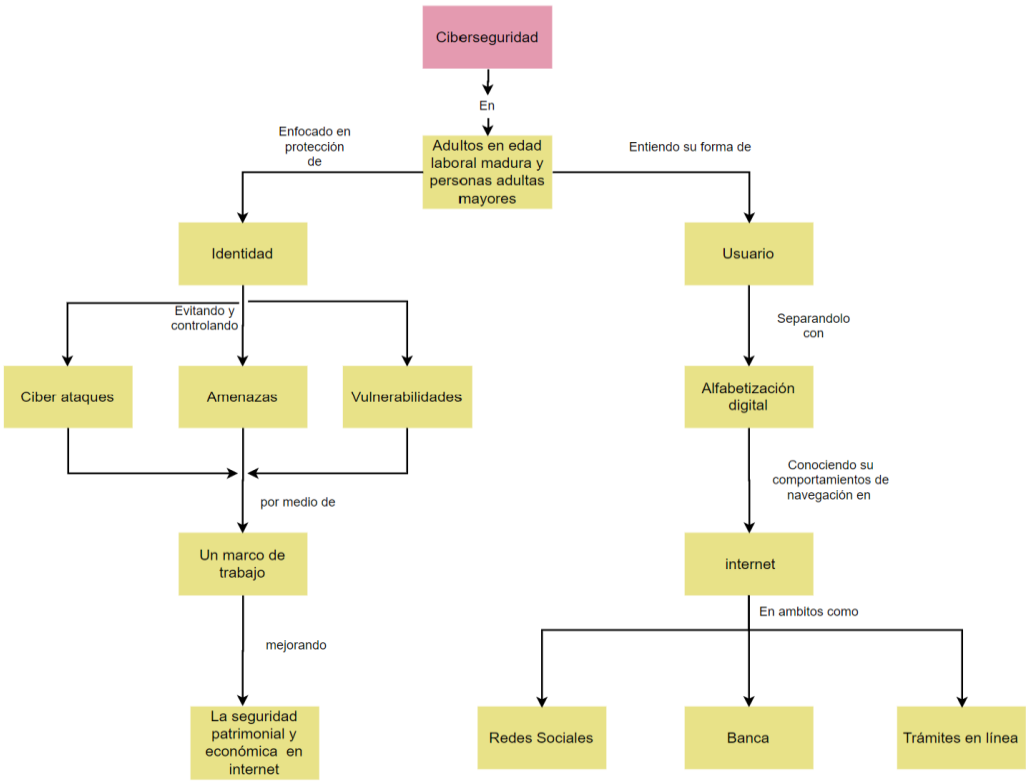


Figura 3

Mapa conceptual

3.3.2. Dimensión epistemológica. A partir de la información que se recopiló en el apartado 1.9 Estado de la cuestión y la aplicación de instrumento a la población de muestra con la ayuda de Ageco, se busca identificar la situación en Costa Rica para las necesidades que son objeto de la presente investigación y que fundamentan la propuesta.

3.3.3. Dimensión axiológica. Como herramienta de evaluación se plantean las siguientes métricas con el objetivo de establecer pesos cuantitativos a los factores incluidos como parte de los objetivos que se plantearon en el apartado 1.6, para los siguientes aspectos:

Tabla 22

Evaluación de criterios para mejorar la seguridad en Internet, aplicada a población atendida por Ageco

Criterio	Peso relativo evaluación
Reconocimiento de características para un sitio *web* oficial relacionado con afectación financiera y afectación de bienes muebles.	15
Uso de autenticación que permite la protección de identidad.	15
Reconocimiento de datos personales, datos personales de acceso restringido, datos personales de acceso irrestricto y datos sensibles.	15
Tratamiento de correos electrónicos de origen desconocido	5
Uso de medios de pago electrónicos en Internet que no sean tipo débito y que cuenten con seguro	10
Uso de navegadores *web* con almacenamiento de historial	5
Uso de sitios *web* que requieren uso de *cookies*	5
Uso de redes inalámbricas públicas o sin credenciales de acceso	10
Uso de actualizaciones para sistema operativo	5
Uso de antivirus y *antimalware*	10
Uso de perfil de usuario diferente a administrador	5

Tabla 23

Evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco

Criterio	Peso relativo evaluación
Ha recibido capacitación sobre uso de computadoras y *software*	10
Conoce lo que significa *estafa informática* según el Código Penal de Costa Rica	15
Conoce lo que significa *suplantación de identidad* según el Código Penal de Costa Rica.	15
Conoce las herramientas habilitadas por el gobierno costarricense para el proceso de autenticación de identidad digital	15
Conoce las principales técnicas para suplantación de identidad que utilizan los ciberdelincuentes	15
Conoce las principales técnicas para estafa informática que utilizan los ciberdelincuentes	15
Cuenta con canales de información sobre temas que permitan mejorar la seguridad en Internet	15

Tabla 24

Evaluación de criterios protección de identidad digital, aplicada a población de muestra atendida por Ageco

Criterio	Peso relativo evaluación
Identifica la importancia de la protección de identidad digital y cómo protegerla	20
Realiza gestión de contraseñas	20
Conoce qué es firma digital	20
Restringe el uso de datos personales de acceso restringido y datos personales sensibles incluidos en redes sociales	10
Uso de autenticación con factores biométricos	10
Uso de doble factor de autenticación	20

Para las tablas de evaluación se plantean los siguientes criterios para determinar el nivel de riesgo presente:

- 0 a 40: Riesgo alto.
- 41 a 80: Riesgo medio.
- 81 a 100: Riesgo bajo.

3.4. Diseño

Se considera el uso de la metodología de ciencia de diseño a partir de la aplicabilidad para los alcances que se plantearon en el punto 1.7.1 del presente documento.

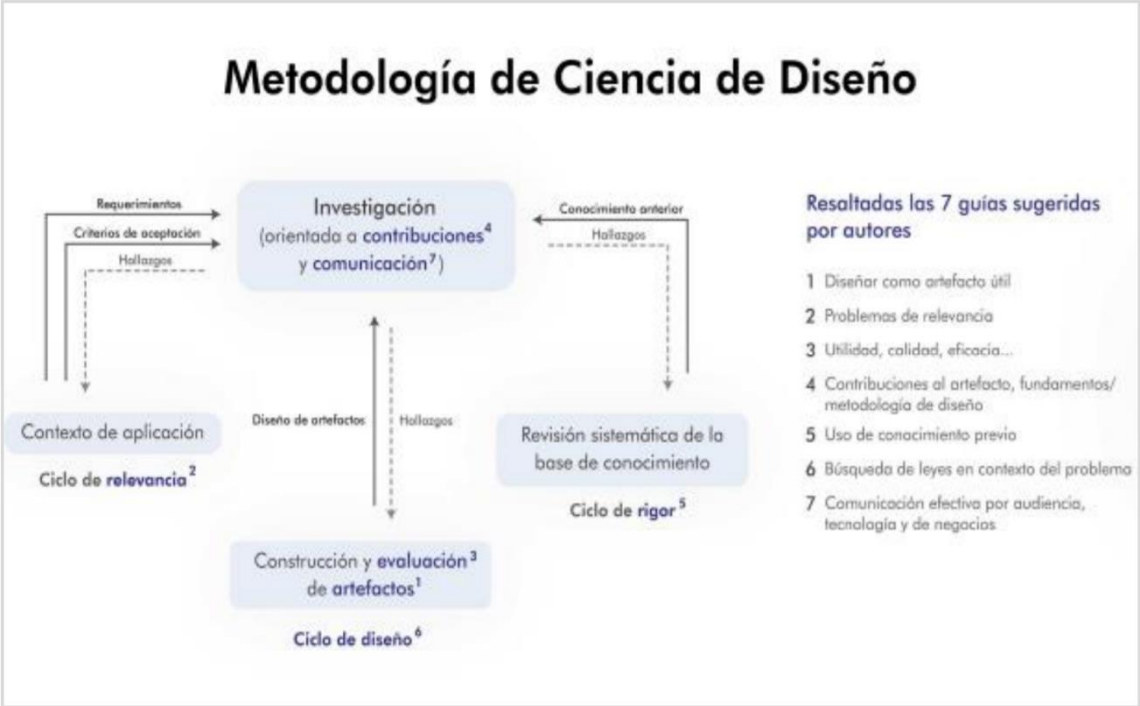


Figura 4

Esquema de ciencia de diseño

Fuente: Adaptación de Hevner y Park (2004) para lecciones impartidas por el tercer autor.

Se identifica cada una de las partes del ciclo para la metodología de diseño, según su contextualización aplicada:

3.4.1. Contexto de aplicación. Asociación Gerontológica Costarricense (Ageco), donde se consideran las personas en edad laboral madura y las personas adultas mayores, a las cuales por medio del cliente se cuentan como parte de la muestra de trabajo.

3.4.2. Construcción y evaluación de artefactos. Los elementos son:

- Tabla de resultados de evaluación de criterios para mejorar la seguridad en Internet, aplicada a la población de muestra atendida por Ageco.
- Tabla de resultados de evaluación de criterios en medición de alfabetización digital, aplicada a la población de muestra atendida por Ageco.

- Tabla de resultados de evaluación de criterios de protección de identidad digital, aplicada a la población de muestra atendida por Ageco.
- Propuesta de marco de trabajo para mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.

3.4.3. Revisión sistemática de la base de conocimiento. Información incluida como parte del apartado 1.9 del estado de la cuestión del presente documento.

3.5. Población y muestreo

A partir de la población a la cual se tiene acceso con el cliente se plantea un criterio de conveniencia por disponibilidad de personas en el segmento de edad definido, un grupo como muestra para la presente investigación por definir en conjunto según disponibilidad de Ageco. Lo anterior para dar validez a los hallazgos del presente estudio.

3.6. Instrumentos de recolección de datos

Arias (2016) indica que: “Se entenderá por técnica de investigación, el procedimiento o forma particular de obtener datos o información” (s. p.). Además, el mismo autor indica que: “Un instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información” (Arias, 2016, s. p.).

Para la recolección de datos se plantea una metodología de *user research*, la cual se define como: “Un conjunto de técnicas de observación y obtención de feedback y análisis de resultados que permiten entender los comportamientos, necesidades y motivaciones de los usuarios de cualquier producto o servicio” (Álvarez, 2016, s. p.). En esta metodología existen diferentes métodos de recolección, según la naturaleza de la investigación realizada se definen dos para la aplicación en el desarrollo del proyecto, las cuales son entrevistas y encuestas.

3.6.1. Entrevistas. Como parte de la estrategia de investigación para obtener datos se plantea realizar entrevistas a representante del Organismo de Investigación Judicial, a representante del Registro Nacional de la Propiedad, a experto en ciberseguridad (con experiencia en los temas que se relacionan con delitos de suplantación identidad y estafa informática), a representante de la Oficina del Consumidor Financiero y a personal docente de la Asociación Gerontológica Costarricense. En todos los casos se busca identificar datos preliminares que reflejan la necesidad actual y sea insumo de información para una segunda etapa de entrevistas, donde a partir de la muestra de participantes asignada por Ageco se identifique la situación de la población objetivo.

Tabla 25

Entrevista para aplicar a representantes del Organismo de Investigación Judicial, relacionada con delitos de suplantación de identidad y estafa informática

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
¿Cómo funciona una investigación a partir de la denuncia?	• Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral
Línea de acción identificada para los delitos de estafa informática y suplantación de identidad considerando afectación patrimonial y económica	
Se identificó la diferenciación según rango de edad y alguna causa para tener la población adulta mayor como objetivo de ataques	
¿Por qué la población de 50 a 64 y más de 65 es más vulnerable?	
¿Cuánta relación han visto entre la alfabetización digital como vulnerabilidad para las víctimas de	

delitos por suplantación de identidad y estafa informática?	madura y personas adultas mayores, que cuentan con alfabetización digital.
¿Cómo han visto que influye la suplantación de identidad como punto base para los delitos investigados?	
Recomendaciones para la población en edad laboral madura y población adulta mayor, cuáles serían con base en la experiencia como investigadora	
Los rangos de edad responden a algún criterio para establecerse en el resumen de información de denuncias	
¿Cuáles dispositivos son los que se identifican con mayor incidencia de ataques?	
¿Cuáles sistemas operativos han identificado con mayor incidencia de ataques?	
¿Las personas en edad laboral madura o adultos mayores han sido afectados por miembros de su familia o por terceros por acceso a información personal?	

Tabla 26

Entrevista para aplicar a representante del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
¿Cómo funciona el vector de ataque para estafas a bienes inmuebles a partir de la información *web* que el registro tiene disponible como pública?	• Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.
¿Tienen algún tipo de historia de este tipo de delitos?	
¿Cómo proceden con las investigaciones de estafas que se relacionan con bienes inmuebles?	
¿Por qué la población de 50 a 64 y más de 65 es más vulnerable?	
¿Han encontrado bases de datos de propiedades y sus propietarios que hayan sido insumos para estafas?	
¿Se han visto casos en los que un notario pueda suplantar su identidad para que por ese medio se cometa el delito de estafa con bienes inmuebles?	
¿Se han encontrado estafas con bienes muebles (por ej.: carros) utilizando como insumo la información disponible en línea del registro de la propiedad??	
A pesar de que la información de propiedades es pública, ¿Cómo se recomienda prevenir este tipo de estafas?	

Tabla 27

Entrevista para aplicar a experto en ciberseguridad, con experiencia en los temas que se relacionan con delitos de suplantación de identidad y estafa informática

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
1. ¿Se identifica a partir de su experiencia una afectación mayor para personas mayores a 50 años, respecto a los otros grupos de población en Costa Rica? 2. ¿Cuál consideran es la mayor vulnerabilidad que aprovechan los delincuentes? 3. ¿Cuáles son las técnicas que según su experiencia utilizan los atacantes con mayor frecuencia? 4. ¿Qué afectación económica estimaría representan los delitos de suplantación de identidad y estafa informática anualmente en Costa Rica? 5. ¿Considera que existe relación entre la alfabetización digital y la mayor posibilidad de ser objetivo de un delito como suplantación de identidad o estafa informática? 6. ¿Qué importancia considera tiene la protección de identidad, como prevención para delitos de suplantación de identidad y estafa informática?	• Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.

7. ¿Cuáles recomendaciones daría a partir de su experiencia para la población de 50 años en adelante, para evitar ser víctimas de delitos de suplantación de identidad y estafa informática	

Tabla 28

Entrevista para aplicar al representante del Registro Nacional de Costa Rica, relacionada con delitos a patrimonio o bienes

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
1. ¿Cuáles gestiones a partir de medios de tecnología de información tiene habilitado el Registro Nacional para que realicen sus usuarios? 2. ¿Cómo se valida la identidad digital de los usuarios, tanto para consultas de información como para los trámites que se encuentren habilitados? 3. ¿Se lleva a cabo un tratamiento especial para datos que se relacionan con adultos mayores, tanto usuarios como adultos mayores como propietarios? 4. Relacionado con los trámites de bienes inmuebles y muebles, consultar ¿cuáles gestiones pueden realizar los notarios por medios digitales en los sistemas del Registro Nacional?	• Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.

5. En cuanto a la autenticación de identidad, ¿Cuáles son los mecanismos habilitados para los notarios con el objetivo de realizar las gestiones que tienen habilitadas? 6. Relacionado con el servicio que brinda el Registro Nacional de alerta registral, conocer en qué consiste el servicio, con qué tipo de bienes se brinda y los costos asociados para los usuarios 7. Según legislación nacional, la información de bienes es pública, sin embargo, agradeceríamos conocer si el Registro Nacional a partir de las denuncias ante OIJ por estafas en bienes muebles e inmuebles ha producido recomendaciones para evitar afectación hacia los usuarios	

Tabla 29

Entrevista para aplicar al representante de la Oficina del consumidor financiero, relacionada con delito estafa informática

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
1. ¿Cuáles son los derechos del consumidor financiero? 2. Considerando la afectación financiera producto del delito de estafa informática, ¿Es responsabilidad de las entidades financieras contar con seguros que permitan a los usuarios recuperar su dinero, una vez demostrado su adecuado resguardo de información?	• Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.

3. ¿Existe algún tratamiento diferenciado para los casos que se relacionan con afectación financiera para personas mayores de 65 años, al ser víctimas del delito de estafa informática? 4. ¿La responsabilidad de demostrar el uso correcto y resguardo de los mecanismos de autenticación de usuario en sus servicios financieros por medio de facilidades *web*, corresponde al usuario, o bien corresponde a la entidad financiera demostrar el mal uso o resguardo por parte del usuario?	

Tabla 30

Entrevista para aplicar a docentes de la Asociación Gerontológica Costarricense

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
¿Cuál es la población en la que se centra la atención de Ageco?	• Definir las características de la población adulta en edad laboral madura y adulta mayor, atendida por la Asociación Gerontológica Costarricense. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad
¿En Ageco existen cursos en donde se haga énfasis en la seguridad de la navegación en Internet?	
De acuerdo con la población que atienden ¿Cuáles características tecnológicas de uso han notado?	
¿Cuál nivel de alfabetización digital notan dentro de la población que atienden?	
¿Cuáles técnicas utilizan para transmitir el contenido de los cursos que brindan a esta población?	

¿Cuáles son las características más importantes que ustedes identifican en esta población que ustedes atienden?	
¿Cuáles medios de comunicación son los que más utilizan ustedes para tener relación con las poblaciones que atienden?	
¿Cuáles recomendaciones nos pueden brindar por su experiencia en el momento de trabajar con esta población?	

Tabla 31

Entrevista para aplicar a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
¿Qué entiende por suplantación de identidad? ¿Tiene claro cuál información es importante proteger para evitar que suplanten su identidad? ¿Qué entiende por estafa informática? ¿Tiene claro cuál información es importante proteger para evitar que le hagan una estafa informática? ¿Tiene claro cuál información es importante proteger para evitar que le afecten financieramente o con sus propiedades?	• Definir las características de la población adulta en edad laboral madura y adulta mayor, atendida por la Asociación Gerontológica Costarricense. • Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. • Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital. • Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona

Cuando tiene que hacer un pago en Internet, ¿qué alternativa usa? ¿Cuáles antivirus utiliza en su computadora? ¿Cómo puede proteger su identidad en Internet? ¿Qué información usted no publica en redes sociales? ¿Cómo reconocer una página *web* real de una falsa? ¿Sabe cómo los delincuentes suplantan la identidad de las personas? ¿Conoce cómo los delincuentes hacen estafas informáticas en Internet? ¿Cómo reacciona cuando le tratan de solicitar información con urgencia por un riesgo o un beneficio para usted? ¿Sabe que el navegador *web* almacena los sitios que se han visitado? Cuando tiene un correo electrónico de un desconocido, ¿Qué hace? Cuando le aparecen ventanas emergentes en su navegador, ¿Qué hace? Cuando recibe una llamada solicitando confirmar sus datos, ¿Qué hace?	adulta mayor, en sitios que expongan su identidad. • Elaborar una propuesta de un marco de trabajo para optimizar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital.

Cuando recibe un correo o un mensaje con un *link* para que acceda, ¿Qué hace? En caso de detectar que le han suplantado su identidad, ¿Cómo procedería? En caso de detectar que le han estafado, ¿Cómo reaccionaría? ¿Conoce los canales de contacto que debe utilizar para plantear una denuncia con su entidad financiera?	

3.6.2. Encuestas. Arias (2016) define encuesta como: "Una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de sí mismos, o en relación con un tema en particular" (s. p.).

Una encuesta en *user research* como método es un cuestionario estructurado que su público objetivo completa generalmente mediante el llenado de un formulario. Las encuestas pueden variar en extensión y formato. Los datos se almacenan en una base de datos y la herramienta de encuesta, por lo general, proporciona algún nivel de análisis de los datos, además de ser revisados por un experto capacitado.

Tabla 32

Cuestionario para aplicar a adultos en edad laboral madura y personas adultas mayores con alfabetización digital

Preguntas de encuesta	Resultado esperado
1- ¿Qué información considera usted que es más importante proteger en Internet? a) Nombre completo, dirección y teléfono	● Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad. ● Preferencias de uso y entorno.

b) Correo electrónico, celular, datos bancarios c) Información de la salud, religión, fotos 2- Cuando tiene que hacer un pago en Internet, ¿Qué alternativa usa? a) Banca en línea b) Pago con tarjeta de crédito c) Pago con tarjeta de débito d) Sinpe Móvil e) Transferencias electrónicas f) Ninguna g) Otra. ___ 3- ¿Utiliza con frecuencia redes inalámbricas gratuitas en sitios públicos para navegar en Internet desde su dispositivo? a) Sí b) No 4- ¿Para navegar en Internet cuál es el dispositivo que utiliza más? a) Celular b) Computadora c) *Tablet* 5- ¿Cuál es el navegador que más utiliza para navegar en Internet? a) Chrome b) Firefox c) Edge d) otro. _____ 6- ¿Utiliza la misma contraseña para todos los sitios, correo y servicios que utiliza en Internet? a) Sí b) No 7- Cuando instala diferentes aplicaciones en el celular revisa los permisos de acceso, ¿Qué solicita la aplicación? a) Sí b) No 8- Cuando utiliza la computadora o el celular, ¿Se encarga de aceptar las actualizaciones del sistema operativo? a) Sí b) No	● Consideraciones para mejorar la seguridad. ● Alternativas para proteger la seguridad.

9- ¿Usted tiene los permisos necesarios para instalar programas en su computadora? a) Sí b) No 10- ¿Ha recibido algún curso de computación? a) Sí b) No 11- ¿Cada cuánto cambia sus contraseñas? a) Cada mes b) Cada 6 meses c) Cada año e) Nunca 12- Según las definiciones que se le presentan a continuación. ¿Cuál cree que es la definición correcta del delito de estafa informática? a) Cuando en perjuicio de una persona física o jurídica se manipulen o se influya en el procesamiento o resultado de datos de un sistema informático para obtener un beneficio indebido para sí mismo o para otra persona. b) Cuando una persona está tomando datos de un sitio *web*, los utiliza para realizar trámites o gestiones en nombre de otra persona en bancos o registro nacional. c) Cuando una persona física o jurídica consienta la manipulación o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema informático, pero valiéndose de algún documento físico entregado por la persona 13- Según las definiciones que se le presentan a continuación, ¿Cuál cree que es la definición correcta del delito de suplantación de identidad? a) Cuando una persona realiza gestiones a nombre de otra persona con su autorización para ayudar con trámites o movimientos bancarios	

b) Cuando una persona se hace pasar por otra, con el fin de obtener beneficios, de generar un fraude u ocasionar un daño. c) Cuando una persona presenta información de identificación de cédula de identidad que por las similitudes de fotografía coinciden con la persona dueña del documento de identificación. 14- ¿Por cuáles medios recibe información sobre recomendaciones para navegar seguro en Internet? a) Redes sociales b) Noticias en televisión o radio c) Familiares d) otro. _____ 15- ¿Tiene conocimiento de lo que es firma digital? a) Sí b) No 16- ¿Cuál de estos medios de doble factor de autenticación utiliza? a) Huella digital b) Facial c) Token o tarjeta dinámica d) Ninguno e) Otro 17-Según la imagen anterior de acuerdo con lo visto en la página *web*, ¿Considera usted que esa página es falsa o verdadera? (Esta pregunta se montará en la herramienta con una imagen de una página falsa para ver si pueden identificar algo y reconocer si es falsa o no) a) Es real b) Es falsa 18- ¿De la imagen de correo electrónico anterior puede reconocer si es falso o verdadero? (Esta pregunta se montará en la herramienta con una imagen de una página falsa para ver si pueden identificar algo y reconocer si es falsa o no) a) Es real b) Es falso	

19- ¿Tiene conocimiento de qué son las *cookies* en una página *web*? a) Sí b) No 20- ¿Tiene conocimiento de las medidas que ofrece el gobierno para ayudar a la población para responder a ataques de estafa informática y suplantación? a) Sí b) No 21- ¿Qué característica cree usted que pueda identificar por parte de un estafador si usted es víctima de un delito de estafa? a) Tono de voz b) Sentido de urgencia c) Hacerlo sentir querido d) Forma de hablar e) Otra. _____ 22- ¿Tiene conocimiento sobre cómo es el procedimiento de denuncia por temas de estafa informática y suplantación en el Organismo de Investigación Judicial? a) Sí b) no	

3.7. Técnicas de análisis de información

Se elabora un mapa conceptual para explicar la metodología que se utiliza para la recolección y análisis de datos, explicando cómo cada una brindará información importante para cubrir un área específica en el planteamiento de la propuesta.

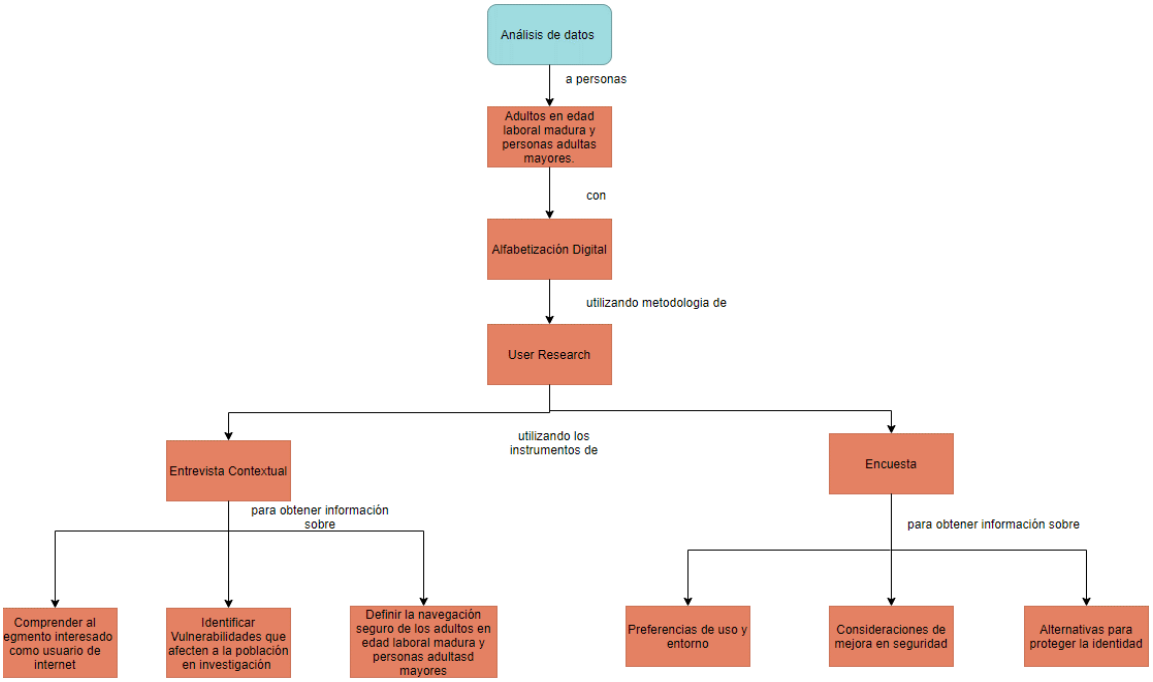


Figura 5

Mapa conceptual que explica la metodología que se utiliza para la recolección y análisis de datos

3.8. Estrategia de desarrollo de la propuesta

En relación con los objetivos específicos que se plantearon se presentan las siguientes estrategias para su desarrollo:

Tabla 33

Estrategia de desarrollo de la propuesta según objetivos específicos

Objetivo específico	Estrategia para el desarrollo
Definir las características de la población adulta en edad laboral madura y adulta mayor, atendida por la Asociación Gerontológica Costarricense.	Entrevista con personal de Ageco para identificar características de la población adulta en edad laboral madura y población adulta mayor, atendida por Ageco.

Definir en qué consiste mejorar la seguridad en Internet para personas adultas en edad laboral madura y personas adultas mayores, considerando la protección de su identidad.	Entrevistas y cuestionarios utilizando la técnica de *user research*, para generar una serie de recomendaciones enfocadas en las 5 funciones del marco de trabajo donde se define una mejor seguridad en Internet en la protección de la identidad.
Identificar las vulnerabilidades que afectan la identidad para personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital.	Entrevistas y cuestionarios utilizando la técnica de *user research* para generar la Tabla 39, Capítulo 5
Comprender las características como usuario en Internet de la persona adulta en edad laboral madura y la persona adulta mayor, en sitios que expongan su identidad.	Entrevistas y cuestionarios utilizando la técnica de *user research* para generar la Tabla 40, Tabla 41 y Tabla 42, Capítulo 5.
Elaborar una propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuentan con alfabetización digital	Se plantea una matriz que considere en sus columnas: delito, función, afectación, categoría y subcategorías. En sus filas se incluye la información relacionada con los delitos de estafa informática y suplantación de identidad, considerando afectación patrimonial bienes inmuebles, así como afectación económica por servicios financieros. La información contenida resumirá la que se recopiló y aportaron los autores producto de la presente investigación.

Capítulo IV. Análisis del diagnóstico

4.1. Aplicación de entrevistas a expertos

Como parte del proceso de análisis de la información y junto con la información que se recopiló en el Capítulo 2, tras la aplicación de los instrumentos de recolección de datos, se obtuvieron los siguientes resultados.

4.1.1. Aplicación de entrevistas a representantes del Organismo de Investigación Judicial. A continuación, se detallan las entrevistas aplicadas a los representantes del OIJ.

4.1.1.1. Entrevista aplicada a Genivieve Segura Robles. Se llevó a cabo una entrevista a la señora Genivieve Segura, quien es parte de la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial. A continuación, se presentan las respuestas obtenidas:

Tabla 34

Respuestas a entrevista con Genivieve Segura de la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial

Preguntas realizadas en la entrevista	Respuestas Genivieve Segura
¿Cómo funciona una investigación a partir de la denuncia?	Todo depende del tipo de delito, aquí en el OIJ se tiene una atención preferencial en las cual hay que atender de inmediato a la persona adulta mayor. Una vez realizada la denuncia se procede a realizar la investigación, primero se hace una entrevista con la persona y recopilación de pruebas de cómo surgió el delito y de acuerdo con esa información recopilada vemos hasta donde podemos llegar nosotros, todo depende del tipo del delito. Se dan muchas denuncias de que pierden el acceso a sus cuentas de redes sociales ese tipo de delito se llama violación de las comunicaciones electrónicas.

¿Han identificado alguna línea de acción para los delitos de estafa informática y suplantación de identidad considerando afectación patrimonial y económica?	En el caso de estafa le corresponde a la sección de FRAUDES, sin embargo, en la parte de suplantación si nos encargamos nosotros. Los delitos que se dan de suplantación funcionan de dos maneras, la primera donde suplantan la identidad con la intención de poder ingresar a las cuentas bancarias y la segunda para hacerse pasar por la persona para solicitar dineros ayudas económicas entre otros timos para obtener dinero. En estos casos es complicado presentar pruebas porque ellos perdieron acceso a sus cuentas, aquí lo que se trata de hacer es tratar de recuperar la cuenta para ver direcciones IP y tratar de dar con el criminal, pero es complicado en muchas veces no nos han dado resultados.
¿Se identificó la diferenciación según rango de edad y alguna causa para tener la población adulta mayor como objetivo de ataques?	Tal vez por el hecho de que tiene menos relación con el dominio de las tecnologías, lo que ustedes me comentaban de alfabetización digital, sin embargo, este tipo de delitos afecta a toda la población en general y no en una en específica.
¿Por qué la población de 50 a 64 y más de 65 es más vulnerable?	En caso podría ser por no tener tanta malicia, sin embargo, no siempre es el caso, lo que sí se ha dado es que muchas personas en esta población denuncian situaciones que no son delitos.
¿Cuánta relación han visto entre la alfabetización digital como vulnerabilidad para las víctimas de delitos por suplantación de identidad y estafa informática?	En realidad no mucha, ya que a los delincuentes van por la persona que caiga en su forma de delinquir y no tanto en las características de la persona.
¿Cómo han visto que influye la suplantación de identidad como punto base para los delitos investigados?	En este caso es un inicio de la cadena para realizar el delito, primero empiezan con la suplantación de identidad en la cual aplican el delito de violación de las comunicaciones electrónicas, después se aprovechan de eso para estafar a terceros como les comentaba anteriormente ya sea tratando de ingresar a

	cuentas bancarias o pidiendo dinero a nombre de otra persona.
Nos puede dar algunas recomendaciones para la población en edad laboral madura y población adulta mayor, ¿Cuáles serían con base en la experiencia como investigadora?	La educación sobre estos temas en esta población es primordial. Hacerlos sentirse más cómodos y quitarles el miedo acerca de estos temas. Que sepan cuáles son los delitos y visibilizar más la población
¿Los rangos de edad responden a algún criterio para establecerse en el resumen de información de denuncias?	Esa información la manejan los de estadísticas dentro del OIJ
¿Cuáles dispositivos son los que se identifican con mayor incidencia de ataques?	Más que todo en teléfonos celulares
¿Cuáles sistemas operativos han identificado con mayor incidencia de ataques?	En este caso no es importante para nosotros el sistema operativo a menos que sean delitos de sabotaje
¿Las personas en edad laboral madura o adultos mayores han sido afectados por miembros de su familia o por terceros por acceso a información personal?	Sí, claro, se han dado casos en donde ayudantes se convirtieron en el actor de amenaza. Es aquí donde es importante tener algún tipo de prevención con las tarjetas que es donde más se han dado este tipo de casos.

4.1.1.2. Primera entrevista aplicada a Yorkssan Carvajal. Se llevó a cabo una entrevista al señor Yorkssan Carvajal quien se desempeña como jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionado con delitos de suplantación de identidad y estafa informática. A continuación, se presentan las respuestas obtenidas:

Tabla 35

Respuestas a entrevista con Yorkssan Carvajal de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos de suplantación de identidad y estafa informática

Preguntas realizadas en entrevista	Anotaciones a partir de respuestas de Yorkssan Carvajal
¿Cómo funciona una investigación a partir de la denuncia?	● Como política Institucional en OIJ se da una atención inmediata para una denuncia de un adulto mayor, para la atención inicial, no así para investigación del caso. Se entrevista el mismo día que la persona formula la denuncia. ● El fraude informático funciona por medio de la compra de bases de datos lícitas e ilícitas. Asimismo, se utiliza información de encuestas en actividades como ferias. Se ha detectado la venta de bases de datos en el sector financiero, por los mismos funcionarios bancarios. ● Los delincuentes no perfilan según rango de edad, lo que hacen es utilizar la base de datos inclusive reutilizando datos. ● La suplantación de identidad se atiende en Delitos Varios. Cuando la suplantación tiene un documento de por medio se atiende en el Departamento de Fraudes, dado que se convierte en falsedad ideológica. ● Se utilizan servicios telefónicos identificados a nombre de personas que no conocen del servicio activo a su nombre. Se menciona que los controles en el caso del operador ICE, hace que este tipo de eventos sean menos probable por lo que los casos identificados se dan con los otros operadores de servicios celulares. ● Se toma información de redes sociales
Línea de acción identificada para los delitos de estafa informática y suplantación de identidad considerando afectación patrimonial y económica	
¿Se identificó la diferenciación según rango de edad y alguna causa para tener la población adulta mayor como objetivo de ataques?	
¿Por qué la población de 50 a 64 y más de 65 es más vulnerable?	
¿Cuánta relación han visto entre la alfabetización digital como vulnerabilidad para las víctimas de delitos por suplantación de identidad y estafa informática?	
¿Cómo han visto que influye la suplantación de identidad como punto base para los delitos investigados?	
Recomendaciones para la población en edad laboral madura y población adulta mayor, ¿cuáles serían con base en la experiencia como investigador?	

¿Los rangos de edad responden a algún criterio para establecerse en el resumen de información de denuncias?	para cometer estafas convencionales. No es posible obtener información dado que las empresas como Facebook u otras no cumplen con convenios internacionales. ● Se confirma la página del Registro Nacional y Tribunal Supremo de Elecciones como fuente de información para estafas con afectación de bienes. Se presenta en la mayor parte de los casos con extranjeros que se encuentran fuera del país. No se encuentra relación hacia personas adultas mayores como afectación predominante. ● $8,000,000 USD se estima la afectación por ingeniería social y fraude informático, para el año 2021, con un aproximado de 300 denuncias mensuales en San José. Se basa en números enmascarados, cuentas destino no trazables, sitios *web* hospedados en el extranjero. ● Dentro de las variantes para estafa informática son para el año 2017 y 2018 las aplicaciones de acceso remoto al equipo. En el 2019 trabajaron la modalidad de correo para buscar restaurar claves en paralelo a llamadas telefónicas, buscando conocer datos de credenciales. ● Bajo acompañamiento de informáticos han desarrollado sitios falsos, utilizando enmascaramiento de los números telefónicos, con el objetivo de que por medio de un *link* el usuario ingrese credenciales de acceso. Es el caso de mayor recurrencia, para el año 2020, a la fecha. ● En las estafas realizadas sacan el dinero por medio de Sinpe, cajeros automáticos, etc. ● No se encuentra relación entre alfabetización digital y las víctimas, dado que igual se registran casos sin que el tener un alto nivel de alfabetización digital haya evitado que sean víctimas. Se
¿Cuáles dispositivos son los que se identifican con mayor incidencia de ataques?	
¿Cuáles sistemas operativos han identificado con mayor incidencia de ataques?	
¿Las personas en edad laboral madura o adultos mayores han sido afectados por miembros de su familia o por terceros por acceso a información personal?	

	identifican personas en diversos cargos y edades, nacionalidades que igualmente han sido víctimas. ● OIJ busca la prevención por medio de describir cómo proceden los estafadores, buscan capacitar como principal estrategia de prevención. ● Se detectan casos en cárceles nacionales como generadores de las estafas. ● Se identifica la modalidad actual de estafa informática como un delito en que se puede conciliar, que genera ganancia de hasta ₡20.000.000 diarios, no requiere *frentear* (personas designadas para estar de cara a la víctima), no requiere estar en sitio, etc. ● El nombre de firma digital lo usan para estafar, no así la solución técnica como suplantación de identidad. Se menciona el ejemplo de personas que buscan trabajo, como personas que han sido víctimas de estafa. Lo que se busca es por medio de una página falsa que las personas ingresen su información, así como el pago por el servicio que están solicitando cumplir. ● La recomendación de OIJ en caso de identificarse ser víctima de una estafa bancaria es comunicarse inmediatamente al banco, dado que son ellos los que pueden visualizar los movimientos y tomar acciones. ● Se mencionan casos con Fondo de Capitalización Laboral por medio de páginas falsas que buscan obtener cuentas de correo y claves. ● No se identifican suplantaciones de número telefónico para llamadas destino, solamente para llamadas entrantes de la víctima. ● Lo que buscan los delincuentes son bases de datos con datos de contacto de

	las víctimas, lo cual pagan con montos sumamente atractivos para los funcionarios que terminan vendiendo dicha información. ● El delito de estafa es concebido por los delincuentes como un delito blanco, donde el delincuente visualiza que no está haciendo un daño. ● Los delincuentes asumen que la mayoría de la población tienen sus accesos a cuentas bancarias en sus teléfonos móviles. ● La estructura de los estafadores se divide en el banquero (entra a la cuenta de la víctima y compran bases de datos), los cazadores (se encuentran en el centro penal y se dedican por comisión de lo que ganan a llamar a las personas y hacerlas caer en la estafa), reclutadores (son los que compran tarjetas, que extraen dinero, mueven efectivo, hacen inversiones). ● Desde la parte preventiva, cualquier llamada desde un banco, municipalidad, etc., tomar el dato de lo que se solicita y cortar la llamada, para posteriormente devolver las llamadas. ● No se han detectado casos de hombre en el medio o vulneración de dispositivos. Lo más cercano fue en el caso de instalación de accesos remotos. ● El utilizar cuentas de correo diferentes es una herramienta para cortar posibilidades. ● Los casos de familiares afectando a adultos mayores son la minoría de los casos registrados. ● La edad y la alfabetización digital no son diferencia para escoger las víctimas. ● El estafador siempre busca establecer una situación de amenaza, buscando inmediatez o estrés, como parte de la estrategia del estafador.

4.1.1.3. Segunda entrevista aplicada a Yorkssan Carvajal. Se llevó a cabo una entrevista al señor Yorkssan Carvajal, quien se desempeña como jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionado con delitos a patrimonio o bienes inmuebles. En este caso se realizó una segunda entrevista, ya que en la primera no se pudieron abarcar temas más profundos que se relacionan con delitos a patrimonios o bienes inmuebles. A continuación, se presentan las respuestas obtenidas:

Tabla 36

Respuestas de entrevista a Yorkssan Carvajal Aguilar jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles

Preguntas realizadas en la entrevista	Respuestas de Yorkssan Carvajal Aguilar
¿Cómo funciona el vector de ataque para estafas a bienes inmuebles a partir de la información *web* que el registro tiene disponible como pública?	Este tipo de delito necesita primordialmente la participación de un notario de forma dolosa o engañada, la parte digital lo que hace es dar los insumos para cómo hacer la documentación y buscar los bienes inmuebles a estafar. Este tipo de estafas son bajas mensualmente, pero muy altas en cantidades de dinero. El 80 % son propiedades de extranjeros, hacen un poder especial suplantando la identidad del dueño y cuando vienen los dueños a Costa Rica ya están vendidas. Acá no distinguen en población de edades solo se basan en los valores de las propiedades y en la plusvalía del lugar.
¿Tienen algún tipo de historial de este tipo de delitos?	Sí, como le decía anteriormente se dan como 5 a 6 casos mensuales, principalmente en lotes de la costa. Estos delincuentes hasta ponen rótulos de se venden en estos tipos de propiedades para luego cometer el delito.

¿Cómo proceden con las investigaciones de estafas que se relacionan con bienes inmuebles?	Primero se realiza la denuncia, se realiza una entrevista con la persona dueña y tenemos un convenio con el registro. Aquí lo primero que se hace es ir al notario que realizó el trámite y de ahí dar con los demás delincuentes.
¿Han encontrado bases de datos de propiedades y sus propietarios que hayan sido insumos para estafas?	No se encuentran bases de datos, porque como hablamos anteriormente la información es pública y ellos consultan del registro directamente.
¿Se han visto casos en los que un notario pueda suplantar su identidad para que por ese medio se cometa el delito de estafa con bienes inmuebles?	Claro que sí, se han dado que algunos notarios utilizan el código de otro para realizar este tipo de delitos o los engañan haciéndolos creer que la información que presentaron para hacer el proceso es real. A partir del servicio Ventanilla Digital del Registro Nacional.
¿Se ha detectado estafas con bienes muebles (por ej.: carros) utilizando como insumo la información disponible en línea del registro de la propiedad?	0 casos, con los vehículos no tenemos ese problema
A pesar de que la información de propiedades es pública, ¿Cómo se recomienda prevenir este tipo de estafas?	Es un tema complicado, aquí lo ideal sería poder monitorear las propiedades o estar ingresando constantemente al sitio del registro. Sería la única solución por el momento.

4.1.2. Entrevista con experto en ciberseguridad. Se llevó a cabo una entrevista con el señor Raúl Rivera, experto en temas de ciberseguridad en Costa Rica, con experiencia en temas que se relacionan con delitos de suplantación de identidad y estafa informática. A continuación, se presentan las respuestas obtenidas:

Tabla 37

Respuestas de entrevista para aplicar a experto en ciberseguridad, con experiencia en los temas que se relacionan con delitos de suplantación de identidad y estafa informática

Preguntas realizadas en la entrevista	Anotaciones a partir respuestas Raúl Rivera
1. ¿Se identifica a partir de su experiencia una afectación mayor para personas mayores a 50 años, respecto a los otros grupos de población en Costa Rica? 2. ¿Cuál considera es la mayor vulnerabilidad que aprovechan los delincuentes? 3. ¿Cuáles son las técnicas que según su experiencia utilizan los atacantes con mayor frecuencia? 4. ¿Qué afectación económica estimaría representan los delitos de suplantación de identidad y estafa informática anualmente en Costa Rica? 5. ¿Considera que existe relación entre la alfabetización digital y la mayor posibilidad de ser objetivo de un delito como suplantación de identidad o estafa informática?	● Ha podido identificar incidentes en adultos mayores o dentro del rango del estudio, sin embargo, menciona que el rango más afectado es de los 18 a 35 años. ● Además, menciona que para generar un cambio en los ciberdelitos es importante actualizar y mejorar las políticas públicas del país. ● También menciona que el principal problema que se tiene es que mientras se tenga que depender de una contraseña los problemas seguirán. Entre las mejoras se encuentra autenticar con algo que uno tiene no con algo que uno sabe, porque con solo saberlo con la ingeniería social es fácil de vulnerar. ● Además, menciona que es un mito lo de la venta de las bases de datos, aunque no se descarta por completo porque hay empresas irresponsables que tienen unas malas políticas dentro de la estructura organizacional que permiten este tipo de fuga. Se afirma que es fuga, ya que ocurren por negligencia de esta empresa. ● Una de las características de los actores de amenaza o atacantes en este caso es hacer sentir querido o con miedo al atacado. Lo que genera dos cosas, una confianza que lo hace dar más información de la cuenta o presión o estrés al darle ese sentido de urgencia a la acción por realizar. Según estadísticas un atacante puede durar de 3 a 7 minutos en llevar a cabo el ataque.

6. ¿Qué importancia considera tiene la protección de identidad, como prevención para delitos de suplantación de identidad y estafa informática? 7. ¿Cuáles recomendaciones daría a partir de su experiencia para la población de 50 años en adelante, para evitar ser víctimas de delitos de suplantación de identidad y estafa informática	● Se indica a don Raúl el dato obtenido a partir de la entrevista con personal de OIJ donde se estima una afectación anual por estafa informática de aproximadamente $8,000,000 USD a lo cual don Raúl menciona que en su experiencia la afectación observada puede alcanzar hasta 5 veces esa estimación, considerando que no en todos los casos se plantean las denuncias. ● Se indica a don Raúl el dato obtenido a partir de entrevista con personal de OIJ donde se afirma que en los casos atendidos han observado que no hay relación entre alfabetización digital y la posibilidad de ser víctima por suplantación de identidad o estafa informática. Ante lo cual don Raúl confirma el comportamiento según su experiencia. ● A partir de la consulta respecto a la protección de la identidad como una alternativa de mejorar la seguridad relacionada con delitos como suplantación de identidad y estafa informática, indica que según su experiencia es parte de las recomendaciones de prevención necesarias para los usuarios. ● Se indica a don Raúl el dato obtenido a partir de entrevista con personal de OIJ donde se afirma que ingeniería social es el principal vector de ataque identificado en el último año, por lo que confirma a partir de su experiencia que es lo que ha podido observar para el último año de eventos. ● Don Raúl indica que a partir de su experiencia ha visto que el segmento de 50 años en delante de población son personas que tienden a platear denunciar ante afectación, diferencia marcada respecto a personas con edades menores a 50 años. ● Generar una mejor propuesta de educación digital, en este caso diferenciado por segmentos. Esto se debe a que todos los segmentos de población aprenden de formas diferentes y no se pueden hacer campañas

	generalizadas. Generar una cultura digital en el país ● Implementar en las personas el detente, piensa y actúa. ● Hay que ir más allá de la tecnología, en este caso pensar más en la parte humana y no tanto en la parte técnica.

4.1.3. Entrevista al representante del Registro Nacional de Costa Rica.

Se llevó a cabo una entrevista al señor Edwin Monge, representante del registro Nacional de Costa Rica, Dirección de servicios. A continuación, se presentan las respuestas obtenidas por parte de la entrevista:

Tabla 38

Respuestas de entrevista para aplicar a representante del Registro Nacional de Costa Rica, relacionado con delitos a patrimonio o bienes

Preguntas realizadas en la entrevista	Anotaciones a partir de respuestas Edwin Monge
1. ¿Cuáles gestiones a partir de medios de tecnología de información tiene habilitado el Registro Nacional para que realicen sus usuarios? 2. ¿Cómo se valida la identidad digital de los usuarios, tanto para consultas de información como para los trámites que se encuentren habilitados? 3. ¿Se lleva a cabo un tratamiento especial para datos que se relacionan con adultos mayores, tanto usuarios como adultos mayores como propietarios? 4. Relacionado con los trámites	● A continuación, le presentamos una descripción de los diferentes servicios que son brindados a través de este portal: http://www.registronacional.go.cr/otros_servicios_linea.htm ● El portal actual se divide en dos: El estático y El transaccional. El portal estático es de acceso libre, no requiere que la persona usuaria se valide. Para el portal transaccional solo se necesita una dirección de correo electrónico válida para ser un usuario autorizado, el cual tiene una contraseña (que puede modificar la persona usuaria cuando lo desee). ● En el portal actual no se hace ninguna distinción por ser adulto mayor. Estamos en

de bienes inmuebles y muebles, consultar ¿Cuáles gestiones pueden realizar los notarios por medios digitales en los sistemas del Registro Nacional? 5. En cuanto a la autenticación de identidad, ¿cuáles son los mecanismos habilitados para los notarios con el objetivo de realizar las gestiones que tienen habilitadas? 6. Relacionado con el servicio que brinda el registro Nacional de Alerta Registral, conocer en qué consiste el servicio, con qué tipo de bienes se brinda y los costos asociados para los usuarios. 7. ¿Según legislación nacional, la información de bienes es pública, sin embargo, agradeceríamos conocer si el Registro Nacional a partir de las denuncias ante OIJ por estafas en bienes muebles e inmuebles ha producido recomendaciones para evitar afectación hacia los usuarios	proceso del desarrollo de un nuevo portal al que se agregan lineamientos de accesibilidad. ● Los notarios tienen a su disposición el Servicio de Ventanilla Digital mediante el cual se pueden presentar documentos al Diario sin tener que asistir a las sedes para esta gestión; se pueden presentar documentos de momento de bienes muebles, inmuebles y personas jurídicas. ● El mecanismo de autenticación es la firma digital del notario, con esto se valida que sea la persona usuaria, que esté *viva* ante el Tribunal Supremo de Elecciones, además, ante la Dirección Nacional de Notariado que esté habilitado para ejercer su profesión. ● El servicio de Alerta Registral está a disposición de cualquier usuario, compra el servicio por un costo de $15 anuales, se pueden alertar tantas sociedades, inmuebles o muebles. Una vez adquirido el servicio en caso de que se presente alguna anotación al bien o sociedad el cliente recibirá, de manera inmediata, una notificación de la situación y en caso de ser una estafa puede solicitar a la Dirección la no inscripción del documento. ● Con respecto a este punto, se tiene una constante comunicación entre los Registros sustantivos, el OIJ y la DNN para agilizar cualquier proceso judicial o administrativo, esto debido a que este tipo de movimientos (estafas) son a nivel extra registral no a nivel interno. Son notarios que se prestan para este tipo de ilícitos donde cumplen a cabalidad con todos los requisitos de forma y fondo

4.1.4. Entrevista a representante de la Oficina del Consumidor Financiero. Se llevó a cabo una entrevista a un representante de la Oficina del Consumidor Financiero. A continuación, se presentan las respuestas obtenidas:

Tabla 39

Respuestas de entrevista a representante de la Oficina del Consumidor Financiero, relacionado con delito de estafa informática

Preguntas realizadas en la entrevista	Anotaciones a partir de respuesta representante Oficina del Consumidor Financiero
1. ¿Cuáles son los derechos del consumidor financiero? 2. Considerando la afectación financiera producto del delito de estafa informática, ¿Es responsabilidad de la entidad financiera contar con seguros que permitan a los usuarios recuperar su dinero, una vez demostrada su adecuado resguardo de información? 3. ¿Existe algún tratamiento diferenciado para los casos que se relacionan con afectación financiera para personas mayores de 65 años, al ser víctimas del delito de estafa informática? 4. ¿La responsabilidad de demostrar el uso correcto y resguardo de los mecanismos de autenticación de usuario en sus servicios financieros por medio de facilidades *web*, corresponde al usuario, o bien corresponde a la entidad financiera demostrar el mal uso o resguardo por parte del usuario?	• Según la Ley de la Promoción de la competencia y Defensa Efectiva del Consumidor (Ley n.º, 7472) los derechos son: derecho a recibir información adecuada, clara, veraz y oportuna; derecho a una relación de consumo justa y equitativa; derecho a la libre elección; derecho a presentar reclamos y quejas; derecho a la no inclusión de cláusulas abusivas; derecho a recibir un trato no discriminatorio; derecho a un tratamiento adecuado de los datos personales y derecho a la protección de los intereses económicos del consumidor. • Los seguros son una herramienta de protección efectiva para las personas consumidoras. En el mercado, actualmente, existen seguros que cubren estafas informáticas, sin embargo, son dirigidos a los consumidores y son de carácter voluntario, es decir, no se les puede obligar a adquirir el seguro. Sería de gran utilidad que las entidades financieras contaran con seguros que protejan las cuentas de sus clientes de estafas informáticas, pero para ello las entidades aseguradoras deben de tener dicho seguro habilitado. • La normativa no establece expresamente un tratamiento diferenciado para los casos de estafas informáticas de adultos mayores. La normativa hace la diferenciación en temas

	de tarjetas de crédito y débito, facilidades en el otorgamiento de créditos hipotecarios, pero no en temas de estafas informáticas. • La carga de la prueba en materia de derecho de consumo le corresponde a la entidad financiera. Es la entidad financiera la que debe demostrar que sus sistemas de seguridad no fueron vulnerados y que más bien fue una conducta o acción del consumidor el que produjo el daño acaecido. Solo se liberan de responsabilidad si logran demostrar que hubo culpa de la víctima, hecho de un tercero o fuerza mayor o caso fortuito. Esto se conoce como la responsabilidad objetiva o la teoría del riesgo creado, que regula el artículo 35 de la Ley n.º 7472 “Régimen de responsabilidad”. El productor, el proveedor y el comerciante deben responder concurrente e independientemente de la existencia de culpa, si el consumidor resulta perjudicado por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su utilización y riesgos. Solo se libera quien demuestre que ha sido ajeno al daño.

4.1.5. Entrevista a docentes de la Asociación Gerontológica Costarricense. Se llevó a cabo una entrevista con profesores y personal administrativo de la Asociación Gerontológica Costarricense, con el fin de identificar una serie de comportamientos en la población en la cual se aplica el proyecto. A continuación, se presentan las respuestas obtenidas:

Tabla 40

Respuestas de entrevista a docentes Asociación Gerontológica Costarricense

Preguntas por realizar con instrumento de entrevista	Objetivos específicos relacionados
¿Cuál es la población en la que se centra la atención de Ageco?	Aunque la población en la cual se enfoca la atención son personas adultas mayores, desde hace unos años se trabaja con personas mayores de 45 años en adelante. En la actualidad, la mayor cantidad de personas son mujeres con casi un 78 % de la población total.
¿En Ageco existen cursos en donde haya énfasis en la seguridad de la navegación en Internet?	En Ageco se dan diferentes cursos, por ejemplo, cursos de dispositivos móviles, redes sociales e Internet. En cada uno se mencionan algunas prácticas de seguridad como contraseñas seguras, huella digital, pero de una manera general y omitiendo temas como pagos en línea o que tengan relación con finanzas. Se han ofrecido cursos en materia de ciberseguridad, pero no han tenido mucha aceptación por parte de la población atendida.
¿De acuerdo con la población que atienden cuáles características tecnológicas de uso han notado?	Lo que más se nota es el uso del celular, en la cual se observó que predomina el uso de dispositivos con Android, sin embargo, sí hay algunas personas que utilizan IOS de Apple. La computadora la utilizan para conectarse a las clases de Ageco, pero en uso general la utilizan cotidianamente de una forma menor que el celular.
¿Cuál nivel de alfabetización digital notan en la población que atienden?	En el caso de la alfabetización digital existen diferentes niveles dentro de la población, desde personas que apenas dominan lo básico hasta otras que por su conocimiento sirven de ayudantes a las personas docentes para explicarles o guiar a los demás compañeros de los

	cursos que se brindan. En temas que se relacionan con la ciberseguridad directamente sí desconocen de algunos términos y algunas personas dentro de la población han recibido algún tipo de ataque informático principalmente por ingeniería social.
¿Cuáles técnicas utilizan para transmitir el contenido de los cursos que brindan a esta población?	Lo principal es empezar desde los conceptos más básicos posibles para que las personas que tal vez no tengan ese conocimiento previo puedan ir alineándose con esos términos y que después la mayoría puedan estar a un mismo nivel. Se enfoca mucho en realizar ejemplos de la vida cotidiana como experiencias entre las mismas personas de la población y así hacer un método más dinámico de aprendizaje.
¿Cuáles son las características más importantes que ustedes identifican en esta población que atienden?	Una de ellas es el interés por aprender, son muy constantes en su aprendizaje, por eso, la mayoría siguen matriculando cursos en Ageco. Son personas muy precavidas, muy respetuosas, tolerantes y solidarias.
¿Cuáles medios de comunicación son los que más utilizan ustedes para tener relación con las poblaciones que atienden?	Los medios más utilizados de comunicación con la población son canales de WhatsApp y Zoom sin dejar de lado el correo electrónico.
¿Cuáles recomendaciones nos pueden brindar por su experiencia en el momento de trabajar con esta población?	La mejor alternativa es una interacción uno a uno donde se pueda generar ese vínculo de confianza con la persona. Ser muy básicos y tratar de explicar temas más orientados a experiencias de la vida cotidiana.

4.1.6. Solicitud de información vía correo electrónico a Banco Nacional de Costa Rica y Banco de Costa Rica, como ejemplos de entidades financieras. Como parte de la investigación, con el objetivo de contar con la información de referencia de entidades financieras, se procedió a contactar al Banco Nacional de Costa Rica, al correo coordinacionoperativadeseguridad@bncr.fi.cr y al Banco de Costa Rica a los correos electrónicos bcr@service-now.com y CentroAsistenciaBCR@bancobcr.com. El fin era obtener respuestas a las preguntas indicadas a continuación, no obstante, no fue posible contar con las respuestas por parte de las entidades financieras.

Preguntas realizadas:

- ¿Cantidad de casos anuales recibidos de denuncias por parte de clientes para los delitos indicados? (de ser posible desde 2016).
- ¿Cantidad de casos anuales recibidos de denuncias por parte de clientes, para la población con edad mayor a 50 años, para los delitos indicados? (de ser posible desde 2016).
- ¿Estimación de afectación económica anual, producto de los casos identificados, para los delitos indicados?
- ¿Vectores de ataque identificados, según las denuncias de clientes, para los delitos indicados?
- ¿Productos bancarios con mayor cantidad de denuncias por parte de clientes para los delitos indicados?
- ¿Cómo se procede ante denuncias de clientes por afectación relacionada con los delitos indicados?
- ¿Cuáles son las evidencias solicitadas por parte del cliente para presentar una denuncia por afectación?
- ¿Cuáles son las recomendaciones para evitar la afectación hacia los clientes y sus productos bancarios, relacionados con suplantación de identidad y estafa informática?

4.2. Análisis de entrevistas a expertos

4.2.1. Análisis de entrevistas representantes Organismo de Investigación Judicial. A continuación, se detallan las entrevistas con los representantes del OIJ.

4.2.1.1. Análisis de entrevista con Genevieve Segura Robles de la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial. En el caso de la entrevista con Genevieve se logró descubrir información valiosa con respecto a cómo se desarrollan las denuncias por este tipo de crímenes, principalmente el de suplantación de identidad que es el que se maneja en esta sección, recordando que la estafa informática le corresponde a la sección de fraudes. También se consultó información importante con respecto a cómo es el *modus operandi* al aplicarse el delito de suplantación de identidad. En el caso de las denuncias es relevante resaltar el trato diferenciado, ya que en los casos de personas adultas mayores como denunciantes se toma la declaración del denunciante el mismo día en que se presenta a realizar la declaración, además de todo el proceso de recopilación de pruebas para avanzar en la investigación.

En el caso propio del delito de suplantación informática se evidenció cómo los atacantes actúan en dos ejes, el primero con la intención de suplantar la identidad y tratar de ingresar a las cuentas bancarias y otro en donde se hacen pasar por otra persona para pedir ayudas económicas. Además, se destaca que, aunque la población de personas en edad laboral madura y personas adultas mayores pueden ser vulnerables por ciertos factores, esto no es algo que tenga que ver en la ejecución de este tipo de delitos, ya que los delincuentes no segmentan poblaciones, en este caso aplican a todas las personas en general.

Asimismo, se descubrió que la alfabetización digital no es un parámetro relevante para cometer este tipo de delitos. Otra característica importante revelada en la entrevista es cómo predomina el uso del teléfono celular como el dispositivo que más se registra en este tipo de ataques, además de que también se evidencia que familiares o terceros que ayudan a estas personas pueden convertirse en los atacantes. Una de las recomendaciones más importantes que menciona la entrevistada es educar a este tipo de poblaciones, quitarles ese miedo o desconocimiento en estos temas, que se sientan más cómodos y que poco a poco con esa educación puedan prevenir este tipo de delitos.

4.2.1.2. Análisis de entrevista con Yorkssan Carvajal jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos de suplantación de identidad y estafa informática. Para la primera entrevista con Yorkssan Carvajal se identificó la priorización que el Organismo de Investigación Judicial aplica para recibir las denuncias que plantean las personas adultas mayores.

Se menciona como el mecanismo con mayor cantidad de denuncias recibidas, las estafas por medio de llamadas telefónicas a partir de bases de datos lícitas e ilícitas como fuente de posibles víctimas que los delincuentes utilizan sin que se haga énfasis según edad. Además, se mencionan las redes sociales como fuente para los delincuentes para obtener información sobre sus víctimas en el proceso de ingeniería social.

A partir de los datos de 300 denuncias mensuales recibidas en el Organismo de Investigación Judicial y una afectación anual estimada de $8,000,000 USD, se estiman las dimensiones del beneficio económico que los delincuentes logran a partir de los delitos de suplantación de identidad y estafa informática en Costa Rica. No obstante, no se identifica una diferenciación por parte de los estafadores al seleccionar sus posibles víctimas según su edad.

Se identifican los ciclos de técnicas que utilizan los delincuentes y según lo que indica el representante del Organismo de Investigación Judicial no son técnicas complejas. Sin embargo, hay periodos en los que los delincuentes recurren a técnicas particulares para la mayoría de sus delitos que se relacionan con suplantación de la identidad y estafa informática.

Además, se identifica la presencia de los profesionales en informática como parte de la red organizada que se relaciona con los delitos objeto de investigación, así como figuras y funciones definidas dentro de la red organizada.

Según los datos obtenidos, no se encuentra relación entre alfabetización digital y las víctimas que son objeto de los delitos de suplantación de identidad y estafa informática. Lo anterior ya que se registran casos tanto en profesionales del área informática como en personas que tienen un bajo nivel de alfabetización digital.

Las estafas se registran dirigidas principalmente a personas con acceso a su información bancaria por medio de sus dispositivos móviles. También se identifica como estrategia del delincuente la búsqueda de establecer una situación de amenaza, inmediatez o estrés, como los factores clave para seguir adelante con materializar los delitos de suplantación de identidad y estafa informática.

Como recomendación del entrevistado se indica que, en caso de ser víctima de estafa informática relacionada con servicios bancarios, el primer paso es comunicarse con el banco correspondiente para poner la denuncia debido a la visibilidad y acción por parte de la entidad financiera. Asimismo, el Organismo de Investigación Judicial busca dar a conocer las principales técnicas de los delincuentes en medios de comunicación como una estrategia para prevenir a la población.

4.2.1.3. Análisis de entrevista con Yorkssan Carvajal jefe de la Sección Especializada en Fraudes del Organismo de Investigación Judicial relacionada con delitos a patrimonio o bienes inmuebles. En el caso de la segunda entrevista con Yorkssan Carvajal, la cual se enfocó primordialmente en los delitos informáticos que se relacionan con patrimonio o bienes inmuebles, se destacaron varios puntos y entre los más importantes se tiene que según la Ley n.º 8968 relacionada con la protección de la persona frente a sus datos personales, clasifica como datos públicos o de acceso irrestricto las propiedades de las personas del país, por lo tanto, se convierte en un dato que no es posible proteger con algún mecanismo. Además, para que este tipo de delitos se puedan realizar, se necesita un notario que, ya sea de forma dolosa o por ser víctima de engaño, incurra en la acción de una posible materialización de una estafa.

En este caso el medio informático solo funciona como búsqueda de insumos en la base de datos pública del Registro Nacional, pero no se puede hacer ningún tipo de acción digital. Los delitos que se registraron en este tipo de crimen se enfocan en personas extranjeras que tienen propiedades en lugares alejados y con un valor muy alto. Cuando estas personas regresan al país ya les han vendido las propiedades. En la parte de bienes muebles se reportan cero delitos por su forma de inscribir este tipo de bienes en el registro nacional.

En conclusión, lo que recomienda el entrevistado es que se esté en constante monitoreo de las propiedades para evitar que este tipo de delitos ocurran. El registro nacional ofrece una alternativa llamada alerta registral en donde se pueden asignar en monitoreo las propiedades y cada vez que exista algún movimiento se le informa inmediatamente al dueño.

4.2.2. Análisis de entrevista experto en ciberseguridad. Se identifica que la afectación mayor por delitos de suplantación de identidad y estafa informática se encuentra en el rango de edad de 18 a 35 años. Además, menciona las políticas públicas como un factor de importancia para la disminución de los ciberdelitos en Costa Rica.

El entrevistado menciona el método de autenticación de usuario y contraseña como una vulnerabilidad explotada comúnmente por la ingeniería social como vector de ataque. Además, indica que las técnicas que utilizan los delincuentes van orientadas en crear temor o afinidad en las víctimas de estafas. Se menciona que los delincuentes tardan de 3 a 7 minutos para realizar la estafa informática con afectación financiera para la víctima.

De acuerdo con la experiencia del entrevistado, la afectación anual por estafa informática con afectación financiera es mucho mayor de la que llega a denunciarse en el Organismo de Investigación Judicial. Asimismo, confirma que, según su experiencia, no se establece una relación de las víctimas de acuerdo con su alfabetización digital. Sin embargo, sí menciona que la población de 50 años en adelante es la que en la mayoría de los casos plantea una denuncia en los casos de estafa informática.

Entre las recomendaciones del entrevistado se menciona generar una mejor propuesta de educación digital, diferenciada por segmentos de edad. Esto se debe a que todos los segmentos de población aprenden de formas diferentes y no se pueden hacer campañas generalizadas. Asimismo, plantea la estrategia *Detecte, piense y actúe* y, por último, ir más allá de la tecnología, pensando en la parte humana y no hacer un énfasis en la parte técnica, para las propuestas de solución para tratar el riesgo.

4.2.3. Análisis de entrevista representante Registro Nacional de Costa Rica. Se menciona que, en el ámbito de Registro Nacional, no se hace distinción para el tratamiento de la información de adultos mayores. El Registro Nacional tiene habilitado el servicio de Ventanilla Digital para los notarios en su trabajo remoto para presentar documentos al Diario, por lo que la firma digital es el mecanismo de autenticación. Por lo anterior, la firma digital se utiliza, tanto en la autenticación para ingreso al servicio Ventanilla Digital del Registro Nacional como la firma digital de los documentos que los notarios presentan para el trámite.

El Registro Nacional cuenta con el servicio de Alerta Registral, como una herramienta para monitorear sociedades, inmuebles y muebles, donde se busca alertar al dueño registral ante cualquier anotación al bien o sociedad. Asimismo, se menciona la comunicación directa entre el Registro Nacional, el Organismo de Investigación Judicial y la Dirección Nacional de Notariado, ya que las estafas se cometen extraregistral, debido a que la documentación presentada en el ámbito de Registro Nacional cumple a cabalidad con todos los requisitos de forma y fondo.

4.2.4. Análisis de entrevista representante Oficina del Consumidor Financiero. Se identifican los derechos del consumidor financiero, lo cual es un insumo valioso para los usuarios al utilizar productos del sistema financiero nacional. Como elemento de consideración se identifica que la no obligatoriedad de contar con seguros de respaldo para los usuarios por parte de las entidades financieras representa un diferenciador muy importante por considerar por la persona usuaria en cuanto a seleccionar la entidad financiera para tener sus recursos.

Asimismo, se establece la base de que es responsabilidad de la entidad financiera demostrar el buen o mal uso por parte del usuario de los mecanismos de autenticación, por lo tanto, es un dato valioso que conocer por parte del usuario.

4.2.5. Análisis de entrevista a docentes de la Asociación Gerontológica Costarricense. En la entrevista con profesores y personal administrativo de Ageco, en la cual se pretendía recopilar información acerca de las personas en edad laboral madura y personas adultas mayores atendidos por ellos, se evidenció una serie de características importantes por considerar para trabajar con esta población. Aunque Ageco prioriza a las personas adultas mayores, desde hace unos años se trabaja con personas de 45 años en adelante y su mayoría son mujeres. En la población que se atiende se evidencian diferentes rangos de alfabetización digital, desde personas que saben lo básico hasta personas que dominan muy bien temas tecnológicos, que más bien sirven de soporte a las personas docentes para ayudarlos a explicar algunos temas a sus demás compañeros en los cursos que brinda Ageco.

En la parte tecnológica se identifica que la mayoría de las personas utiliza como dispositivo principal el celular y en menor medida la computadora, esta última la utilizan para recibir clases virtuales. Entre los medios de comunicación que usa Ageco están el WhatsApp, Zoom y el correo electrónico. En el área de navegación segura Ageco se enfatiza en varios cursos que se relacionan con tecnología, por ejemplo, dispositivos móviles, redes sociales e Internet, sin embargo, en temas de seguridad, aunque sí enfatizan en temas importantes como huella digital y contraseñas seguras, se hace de una forma general.

Según informan los mismos profesores y personal administrativo se ha querido abrir cursos que se relacionan con ciberseguridad, pero no han tenido mucha aceptación por parte de la población. Además, es importante mencionar que se identifica que varias personas atendidas por Ageco han recibido algún tipo de ataque por ingeniería social.

Otras características de la población, según informan los profesores y personal administrativo, es que son personas con mucho interés por aprender. Para trabajar con ellas es importante ser muy básicos, empezar desde conceptos más sencillos y transmitirles con ejemplos de la vida cotidiana para que su aprendizaje sea todavía mejor. Además, es relevante tener una relación uno a uno en donde se crea un vínculo de confianza para tener la información de una mejor manera.

4.3. Análisis y resultados de entrevistas a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense

Para medir de forma cualitativa algunos comportamientos de navegación segura en Internet en la población de personas en edad laboral madura y adultas mayores de Ageco y como parte del proceso de análisis junto con la información que se recopiló en el Capítulo 2 y la elaboración de instrumentos del apartado 3.6 se aplicó una entrevista a un total de 15 personas dentro de la Asociación Gerontológica Costarricense. Las preguntas se enfocaron en responder información en diferentes etapas de una posible amenaza informática que van desde identificar, proteger, detectar, responder y recuperarse sobre algún tipo de ataque. De las entrevistas se obtuvieron los siguientes resultados.

Tabla 41

Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función identificar la propuesta marco de trabajo

Funciones en marco de trabajo	Preguntas por realizar con instrumento de entrevista	Parametrización para análisis de respuestas por parte del entrevistador			
		Parámetro	Cantidad registrada	Parámetro	Cantidad registrada
Identificar	¿Qué entiende por suplantación de identidad?	Logra identificar concepto	11	No logra identificar concepto	4
	¿Tiene claro qué información es importante proteger para evitar que suplante su identidad?	Cita información a proteger	11	No logra identificar información a proteger	4
	¿Qué entiende por estafa informática?	Logra identificar concepto	10	No logra identificar concepto	5
	¿Tiene claro qué información es importante proteger para evitar que le hagan una estafa informática?	Cita información a proteger	11	No logra identificar información a proteger	4

	¿Tiene claro qué información es importante proteger para evitar que le afecten financieramente o con sus propiedades?	Cita información a proteger	12	No logra identificar información a proteger	3

En la función de identificar los diferentes riesgos en los cuales se enfoca el proyecto, relacionado con los delitos tipificados en el Código Penal de suplantación de identidad y estafa informática, la mayoría de los entrevistados lograron establecer una definición de estos tipos de delitos. Además, pudieron identificar algunas acciones para proteger información personal y así evitar que puedan sufrir de algún tipo de suplantación o estafa informática, tanto en la parte financiera como patrimonial.

Tabla 42

Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función proteger, propuesta marco de trabajo

Funciones en marco de trabajo	Preguntas por realizar con instrumento de entrevista	Parametrización para análisis de respuestas por parte del entrevistador							
		Parámetro	Cantidad registrada	Parámetro	Cantidad registrada	Parámetro	Cantidad registrada	Parámetro	Cantidad registrada
Proteger	Cuando tiene que hacer un pago en Internet, ¿qué alternativa usa?	Utiliza tarjeta debito	10	Utiliza tarjeta crédito	5	Utiliza transferencias electrónicas	10	Utiliza Simpe Móvil	11
	¿Cuáles antivirus utiliza en su computadora?	Identifica un antivirus de paga	7	Identifica un antivirus de uso gratuito	8				
	¿Cómo puede proteger su identidad en Internet?	Cita mecanismos para proteger	10	No logra identificar mecanismo	5				

				s para proteger					
	¿Qué información usted no publica en redes sociales?	Logra identificar información que protege en redes sociales	13	No logra identificar información que protege en redes sociales	2				

En la función de proteger se identifica que la mayoría de los entrevistados utilizan medios informáticos para realizar diferentes pagos a través de Internet, entre los principales está el Sinpe Móvil, seguido de pagos con tarjetas de débito y transferencias electrónicas en los distintos sistemas bancarios, con un grado menor utilizan tarjetas de crédito. Algunos entrevistados para hacer este tipo de acciones bancarias usan principalmente la computadora y la minoría poseen algún tipo de antivirus de paga, los demás emplean antivirus de versiones gratuitas. En las preguntas que se relacionan con la protección de su identidad en Internet y las medidas que utilizan, en la mayoría de los entrevistados predomina una característica de ser precavidos, por lo tanto, se cuidan mucho en la información que suben a sus redes sociales y si no conocen algo mejor evitan abrirlo o explorarlo.

Tabla 43

Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función proteger, propuesta marco de trabajo

Funciones en marco de trabajo	Preguntas por realizar con instrumento de entrevista	Parametrización para análisis de respuestas por parte del entrevistador			
		Parámetro	Cantidad registrada	Parámetro	Cantidad registrada
Detectar	¿Cómo reconoce una página *web* real de una falsa?	Logra dar elementos para diferenciar una página *web* falsa	3	No logra dar elementos para diferenciar una página *web* falsa	12
	¿Sabe cómo los delincuentes suplantan la identidad de las personas?	Cuenta con información riesgos	8	No cuenta con información de los riesgos	7
	¿Conoce cómo los delincuentes hacen estafas informáticas en Internet?	Cuenta con información riesgos	9	No cuenta con información de los riesgos	6
	¿Cómo reacciona cuando le tratan de solicitar información con urgencia por un riesgo o un beneficio para usted?	Logra cortar la situación de riesgo	14	Es vulnerable a una situación de estafa	1

	¿Sabe que el navegador *web* almacena los sitios que se han visitado?	Conoce el historial de navegación	11	No conoce el historial de navegación	4

En la función de detectar se identifica el desconocimiento para la mayoría de los entrevistados, para puntos de reconocimiento de sitio *web* auténtico, por ende, una necesidad identificada para la población en estudio. En cuanto a la detección de suplantación de identidad y estafa informática, para las personas entrevistadas existe un balance en los casos en los que se cuenta con información y en los que se desconocen los elementos que utilizan los delincuentes para cometer los delitos. No obstante, las personas entrevistadas muestran una clara identificación del *sentido de urgencia* como un factor indicador de un intento de ejecutar una estafa, lo que permite la prevención de ser víctima de los delitos en estudio.

En cuanto a la información de historiales de navegación para el navegador *web* que se utiliza, se muestra que la población entrevistada cuenta con información técnica que les permite conocer funcionalidades del navegador y en el caso del historial las funcionalidades y riesgos que puede tener la información almacenada.

Tabla 44

Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función responder, propuesta marco de trabajo

Funciones en marco de trabajo	Preguntas por realizar con instrumento de entrevista	Parametrización para análisis de respuestas por parte del entrevistador			
		Parámetro	Cantidad registrada	Parámetro	Cantidad registrada
Responder	Cuando tiene un correo electrónico de un desconocido, ¿Qué hace?	Actúa preventivamente	14	Explora a pesar del riesgo	1
	Cuando le aparecen ventanas emergentes en su navegador, ¿Qué hace?	Actúa preventivamente	13	Explora a pesar del riesgo	2
	Cuando recibe una llamada solicitando confirmar sus datos, ¿Qué hace?	Actúa preventivamente	15	Se expone al riesgo	
	Cuando recibe un correo o un mensaje con un *link* para que acceda, ¿Qué hace?	Actúa preventivamente	15	Se expone al riesgo	

En la función de responder se identifica una marcada línea preventiva para la población entrevistada, donde ante indicadores de riesgo como correos de origen desconocido, ventanas emergentes en medio de una navegación, llamadas telefónicas solicitando o intentando validar información, así como *links* de acceso, ya sea en mensaje o correo electrónico, la respuesta es evitar el riesgo. Lo anterior denota conocimiento de posibles situaciones que les pueden poner en riesgo y, por ende, muestra que se ha recibido información a partir de los medios a los cuales tienen acceso, relacionado con prevención como respuesta ante la duda.

Tabla 45

Respuestas de entrevista a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense, función recuperar, propuesta marco de trabajo

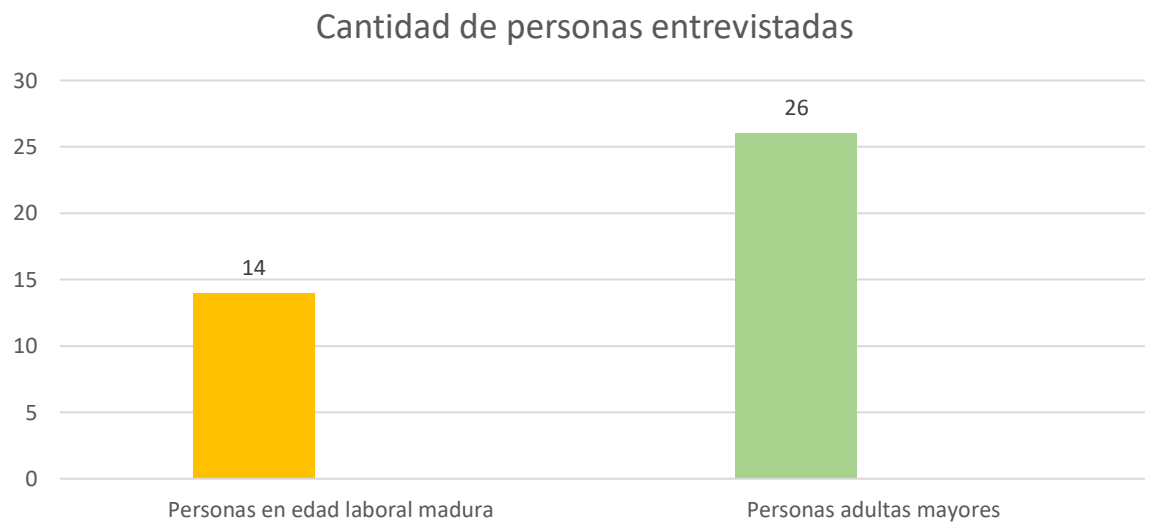
Funciones en marco de trabajo	Preguntas por realizar con instrumento de entrevista	Parametrización para análisis de respuestas por parte del entrevistador			
		Parámetro	Cantidad registrada	Parámetro	Cantidad registrada
Recuperar	En caso de detectar que le han suplantado su identidad, ¿Cómo procedería?	Logra tener información sobre el uso de su identidad digital	10	No logra tener información sobre el uso de su identidad digital	5
	En caso de detectar que le han estafado, ¿Cómo reaccionaría?	Identifica información para hacer una denuncia con posibles elementos de prueba	12	No conoce posibles elementos para pruebas	3
	¿Conoce los canales de contacto que debe utilizar para plantear una denuncia con su entidad financiera?	Identificar los canales para hacer una denuncia	11	No logra identificar los canales para hacer una denuncia	4

En la función de recuperar, se identifica que la población consultada cuenta con información de utilidad sobre cómo proceder en caso de detectar ser víctimas de suplantación de identidad, respuesta en caso de detectar ser víctima de estafa informática, así como los teléfonos de contacto para realizar las denuncias, ya sea en la entidad financiera como en el Organismo de Investigación Judicial.

4.4. Aplicación de cuestionarios

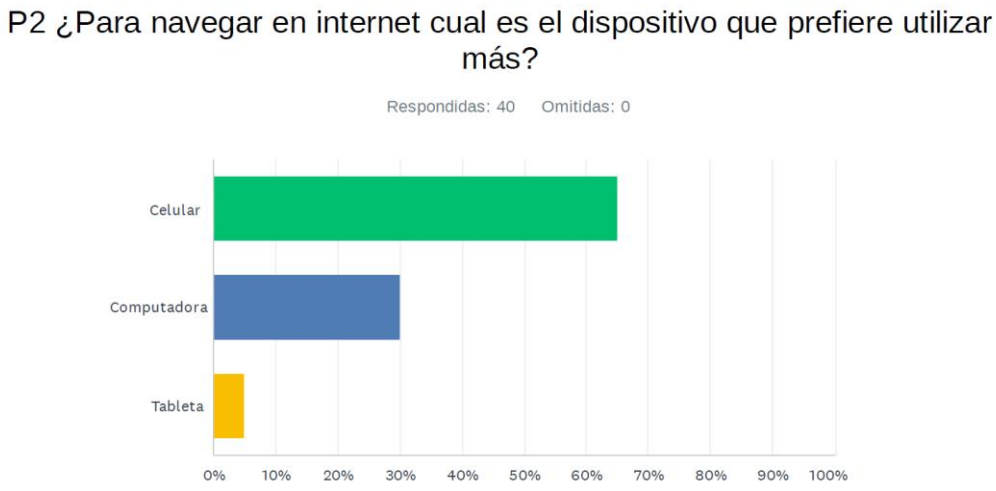
Para medir de forma cuantitativa algunos comportamientos de navegación en Internet en la población de personas en edad laboral madura y adultas mayores de Ageco y como parte del proceso de análisis junto con la información que se recopiló en el Capítulo 2 y la elaboración de instrumentos del apartado 3.6 se aplicó un cuestionario a un total de 40 personas dentro de la Asociación Gerontológica Costarricense. El cuestionario evidenció los siguientes resultados:

4.4.1. Pregunta 1. Digite su edad.



Para segmentar mejor las respuestas se dividieron en las poblaciones en las cuales se enfoca el proyecto, esto también brinda información para verificar que todas las personas encuestadas estén dentro del rango aceptado. De los 40 encuestados 14 fueron del segmento de edad laboral madura con un porcentaje del 35 %, mientras que 26 fueron del segmento de persona adulta mayor con un porcentaje del 65 % de las personas encuestadas.

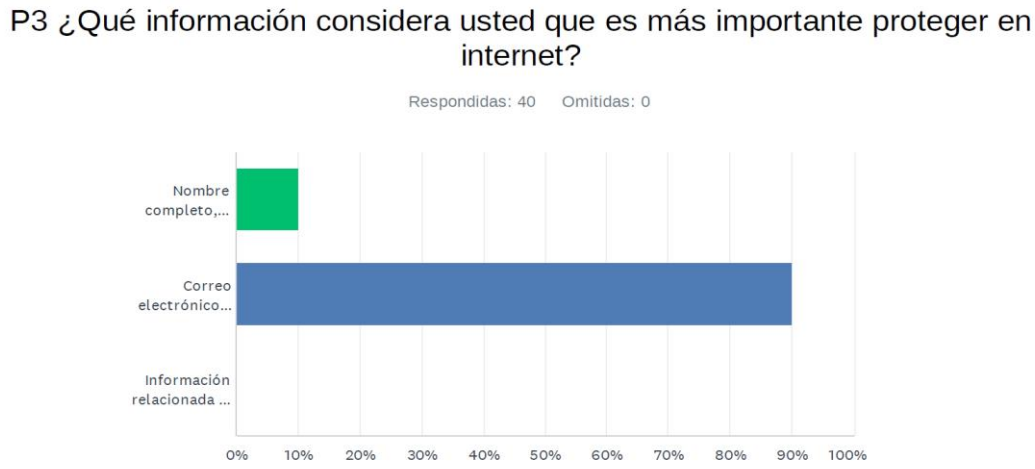
4.4.2. Pregunta 2. Dispositivo para navegar.



OPCIONES DE RESPUESTA	RESPUESTAS	
Celular	65.00%	26
Computadora	30.00%	12
Tableta	5.00%	2
TOTAL		40

De acuerdo con la información brindada la mayoría de las personas encuestadas prefiere el uso del celular para navegar en Internet.

4.4.3. Pregunta 3. Información importante.

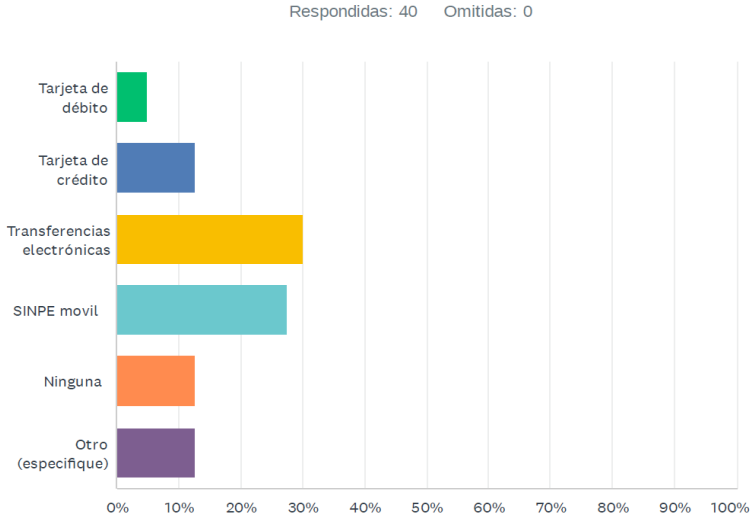


OPCIONES DE RESPUESTA	RESPUESTAS	
Nombre completo, dirección y teléfono	10.00%	4
Correo electrónico ,celular y datos bancarios	90.00%	36
Información relacionada a salud, religión y fotos	0.00%	0
TOTAL		40

La mayor parte de las personas encuestadas considera el correo electrónico, número de celular y datos bancarios como la información más importante que proteger.

4.4.4. Pregunta 4. Alternativa pago de Internet.

P4 ¿Cuándo tiene que hacer un pago en internet, que alternativa usa?



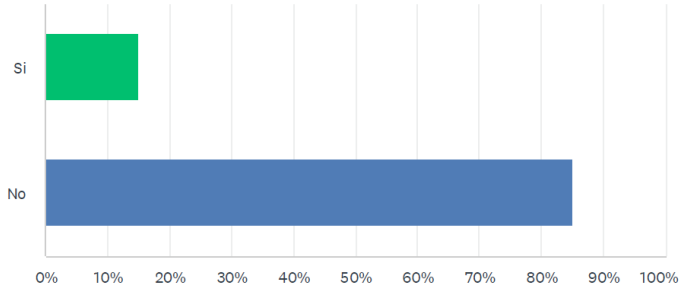
OPCIONES DE RESPUESTA	RESPUESTAS	
Tarjeta de débito	5.00%	2
Tarjeta de crédito	12.50%	5
Transferencias electrónicas	30.00%	12
SINPE movil	27.50%	11
Ninguna	12.50%	5
Otro (especifique)	12.50%	5
TOTAL		40

La alternativa que más utilizan las personas encuestadas son las transferencias electrónicas.

4.4.5. Pregunta 5. Uso de redes inalámbricas.

P5 ¿Utiliza frecuentemente redes inalámbricas gratuitas en sitios públicos para navegar en internet desde su dispositivo

Respondidas: 40 Omitidas: 0



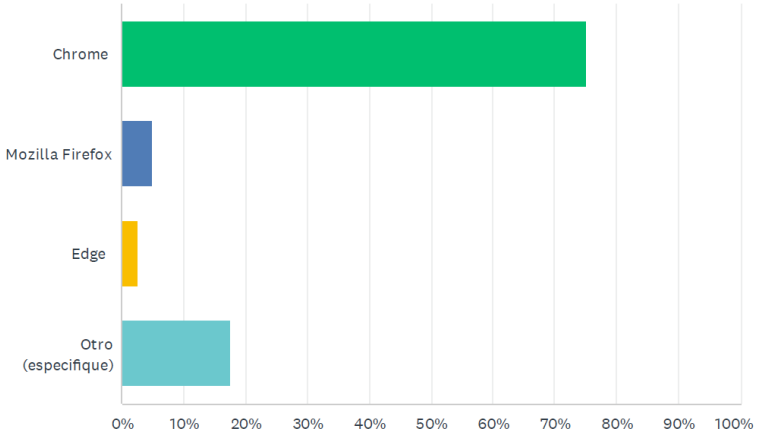
OPCIONES DE RESPUESTA	RESPUESTAS	
Si	15.00%	6
No	85.00%	34
TOTAL		40

La mayoría de las personas encuestadas no utiliza las redes wifi gratuitas en sitios públicos para navegar.

4.4.6. **Pregunta 6.** Navegador utilizado.

P6 ¿Cuál es el navegador que utiliza más al navegar en internet?

Respondidas: 40 Omitidas: 0



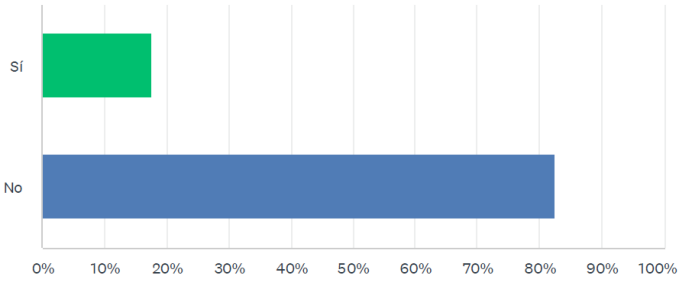
OPCIONES DE RESPUESTA	RESPUESTAS	
Chrome	75.00%	30
Mozilla Firefox	5.00%	2
Edge	2.50%	1
Otro (especifique)	17.50%	7
TOTAL		40

En preferencia de navegadores, la opción que más utilizan las personas encuestadas es Google Chrome.

4.4.7. Pregunta 7. Uso de contraseña.

P7 ¿Utiliza la misma contraseña para todos los sitios, correo y servicios que utiliza en internet?

Respondidas: 40 Omitidas: 0



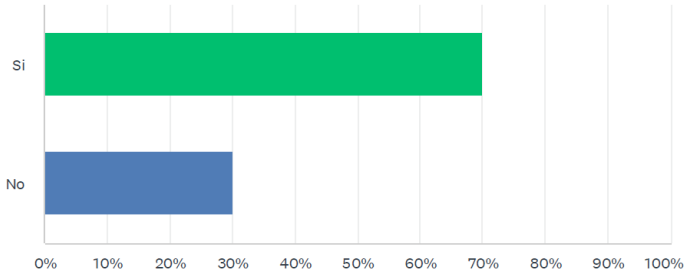
OPCIONES DE RESPUESTA	RESPUESTAS	
Sí	17.50%	7
No	82.50%	33
TOTAL		40

De acuerdo con los resultados de la pregunta 7, la mayoría de las personas encuestadas no usa la misma contraseña para todos los servicios que utilizan en Internet.

4.4.8. Pregunta 8. Actualizaciones de sistema operativo.

P8 ¿Cuándo utiliza la computadora o el celular, realiza las actualizaciones que le ofrece el sistema operativo?

Respondidas: 40 Omitidas: 0



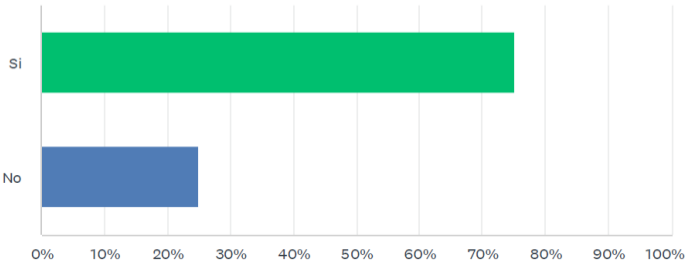
OPCIONES DE RESPUESTA	RESPUESTAS	
Si	70.00%	28
No	30.00%	12
TOTAL		40

De los datos arrojados de la pregunta 8, el 30 % de las personas encuestadas no realiza las actualizaciones que brindan los sistemas operativos y el 70 % sí lo hace.

4.4.9. Pregunta 9. Permisos para instalar programas.

P9 ¿Cuándo utiliza la computadora tiene los permisos necesarios para instalar diferentes programas?

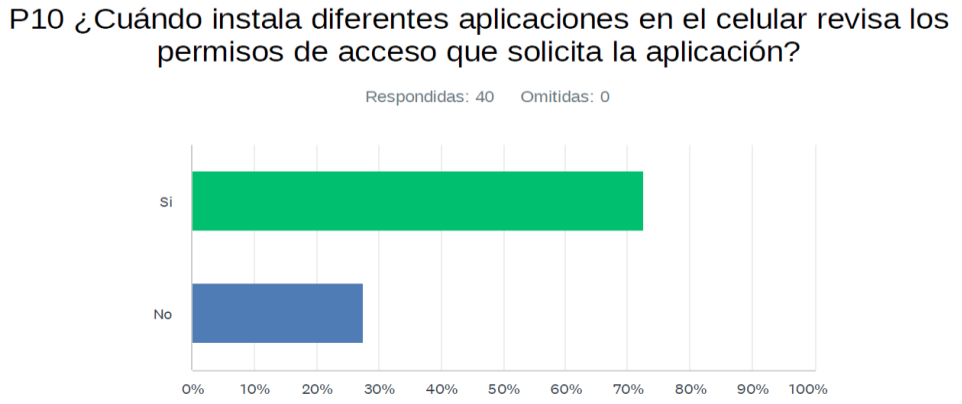
Respondidas: 40 Omitidas: 0



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	75.00%	30
No	25.00%	10
TOTAL		40

La mayoría de las personas entrevistadas posee permisos de administrador en sus computadoras para instalar programas solo el 25 % no lo tiene.

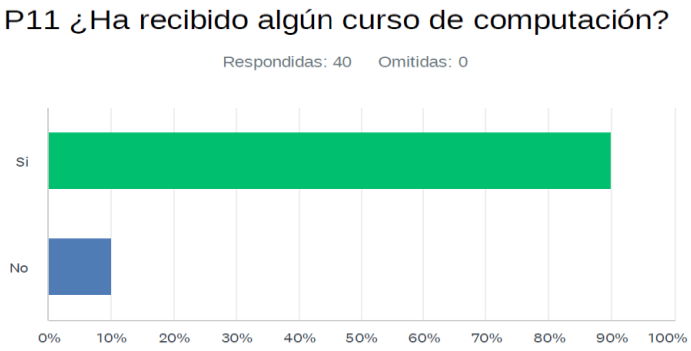
4.4.10. Pregunta 10. Permisos de acceso de la aplicación.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	72.50%	29
No	27.50%	11
TOTAL		40

La mayor parte de las personas encuestadas al instalar alguna aplicación en su dispositivo móvil sí revisa la solicitud de permisos que trae la aplicación.

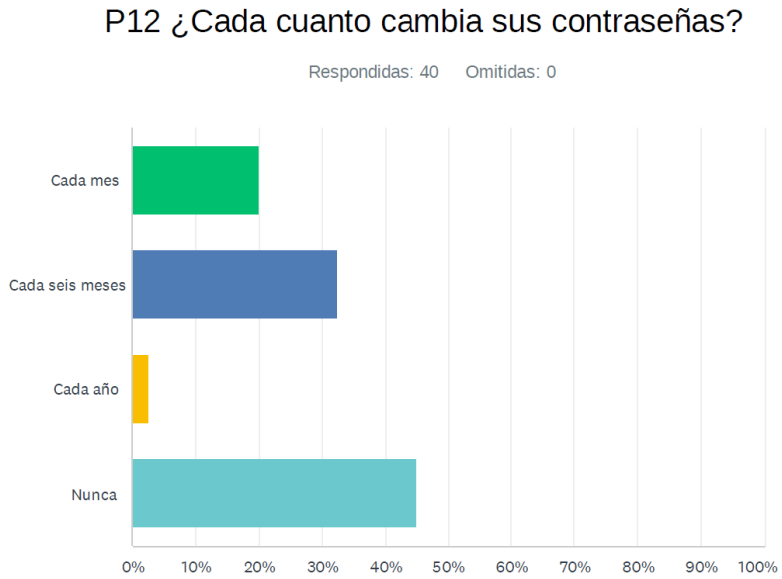
4.4.11. Pregunta 11. Curso de computación.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	90.00%	36
No	10.00%	4
TOTAL		40

De las 40 personas encuestadas el 90 % ha recibido alguna formación en temas de computación por lo que tiene cierto grado de alfabetización digital.

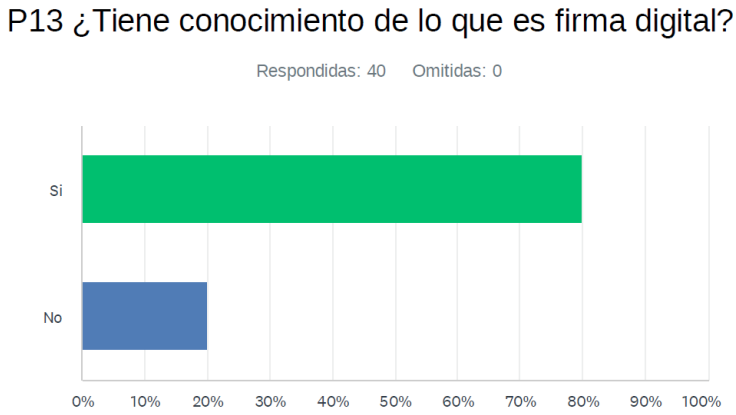
4.4.12. Pregunta 12. Cambio de contraseñas.



OPCIONES DE RESPUESTA	RESPUESTAS	
Cada mes	20.00%	8
Cada seis meses	32.50%	13
Cada año	2.50%	1
Nunca	45.00%	18
TOTAL		40

De los entrevistados en un porcentaje mayor no cambian sus contraseñas en ningún momento, el 32.5 % las cambia cada 6 meses y en porcentajes menores la cambian cada mes o cada año.

4.4.13. Pregunta 13. Conocimiento firma digital.



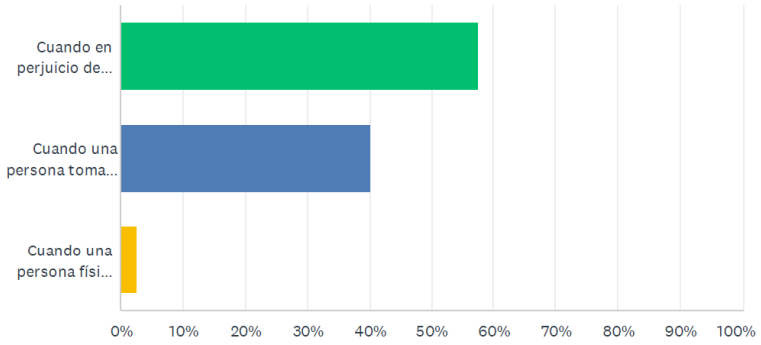
OPCIONES DE RESPUESTA	RESPUESTAS	
Si	80.00%	32
No	20.00%	8
TOTAL		40

La mayor cantidad de personas encuestadas tiene algún conocimiento de qué es firma digital.

4.4.14. Pregunta 14. Definición estafa informática.

P14 Según las definiciones que se le presentan a continuación. ¿Cuál creé que es la definición correcta del delito de estafa informática?

Respondidas: 40 Omitidas: 0

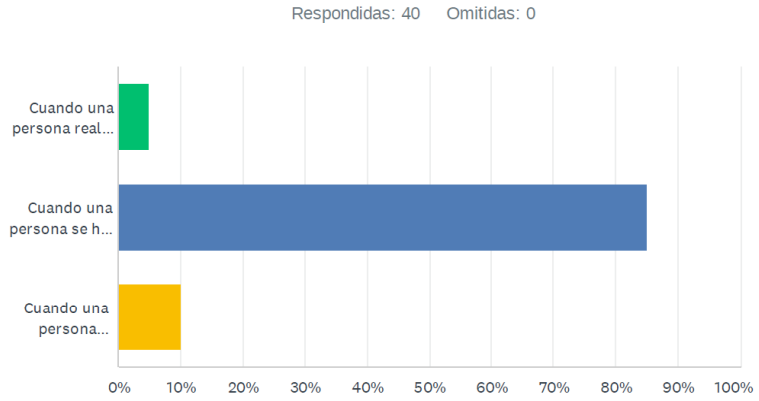


OPCIONES DE RESPUESTA	RESPUESTAS	
Cuando en perjuicio de una persona física o jurídica se manipulen o se influya en el procesamiento o resultado de datos de un sistema informático para obtener un beneficio indebido para si mismo o para otra persona.	57.50%	23
Cuando una persona tomando datos de un sitio web, los utiliza para realizar tramites o gestiones en nombre de otra persona en bancos o registro nacional.	40.00%	16
Cuando una persona física o jurídica, consienta la manipulación o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema informático, pero valiéndose de algún documento físico entregado por la persona	2.50%	1
TOTAL		40

De los 40 encuestados el 57 % tuvo una definición más clara del delito de estafa informática, en el resto de los porcentajes fue un poco más alejada.

4.4.15. Pregunta 15. Definición suplantación de identidad.

P15 Según las definiciones que se le presentan a continuación. ¿Cuál creé que es la definición correcta del delito de Suplantación de identidad?

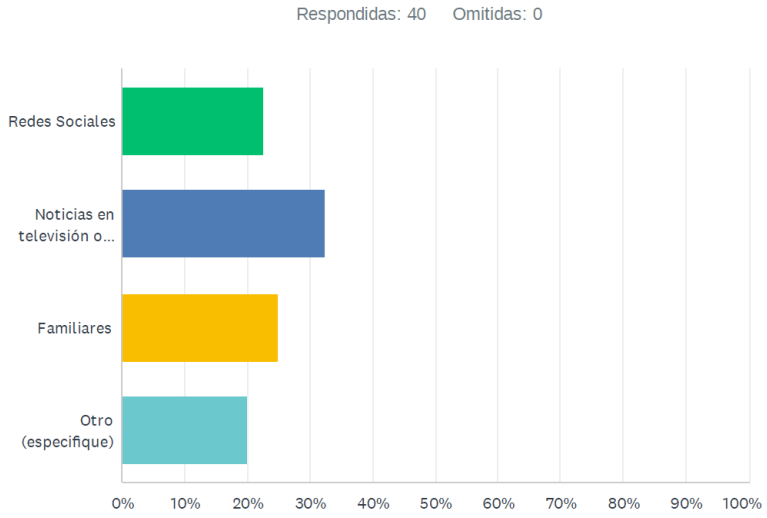


OPCIONES DE RESPUESTA	RESPUESTAS	
Cuando una persona realiza gestiones a nombre de otra persona con su autorización para ayudar con trámites o movimientos bancarios	5.00%	2
Cuando una persona se hace pasar por otra con el fin de obtener beneficios, de generar un fraude u ocasionar un daño.	85.00%	34
Cuando una persona presenta información de identificación de cédula de identidad que por las similitudes de fotografía coinciden con la persona dueña del documento de identificación.	10.00%	4
TOTAL		40

Similar a la pregunta anterior, la mayoría de las personas encuestadas indicó una definición más clara del delito de suplantación de identidad en un 85 %.

4.4.16. Pregunta 16. Medios para recomendaciones de navegación segura.

P16 ¿Por cuales medios recibe información sobre recomendaciones de navegación segura en internet?

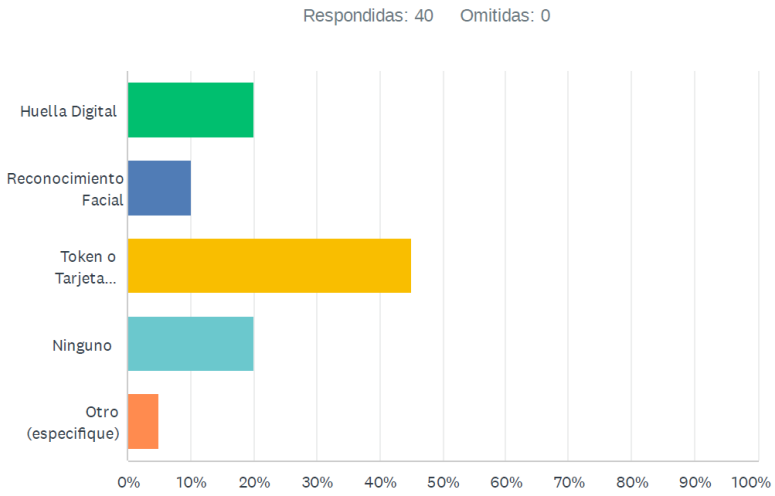


OPCIONES DE RESPUESTA	RESPUESTAS	
Redes Sociales	22.50%	9
Noticias en televisión o radio	32.50%	13
Familiares	25.00%	10
Otro (especifique)	20.00%	8
TOTAL		40

Según la información de las personas encuestadas la mayoría recibe información relacionada con navegación segura en Internet de noticias en diferentes medios o familiares. En porcentajes menores lo hacen de redes sociales u otros medios como el mismo Ageco.

4.4.17. Pregunta 17. Medios de doble factor usados.

P17 ¿Cuál de estos medios de doble factor de autenticación utiliza?



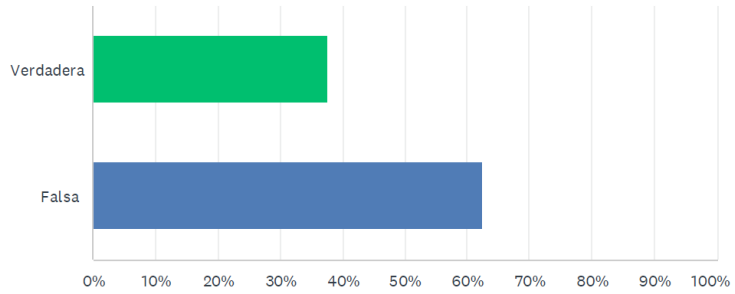
OPCIONES DE RESPUESTA	RESPUESTAS	
Huella Digital	20.00%	8
Reconocimiento Facial	10.00%	4
Token o Tarjeta dinámica	45.00%	18
Ninguno	20.00%	8
Otro (especifique)	5.00%	2
TOTAL		40

El medio de doble factor de autenticación por parte de las personas encuestadas que más utilizan es el *token* o tarjeta dinámica, seguido en porcentajes menores de otras opciones. El 20 % de las personas encuestadas no utiliza ninguno.

4.4.18. Pregunta 18. Página falsa o verdadera.

P18 Según la imagen anterior de acuerdo a lo visto en la página web, considera usted que esa página es falsa o verdadera.?

Respondidas: 40 Omitidas: 0



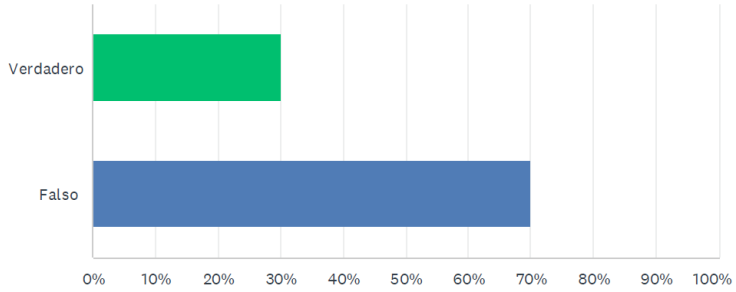
OPCIONES DE RESPUESTA	RESPUESTAS	
Verdadera	37.50%	15
Falsa	62.50%	25
TOTAL		40

En la pregunta n.º 18 se utilizó como referencia una página verdadera de un ente financiero nacional. Solo el 37.5 %de las personas encuestadas indicó que efectivamente era verdadera, el resto señaló que era falsa.

4.4.19. Pregunta 19. Correo electrónico falso o verdadero.

P19 ¿De la imagen de correo electrónico anterior puede reconocer si es falso o verdadero?

Respondidas: 40 Omitidas: 0

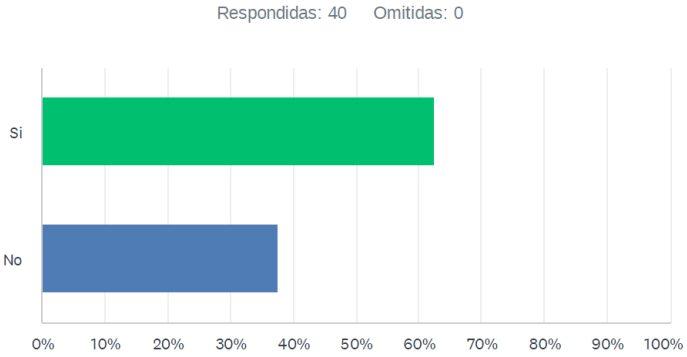


OPCIONES DE RESPUESTA	RESPUESTAS	
Verdadero	30.00%	12
Falso	70.00%	28
TOTAL		40

En la pregunta n.º 19 se utilizó como referencia una imagen de un correo electrónico falso a nombre del servicio de correo nacional. En este caso la mayoría de las personas encuestadas con un 70 % indicó que efectivamente ese correo era falso, el resto señaló que era verdadero.

4.4.20. Pregunta 20. Conocimiento de las *cookies*.

P20 ¿Tiene conocimiento de que son las cookies en una página web?



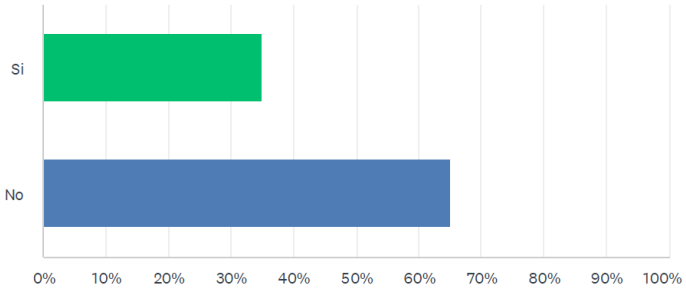
OPCIONES DE RESPUESTA	RESPUESTAS	
Si	62.50%	25
No	37.50%	15
TOTAL		40

De las personas encuestadas la mayoría afirma tener algún tipo de conocimiento de qué son las *cookies* en una página *web*, el resto desconoce del término.

4.4.21. Pregunta 21. Conocimiento medidas gubernamentales.

P21 ¿Tiene conocimiento de las medidas que ofrece el gobierno para ayudar a la población para responder a ataques de estafa informática y suplantación?

Respondidas: 40 Omitidas: 0

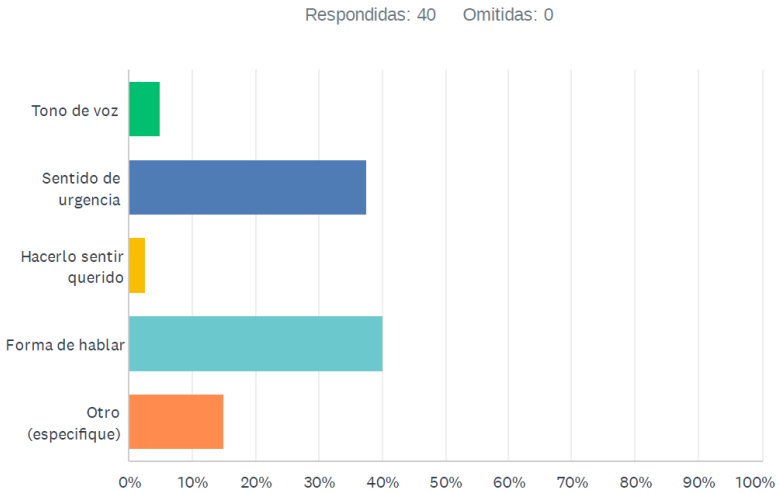


OPCIONES DE RESPUESTA	RESPUESTAS	
Si	35.00%	14
No	65.00%	26
TOTAL		40

La mayoría de las personas encuestadas afirma no conocer de medidas que ofrece el gobierno por medio de diferentes entes para responder a ataques que se relacionan con estafa informática o suplantación de identidad.

4.4.22. Pregunta 22. Características del estafador.

P22 ¿Qué característica cree usted que pueda identificar por parte de un estafador si usted está siendo víctima de un delito de estafa?



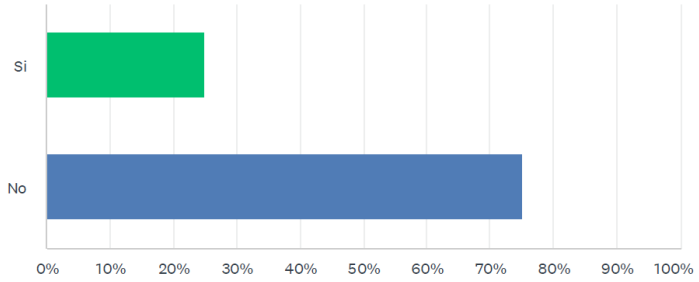
OPCIONES DE RESPUESTA	RESPUESTAS	
Tono de voz	5.00%	2
Sentido de urgencia	37.50%	15
Hacerlo sentir querido	2.50%	1
Forma de hablar	40.00%	16
Otro (especifique)	15.00%	6
TOTAL		40

En un eventual ataque de estafa las personas encuestadas indicaron que una de las características más identificables por parte de un estafador es la forma de hablar, seguido por el sentido de urgencia que expresan.

4.4.23. Pregunta 23. Procedimiento de denuncia.

P23 ¿Tiene conocimiento de cómo es el procedimiento de denuncia por temas de estafa informática y suplantación en el organismo de investigación judicial?

Respondidas: 40 Omitidas: 0



OPCIONES DE RESPUESTA	RESPUESTAS	
Si	25.00%	10
No	75.00%	30
TOTAL		40

La mayoría de las personas encuestadas desconoce cómo es el proceso de denuncia por estos delitos en el Organismo de Investigación Judicial.

Capítulo V. Propuesta de solución

5.1. Definición del marco de trabajo para mejorar la navegación en Internet de personas en edad laboral madura y persona adulta mayor

5.1.1. Justificación de la elaboración y propuesta. A partir de la investigación realizada desde los antecedentes del problema, estado de la cuestión, marco conceptual y con lo que se planteó en el marco metodológico y la información que se recopiló como parte del análisis de diagnóstico donde se recopilaron insumos tanto de instituciones de gobierno relacionadas, expertos en el tema y la información que fue posible conocer a partir del acceso a una muestra de población para el grupo objeto de estudio, coordinado con la Asociación Gerontológica Costarricense, se plantea la propuesta del marco de trabajo. El objetivo es que sea una herramienta de consulta, considerando los alcances definidos para delitos y afectaciones cuyo enfoque tiene la presente propuesta.

Con este fin, la propuesta considera las etapas de identificar, proteger, detectar, responder y recuperar. Al tomar como referencia el Ciclo de Deming y el marco de ciberseguridad del National Institute of Standards and Technology (NIST), plantea considerarse como una herramienta de consulta para la población en edad laboral madura y adulta mayor. Esta propuesta plantea su énfasis en las etapas preventivas, que permitan realizar un trabajo de concientización y aporte de herramientas prácticas para la población objeto de esta propuesta.

5.1.2. Comprensión de la población. De acuerdo con el análisis realizado en el Capítulo IV a los diferentes instrumentos aplicados, tanto a los expertos como a la población en edad laboral madura y adulta mayor de la Asociación Gerontológica Costarricense, es posible definir una serie de características para comprender la población. Además, se puede aplicar en el marco de trabajo propuesto una relación de recomendaciones o buenas prácticas ligadas a los mayores delitos informáticos que recibe esta población y contribuir así en una mejora en la seguridad de la navegación en Internet para estas personas.

Según lo propuesto en el apartado 3.3 del marco metodológico se realizó una serie de rúbricas como parte de la dimensión axiológica del enfoque alternativo que se utiliza para medir cuantitativamente la cantidad de riesgo en la que se encuentra la población atendida en el estudio. Estas se usaron en los instrumentos de recolección de datos en los tres ejes principales que son seguridad en Internet, alfabetización digital e identidad y se obtuvieron los siguientes resultados.

5.1.2.1. Vulnerabilidades que se identificaron en la población en edad laboral madura y adulta mayor de la Asociación Gerontológica Costarricense.

De acuerdo con el análisis de los instrumentos aplicados que se presentaron y analizaron en el Capítulo IV se determina una serie de vulnerabilidades o puntos débiles en la población en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense.

Tabla 46

Identificación de vulnerabilidades según instrumentos a personas en edad laboral madura y adultos mayores con alfabetización digital en la Asociación Gerontológica Costarricense

Vulnerabilidades que se identifican		Justificación
1	Identificación de sitios fraudulentos.	Según los datos del cuestionario y entrevistas se identifica que a la población se le dificulta reconocer diferencias entre sitios fraudulentos y sitios reales.
2	Mecanismos de control de contraseñas.	Con los datos recopilados en los instrumentos aplicados se identifica que la población no cambia la contraseña constantemente, en algunos casos utilizan la misma para varios sitios, las guardan en sitios físicos y no utilizan técnicas de construcción de contraseñas seguras. Además, la mayoría no utiliza mecanismos de doble factor de autenticación para mejorar la seguridad.
3	Desconocimiento de términos que se relacionan con protección de datos.	Se identifica desconocimiento en identificar cuáles datos se consideran restringidos, públicos y sensibles
4	Concientización y educación sobre ciberseguridad.	Aunque se identifica en la población una actitud precavida y de mucha seguridad en temas de Internet, a veces ese mismo temor los hace abandonar las tecnologías para diferentes actividades. La falta de conocimiento y educación en temas de ciberseguridad les hace tener más temor de la cuenta y les crea ese rechazo por utilizar el Internet o herramientas tecnológicas creyendo que la mayoría de las cosas son malas y peligrosas.

5	Desconocimiento sobre cómo actuar después de un delito en términos legales.	Se identifica que hay desconocimiento sobre cómo actuar después de la materialización de un delito y cómo responder en términos legales.

5.1.2.1. Resultados evaluación de criterios para mejorar la seguridad en Internet, aplicada a población de muestra atendida por Ageco. De acuerdo con la aplicación de los instrumentos del Capítulo 3.6 y su relación con la dimensión axiológica se lleva a cabo la siguiente evaluación de criterios para mejorar la seguridad en Internet, aplicada a la población de muestra atendida por Ageco.

Tabla 47

Resultados evaluación de criterios para mejorar la seguridad en Internet, aplicada a población de muestra atendida por Ageco

Criterio	Peso relativo evaluación	Pregunta relacionada	Instrumento	Tamaño de muestra	Escala de valoración	Valores obtenidos	Peso porcentual resultante
Reconocimiento de características para un sitio *web* oficial relacionado con afectación financiera y afectación de bienes muebles.	15 %	¿Cómo reconoce una página *web* real de una falsa?	Entrevista	15	1 a 5 = 5 % 6 a 10 = 10 % 11 a 15 = 15 %	3 personas logran reconocer	5 %
Uso de autenticación que permite protección de identidad.	15 %	¿Utiliza la misma contraseña para todos los sitios, correo y servicios que utiliza en Internet?	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 % 28 a 40 = 15 %	33 personas no utilizan la misma contraseña	15 %

Reconocimiento de datos personales, datos personales de acceso restringido, datos personales de acceso irrestricto y datos sensibles.	15 %	¿Qué información considera usted que es más importante proteger en Internet?	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 % 28 a 40 = 15 %	36 personas identifican datos sensibles	15 %
Tratamiento de correos electrónicos de origen desconocido	5 %	Cuando tiene un correo electrónico de un desconocido, ¿Qué hace?	Entrevista	15	1 a 7 = 2 % 8 a 15 = 5 %	14 personas actúan preventivamente	5 %
Uso de medios de pago electrónicos en Internet que no sean tipo débito y que cuenten con seguro	10 %	Cuando tiene qué hacer un pago en Internet, ¿Qué alternativa usa?	Cuestionario	40	1 A 20 = 5 % 21 A 40 = 10	38 personas no utilizan tarjeta de débito	10 %
Uso de navegadores *web* con almacenamiento de historial	5 %	¿Sabe que el navegador *web* almacena los sitios que se han visitado?	Entrevista	15	1 a 7 = 2 % 8 a 15 = 5 %	11 personas limpian historial	5 %

Uso de sitios *web* que requieren uso de *cookies*	5 %	¿Tiene conocimiento de qué son las *cookies* en una página *web*?	Cuestionario	40	1 a 20 = 2 % 21 a 40 = 5 %	25 personas conocen las *cookies*	5 %
Uso de redes inalámbricas públicas o sin credenciales de acceso	10 %	¿Utiliza con frecuencia redes inalámbricas gratuitas en sitios públicos para navegar en Internet desde su dispositivo?	Cuestionario	40	1 a 20 = 5 % 21 a 40 = 10 %	34 personas no utilizan redes inalámbricas públicas	10 %
Uso de actualizaciones para sistema operativo	5 %	Cuando utiliza la computadora o el celular realiza las actualizaciones, ¿Qué le ofrece el sistema operativo?	Cuestionario	40	1 a 20 = 2 % 21 a 40 = 5 %	28 personas sí actualizan sistema operativo	5 %

Uso de antivirus y *antimalware*	10 %	¿Cuáles antivirus utiliza en su computadora?	Entrevista	15	1 a 5 = 5 % 6 a 15 = 10 %	7 personas identifican usar un antivirus de paga	10 %
Uso de perfil de usuario diferente a administrador	5 %	¿Cuándo utiliza la computadora tiene los permisos necesarios para instalar diferentes programas?	Cuestionario	40	1 a 20 = 5 % 21 a 40 = 2 %	30 personas utilizan usuario administrador	2 %

Para la evaluación se obtiene un resultado de un 87 % para los criterios para mejorar la seguridad en Internet, aplicada a la población de muestra atendida por Ageco. De acuerdo con las escalas de medición de riesgo propuestas de 0 a 40: riesgo alto, 41 a 80: riesgo medio, 81 a 100: riesgo bajo, se determina un riesgo bajo para la muestra de población consultada.

5.1.2.2. Resultados evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco. De acuerdo con la aplicación de los instrumentos del Capítulo 3.6 y su relación con la dimensión axiológica, se lleva a cabo la siguiente evaluación de criterios en medición de alfabetización digital, aplicada a la población de muestra atendida por Ageco.

Tabla 48

Resultados evaluación de criterios en medición de alfabetización digital, aplicada a población de muestra atendida por Ageco

Criterio	Peso relativo evaluación	Pregunta relacionada	Instrumento	Tamaño de muestra	Escala de valoración	Valores Obtenidos	Peso porcentual resultante
Ha recibido capacitación sobre el uso de computadoras y *software*	10 %	¿Ha recibido algún curso de computación?	Cuestionario	40	1 a 20 = 5 % 21 a 40 = 10 %	36 personas	10 %
Conoce lo que significa *estafa informática* según el Código Penal de Costa Rica	15 %	Según las definiciones que se le presentan a continuación, ¿Cuál cree que es la definición correcta del delito de estafa informática?	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 % 28 a 40 = 15 %	23 personas logran identificar el concepto	10 %
Conoce lo que significa *suplantación de identidad* según el	15 %	Según las definiciones que se le presentan a continuación,	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 %	34 personas logran identificar el concepto	15 %

Código Penal de Costa Rica.		¿Cuál cree que es la definición correcta de suplantación de identidad?			28 a 40 = 15 %		
Conoce las herramientas habilitadas por el gobierno costarricense para el proceso de autenticación de identidad digital	15 %	¿Tiene conocimiento de lo que es firma digital?	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 % 28 a 40 = 15 %	32 personas conocen lo que es firma digital	15 %
Conoce las principales técnicas para suplantación de identidad que utilizan los ciberdelincuentes	15 %	¿Sabe cómo los delincuentes suplantan la identidad de las personas?	Entrevista	15	1 a 5 = 5 % 6 a 10 = 10 % 11 a 15 = 15 %	8 personas logran identificar	10 %
Conoce las principales técnicas para estafa informática que utilizan los ciberdelincuentes	15 %	¿Conoce cómo los delincuentes hacen estafas en Internet?	Entrevista	15	1 a 5 = 5 % 6 a 10 = 10 % 11 a 15 = 15 %	9 personas logran identificar	10 %

Cuenta con canales de información sobre temas que permitan mejorar la seguridad en Internet	15 %	¿Por cuáles medios recibe información sobre recomendaciones para navegación segura en Internet?	Cuestionario	40	1 a 13 = 5 % 14 a 27 = 10 % 28 a 40 = 15 %	32 personas cuentan con canales	15 %

Para la evaluación se obtiene un resultado de un 85 % para criterios en medición de alfabetización digital, aplicada a la población de muestra atendida por Ageco. De acuerdo con las escalas de medición de riesgo propuestas de 0 a 40: riesgo alto, 41 a 80: riesgo medio, 81 a 100: riesgo bajo, se determina un riesgo bajo para la muestra de población consultada.

5.1.2.3. Resultados de la evaluación de criterios de protección de identidad digital, aplicada a la población de muestra atendida por Ageco. De acuerdo con la aplicación de los instrumentos del Capítulo 3.6 y su relación con la dimensión axiológica, se lleva a cabo la siguiente evaluación para medir el riesgo de la protección de identidad en Internet.

Tabla 49

Resultados evaluación de criterios protección de identidad digital, aplicada a población de muestra atendida por Ageco

Criterio	Peso Relativo Evaluación	Pregunta relacionada	Instrumento	Tamaño de muestra	Escala de valoración	Valores Obtenidos	Peso porcentual resultante
Identifica la importancia de la protección de identidad digital y cómo protegerla	20	¿Cómo puede proteger su identidad en Internet?	Entrevista	15	1 a 7 = 10 % 8 a 15 = 20 %	10 personas identifican alternativas	20 %
Realiza gestión de contraseñas	20 %	¿Cada cuánto cambia sus contraseñas?	Cuestionario	40	1 a 13 = 7 % 14 a 27 = 15 % 28 a 40 = 20 %	22 personas gestionan	15 %
Conoce qué es firma digital	20 %	¿Tiene conocimiento de lo que es firma digital?	Cuestionario	40	1 a 13 = 7 % 14 a 27 = 15 % 28 a 40 = 20 %	32 personas indican conocer firma digital	20 %

Restringe el uso de datos personales de acceso restringido y datos personales sensibles incluidos en redes sociales	10 %	¿Qué información usted no publica en redes sociales?	Entrevista	15	1 a 7 = 5 % 8 a 15 = 10 %	13 personas restringen información	10 %
Uso de autenticación con factores biométricos	10 %	¿Cuál de estos medios de doble factor de autenticación utiliza?	Cuestionario	40	1 a 20 = 5 % 21 a 40 = 10 %	4 personas utilizan un factor biométrico	5 %
Uso de doble factor de autenticación	20 %	¿Cuál de estos medios de doble factor de autenticación usa?	Cuestionario	40	1 a 13 = 7 % 14 a 27 = 15 % 28 a 40 = 20 %	32 personas utilizan un segundo factor	20 %

Para la evaluación se obtiene un resultado de un 90 % para los criterios de protección de identidad digital, aplicada a la población de muestra atendida por Ageco. De acuerdo con las escalas de medición de riesgo propuestas de 0 a 40: riesgo alto, 41 a 80: riesgo medio, 81 a 100: riesgo bajo, se determina un riesgo bajo para la muestra de población consultada.

5.2. Lógica del marco de trabajo

5.2.1. Referencia para la construcción. Para la construcción del marco de trabajo se utiliza como referencia el marco para la mejora de la seguridad cibernética en infraestructuras críticas del Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América (NIST), en su versión 1.1. La NIST (2019) indica que:

> El Marco se enfoca en el uso de impulsores de negocios para guiar las actividades de seguridad cibernética y en la consideración de los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de la organización (s. p.).

Aunque el marco de la NIST se enfoca en infraestructuras críticas de las organizaciones, se decide usar de referencia por su lógica de etapas e identificación de riesgos, la cual se decide implementar y adaptar a las necesidades y alcances que se cubren en el presente trabajo.

5.2.2. Etapas del marco de trabajo. En cuanto a la referencia que se utiliza y con base en los delitos más importantes que se identifican en el estudio que afectan a la población en edad laboral madura y adulta mayor, se establecen cinco etapas o funciones básicas para manejar los delitos en diferentes ámbitos. Las funciones que se utilizan y referencian del marco de trabajo de NIST son identificar, proteger, detectar, responder y recuperar.

5.2.2.1. Función identificar. El marco de ciberseguridad NIST (2018) define la etapa identificar, como:

> Comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades. Las actividades en la Función Identificar son fundamentales para el uso efectivo del Marco. Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de seguridad cibernética relacionados permiten que una organización se enfoque y priorice sus esfuerzos de manera consistente con su estrategia de gestión de riesgos y sus necesidades empresariales (s. p.).

Con referencia al marco propuesto para mejorar la navegación en Internet de personas en edad laboral madura y persona adulta mayor, se utiliza esta etapa para identificar los principales componentes que pueden ser parte de un delito de estafa informática o suplantación de identidad. Además, se define cada uno según la Ley n.º 8968 en relación con la Protección de la Persona Frente al Tratamiento de sus Datos Personales. Asimismo, se identifican los métodos que más utilizan los delincuentes en dos ámbitos cubiertos en el trabajo que son la afectación financiera y afectación patrimonial.

5.2.2.2. Función proteger. La NIST (2018) define la etapa proteger como: “Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de seguridad cibernética” (s. p.).

De acuerdo con la aplicación que se implementó en el marco propuesto, la etapa proteger contiene una serie de elementos que se identificaron en la etapa posterior en las dos afectaciones. En este caso se lleva a cabo o menciona una serie de buenas prácticas para proteger y prevenir que se materialice alguno de los dos delitos abarcados en el desarrollo del marco.

5.2.2.3. Función detectar. Según la NIST (2018) la etapa detectar se define como la acción de:

> Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética. La Función Detectar permite el descubrimiento oportuno de eventos de seguridad cibernética. Los ejemplos de categorías de resultados dentro de esta función incluyen: Anomalías y eventos, Monitoreo continuo de seguridad y Procesos de detección (s. p.).

En el ámbito del marco propuesto para mejorar la navegación en Internet de personas en edad laboral madura y personas adultas mayores en la Asociación Gerontológica Costarricense se establece en esta etapa una serie de características para tener en cuenta. Lo anterior sobre todo en los diferentes métodos o vectores de ataque que utilizan los delincuentes para identificar en este caso que sea víctima en un momento dado de un ataque de estafa informática o de suplantación de identidad, siempre enfocado en las dos afectaciones centrales que son la financiera y patrimonial.

5.2.2.4. Función responder. La etapa o función responde dentro del marco para la mejora de la seguridad cibernética en infraestructuras críticas del NIST (2018) como: “Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética. La función Responder respalda la capacidad de contener el impacto de un posible incidente de seguridad cibernética” (s. p.).

En cuanto a la aplicación que se le da en el marco propuesto, se utiliza esta etapa de responder para identificar cuáles acciones se deben realizar en el momento que una persona sea víctima de un ataque. Esto con la finalidad de cortar la cadena del método que se emplea y no permitir ninguna afectación, ya sea financiera o patrimonial.

5.2.2.5. Función recuperar. La NIST (2018) define en su marco de ciberseguridad la etapa o función recuperar como el:

> Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética La función Recuperar admite la recuperación oportuna a las operaciones normales para reducir el impacto de un incidente de seguridad cibernética (s. p.).

Con referencia a la aplicación del marco propuesto, en la etapa de recuperar se recomienda una serie de acciones por realizar en caso de que se materialice alguno de los delitos abarcados en la investigación en cualquiera de los ámbitos, tanto financieros como patrimoniales.

5.3. Desarrollo del marco

5.3.1. Propuesta función identificar. En la Tabla 50 se presenta una propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital.

Tabla 50

Función identificar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital

Función	Afectación	Categoría	Subcategoría 1	Subcategoría 2	Subcategoría 3	Subcategoría 4
Identificar		Concepto de delitos	Estafa Informática	Código Penal Costa Rica, Artículo 217 bis: “En perjuicio de una persona física o jurídica, manipule e influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro”.		

			Suplantación de identidad	Código Penal Costa Rica, Artículo 230: “Suplantación de identidad. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero”.		
	Financiera	Información que proteger	Datos personales de acceso irrestricto según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales	Nombre completo		
				Número de identificación cédula de identidad		
				Fecha de nacimiento		
			Datos sensibles según Ley n.º 8968 Protección de la Persona Frente al	Fotografía		

			Tratamiento de sus Datos Personales			
			Datos personales de acceso restringido según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales	Correo electrónico	Usuarios	
					Contraseña	
					Doble factor autenticación	
				Dirección física		
				Información salarial		
				Información laboral		
				Números telefónicos		
				Datos Bancarios	Entidad con que se tienen servicios bancarios	
					Información de productos bancarios con	

					que se cuente	
					Números de cuenta	
					Numeración de tarjetas y pin	
					Estados de cuenta financieros	
					Credenciales de acceso	Usuarios
						Contraseña
						Multifactor habilitado por el servicio bancario
						Firma digital y su contraseña de uso

		Métodos que utilizan los delincuentes	Ingeniería social	Correos maliciosos que incluyen archivos o *links*		
				Sentido de urgencia		
				Búsqueda de generar ámbito de confianza		
				Comprometer información sensible (credenciales, números TC)		
				Mensajería SMS		
				Extracción de información personal (insumos para cometer delitos)		
			sitios *web* falsos entidades financieras	Se busca obtener credenciales de autenticación (comprometer credenciales)		
				Se busca persuadir al usuario para que acceda al sitio		

			Vishing	Uso de temas de actualidad para provocar atracción		
			Instalación de *remote desktop*	Se busca tener acceso remoto al equipo		
				Se busca tener nivel de control del equipo		
			Enmascarado número telefónico origen	Utilizando aplicaciones los delincuentes logran simular números origen de entidades financieras		
			Suplantación de funcionarios de instituciones o empresas	Delincuentes se hacen pasar por funcionarios con el objetivo de obtener datos personales o realizar cobros fraudulentos.		
			Depósito bancario falso producto de gestión en Internet	Los delincuentes simulan comprobantes de transferencias de entidades bancarias		
			Ventanas emergentes en el navegador al	Por medio de ventanas emergentes con información de interés para la víctima, se		

			acceder en sitios *web* (redirecciona a sitios maliciosos)	busca provocar en la víctima el ingreso de la víctima a sitios maliciosos		
	Bienes inmuebles	Información que proteger	Datos de acceso irrestricto	Propiedades		
				Sociedades	Información de activos de sociedades	
					Información de junta directiva de sociedad	
		Métodos que utilizan los delincuentes	Participación de notarios	El notario presenta información en el Registro Nacional a partir de un engaño por parte del estafador, o bien con dolo en su accionar.		
			Consulta de información de acceso irrestricto del Registro Nacional	El delincuente recolecta información como parte del proceso de ingeniería social.		

Como primer paso, la propuesta plantea la importancia de que la población objetivo tenga identificada información que puede utilizar un delincuente para generar afectación financiera o bienes inmuebles y con esto tomar las medidas preventivas y de manejo de sus activos de información por medio de los controles recomendados. Lo anterior para mantener en resguardo esta información personal y para el caso de información pública tomar las medidas preventivas.

5.3.1.1. Concepto de delitos. A partir del enfoque de la propuesta relacionada con los delitos de mayor cantidad de denuncias según lo identificado con la información obtenida del Organismo de Investigación Judicial, en el apartado de antecedentes del Capítulo 1, se parte de la conceptualización de los delitos de acuerdo con el Código Penal de Costa Rica. Estos referidos a estafa informática de acuerdo con el artículo 217 bis y el delito de suplantación de identidad, según el artículo 230.

5.3.1.1.1. Estafa informática. La conceptualización del delito de estafa informática tiene como propósito que la población objetivo de la propuesta logre identificar los alcances de lo tipificado en el Código Penal de Costa Rica y con esto reconocer cuando se encuentre en un posible riesgo asociado, o bien reconocer una afectación relacionada con este delito.

5.3.1.1.2. Suplantación de identidad. La conceptualización del delito de suplantación de identidad tiene como propósito que la población objetivo de la propuesta logre identificar los alcances de lo tipificado en el Código Penal de Costa Rica y con esto reconocer cuando se encuentre en un posible riesgo asociado, o bien reconocer una afectación relacionada con este delito.

5.3.1.2. Afectación financiera. En los siguientes apartados se presenta toda la información relacionada con la afectación financiera.

5.3.1.2.1. Información que proteger. Con el objetivo de identificar riesgos asociados con posible afectación financiera a partir de los delitos de estafa informática y suplantación de identidad, se plantean temas que la población objetivo de la propuesta debe identificar como elementos a los cuales se debe dar tratamiento para proteger y evitar ser víctima de un delito. Asimismo, se plantea que la población reconozca los métodos que utilizan los delincuentes.

5.3.1.2.1.1. Datos personales de acceso irrestricto según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. Según la Ley n.º 8968, artículo 9, se define como:

> Datos personales de acceso irrestricto son los contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. No se considerarán contemplados en esta categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular.

En esta categoría se identifica el nombre completo, número de identificación de cédula de identidad, fecha de nacimiento.

5.3.1.2.1.2. Datos sensibles según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. Según la Ley n.º 8968, artículo 9, se define como:

> Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros.
>
> En esta categoría se identifica la fotografía.

5.3.1.2.1.3. Datos personales de acceso restringido según Ley n.º 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales. Según la Ley n.º 8968, artículo 9, se define como:

> Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.

En esta categoría se identifica el correo electrónico, dirección física, información salarial, información laboral, números telefónicos y datos bancarios (entidad que brinda servicios, productos bancarios con que se cuenta, numeración de tarjetas y pin, números de cuenta, estados de cuenta financieros, credenciales de acceso).

5.3.1.2.2. Métodos que utilizan los delincuentes. Aunque los métodos que utilizan los delincuentes varían en el tiempo y a partir de la tecnología disponible, se identifican las principales técnicas orientadas al usuario final. Lo anterior mediante la investigación realizada de la técnica que se utiliza a la fecha a partir de la tecnología disponible.

5.3.1.2.2.1. Ingeniería social. Entre las variantes que corresponden con ingeniería social se encuentran factores que es necesario identificar como indicadores de riesgo, como:

1. Correos maliciosos que provengan de origen desconocido, con temas no solicitados y en algunos casos solicitar ingresar a *links* para la actualización de datos, o bien verificar información bancaria.
2. Sentido de urgencia, es un indicador muy importante debido a que busca que, por parte del usuario, se tome una acción contratiempo, sin dar tiempo de analizar el contexto, ya sea con la justificante de una afectación financiera en desarrollo o que si no se aprovecha la oportunidad que se está presentando dejará de recibir un beneficio.

3. Búsqueda de generar un ámbito de confianza, cuando terceros no conocidos por la persona usuaria buscan establecer por medio de una llamada telefónica o comunicación vía correo electrónico y solicitar información, o bien se solicita ingresar a sitios aportando el *link.*

4. Comprometer información sensible (credenciales, números TC). La numeración física de las tarjetas es un dato sensible que debe resguardarse y estar vigilantes sobre su uso, debido a que son insumos que permiten a los delincuentes realizar cargos sobre la cuenta bancaria del usuario. Por esta razón, en todo momento es necesario que la persona usuaria tenga en su custodia los plásticos de tarjetas con que cuente, así como las credenciales de acceso para los medios digitales de consulta de información relacionada.

5. Mensajería SMS, es una alternativa que utilizan los delincuentes en la que, a través de mensajes masivos, o bien al seleccionar a sus víctimas, envían información de interés mediante un *link* adjunto, o bien solicitando una respuesta, lo cual se convierte en un medio para cometer un delito.

6. Extracción de información personal (insumos para cometer delitos). En este punto la información compartida en redes sociales, la información entregada en cuestionarios donde se piden datos por concursos, o bien ofertas a las cuales se busca aplicar, son parte del proceso para extraer información personal que alimenta bases de datos lícitas que utilizan los delincuentes para cometer delitos de suplantación de identidad, así como estafa informática.

5.3.1.2.2.2. Sitios web falsos de entidades financieras. Por medio de los sitios *web* falsos de entidades financieras en los que la persona usuaria debe ingresar información de credenciales o numeración de autenticación de dispositivos de segundo factor de autenticación, los delincuentes buscan extraer datos del usuario. Asimismo, es importante que la persona usuaria identifique que los sitios *web* falsos de entidades financieras se buscan acceder por medio de la combinación con otros métodos por parte de los delincuentes.

5.3.1.2.2.3. Vishing. El *vishing* utiliza el lenguaje verbal para estafar a los usuarios persuadiéndolos para que realicen acciones que creen que les benefician, o bien para evitar una afectación en desarrollo. Con frecuencia, el *vishing* comienza donde termina el *phishing*. Esta técnica, según la información aportada por el Organismo de Investigación Judicial, es la predominante en Costa Rica, en el último año, de acuerdo con las denuncias recibidas.

5.3.1.2.2.4. Instalación de remote desktop. Se trata de personas desconocidas que se identifican como servicios de soporte y ayuda con equipo informático, ya sea equipos de escritorio, portátiles o dispositivos móviles y que buscan instalar aplicaciones de acceso remoto para realizar acciones de soporte al usuario sin que sea un servicio solicitado por la persona usuaria. Aunque empresas brindan esta modalidad de asistencia, se hace solamente con un caso de reporte solicitado por la persona usuaria con una garantía vigente del equipo.

En los casos de instalación de herramientas como parte de un servicio de soporte solicitado es importante que la persona usuaria siempre esté consciente de la aplicación que se solicita instalar, así como proceder con la desinstalación tan pronto la sesión de soporte finalice.

5.3.1.2.2.5. Enmascarado número telefónico origen. A partir de aplicaciones disponibles en el mercado es posible que se despliegue en el identificador de número telefónico un número manipulado que no corresponde al real, por lo tanto, es una herramienta que emplean los delincuentes para generar credibilidad en la persona usuaria. Por esta razón, el número que se despliega en los identificadores es modificable y, por esto, es importante tomar consciencia al recibir llamadas telefónicas que se relacionan con temas financieros, entre otros.

5.3.1.2.2.6. Suplantación de funcionarios de instituciones o empresas. Los casos de usuario que son contactados, ya sea telefónicamente o vía correo electrónico, en los que se busca obtener datos o realizar gestiones asociadas con instituciones públicas o servicios bancarios, no corresponden al proceder de estas entidades. Es importante que la persona usuaria tome en cuenta que, al investigar información disponible en Internet, los delincuentes pueden obtener insumos de información sobre la persona usuaria que les permiten generar credibilidad.

5.3.1.2.2.7. Depósito bancario falso producto de gestión en Internet. Según la información obtenida del Organismo de Investigación Judicial, esta técnica es muy utilizada por los delincuentes en el último año, donde por medio de una imagen hacen creer al usuario que se le ha realizado un pago y buscan presionar al usuario para que no valide el depósito en sus cuentas bancarias. Generalmente, se ha asociado con usuarios que se encuentran en proceso de venta de artículos o servicios.

5.3.1.2.2.8. Ventanas emergentes en el navegador al acceder en sitios web (redirecciona a sitios maliciosos). Al acceder a determinados sitios *web* es posible que se activen ventanas emergentes que pueden contener información atractiva o de interés para la persona usuaria. Sin embargo, es importante que la persona usuaria identifique que estas ventanas o enlaces pueden redirigir a sitios *web* con posibilidad de descarga de *malware* que puede afectar o comprometer el equipo, ya sea de escritorio, portátil o dispositivo móvil.

5.3.1.3. Afectación por bienes inmuebles. En los siguientes apartados se detalla la información relacionada con la afectación por bienes inmuebles.

5.3.1.3.1. Información que proteger. A continuación se define la información por proteger.

5.3.1.3.1.1. Datos de acceso irrestricto. Información que se encuentra disponible en el Registro Nacional de la República de Costa Rica, en su portal *web*, por el principio de publicidad registral es de consulta pública. Por este motivo son insumos que un delincuente puede utilizar para materializar un delito relacionado con bienes muebles o inmuebles.

5.3.1.3.2. Métodos que utilizan los delincuentes. Seguidamente se definen los métodos que utilizan los delincuentes.

5.3.1.3.2.1. Participación de notarios. El Registro Nacional de la República de Costa Rica es una institución que entre sus funciones está proceder según lo solicitado por personas notarias de Costa Rica, que se encuentren autorizadas debidamente por la Dirección Nacional de Notariado, para ejercer sus funciones, quienes cuentan con fe pública en materia de bienes muebles e inmuebles. Por lo tanto, son responsabilidad de las personas notarias las solicitudes que se presentan para su trámite al cumplir con los requisitos y procedimiento, así como la verificación de identidad de las partes involucradas. Por este motivo, las personas notarias pueden participar en la materialización de un delito ya sean como objeto de una suplantación de identidad, o bien sean partícipes del delito.

5.3.1.3.2.2. Consulta de información de acceso irrestricto del Registro Nacional. Debido a que la información de bienes inmuebles y muebles de Costa Rica corresponde a datos personales de acceso irrestricto, los delincuentes tienen información de consulta disponible en servicios del Registro Nacional. Por esta razón, los usuarios deben ser conscientes de este riesgo.

5.3.2. Propuesta función proteger. En la Tabla 51 se muestra la propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuenta con alfabetización digital.

Tabla 51

Función proteger, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores, que cuenta con alfabetización digital

Función	Afectación	Categoría	Subcategoría 1	Subcategoría 2
Proteger	Concientización	Medios de información	Información de recomendaciones en temas de seguridad a partir de redes sociales como fuente de información	Obtener información de Asociación Bancaria Costarricense, sitios *web* oficiales de servicios bancarios, perfiles de Facebook para especialistas en temas de ciberseguridad.
			Personas de confianza para consulta	Contar con personas de confianza que puedan brindar apoyo para atender dudas sobre uso de tecnología y riesgos de ciberseguridad
			Medios oficiales del gobierno	Obtener información de sitios *web* oficiales de Micitt, Conapam, Organismo de Investigación Judicial, Registro Nacional.
		Cursos de capacitación	Ofimática y acceso a Internet	Desarrollo de habilidades y alfabetización digital.
			Concientización en temas de seguridad	Desarrollo de habilidades y alfabetización digital.

	Financiera	Datos bancarios	Institución bancaria que brinda servicios	Resguardar información de entidad bancaria que se utiliza
			Productos bancarios con que se cuenta	Resguardar la información de productos bancarios que se utilizan con la entidad financiera debido a que es un insumo de identificación de superficie de ataque por parte de los delincuentes.
			Número de cuenta	Resguardar información de número de cuenta que se utiliza
			Seguro de tarjetas	Habilitar el servicio de seguro, ya sea para tarjetas de crédito o tarjetas de débito según las posibilidades habilitadas por la entidad financiera.
			Estados de cuenta	Resguardar información de estados de cuenta debido a que representa ingresos y egresos
		Credenciales de acceso para asegurar identidad	Usuario	Datos públicos, ya que los bancos utilizan el número de cédula del cliente como usuario. En caso de entidades financieras con usuario generado, resguardar esta información.

		digital	Contraseña	Utilizar las políticas de la entidad financiera para generar una frase con sentido personal, como contraseña, reemplazando las vocales con números o caracteres especiales.
				Utilizar diferentes credenciales de acceso para cada acceso a entidad financiera, o bien servicio que requiera autenticación. Nunca se debe utilizar la misma contraseña en todos los servicios y mucho menos utilizar la misma contraseña de servicios de uso gratuito (ejemplo Facebook, Gmail, etc.), para los servicios bancarios.
				Utilizar gestores digitales para generar y resguardar contraseñas.
				Frecuencia de actualización de contraseñas.
				Utilizar los servicios de reconocimiento por medio de autenticación biométrica.

			Firma digital	Resguardar tarjeta física y dispositivo de lectura. Utilizar gestores digitales para generar y resguardar contraseña.
		Métodos de múltiple factor de autenticación entregado por entidad financiera	OTP (*one time password*)	Resguardar en lugar seguro y no accesible para terceros
			Tarjeta dinámica	Contar con alternativas de autenticación con factores biométricos según entidad financiera
			Métodos de autenticación biométricos	Contar con alternativas de autenticación con factores biométricos según entidad financiera
			Aplicaciones en dispositivos móviles	Resguardar en lugar seguro y no accesible para terceros
			Clave de acceso	Utilizar extensiones verificadas por la tienda oficial, para mejorar la seguridad, que permiten bloquear publicidad, ventanas emergentes, etc.
		Métodos de acceso a servicios bancarios	Navegadores en equipos de escritorio, equipos portátiles y dispositivos móviles	Utilizar navegadores enfocados en la privacidad.
				Utilizar motores de búsqueda enfocados

				en la privacidad.
				Configuración de navegador para borrado de historial al cerrar.
				Borrado de *cookies* antes del inicio de sesión en un sitio *web* de entidad financiera.
				Verificación de certificados, en el campo emitido para validar que corresponda con la entidad financiera.
				No almacene en el dispositivo móvil información como claves de acceso, pin u otros datos de información sensible.
				Mantener actualizadas a sus últimas versiones los navegadores.
				Uso de autenticación de acceso al dispositivo, por medio de datos biométricos.
				Utilizar la opción de salida dentro del sitio *web* oficial del banco, antes de cerrar la ventana de navegación dentro

				del navegador que se utiliza.
				No abrir otras páginas *web* mientras se llevan a cabo gestiones en el sitio oficial de la entidad financiera.
			Aplicaciones dispositivos móviles	Utilizar la opción de salida de la aplicación del banco antes de cerrar la ventana en el dispositivo móvil.
				Si no se utiliza el Bluetooth, wifi, NFC, Phone Visibility, proceda a desactivarlos
				No almacene en el dispositivo móvil información como claves de acceso, pin u otros datos de información sensible.
				Uso de alternativas para solicitar autenticación al abrir aplicaciones
		Seguridad en dispositivo de acceso	Equipo de escritorio o equipo portátil	Tener instalado un aplicativo *antimalware* de paga, a partir de los servicios que ofrece respecto una opción gratuita.
				Utilizar una cuenta de usuario sin privilegios de instalación de *software*,

				con el objetivo de detectar cuando el sistema operativo se encuentra en un proceso de instalación de *software*, de manera que la persona usuaria tenga que ingresar una contraseña para instalar la aplicación.
				No utilizar redes públicas gratuitas para acceso a Internet. En caso de tener que utilizar una red pública, utilizar servicio de Virtual Private Network (VPN) para cifrar el tráfico que se mueve en la red por medio de la cual se realiza la conexión.
				Mantener actualizado el sistema operativo, mediante la habilitación de actualizaciones automáticas de Windows.
			Dispositivo móvil	Mantener actualizado el sistema operativo, mediante la habilitación de actualizaciones automáticas.
				Mantener instalada una herramienta de antivirus en el dispositivo móvil
				Para la descarga de aplicaciones utilizar

				los mercados oficiales según el fabricante del dispositivo (PlayStore, AppGalery, *App* Store)
				Utilizar alternativas de autenticación biométrica para el acceso a desbloqueo del dispositivo.
				No utilizar redes públicas gratuitas para acceso a Internet. En caso de tener que utilizar una red pública, utilizar servicio de Virtual Private Network (VPN) para cifrar el tráfico que se mueve en la red por medio de la cual se realiza la conexión.
				Verificar antes de la instalación de aplicaciones los permisos solicitados respecto a la funcionalidad deseada de la aplicación.
		Servicios de seguridad que brinda la entidad financiera	De acuerdo con las opciones que cada entidad financiera tiene disponibles, implementarlas. Por ejemplo, límites de transacciones, notificaciones de cuentas favoritas, notificaciones de transferencias, uso de tarjetas virtuales para compras en Internet, notificaciones	

			al realizar cambio de contraseña.	
		Información de huella digital del usuario en Internet	Publicación en redes sociales	No publicar información privada o información sensible según la ley de protección de datos.
				Con el objetivo de que no sea posible fácilmente por los delincuentes validar la identidad de una persona, o bien inferir las claves de acceso por utilizar, no publicar nombre completo, edad, nombres o imágenes de miembros de familia, nombre o imágenes de mascotas, pasatiempos, fechas de nacimiento, lugar de habitación, grupos sociales a los que pertenezca.
			Identificación de cuenta de correo asociada con notificaciones por parte de entidad bancaria que brinda servicios	Utilizar cuentas de correo exclusivas para notificaciones bancarias, de manera que no sean las cuentas de correo que se entregan para recibir información en general.
	Bienes	Datos relacionada con bienes inmuebles y muebles	Información disponible en el Registro Nacional	Es importante conocer que es información clasificada como pública en la Ley de Protección de Datos. Sin embargo, el registro permite a los usuarios verificar en su sitio *web* la información de bienes inmuebles y

				muebles. Adicionalmente, el registro Nacional cuenta con el servicio de alerta registral, donde la persona usuaria que contrate el servicio recibe notificaciones con cualquier anotación realizada para los bienes muebles e inmuebles.
			Información de planos o certificaciones que se tengan en físico.	No compartir por medios digitales como redes sociales fotografías o archivos digitalizados a partir del documento físico.
		Información de huella digital del usuario en Internet	Publicación en redes sociales	Con el objetivo de que no sea posible fácilmente por los delincuentes validar la identidad de una persona no publicar nombre completo, edad, nombres o imágenes de miembros de familia, fechas de nacimiento, lugar de habitación, grupos sociales a los que pertenezca.

5.3.2.1. Concientización. Para tener una mejor protección de los datos y prevenir ataques como estafa informática y suplantación de identidad es importante crear consciencia y mantenerse informado sobre estos temas. Lo anterior para estar al tanto de nuevas técnicas de ataque y, sobre todo, cómo prevenir que se pueda tener algún grado de afectación.

5.3.2.1.1. Medios de información. Existen diferentes medios de información en los cuales se puede encontrar recomendaciones, noticias y buenas prácticas en temas de seguridad y protección de datos. Es importante que esos medios sean de confianza y actualizados, algunos de los medios en los cuales se puede contar son los siguientes.

5.3.2.1.1.1. Información de recomendaciones en temas de seguridad a partir de redes sociales como fuente de información. En redes sociales existen diferentes perfiles como la Asociación Bancaria Costarricense, perfiles de sitios bancarios oficiales y especialistas en ciberseguridad que pueden ayudar a mantenerse informado y actualizado en temas de buenas prácticas para prevenir ataques cibernéticos. En Costa Rica existen páginas como Whitejaguars, Noches de ciberseguridad o más tecnología que enfatizan en estos temas de capacitación y concientización.

5.3.2.1.1.2. Personas de confianza para consulta. Se considera importante tener personas de confianza dentro de la familia o amigos que puedan ayudar o aclarar dudas sobre algunos temas que se relacionan con ciberseguridad. Sin embargo, se debe tener cierto grado de malicia porque también se han presentado casos de personas que son cómplices en ataques a sus propios familiares.

5.3.2.1.1.3. Medios oficiales del gobierno. Es importante obtener información en medios oficiales del gobierno, los cuales brindan campañas de concientización y educación en temas de ciberseguridad e informan de medidas de prevención al respecto. Algunos de los más importantes son el Micitt, Conapam, el Organismo de Investigación Judicial y el Registro Nacional..

5.3.2.1.2. Cursos de capacitación. En cuanto a cursos de capacitación para mantenerse informado, primero es importante generar cierto grado de habilidades y alfabetización digital en términos de manejo del sistema operativo, programas o aplicaciones y navegación en Internet. Lo anterior para tener un mejor dominio de conceptos y entender mejor algunos métodos de protección y prevención. Algunas entidades como Ageco y las municipalidades imparten este tipo de cursos para educar a la población en estos términos.

5.3.2.2. Afectación financiera. En los siguientes apartados se presenta información relevante relacionada con la afectación financiera.

5.3.2.2.1. Protección a datos bancarios. Para proteger los datos bancarios que se identificaron previamente en la función identificar es importante tener una serie de medidas, ya que en manos de ciberdelincuentes estos datos pueden ser muy útiles para concretar un delito. Algunas medidas de protección son:

5.3.2.2.1.1. Institución bancaria en la cual se tiene servicios. En la medida de lo posible se recomienda mantener en secreto la entidad bancaria donde se tienen servicios. Esto para generar un grado más de privacidad y seguridad al servicio bancario.

5.3.2.2.1.2. Productos bancarios con que se cuenta. Además, dentro de lo posible se recomienda mantener en secreto los productos bancarios que se utilizan en la entidad financiera, entiéndase servicios como cuentas de ahorros, cuentas corrientes, ahorros programados, tarjetas, entre otros. Lo anterior para generar un grado más de privacidad y seguridad al servicio bancario.

5.3.2.2.1.3. Número de cuenta. Se recomienda como medida de protección mantener protegidos o en secreto los números de cuenta. Aunque son necesarios para hacer transacciones es importante resguardarlos y tratar de no exponerlos en lugares como redes sociales o canales de comunicación inseguros.

5.3.2.2.1.4. Seguro de tarjetas. Se recomienda como medida de protección asegurar las tarjetas, tanto de débito como crédito, esto para proteger el dinero en caso de algún tipo de incidente sobre estos medios bancarios. Este método es una garantía de recuperación de dinero.

5.3.2.2.1.5. Estados de cuenta. Al igual que los productos bancarios y la entidad es importante mantener en secreto y protegidos los estados de cuenta recibidos por medio de correos electrónicos o generados por los sistemas financieros. Esto se debe a que esta información representa ingresos y egresos a las cuentas personales y pueden servir de insumo para generar algún tipo de ataque.

5.3.2.2.2. Protección a credenciales de acceso para asegurar la identidad digital. Para proteger las credenciales de acceso para asegurar la identidad digital que se identificó previamente en la función identificar es importante tener una serie de medidas, ya que los accesos a estas por parte de delincuentes pueden generar el desarrollo de un delito de estafa o suplantación y provocar pérdidas económicas muchas veces irreversibles. Algunas medidas de protección son:

5.3.2.2.2.1. Usuario. En algunas entidades financieras se utiliza como identificador de usuario la cédula y al ser un dato de acceso público según la Ley n.º 8969 esta no se puede proteger. En otras instituciones utilizan otro tipo de identificador de usuario, el cual es importante mantenerlo en secreto y no publicarlo en lugares inseguros ni darlo a personas que no son de confianza.

5.3.2.2.2.2. Contraseña. La contraseña es importante mantenerla en secreto y en un lugar seguro, además, utilizar diferentes técnicas para crearla. Por ejemplo, usar las políticas de creación de contraseñas de la entidad bancaria de uso, generar frases de sentido personal como contraseñas en las que se cambien vocales con número o caracteres especiales.

Para proteger los accesos se recomienda utilizar diferentes credenciales de acceso para cada entidad financiera, o bien un servicio que requiera autenticación, así como una actualización periódica. Nunca se debe usar la misma contraseña en todos los servicios y mucho menos utilizar la misma contraseña de servicios de uso gratuito (ejemplo Facebook, Gmail, etc.), para los servicios bancarios.

Una alternativa para mantener seguras las contraseñas es el uso de gestores digitales de contraseñas o bóvedas, los cuales permiten la creación de contraseñas con condiciones especiales y su almacenaje. La única contraseña que se debe resguardar es la maestra, la cual abrirá el gestor o bóveda digital de contraseñas. En la actualidad, en el mercado existe gran variedad de gestores, tanto gratuitos como de paga que facilitan considerablemente la gestión y seguridad de las contraseñas personales no solo en entidades financieras, sino también en cualquier aplicación o página de uso diario. También es importante habilitar servicios de reconocimiento de autenticación biométrica si es posible para dar una capa más de seguridad al acceso.

5.3.2.2.2.3. Firma digital. Si se posee un acceso por autenticación con firma digital es importante siempre resguardarla en un lugar seguro y nunca prestar o darla a un tercero. Asimismo, es muy relevante proteger el pin de activación y no dejarlo expuesto para que puedan identificarlo terceros.

5.3.2.2.3. Protección a métodos de múltiple factor de autenticación entregado por entidad financiera. Para proteger los métodos de doble factor de autenticación que brinda la entidad financiera es importante tener una serie de medidas de seguridad, ya que estos métodos en manos de delincuentes facilitan la materialización de un delito y, por ende, el robo económico de las cuentas asociadas con este mecanismo. Algunas medidas de protección son las siguientes:

5.3.2.2.3.1. OTP (one time password). Se debe resguardar en un lugar seguro y no accesible para terceros. Es importante mencionar que este dispositivo puede darse de dos maneras, la primera con un dispositivo físico y la segunda al generarlo con una aplicación secundaria de la entidad financiera. Es relevante proteger el dispositivo y no compartir los códigos generados por ningún motivo, si es de manera digital se debe proteger la aplicación de ser posible con autenticación biométrica. Esta es información que ningún banco pedirá nunca.

5.3.2.2.3.2. Tarjeta dinámica. Para la tarjeta dinámica es importante nunca compartir ningún tipo de fotografía de ella ni prestarla a terceros. Este tipo de dispositivo sirve como validador de movimientos y matrículas de cuentas, por lo que alguna fuga de esta información pone en peligro las cuentas.

5.3.2.2.3.3. Métodos de autenticación biométricos. Es importante habilitar factores biométricos en las aplicaciones bancarias o en los accesos a estas plataformas para generar una capa adicional de seguridad con factores físicos propios de la persona, lo cual es muy complicado para los delincuentes obtener.

5.3.2.2.3.4. Aplicaciones en dispositivos móviles. Para proteger el ingreso no autorizado en aplicaciones móviles financieras es importante utilizar algún tipo de autenticación biométrica o alternativa de ocultamiento de aplicación que brinda el sistema operativo móvil. Estas características ayudan a generar más seguridad de entrada a las aplicaciones financieras y así prevenir que otra persona pueda ingresar fácilmente.

5.3.2.2.4. Protección a métodos de acceso a servicios bancarios. Los métodos de acceso más identificados para ingresar a los servicios bancarios son los navegadores en los equipos de escritorio o móviles y las aplicaciones propias de las entidades financieras. Para crear un ambiente más seguro en el momento de ingresar a estas plataformas se recomiendan las siguientes medidas de protección.

5.3.2.2.4.1. Navegadores en equipos de escritorio, equipos portátiles y dispositivos móviles. Para brindar mejor protección al navegador *web*, que es la ventana más importante para entrar a los servicios bancarios, se recomiendan diferentes acciones. Por ejemplo, para prevenir o bloquear publicidad o ventanas emergentes en el navegador se aconseja instalar algún tipo de bloqueador desde la tienda oficial del navegador y con una buena calificación esto impedirá y bloqueará todo tipo de mensaje publicitarios o ventanas emergentes.

Otra alternativa es utilizar navegadores enfocados en la privacidad, los cuales poseen por defecto bloqueadores de publicidades y rastreadores, sesiones privadas de navegación y buscadores enfocados en la privacidad, algunos ejemplos son Brave, Mozilla, Opera y Vivaldi. Además, se recomienda usar buscadores enfocados en la privacidad, los cuales bloquean rastreadores que se utilizan para *marketing* o simplemente para ver los movimientos en Internet que realiza una persona, por ejemplo, *duck go* y *brave search*.

En términos de usabilidad se recomienda borrar periódicamente o programar en el navegador que se borre el historial y las *cookies* al cerrarlo, esto limpiará el navegador y eliminará algún tipo de rastreador. También es importante que al ingresar a una página bancaria se revise el certificado para validar que es una página original.

Lo anterior se realiza en primer término al digitar la dirección de la entidad financiera en la barra de búsqueda, con el objetivo de validar que sea la dirección oficial y, en segundo término, se da clic en el candado de la página, después en ver certificado y ahí se puede verificar que si está emitido para la dirección del banco la página es totalmente verdadera. Además, es relevante estar atento a las actualizaciones del navegador, ya que cada actualización mejorará la seguridad de diferentes vulnerabilidades que se puedan encontrar.

En términos de estar dentro de una plataforma bancaria en el navegador se recomienda como medida de protección no abrir otras páginas *web* mientras se llevan a cabo gestiones en el sitio oficial de la entidad financiera. Además, una vez terminadas las gestiones bancarias se aconseja dar clic en el botón de cerrar sesión, esto para verificar que la sesión se cerró correctamente.

5.3.2.2.4.2. 2. Aplicaciones de dispositivos móviles. Como método de seguridad y protección en el acceso por medio de aplicación de dispositivo móvil se recomienda no almacenar información como claves de acceso, pin u otros datos sensibles. Antes de entrar a la aplicación bancaria si no se utiliza el Bluetooth, wifi, NFC o Phone Visibility estos se deben desactivar. En caso de requerir almacenar la información de autenticación es fundamental utilizar aplicaciones de gestión de contraseñas que se obtengan de las tiendas oficiales según el sistema operativo del dispositivo, con el objetivo de asegurar su procedencia.

Cuando se utilice la aplicación y no una vez realizados los trámites necesarios se recomienda utilizar la opción de salida de la aplicación del banco antes de cerrar la ventana en el dispositivo móvil, esto con el fin de verificar que la sesión se cerró correctamente y no quedó abierta como proceso en el dispositivo móvil. Para brindar todavía más seguridad de ingreso a la aplicación se aconseja usar la autenticación por medio de biometría, esto genera una capa de seguridad más fuerte.

5.3.2.2.5. Protección y seguridad en dispositivos de acceso. En los dispositivos en los que se accede a los servicios bancarios también es importante tener una serie de consideraciones para fortalecer la seguridad. En estos los delincuentes se pueden aprovechar de vulnerabilidades presentes en ellos e instalar código malicioso para espiar, extraer o dar acceso remoto al dispositivo. Algunas recomendaciones para proteger los dispositivos son las siguientes:

5.3.2.2.5.1. Equipo de escritorio o portátil. Es importante mantener activadas y constantemente instaladas las actualizaciones del sistema operativo que se sugieren, ya que estas ayudan a disminuir vulnerabilidades encontradas y mejoran la seguridad del sistema operativo. Una buena práctica para prevenir la instalación de *software* malicioso es utilizar una cuenta de usuario sin privilegios de instalación de *software*, esto con el objetivo de detectar cuando el sistema operativo se encuentra en un proceso de instalación de *software*, de manera que la persona usuaria tenga que ingresar una contraseña para instalar la aplicación. En el momento que aparece la notificación se descarta totalmente la instalación del *software* malicioso.

Asimismo, es importante que el dispositivo tenga algún tipo de *antimalware* instalado, con el fin de prevenir infecciones. Principalmente, se recomienda que sea de paga para que se pueda contar con mayores funciones de protección con respecto a *antimalware* gratuitos.

Otra práctica para mantener protegido el dispositivo es no utilizar redes públicas gratuitas para acceso a Internet. En caso de tener que usar una red pública, se recomienda emplear un servicio de Virtual Private Network (VPN) para cifrar el tráfico que se mueve en la red por medio de la cual se realiza la conexión. En el mercado existen diferentes servicios de VPN, tanto de paga como gratuitos y algunos ejemplos son Nordvpn, Cyberghost, Protonvpn, entre otros. La mayoría posee servicios gratuitos que se mejoran con paquetes de pago.

Por último, es fundamental que los servicios que se utilicen ofrezcan mecanismos de autenticación, autorización y encriptación, con el objetivo de tener comprobación de identidad al acceder a estos.

5.3.2.2.5.2. Dispositivo móvil. Al igual que en los dispositivos de escritorio o portátiles es importante mantener las últimas actualizaciones del sistema operativo instaladas, ya que estas mejoran la seguridad y eliminan alguna vulnerabilidad encontrada. En el caso de los dispositivos móviles es relevante solo descargar aplicaciones que provengan de mercados oficiales según el fabricante del dispositivo (PlayStore, App Gallery, App Store), esto porque los mercados de terceros pueden tener versiones modificadas de aplicaciones que ponen en peligro la privacidad.

Es recomendable evitar utilizar redes wifi gratuitas, en especial si se quiere entrar a algún tipo de servicio bancario, en el caso de navegación se debe usar algún servicio de VPN mencionado. Además, es fundamental asegurarse de que el banco cuente con autenticación y encriptación, con el objetivo de aumentar la seguridad hacia el tratamiento de identidad del usuario.

Cada vez que se instale una aplicación se deben verificar los permisos solicitados respecto a la funcionalidad deseada de esta. Lo anterior para tener un control de lo que se está instalando y verificar que no se instale un permiso que no sea de acuerdo con la función específica de la aplicación instalada.

Aunque los sistemas operativos móviles generan por sí solos un grado de seguridad con sus actualizaciones se recomienda instalar algún servicio de *antimalware* para añadir todavía más seguridad. Además, se aconseja habilitar servicios de biometría para los accesos al dispositivo para generar una capa adicional de seguridad en el ingreso.

5.3.2.2.6. Protección en servicios de seguridad que brinda la entidad financiera. De acuerdo con las opciones que cada entidad financiera tiene disponibles, se recomienda activar alguna serie de servicios de seguridad que brinda la organización que permiten monitorear y tener un mejor control de cada una de las transacciones que se realicen en las cuentas asociadas con el servicio bancario. Algunas medidas que se pueden implementar son los límites de transacciones, notificaciones de cuentas favoritas, notificaciones de transferencias, uso de tarjetas virtuales para compras en Internet, notificaciones al realizar cambio de contraseña, bloqueo por zona geográfica para no permitir movimientos en el extranjero y solicitud de biometría para completar una transacción...

5.3.2.2.7. Protección en la información de huella digital del usuario en Internet. Una huella digital es un concepto que abarca todos los registros y rastros que se dejan al usar Internet. En la mayoría de los casos son beneficiosas para la persona usuaria, pero en otros casos pueden ser perjudiciales porque nunca son intrascendentes. En estos casos es importante proteger lo que se publica en el Internet que puede afectar o inferir como insumo para que un delincuente utilice esta información para materializar un delito. Algunas medidas de protección son las siguientes:

5.3.2.2.7.1. Publicación en redes sociales. De acuerdo con los diferentes tipos de datos clasificados en la Ley n.º 8968, previamente descritos en la función identificar, es importante no publicar información privada o sensible en redes sociales o medios inseguros. Además, con el objetivo de que no sea posible para los delincuentes validar la identidad de una persona, o bien inferir las claves de acceso por utilizar, se recomienda no publicar nombre completo, edad, nombres o imágenes de miembros de familia, nombre o imágenes de mascotas, pasatiempos, fechas de nacimiento, lugar de habitación y grupos sociales a los que pertenezca.

5.3.2.2.7.2. Identificación de cuenta de correo asociada con notificaciones por parte de la entidad bancaria que brinda los servicios. Para tener un mejor control de la información bancaria se recomienda tener un correo específico que solo se utilice para este medio. Esto permite que si llegan mensajes bancarios a otros correos electrónicos que no se dieron para este motivo se descarten como intentos de estafas o correos falsos. Cabe mencionar que también existen servicios de correo electrónico enfocados en la privacidad, uno de ellos es Proton mail, este tipo de servicio es una gran alternativa para usar como correo enlazado a la entidad bancaria.

5.3.2.3. Afectación por bienes inmuebles. En los siguientes apartados se presenta información relevante relacionada con la afectación por bienes inmuebles.

5.3.2.3.1. Datos que se relacionan con bienes inmuebles y muebles. Como parte de proteger la información relacionada con bienes inmuebles se deben tomar en cuenta las siguientes consideraciones.

5.3.2.3.1.1. Información disponible en el Registro Nacional. Es importante conocer que la información relacionada con bienes inmuebles, muebles y sociedades está clasificada como pública en la Ley de Protección de Datos. Sin embargo, el Registro Nacional permite a los usuarios verificar en su sitio *web* la información de bienes inmuebles y muebles por si se ha realizado algún tipo de movimiento. Además de esto, el Registro Nacional cuenta con el servicio de alerta registral, en el que la persona usuaria que contrate el servicio recibe notificaciones con cualquier anotación realizada para los bienes muebles e inmuebles. Este servicio tiene un costo de $15 USD anuales y se activa en el Registro Nacional.

5.3.2.3.1.2. Información de planos o certificaciones que se tengan en físico. Es importante no compartir, ya sea por redes sociales o medios inseguros, fotografías o archivos digitalizados a partir del documento físico. Lo anterior ya que esto puede servir de insumo para que delincuentes puedan realizar la materialización de un delito a partir de esta información.

5.3.2.3.2. Información de huella digital del usuario en Internet. Con el objetivo de que no sea posible para los delincuentes validar la identidad de una persona, se recomienda no publicar nombre completo, edad, nombres o imágenes de miembros de familia, fechas de nacimiento, lugar de habitación y grupos sociales a los que pertenezca. A pesar de que los delitos a patrimonio son en menor cantidad, sí suceden y es importante ser precavidos.

5.3.3. Propuesta función detectar. En la Tabla 52 se muestra la propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital.

Tabla 52

Función detectar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital

Función	Afectación	Categoría	Subcategoría 1	Subcategoría 2	Subcategoría 3	Subcategoría 4
Detectar	Financiera	Métodos de acceso a servicios bancarios	Ingeniería social	*Vishing*	El delincuente busca generar un sentido de urgencia o vínculo de confianza con la víctima, para obtener información de credenciales de acceso o medios complementarios de autenticación, ya sea que la víctima entregue la información a través de la llamada telefónica, o bien por medio de provocar que la víctima ingrese a un sitio fraudulento para obtener las credenciales de acceso e información complementaria de autenticación.	

				Phishing	Correo electrónico. Se detecta un origen que no corresponde en el dominio de la cuenta de correo oficial respeto a la entidad financiera, se detectan problemas de redacción reflejados en el cuerpo del correo. Se detecta una solicitud de ingresar para responder a la actualización de información hacia la entidad financiera. Se detecta un *link* para acceso al sitio *web* de la entidad financiera como parte del correo electrónico. Los correos electrónicos que no son el dominio oficial de la entidad financiera, como contratacionesmarca @gmail.com, marcaempleoscr@outlook.com, laboralesmarca@yaho	

					o.com, haciendagobierno@gmail.com, firmadigitalbanco@gmail.com, bncr@gmail.com, bcr@gmail.com, bacsanjose@gmail.com, bancoproamerica@gmail.com, son un claro indicador de un correo malicioso que busca hacer caer en una estafa informática.	
					Depósito bancario falso producto de gestión en Internet. Este es un indicador claro cuando se ofrece realizar pagos por adelantado para servicios u objetos que se estén negociando. Asimismo, las notificaciones de errores en transferencias, o bien Sinpe Móvil, buscando	

					la devolución del dinero en un plazo urgente aportando un documento que cumple con las características reales según la imagen.	
					Reconocimiento de sitios *web* oficiales de entidad financiera	Verificación de dirección electrónica oficial (la persona usuaria ingresa el URL oficial), validación de certificado de seguridad sitio *web* (quién emite el certificado, para quién emite el certificado, la vigencia de validez del certificado, que sea certificado válido).
					Sitios *web* falsos a partir de *link* en correos electrónicos, difusión de redes sociales y mensajes	

					de SMS en dispositivo móvil, o bien *links* por medio de WhatsApp. En esto se puede observar que el *link* indicado tiene una estructura diferente a la oficial para el acceso al sitio *web* de la entidad financiera. Cuando se solicita acceder a un *link* que ha sido entregado como parte de la información por los medios indicados es una clara señal de un intento de direccionamiento a un sitio *web* falso.	
					Suplantación de funcionarios de instituciones o empresas, donde los delincuentes comienzan a solicitar datos financieros.	

			Instalación de *remote desktop*.	Cuando sin solicitar servicio de soporte de un artículo en periodo de garantía se solicita la instalación de *software* específico para acceder remotamente el equipo, o bien con la justificación de agilizar un trámite bancario, o bien atender dudas del cliente en la misma página *web* de la entidad financiera.		
	Bienes	Métodos que utilizan los delincuentes	Información de bienes muebles o inmuebles	Por medio del servicio de alerta registral ofrecido por el Registro Nacional es posible detectar gestiones que se llevan a cabo con los bienes		

				muebles o inmuebles. Por eso, se pueden detectar posibles movimientos fraudulentos.		
				Por medio de la consulta periódica de información disponible en el sitio *web* es posible para los usuarios confirmar el estado de los bienes muebles o inmuebles. Por eso, se pueden detectar posibles movimientos fraudulentos.		
			Vishing	En estos casos los delincuentes comienzan a solicitar datos de bienes inmuebles o muebles, por lo tanto, es un indicador de una		

				posible estafa informática. El delincuente busca información de números de finca para bienes inmuebles, o bien números de placa, por ejemplo, para bienes muebles.		

5.3.3.1. Afectación financiera. En los siguientes apartados se presenta información relevante relacionada con la afectación financiera.

5.3.3.1.1. Métodos de acceso a servicios bancarios. A continuación, se detallan:

5.3.3.1.1.1. Ingeniería social. Entre las diferentes variantes de ingeniería social se plantean las siguientes a partir de la investigación realizada e información obtenida del Organismo de Investigación Judicial.

5.3.3.1.1.1.1. Vishing. Se detecta que la persona usuaria se encuentra en esta modalidad cuando el delincuente busca generar un sentido de urgencia o vínculo de confianza con la víctima para obtener información de credenciales de acceso o medios complementarios de autenticación. Lo anterior puede ocurrir ya sea que la víctima entregue la información a través de la llamada telefónica, o bien por medio de provocar que la víctima ingrese a un sitio fraudulento para obtener las credenciales de acceso e información complementaria de autenticación.

5.3.3.1.1.1.2. Phishing. Se detecta que la persona usuaria se encuentra en esta modalidad cuando:

- El origen del correo electrónico no corresponde al dominio de la cuenta de correo oficial.
- Se encontraron problemas de redacción reflejados en el cuerpo del correo.
- Se detecta una solicitud de ingresar para responder a la actualización de información hacia la entidad financiera.
- Se detecta un *link* para acceso al sitio *web* de la entidad financiera como parte del correo electrónico.
- Al notar que los correos electrónicos no son el dominio oficial de la entidad financiera, con casos como @gmail.com, @outlook.com, @yahoo.com, entre otros, es un claro indicador de un correo malicioso que busca hacer caer en una estafa informática.

- Se recibe un depósito bancario falso producto de gestión en Internet.
- Ofrecen realizar pagos por adelantado para servicios u objetos que se estén negociando.
- Notificaciones de errores en transferencias, o bien Sinpe Móvil, buscando la devolución del dinero en un plazo urgente aportando un documento que cumple con las características reales según la imagen.
- Sitios *web* falsos a partir de *link* en correos electrónicos, difusión de redes sociales y mensajes de SMS en dispositivo móvil, o bien *links* por medio de WhatsApp.
- El *link* indicado tiene una estructura diferente a la oficial para el acceso al sitio *web* de la entidad financiera.
- Se solicita acceder a un *link* que ha sido entregado como parte de la información por los medios indicados, lo cual es una clara señal de un intento de direccionamiento a un sitio *web* falso.
- Suplantación de funcionarios de instituciones o empresas, donde los delincuentes comienzan a solicitar datos financieros.
- Para detectar sitios *web* falsos de entidades financieras es necesario:
- Verificar la dirección electrónica oficial (la persona usuaria ingresa el URL oficial).
- Validar el certificado de seguridad del sitio *web* (quién emite el certificado, para quién emite el certificado, la vigencia de validez del certificado, que sea certificado válido).

5.3.3.1.1.2. Instalación de remote desktop. Se detecta que la persona usuaria se encuentra en esta modalidad cuando:

- Sin solicitar servicio de soporte de un artículo en periodo de garantía se solicita la instalación de *software* específico para acceder remotamente al equipo.

- Con la justificación de agilizar un trámite bancario, o bien atender dudas del cliente en la misma página *web* de la entidad financiera.

5.3.3.2. Afectación por bienes inmuebles. En los siguientes apartados se presenta información relevante relacionada con la afectación por bienes inmuebles.

5.3.3.2.1. Métodos que utilizan delincuentes. A continuación, se detallan:

5.3.3.2.1.1. Información de bienes muebles o inmuebles. Al considerar que son datos de uso irrestricto, para detectar la afectación relacionada con bienes es necesario:

- Por medio del servicio de alerta registral ofrecido por el Registro Nacional es posible detectar gestiones que se llevan a cabo con los bienes muebles o inmuebles. Por eso, se pueden detectar posibles movimientos fraudulentos.

- Por medio de la consulta periódica de información disponible en el sitio *web* es posible para los usuarios confirmar el estado de los bienes muebles o inmuebles. Por eso, se pueden detectar posibles movimientos fraudulentos.

5.3.3.2.1.2. 2. Vishing. Se detecta que la persona usuaria se encuentra en esta modalidad cuando con argumentos de colaborar con trámites, o bien venta de bienes muebles o inmuebles, los delincuentes comienzan a solicitar datos sobre esto, por lo tanto, es un indicador de una posible estafa informática. El delincuente busca información de números de finca para bienes inmuebles, o bien números de placa, por ejemplo, para bienes muebles.

5.3.4. Propuesta función responder. En la Tabla 53 se muestra la propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital.

Tabla 53

Función responder, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital

Función	Afectación	Categoría	Subcategoría 1	Subcategoría 2	Subcategoría 3
Responder	Financiera	Métodos de acceso a servicios bancarios	Ingeniería social	*Vishing*	Finalizar la llamada y llamar a la entidad financiera para validar la alerta recibida. En estos casos es fundamental tener claro que los delincuentes son profesionales en la manipulación hacia las víctimas, por lo tanto, cuanto más se les permita hablar, más posibilidades se generan que exista persuasión del delincuente hacia la víctima.
				Phishing	Los servicios financieros no solicitan actualizar información mediante correo electrónico, por lo tanto, ante solicitudes de este tipo se debe incluir el correo en la bandeja de correos no deseados, o bien bandeja de *spam*, para que quede registrado el origen fraudulento y se filtre y redireccione en futuros correos recibidos en el tiempo y eso

					permita identificar fácilmente nuevos intentos de estafa informática.
					Las no se debe acceder a las ventanas emergentes, por lo tanto, se deben cerrar.
					Cualquier depósito bancario indicado debe validarse en la página oficial de la entidad financiera, sin este paso no se puede verificar el depósito. Asimismo, para casos de posibles errores en depósitos por medio de Sinpe Móvil es necesario validar el estado de cuenta en el sitio oficial de la organización financiera, como requisito fundamental antes de ver la posibilidad de realizar alguna devolución hacia una persona, que para este caso se debe llevar a cabo la toma de datos de la persona. Una gestión de devolución nunca debe hacerse el mismo día de la solicitud, ya que a un delincuente le interesa que

					las acciones sean inmediatas.
					No se debe acceder a ningún *link* recibido por medio de un correo electrónico, mensaje a través de una red social, mensajería de texto, para direccionarse al sitio *web* oficial de ninguna entidad financiera. Siempre para acceder al sitio *web* oficial es fundamental, digitar la dirección *web* oficial de la entidad financiera en el buscador *web*. Asimismo, en caso de recibir un *link*, al posicionarse con el cursor sobre el *link* (sin acceder al mismo), se visualiza la dirección real a la cual se realizaría el redireccionamiento, con lo cual se puede confirmar el intento de inicio del proceso de estafa informática.
				Enmascarado número telefónico origen	No se debe asegurar que una llamada corresponde a una entidad financiera por el número mostrado en el identificador de llamada, debido a que existen herramientas para enmascarar

					números telefónicos origen desde los cuales se hace la llamada telefónica. Asimismo, una organización financiera nunca se comunicará con un cliente para pedir información bancaria o elementos de autenticación como *password*, números de seguridad de verificación, entre otros.
				Suplantación de funcionarios de instituciones o empresas	Finalizar la llamada y llamar a la institución o empresa para validar la solicitud recibida. En estos casos es fundamental tener claro que los delincuentes son profesionales en la manipulación hacia las víctimas, por lo tanto, cuanto más se les permita hablar, más posibilidades se generan que exista persuasión del delincuente hacia la víctima.
				Aplicar recomendación, Detente, Piensa y Actúa	Ante una condición que genere sospecha, no dejarse llevar por la reacción primaria, sino analizar la situación y sus posibles riesgos, para tomar una decisión sobre

					cómo proceder de una manera preventiva.
			Instalación de remote desktop.	Nunca permitir que se haga la instalación de un *software* por parte de una persona que afirma representar una entidad financiera u otra empresa.	
				En caso de detectar que hay una sesión remota activa no autorizada apagar el equipo inmediatamente, con lo cual la sesión remota se desconecta.	
				Utilizar cuenta de usuario con privilegios de instalación, para que cuando una instalación en el	

				sistema operativo sea solicitada, se pida la clave de validación. Lo anterior como un filtro para detectar cualquier instalación en el sistema.	
	Bienes	Métodos que utilizan los delincuentes	Información de bienes muebles o inmuebles	Con la revisión en el sitio *web* del Registro Nacional o bien con el servicio alerta registral en caso de que se presente alguna anotación al bien o sociedad el cliente recibirá, de manera inmediata, una notificación de la situación y en caso de ser una estafa puede solicitar a la Dirección la no inscripción del documento.	

			Vishing	Finalizar la llamada y llamar a la institución o empresa para validar la solicitud recibida. En estos casos es fundamental tener claro que los delincuentes son profesionales en la manipulación hacia las víctimas, por lo tanto, cuanto más se les permita hablar, más posibilidades se genera que exista persuasión.	

5.3.4.1. Afectación financiera. En los siguientes apartados se presenta información relevante relacionada con la afectación financiera.

5.3.4.1.1. Respuesta de ataques a los métodos de acceso a servicios bancarios. Una vez detectado un comportamiento o conducta anormal en cualquier tema relacionado con servicios bancarios identificados previamente en la función detectar, se tiene que realizar una serie de consideraciones para responder en el momento y detener que el posible delito pueda darse a cabo.

5.3.4.1.1.1. Ingeniería social. En temas de ingeniería social en las diferentes formas que puede darse o materializarse se recomienda seguir las siguientes recomendaciones:

5.3.4.1.1.1.1. Vishing. Inmediatamente después de detectar algo anómalo en la supuesta llamada de la entidad financiera se recomienda finalizar la llamada y llamar a la organización financiera de vuelta para validar la alerta recibida. En estos casos es fundamental tener claro que los delincuentes son profesionales en la manipulación hacia las víctimas, por lo tanto, cuanto más se les permita hablar, más posibilidades se generan de que exista persuasión del delincuente hacia la víctima.

5.3.4.1.1.1.2. Phising. Una vez detectado un correo falso es importante recordar que los servicios financieros no solicitan actualizar información mediante correo electrónico, por lo tanto, ante solicitudes de este tipo, se debe incluir el correo en la bandeja de correos no deseados, o bien bandeja de *spam*, para que quede registrado el origen fraudulento para que se filtre y redireccione en futuros correos recibidos en el tiempo y eso permita identificar fácilmente nuevos intentos de estafa informática. También es relevante recordar que no se debe acceder a ningún *link* recibido por medio de un correo electrónico, mensaje a través de una red social, mensajería de texto, para direccionarse al sitio *web* oficial de ninguna entidad financiera. Para acceder al sitio *web* oficial se recomienda digitar la dirección *web* oficial de la organización financiera en el navegador *web*. Asimismo, en caso de recibir un *link*, al posicionarse con el cursor sobre el *link* (sin acceder al mismo), se visualiza la dirección real a la cual se realizaría el redireccionamiento, con lo cual se puede confirmar el intento de inicio del proceso de estafa informática.

En el caso de que se identifiquen características sospechosas en la ejecución de algún negocio de compra o venta, utilizando las redes sociales o alguna página de Internet, es importante recordar que cualquier depósito bancario indicado debe validarse en la página oficial de la entidad financiera, sin este paso no se puede dar verificar el depósito. Asimismo, para casos de posibles errores en depósitos por medio de Sinpe Móvil, es necesario validar el estado de cuenta en el sitio oficial de la organización financiera, como requisito fundamental antes de ver la posibilidad de realizar alguna devolución hacia una persona, que para este caso se debe llevar a cabo la toma de datos de la persona. Una gestión de devolución nunca debe hacerse el mismo día de la solicitud, ya que a un delincuente le interesa que las acciones sean inmediatas.

Además, si se detecta algún movimiento anormal en la navegación con una ventana emergente, estas no deben accederse y se deben cerrar inmediatamente.

5.3.4.1.1.1.3. Enmascarado número telefónico origen. No se debe asegurar que una llamada corresponde a una entidad financiera por el número mostrado en el identificador de llamada, debido a que existen herramientas para enmascarar números telefónicos origen desde los cuales se hace la llamada telefónica. Asimismo, una organización financiera nunca se comunicará con un cliente para pedir información bancaria o elementos de autenticación como contraseñas, números de seguridad de verificación, entre otros. Una manera de responder a esta situación es cortar la llamada y devolverla a la entidad bancaria para comprobar si es verdadera.

5.3.4.1.1.1.4. Suplantación de funcionarios de instituciones o empresas. Al igual que en la técnica de *vishing* en la que se hacen pasar por un personero de la entidad bancaria, se recomienda finalizar inmediatamente la llamada y llamar a la institución o empresa para validar la solicitud recibida. En estos casos es fundamental tener claro que los delincuentes son profesionales en la manipulación hacia las víctimas, por lo tanto, cuanto más se les permita hablar, más posibilidades se generan de que exista persuasión del delincuente hacia la víctima.

5.3.4.1.1.1.5. Aplicar recomendación, detente, piensa y actúa. Ante una condición que genere sospecha no se debe dejar llevar por la reacción primaria, sino analizar la situación y sus posibles riesgos, para tomar una decisión sobre cómo proceder de una manera preventiva. Siempre hay que detenerse, pensar y actuar.

5.3.4.1.1.2. Instalación de remote desktop. Nunca se debe permitir la instalación de un *software* por parte de una persona que afirma representar una entidad financiera u otra empresa. Se recomienda utilizar una cuenta de usuario sin privilegios de instalación, para que cuando se solicite una instalación en el sistema operativo se pida la clave de validación. Lo anterior como un filtro para detectar cualquier instalación en el sistema, además, en caso de detectar que hay una sesión remota activa no autorizada, apagar el equipo inmediatamente, con lo cual la sesión remota se desconecta.

5.3.4.2. Afectación de bienes inmuebles. En los siguientes apartados se presenta información relevante relacionada con la afectación de bienes inmuebles.

5.3.4.2.1. Métodos que utilizan los delincuentes. En la afectación de bienes inmuebles una vez reveladas algunas situaciones sospechosas que se identificaron en la función detectar se recomiendan las siguientes acciones.

5.3.4.2.1.1. Información de bienes muebles o inmuebles. En el momento que se sospeche de algún intento de estafa en algún bien inmueble se puede realizar la revisión en el sitio *web* del Registro Nacional o bien con el servicio alerta registral mencionado en la función proteger del presente marco de trabajo. En caso de que se presente alguna anotación al bien o sociedad el cliente con el servicio de alerta registral recibirá, de manera inmediata, una notificación de la situación y en caso de ser una estafa puede solicitar a la Dirección la no inscripción del documento.

5.3.4.2.1.2. Vishing. De igual manera, si se recibe una llamada de alguna persona haciéndose pasar por empleado municipal o del Registro y pida información registral, se recuerda y recomienda terminar la llamada y llamar a la institución para verificar la solicitud recibida. En estos casos debe quedar claro que el delincuente es un profesional manipulador de víctimas, por lo que cuanto más se le permita hablar, más probable es que el delincuente convenza a la víctima.

5.3.5. Propuesta función recuperar. En la Tabla 54 se muestra la propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital.

Tabla 54

Función recuperar, propuesta de un marco de trabajo para mejorar la seguridad en Internet para las personas en edad laboral madura y personas adultas mayores que cuenta con alfabetización digital

Función	Afectación	Categoría
Recuperar	Financiera	Ponerse en contacto con los números oficiales de la entidad financiera con el objetivo de reportar la estafa informática, o bien el intento de estafa informática, para que la organización financiera proceda con los protocolos de seguridad establecidos.
		Realizar la denuncia ante el Organismo de Investigación Judicial, rescatando los elementos de prueba que fueron posibles recolectar.
		Buscar asesoramiento con un profesional en derecho con especialización en materia de delitos informáticos
	Bienes	Realizar la denuncia ante el Organismo de Investigación Judicial, rescatando los elementos de prueba que fueron posibles recolectar. El Organismo de Investigación Judicial se encarga de llevar a cabo la coordinación con el Registro Nacional
		Buscar asesoramiento con un profesional en derecho con especialización en materia de delitos informáticos.

5.3.5.1. Afectación financiera. Si llegara a ocurrir la materialización de algún delito es importante ponerse en contacto con los números oficiales de la entidad financiera con el objetivo de reportar la estafa informática, o bien el intento de esta, para que la organización financiera proceda con los protocolos de seguridad establecidos. Es relevante recordar que el vacío de cuentas se lleva a cabo de 3 a 7 minutos por lo que se debe ser sumamente rápido.

Además, se debe realizar la denuncia en el Organismo de Investigación Judicial y es relevante mencionar que la persona mayor de 65 años tiene una atención priorizada y se les realiza la toma de la denuncia de manera más rápida. Cabe señalar que es importante llevar la máxima cantidad de pruebas que fue posible recolectar, independientemente de si es un delito de estafa informática o suplantación de identidad. Una vez recolectada la información se procede con el proceso de investigación. Si la denuncia y la investigación avanzan en términos favorables es recomendable asesorarse con un abogado especialista en derecho informático.

5.3.5.2. Afectación de bienes inmuebles. Si se llegara a materializar un delito en una afectación patrimonial es importante realizar la denuncia en el Organismo de Investigación Judicial, rescatando los elementos de prueba que fue posible recolectar. El Organismo de Investigación Judicial se encarga de llevar a cabo la coordinación con el Registro Nacional y la investigación.

5.4. Guía de aplicación rápida

Como herramienta de primera consulta para facilitar el uso del marco de trabajo propuesto se desarrolla la presente guía de aplicación rápida para cada una de las funciones definidas.

5.4.1. Función identificar. Se utiliza esta etapa para identificar los principales componentes que pueden ser parte de un delito de estafa informática o suplantación de identidad. Además, se define cada uno según la Ley n.º 8968 en relación con la protección de la persona frente al tratamiento de sus datos personales y se identifican los métodos que más utilizan los delincuentes, en dos ámbitos cubiertos en el trabajo que son la afectación financiera y la patrimonial.

- Identificar el concepto de delito estafa informática.
- Identificar el concepto de delito suplantación identidad.
- Identificar los datos personales de acceso irrestricto.
- Identificar los datos sensibles.
- Identificar los datos personales de acceso restringido.
- Identificar la ingeniería social.
- Identificar los sitios *web* falsos para entidades financieras.
- Identificar el *vishing*.
- Identificar la instalación de herramientas *remote desktop*.
- Identificación del enmascarado número telefónico origen.
- Identificación de suplantación de funcionarios de instituciones o empresas.
- Identificación de métodos que utilizan los delincuentes para afectar bienes muebles o inmuebles.

5.4.2. Función proteger. En la etapa proteger se menciona una serie de buenas prácticas para salvaguardar correctamente los elementos que se identificaron en la etapa anterior en relación directa con una posible materialización de un ataque informático. Algunas acciones que se recomiendan para proteger son:

- Es importante estar en constante capacitación de temas de ciberseguridad, además de mantenerse informado con los sitios oficiales del gobierno o páginas especializadas en estos temas.

- Es importante que nunca se compartan datos bancarios y mantener aseguradas las credenciales de acceso, esto primero al crear contraseñas seguras, que no se utilicen en otros servicios y se refuerce con biometría o firma digital. Una alternativa es utilizar gestores de contraseñas para almacenar y crear contraseñas más fuertes.
- Nunca compartir con nadie los métodos de múltiple factor de autenticación entregados por la entidad financiera (tarjeta dinámica, otp y clave).
- Asegurar los navegadores en equipos de escritorio, equipos portátiles y dispositivos móviles utilizando motores de búsqueda y navegadores enfocados en la privacidad.
- En los dispositivos móviles tener antivirus y no almacenar información importante en ellos como pin, claves de acceso, entre otros.
- En la seguridad en dispositivos de acceso es importante tener actualizados los dispositivos, tener antivirus, utilizar doble factor de autenticación para ingresar a ellos, descargar aplicaciones de tiendas reconocidas y si se está en una red gratuita usar algún servicio de VPN para cifrar el tráfico. El servicio al cual se accede es fundamental que cuente con la posibilidad de autorización y autenticación para la persona usuaria, con el objetivo de asegurar su identidad.
- Utilizar servicios de seguridad que brinda la entidad financiera como límite de transacciones, tarjetas virtuales, notificaciones de movimientos al correo, entre otras.
- Cuidar la información de huella digital del usuario en Internet, en todo lo que se publique en redes sociales, además de utilizar un correo electrónico específico para la entidad bancaria y otro para redes sociales u otros servicios de Internet.

- En relación con los bienes, al ser públicos cualquier persona puede acceder a ellos, sin embargo, si se quieren proteger se puede activar el servicio de alerta registral para tener un mejor monitoreo de estos.

5.4.3. Función detectar. En esta etapa se establece una serie de características para tener en cuenta, sobre todo en los diferentes métodos o vectores de ataque que utilizan los delincuentes para identificar en este caso que la persona sea víctima en un momento dado de un ataque de estafa informática o de suplantación de identidad. Esta etapa se enfoca en las dos afectaciones centrales que son la financiera y la patrimonial.

- Detectar métodos por parte de delincuentes para tener acceso a servicios bancarios.
- Detectar métodos que utilizan los delincuentes para la afectación de bienes inmuebles o muebles.

5.4.4. Función responder. En esta etapa responder se identifica una serie de acciones por realizar en caso de que una persona sea víctima de un ataque de suplantación de identidad o estafa informática, en el ámbito financiero o patrimonial que previamente se haya detectado en la etapa anterior. Algunas acciones por llevar a cabo para responder en un eventual ataque son:

- Finalizar la llamada y llamar a la entidad financiera para validar la alerta recibida.
- Los servicios financieros no solicitan actualizar información mediante correo electrónico, por lo tanto, ante solicitudes de este tipo, se debe incluir el correo en la bandeja de correos no deseados, o bien la bandeja de *spam.*
- Las ventanas emergentes no deben accederse, por lo tanto, se deben cerrar.
- Cualquier depósito bancario indicado debe validarse en la página oficial de la entidad financiera.

- No se debe acceder a ningún *link* recibido por medio de un correo electrónico, mensaje a través de una red social o mensajería de texto, para direccionarse al sitio *web* oficial de ninguna entidad financiera.

- Ante una condición que genere sospecha, no dejarse llevar por la reacción primaria, sino analizar la situación y sus posibles riesgos, para tomar una decisión sobre cómo proceder de una manera preventiva.

- Nunca permitir que una persona que afirma representar una entidad financiera u otra empresa instale un *software*.

- Utilizar cuenta de usuario con privilegios de instalación, para que cuando se solicite una instalación en el sistema operativo se pida la clave de validación.

- En caso de ataques a patrimonio, con la revisión en el sitio *web* del Registro Nacional o bien con el servicio alerta registral en caso de que se presente alguna anotación, el cliente recibirá, de manera inmediata, una notificación de la situación y si se trata de una estafa puede solicitar a la Dirección la no inscripción del documento.

5.4.5. Función recuperar. En esta etapa se establece cuáles acciones se pueden tomar si se materializó un delito de suplantación de identidad o estafa informática hacia la persona. Entre las principales acciones por realizar se encuentran:

- Ponerse en contacto con los números oficiales de la entidad financiera con el objetivo de reportar la estafa informática, o bien el intento de esta, para que la organización financiera proceda con los protocolos de seguridad establecidos.

- Realizar la denuncia ante el Organismo de Investigación Judicial, rescatando los elementos de prueba que fue posible recolectar. Es importante recordar que si la persona es adulta mayor tiene prioridad en la denuncia.
- Buscar asesoramiento con un profesional en derecho con especialización en materia de delitos informáticos, esto en caso de que la denuncia avance correctamente.

Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

6.1.1. Conclusiones del objetivo n.º 1. Se alcanzó este objetivo y se concluye lo siguiente:

- Se definió una serie de características propias de la población meta de este trabajo, esto gracias a la investigación de trabajos previos y el análisis de los instrumentos aplicados, tanto a expertos como a la población. Entre las características principales se evidenció una actitud precavida con todo lo que respecta a manejo de tecnologías y utilización de Internet, además, gracias a esa característica de ser precavidos se identifica que esta población es menos atacada que las personas mayores de 18 años y menores de 40 años. Se identifica también que al generarse un vínculo de confianza en esta población pueden lograr que brinden información que puede servir de insumo para materializar algún tipo de delito.
- Se logra definir también como característica el miedo al uso de las tecnologías. Ese miedo, además de la evidencia de desconocimiento en temas de ciberseguridad genera que utilicen muy poco los medios electrónicos o digitales para hacer diferentes gestiones y prefieran hacerlas de manera física.
- Se identifica que esta población mayoritariamente utiliza los dispositivos celulares para navegar, usar redes sociales y realizar diferentes tipos de gestiones en Internet.

6.1.2. Conclusiones del objetivo n.º 2. Se alcanzó este objetivo y se concluye lo siguiente:

- Se identificó que uno de los mayores aportes para mejorar la seguridad en Internet es la educación en temas de protección de datos y concientización. Además, es importante contar con cierto nivel de alfabetización digital para comprender de una manera más acertada diferentes conceptos que se relacionan con mejores prácticas en ciberseguridad en el ámbito personal.

6.1.3. Conclusiones del objetivo n.º 3. Se alcanzó este objetivo y se concluye lo siguiente:

- Se logra identificar con base en el análisis de instrumentos y estudios previos una serie de vulnerabilidades que afectan a la población de personas adultas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital en la Asociación Gerontológica Costarricense. Entre las principales vulnerabilidades se encuentra la identificación de sitios fraudulentos, manejo de contraseñas, desconocimiento en protección de datos enfocado principalmente en evitar ataques, ya sean financieros o patrimoniales, desconocimiento en temas de seguridad y métodos sobre cómo actuar en términos legales si se sufre algún tipo de afectación orientada en los delitos que principalmente que aquejan a esta población que son la suplantación de identidad y la estafa informática.

6.1.4. Conclusiones del objetivo n.º 4. Se alcanzó este objetivo y se concluye lo siguiente:

- Se identifica que la población adulta en edad laboral madura y la persona adulta mayor de la Asociación Gerontológica Costarricense le da un uso restringido a Internet en sitios en los que puedan exponer su identidad. La mayoría de las personas tiene como principal característica ser precavidas, esto hace que no publiquen mucha información que las pueda exponer, además, los sitios bancarios tratan de no utilizarlos digitalmente o utilizar a un tercero de confianza para realizar las gestiones.

6.1.5. Conclusiones del objetivo n.º 5. Se alcanzó este objetivo y se concluye lo siguiente:

- Debido a la recopilación de trabajos anteriores y el análisis de investigaciones enfocadas en la población atendida, se logra elaborar un marco de trabajo referenciado en la lógica de marco de ciberseguridad de la NIST. Para esto se desarrolla cada una de las funciones y se adaptan a las necesidades y características de las personas en edad laboral madura y personas adultas mayores que cuentan con alfabetización digital de la Asociación Gerontológica Costarricense, orientadas a las afectaciones, tanto económicas como patrimoniales y enfocadas en los delitos de estafa informática y suplantación de identidad que son los que más sufre está población según el Organismo de Investigación Judicial.

6.1.6. Conclusiones del objetivo general. Se alcanzó este objetivo y se concluye lo siguiente:

- Con base en la recopilación de datos de estudios previos y el análisis de instrumentos aplicados se logró elaborar un marco de trabajo enfocado en la población atendida y orientado a los delitos y afectaciones a los que son más vulnerables las personas en edad laboral madura y personas adultas mayores costarricenses que cuentan con alfabetización digital de la Asociación Gerontológica Costarricense.

- Se propone este marco como base para el desarrollo de cursos para capacitar a esta población en Ageco. Además, se plantea una guía para mejorar la seguridad en cualquier uso que se pueda dar a Internet en el que las personas se vean expuestas a algún tipo de peligro.

6.2. Recomendaciones

A continuación, se presentan algunas recomendaciones de la experiencia en el trabajo, tanto desde el punto de vista técnico como desde la perspectiva de la gestión de tiempo y recursos:

- Debido al ámbito en el que se desarrolló el proyecto en el cual se le hicieron entrevistas a varios expertos que se relacionan con delitos informáticos y a personas que trabajan con la población de personas adultas en edad laboral madura y adultos mayores, se recomienda para trabajos futuros mantener esa consulta con estos profesionales y con la sección de delitos informáticos y fraudes del Organismo de Investigación Judicial y personas profesionales en ciberseguridad en áreas bancarias. Lo anterior para añadir a la investigación mayor validez y credibilidad en los resultados.

- Al ser la presente una investigación en conjunto, se recomienda utilizar herramientas colaborativas para tener un mejor manejo de las versiones y actualizaciones que se presentan en el proyecto. Esto también permite generar un respaldo automático y proteger la pérdida del archivo o información dentro de este.

- El resultado del marco de trabajo se recomienda implementarlo en varios ámbitos, ya sea que funcione como insumo para crear cursos dirigidos específicamente a la población que atiende la Asociación Gerontológica Costarricense en materia de ciberseguridad o como una guía personal para consultar y guiar cómo actuar en los delitos que más afectan a la población de personas en edad laboral madura y adultos mayores, que son los de estafa informática y suplantación de identidad.

- Se recomienda que aparte de la guía que ofrece el marco de trabajo elaborado de cómo actuar antes, durante o después de un ataque de estafa informática o suplantación de identidad en la población adulta en edad laboral madura y adultos mayores, se esté atento a información nueva que se pueda generar con nuevos métodos de operación de los delincuentes. Lo anterior ya que estos cambian con el transcurso de los años, sin embargo, el objetivo del ataque es el mismo, obtener acceso a datos importantes de las personas para tener un beneficio de esto.

Referencias

Ahmed, E.; DeLuca, B.; Hirowski, E.; Magee, C.; Tang, I. y Coppola, J. F. (2017). *Biometrics: Password replacement for elderly? 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. https://doi.org/10.1109/lisat.2017.8001958

Álvarez, C. (2019, 27 de junio). *Métodos de validación y user research*. https://wildwildweb.es/es/blog/metodos-de-validacion-y-user-research

Arias, F. (2016). *El proyecto de investigación*. Introducción a la metodología científica. Editorial Episteme.

Asale, R. (s. f.). *Suplantar*. Diccionario de la lengua española. Edición del Tricentenario. https://dle.rae.es/suplantar

Asociación Gerontológica Costarricense. (s. f.). *Nuestra labor*. https://ageco.org/nuestra-labor/

Blackwood-Brown, C.; Levy, Y. y D'Arcy, J. (2019). Cybersecurity Awareness and Skills of Senior Citizens: A. Motivation Perspective. *Journal of Computer Information Systems, 61*(3), 195-206. https://doi.org/10.1080/08874417.2019.1579076

Camacho, B. G. (2020, 15 de septiembre). *II Informe Estado de Situación de la Persona Adulta Mayor en Costa Rica*. https://www.kerwa.ucr.ac.cr/handle/10669/81562

Chen, M. Y. (2022). Establishing a Cybersecurity Home Monitoring System for the Elderly. *IEEE Transactions on Industrial Informatics, 18*(7), 4838-4845. https://doi.org/10.1109/tii.2021.3114296

Cisco (2022, 25 de marzo). *¿Qué es la ciberseguridad?* https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Hütt Herrera, H. (s. f.). *Las redes sociales: una nueva herramienta de difusión*. https://www.redalyc.org/pdf/729/72923962008.pdf

Kaspersky (2020, 1 de diciembre). *¿Qué es la ciberseguridad?* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kiziryan, M. (2021, 10 de marzo). *Sistema financiero*. Economipedia. https://economipedia.com/definiciones/sistema-financiero.html

Mcdonald, N. y Mentis, H. M. (2021). Citizens Too: Safety Setting Collaboration Among Older Adults with Memory Concerns. *ACM Transactions on Computer-Human Interaction, 28*(5), 1-32. https://doi.org/10.1145/3465217

Mentis, H. M.; Madjaroff, G.; Massey, A. y Trendafilova, Z. (2020). The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), 1-19. https://doi.org/10.1145/3415235

Morrison, B. A. (s. f.). *A Mixed Methods Approach to Understanding Cyber-Security Vulnerability in the Baby Boomer Population-ProQuest*. https://www.proquest.com/openview/20fbce6b1822faa8476310bf40c68f4b/1?pq-origsite=gscholar&cbl=44156

Morrison, B. A. (s. f.). *Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults*. Frontiers. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00623/full?luicode=10000011&lfid=231522type%3D1%26t%3D10%26q%3D%23075%23&featurecode=newtitle%E7%9C%8B%E8%B5%B7&u=https:%2F%2Fwww.frontiersin.org%2Farticles%2F10.3389%2Ffpsyg.2020.00623%2Fabstract%E2%80%8B

Nicholson, J.; Coventry, L. y Briggs, P. (2019). *If It Important It Will Be A Headline.*

Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. https://dl.acm.org/doi/10.1145/3290605.3300579

Nicholson, J.; Morrison, B.; Dixon, M.; Holt, J.; Coventry, L. y McGlasson, J. (2021). *Training and Embedding Cybersecurity Guardians in Older Communities*. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411764.3445078

NIST (2018, 16 de abril). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf

Pérez, A. (2021, 10 de febrero). *¿Estándares, metodologías o marcos de trabajo? ¿Sabes diferenciarlos?* Ceolevel. https://www.ceolevel.com/estandares-metodologias-o-marcos-de-trabajo-sabes-diferenciarlos#:%7E:text=Un%20marco%20de%20trabajo%20es,nuevos%20problemas%20de%20%C3%ADndole%20similar

Poggi, N. (2020, 28 de julio). *Ciberamenazas: Qué Son, Cómo te Afectan y Qué Puedes Hacer al Respecto*. The Missing Report. https://preyproject.com/blog/es/ciberamenazas-que-son-como-te-afectan-y-que-puedes-hacer-al-respecto/

Real Academia Española. (s. f.). *Diccionario de la legua española*. https://dpej.rae.es/lema/estafa-inform%C3%A1tica

Sannd, P. y Cook, D. M. (2018). *Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and phishing Attacks*. 2018 Fourteenth International Conference on Information Processing (ICINPRO). https://doi.org/10.1109/icinpro43533.2018.9096878

Sistema Costarricense de Información Jurídica. (s. f.). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal*.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

Tan, S.; Vergara, R.; Khan, N. y Khan, S. (2020). Cybersecurity and Privacy Impact on Older Persons Amid COVID-19: A Socio-Legal Study in Malaysia. *Asian Journal Of Research In Education And Social Sciences, 2*(2), 72-76. https://myjms.mohe.gov.my/index.php/ajress/article/view/9697

Techopedia (2019, 5 de febrero). *Cyberattack*. https://www.techopedia.com/definition/24748/cyberattack

Techopedia (2020, 17 de agosto). *Internet*. https://www.techopedia.com/definition/2419/internet

Techopedia (2022, 8 de abril). *Vulnerability*. https://www.techopedia.com/definition/13484/vulnerability#:%7E:text=Vulnerability%20is%20a%20cyber-security,security%20exposed%20to%20a%20threat

Unesco (2022, 21 de abril). *Los nuevos desafíos de la alfabetización*. https://www.unesco.org/es/articles/los-nuevos-desafios-de-la-alfabetizacion

Vargas, A. I. (2004). Guía para elaborar una propuesta de investigación. *Revista Educación*, *29*(0379-7082), 92. revistas.ucr.ac.cr/index.php/educacion/article/viewFile/2241/2200

Bibliografía

AnyDesk. (s. f.). *AnyDesk: The Fast Remote Desktop Application*. https://anydesk.com/es/abuse-prevention

BCR. (s. f.). *Seguridad*. Recomendaciones generales para su seguridad. https://www.bancobcr.com/wps/portal/bcr/bancobcr/soporte/seguridad/

Campos, G. E. (2018, 20 de junio). *Cómo proporcionar ciberseguridad a los adultos mayores en sus dispositivos*. CIO MX. https://cio.com.mx/como-proporcionar-ciberseguridad-a-los-adultos-mayores-en-sus-dispositivos/

Ecija (2020, 30 de noviembre). *Costa Rica: De la UPAD al repositorio de datos biométricos*. https://ecija.com/sala-de-prensa/costa-rica-de-la-upad-al-repositorio-de-datos-biometricos/

Government of Canada. (s. f.). *How to help the older adult in your life get cyber safe*. https://www.getcybersafe.gc.ca/en/blogs/how-help-older-adult-your-life-get-cyber-safe

IT Now (2017, 28 de noviembre). *La biometría, el nuevo aliado para cuidar la identidad digital de los ciudadanos*. Revista IT Now. https://revistaitnow.com/it_connect/la-biometria-el-nuevo-aliado-para-cuidar-la-identidad-digital-de-los-ciudadanos/

Media. (s. f.). *¿Qué significa identidad digital y cuáles derechos están asociados a ella?* https://blog.signaturit.com/es/mas-alla-de-la-reputacion-online-que-se-entiende-por-identidad-digital-y-que-derechos-estan-asociados-a-ella

Méndez, J. (2022, 10 de febrero). *Consejos para el uso seguro del Internet en la adultez mayor. Verdeza | Residencial para adulto mayor | Atención Profesional*. https://verdeza.com/2022/02/10/consejos-para-el-uso-seguro-del-internet-en-la-adultez-mayor%EF%BF%BC/

París, M. (2020, 9 de diciembre). *Costa Rica y los peligros que viven los datos personales*. Ipandetec. https://www.ipandetec.org/2020/12/14/datos-personales-costa-rica/

Seguros SURA (2021, 7 de septiembre). *Adultos mayores y la tecnología: una relación que hay que atender con ciberseguridad*. https://segurossura.com/blog/conectividad/adultos-mayores-y-la-tecnologia-una-relacion-que-hay-que-atender-con-ciberseguridad/

Thorne, A. (2022, 23 de febrero). *What Is The Difference Between Ux Research And User Testing?* Factory Pattern. https://factorypattern-co-uk.translate.goog/difference-ux-testing-user-research/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419

Torresburriel Estudio (2022, 7 de febrero). *Cómo diseñar mejores cuestionarios para UX*. https://www.torresburriel.com/weblog/2021/08/09/disenar-mejores-cuestionarios/

Usability.gov. (s. f.). *User Research Basics*. https://www.usability.gov/what-and-why/user-research.html

YouTube (2014, 26 de noviembre). *Firma digital: Autenticación en Internet y firma de documentos electrónicos*. https://www.youtube.com/watch?v=Apxvd0KvJ3U