UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Medidas de protección digital en redes de datos

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A N

Angel David Rea Aparicio

Diego Jair Crisantos Martinez

DIRECTORA DE TESIS

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado MEDIDAS DE PROTECCION DIGITAL EN LAS REDES DE DATOS que presenté para obtener el titulo de INGENIERO EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

ANGEL DAVID REA APARICIO
Número de cuenta: 315234820

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado MEDIDAS DE PROTECCION DIGITAL EN REDES DE DATOS que presenté para obtener el titulo de INGENIERO EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

DIEGO JAIR CRISANTOS MARTINEZ
Número de cuenta: 317029264

Índice

0. Introducción **10**
1. Metodología inductiva **13**
1.1. Definición del problema 14
1.2. Hipótesis 23
1.3. Objetivo central 23
1.4. Objetivos secundarios 23
1.5. Actividades a realizar para alcanzar los objetivos 23
1.6. Metodología de trabajo 24
1.7. Resultados esperados 26
2. Descripción de una red de datos **28**
2.1. Propiedades 29
2.2. Normas de instalación 32
2.3. Medios aéreos y terrestres 43
2.4 Interferencias 46
3. Funcionamiento de internet **50**
3.1. IP y dominios 51
3.2. Redes públicas y privadas 60
3.3. Servidores y conexión global 62
3.4. Conexiones móviles 64
3.5. Velocidad y banda ancha 69
4. Seguridad **72**
4.1. Triunvirato de la Seguridad 73
4.2. Acceso a la Red 83
4.3. Normas y Estándares 90
4.4. Antivirus 93
4.5. VLANs - VPN 95
4.6. Respaldos - Limpieza de archivos 100
4.7. Ataques, amenazas y planes de contingencia 103
5. Impacto ambiental **114**
5.1. Contaminación por uso de las redes 115
5.2. Consumo de energía 117
5.3. Deterioro de las redes 119
5.4. Tiempo de vida de los dispositivos 120
5.5. Recomendaciones para aumentar la vida útil de los dispositivos de red 122
5.6. Actualización de las redes 124

5.7. Gestión de Residuos : Reparación y Reciclaje..... 125
6. Manual..... 128
6.0. Introducción..... 134
6.1. Cómo encontrar la dirección IP de tu dispositivo..... 135
6.2. Creación de contraseñas seguras..... 149
6.3. Almacenamiento seguro de contraseñas..... 153
6.4. Cómo cambiar la contraseña del módem telmex..... 163
6.5. Cómo configurar IP Estática en tu Módem Telmex..... 174
6.6. Cómo configurar una VPN en tu Módem..... 184
6.7. Cómo actualizar mi sistema operativo..... 192
6.8. Limpieza de archivos en Windows..... 210
6.9. Cómo crear una copia de seguridad con Windows..... 233
6.10. Cómo Identificar Correos Electrónicos con malware..... 250
6.11. Verificar qué dispositivos están conectados a un módem Telmex..... 266
6.12. Manejo Seguro de Información Personal en Redes Sociales..... 275
6.13. Manejo Seguro de Información Personal en Línea..... 278
6.14. Recomendaciones..... 282
7. Resultado, impacto y conclusiones..... 286
Glosario de Términos..... 289
Bibliografía..... 295
Mesografía..... 297

Índice de Figuras

0. Introducción **10**
1. Metodología inductiva **13**
Figura 1.1 Personas que usan internet (% de la población) 14
Figura 1.2 Uso de dispositivos conectados a internet en 2023 15
Figura 1.3 Resultados de la ENDUTIH que muestra el aumento del uso de internet a través de los años 16
Figura 1.4 Aumento de usuarios en internet 17
Figura 1.5 Principales actividades que realizan los internautas mexicanos - porcentaje ... 18
Figura 1.6 Top 10 de países con mayor cibercriminalidad 19
Figura 1.7 ¿En algún momento se ha informado sobre los riesgos cibernéticos (a través de publicaciones, páginas oficiales, redes sociales, búsquedas en Internet, televisión, revistas, etc.)? 21
Figura 1.8 ¿Qué tan seguras se sienten las personas usuarias cuando se conectan a Internet a través de Wi-Fi en lugares públicos (transporte público, parques, aeropuertos, restaurantes, plazas comerciales, etc.)? 22
2. Descripción de una red de datos **28**
Figura 2.1 Propiedades de una red 30
Figura 2.2 Elementos de una red 31
Figura 2.3 Intersección de zona de conexión entre dos redes 36
Figura 2.4 Cobertura de los estándares 802.11 38
Figura 2.5 Absorción de las ondas de radiofrecuencia 40
Figura 2.6 Diagrama de cálculo para Zonas de Fresnel 43
Figura 2.7 Espectro de ondas electromagnéticas 46
3. Funcionamiento de internet **50**
Figura 3.1 Estructura de una dirección IPv4 52
Figura 3.2 Estructura de una dirección IPv6 53
Figura 3.3 Mapa de Cableado Submarino 56
Figura 3.4 Estructura de un dominio 58
Figura 3.5 Red pública y privada 60
Figura 3.6 Direcciones IP públicas frente a privadas 62
Figura 3.7 Registro de Internet Regional 63
Figura 3.8 Antenas de telefonía móvil 65
Figura 3.9 Antenas de telefonía móvil 66
Figura 3.10 Identificación red móvil 68
Figura 3.11 Cobertura móvil en la Ciudad de México 68

Figura 3.12 Cobertura móvil en México....69
4. Seguridad....72
Figura 4.1 Triada de la seguridad....73
Figura 4.2 Clasificación general de amenazas....78
Figura 4.3 Contexto de la seguridad y sus relaciones....82
Figura 4.4 Firewall....87
Figura 4.5 Filtrado MAC....89
Figura 4.6 Ciclo Deming....92
Figura 4.7 Red VLAN....95
Figura 4.8 Medios de almacenamiento....102
Figura 4.9 Sitio fraudulento....107
Figura 4.10 Conexión segura....109
5. Impacto ambiental....114
Figura 5.1 Ciclo de mejora continua....118
6. Manual....1
Figura 6.1 Dirección IP en Windows paso 1....137
Figura 6.2 Dirección IP en Windows paso 2....138
Figura 6.3 Dirección ip en Windows paso 3....139
Figura 6.4 Dirección ip en Windows paso 4....140
Figura 6.5 Dirección ip en Windows paso 5....141
Figura 6.6 Dirección ip en samsung paso 1....142
Figura 6.7 Dirección ip en samsung paso 2....142
Figura 6.8 Dirección ip en samsung paso 3....143
Figura 6.9 Dirección ip en samsung paso 4....143
Figura 6.10 Dirección ip en samsung paso 5....144
Figura 6.11 Dirección ip en motorola paso 1....145
Figura 6.12 Dirección ip en motorola paso 2....145
Figura 6.13 Dirección ip en motorola paso 3....146
Figura 6.14 Dirección ip en motorola paso 4....146
Figura 6.15 Dirección ip en motorola paso 5....147
Figura 6.16 LastPass paso 1....154
Figura 6.17 LastPass paso 2....155
Figura 6.18 LastPass paso 3....156
Figura 6.19 LastPass paso 4....156
Figura 6.20 LastPass paso 5....157
Figura 6.21 LastPass paso 6....158
Figura 6.22 LastPass paso 7....159

Figura 6.23 LastPass paso 8..... 160
Figura 6.24 LastPass paso 9..... 161
Figura 6.25 Cambiar contraseña modem telmex paso 1..... 164
Figura 6.26 Cambiar contraseña modem Telmex paso 2..... 165
Figura 6.27 Cambiar contraseña modem telmex paso 3..... 166
Figura 6.28 Cambiar contraseña modem telmex paso 4..... 167
Figura 6.29 Cambiar contraseña modem telmex paso 5..... 168
Figura 6.30 Cambiar contraseña modem telmex paso 6..... 169
Figura 6.31 Cambiar contraseña modem Telmex paso 7..... 170
Figura 6.32 Cambiar contraseña modem Telmex paso 8..... 171
Figura 6.33 Cambiar contraseña modem Telmex paso 9..... 172
Figura 6.34 Cambiar contraseña modem Telmex paso 1..... 176
Figura 6.35 Cambiar contraseña modem Telmex paso 2..... 177
Figura 6.36 Cambiar contraseña modem Telmex paso 3..... 178
Figura 6.37 Cambiar contraseña modem Telmex paso 4..... 179
Figura 6.38 Cambiar contraseña modem Telmex paso 5..... 180
Figura 6.39 Cambiar contraseña modem Telmex paso 6..... 181
Figura 6.40 Cambiar contraseña modem Telmex paso 7..... 182
Figura 6.41 Cambiar contraseña modem Telmex paso 8..... 182
Figura 6.42 Cambiar contraseña modem Telmex paso 9..... 183
Figura 6.43 Configurar una VPN en tu módem paso 1..... 185
Figura 6.44 Configurar una VPN en tu módem paso 2..... 186
Figura 6.45 Configurar una VPN en tu módem paso 3..... 187
Figura 6.46 Configurar una VPN en tu módem paso 4..... 188
Figura 6.47 Configurar una VPN en tu módem paso 5..... 189
Figura 6.48 Configurar una VPN en tu módem paso 6..... 190
Figura 6.49 Actualización de sistema operativo Windows paso 1..... 194
Figura 6.50 Actualización de sistema operativo Windows paso 2..... 195
Figura 6.51 Actualización de sistema operativo Windows paso 3..... 196
Figura 6.52 Actualización de sistema operativo Windows paso 4..... 197
Figura 6.53 Actualización de sistema operativo Windows paso 5..... 198
Figura 6.54 Actualización de sistema operativo Windows paso 6..... 199
Figura 6.55 Actualización de sistema operativo Windows paso 7..... 200
Figura 6.56 Actualización de sistema operativo Windows paso 8..... 201
Figura 6.57 Actualización de sistema operativo samsung paso 1..... 202
Figura 6.58 Actualización de sistema operativo samsung paso 2..... 202
Figura 6.59 Actualización de sistema operativo samsung paso 3..... 203

Figura 6.60 Actualización de sistema operativo samsung paso 4.....203
Figura 6.61 Actualización de sistema operativo samsung paso 5..... 204
Figura 6.62 Actualización de sistema operativo samsung paso 6.....204
Figura 6.63 Actualización de sistema operativo samsung paso 7..... 205
Figura 6.64 Actualización de sistema operativo motorola paso 1..... 206
Figura 6.65 Actualización de sistema operativo motorola paso 2.....206
Figura 6.66 Actualización de sistema operativo motorola paso 4.....207
Figura 6.67 Actualización de sistema operativo motorola paso 5..... 207
Figura 6.68 Actualización de sistema operativo motorola paso 6.....208
Figura 6.69 Actualización de sistema operativo motorola paso 7.....208
Figura 6.70 Limpieza de archivos temporales paso 1.....212
Figura 6.71 Limpieza de archivos temporales paso 2.....213
Figura 6.72 Limpieza de archivos temporales paso 3..... 214
Figura 6.73 Limpieza de archivos temporales paso 4..... 215
Figura 6.74 Limpieza de archivos temporales paso 5..... 216
Figura 6.75 Liberar espacio en disco paso 1..... 217
Figura 6.76 Liberar espacio en disco paso 2.....218
Figura 6.77 Liberar espacio en disco paso 3.....219
Figura 6.78 Liberar espacio en disco paso 4..... 220
Figura 6.79 Liberar espacio en disco paso 5..... 221
Figura 6.80 Liberar espacio en disco paso 6.....222
Figura 6.81 Desinstalar programas innecesarios paso 1..... 223
Figura 6.82 Desinstalar programas innecesarios paso 2.....224
Figura 6.83 Desinstalar programas innecesarios paso 3..... 225
Figura 6.84 Desinstalar programas innecesarios paso 4.....226
Figura 6.85 Desinstalar programas innecesarios paso 5..... 227
Figura 6.86 Desinstalar programas innecesarios paso 6.....228
Figura 6.87 Herramienta para limpieza de disco paso 1.....229
Figura 6.88 Herramienta para limpieza de disco paso 2.....230
Figura 6.89 Herramienta para limpieza de disco paso 3..... 231
Figura 6.90 Herramienta para limpieza de disco paso 4..... 232
Figura 6.91 Copia de seguridad con Windows paso 1..... 234
Figura 6.92 Copia de seguridad con Windows paso 2..... 235
Figura 6.93 Copia de seguridad con Windows paso 3..... 236
Figura 6.94 Copia de seguridad con Windows paso 4..... 237
Figura 6.95 Copia de seguridad con Windows paso 5..... 238
Figura 6.96 Copia de seguridad con Windows paso 6.....239

Figura 6.97 Copia de seguridad con Windows paso 7....240
Figura 6.98 Copia de seguridad con Windows paso 8....241
Figura 6.99 Copia de seguridad con Windows paso 9....242
Figura 6.100 Copia de seguridad con Windows paso 10....243
Figura 6.101 Copia de seguridad con Windows paso 11....244
Figura 6.102 Copia de seguridad con Windows paso 12....245
Figura 6.103 Copia de seguridad con Windows paso 13....246
Figura 6.104 Copia de seguridad con Windows paso 14....247
Figura 6.105 Copia de seguridad con Windows paso 15....248
Figura 6.106 verificar remitente....251
Figura 6.107 Correo con remitente correcto....252
Figura 6.108 Correo con remitente incorrecto....253
Figura 6.109 Correo con nombre real....254
Figura 6.110 Correo sin nombre....255
Figura 6.111 Correo con nombre del e-mail....256
Figura 6.112 Correo sin errores....257
Figura 6.113 Correo con errores gramaticales....258
Figura 6.114 Correo con URL correcta....259
Figura 6.115 Correo con URL falsa....260
Figura 6.116 Correo con archivos maliciosos....261
Figura 6.117 Correo de urgencia....262
Figura 6.118 Correo con datos reales....263
Figura 6.119 Correo con información genérica....264
Figura 6.120 Dispositivos conectados a mi red paso 1....267
Figura 6.121 Dispositivos conectados a mi red paso 2....268
Figura 6.122 Dispositivos conectados a mi red paso 3....269
Figura 6.123 Dispositivos conectados a mi red paso 4....270
Figura 6.124 Dispositivos conectados a mi red paso 5....271
Figura 6.125 Dispositivos conectados a mi red paso 6....272
Figura 6.126 Dispositivos conectados a mi red paso 7....273
Figura 6.127 Conexión segura....280
7. Resultado, impacto y conclusiones....286
Glosario de Términos....289
Bibliografía....295
Mesografía....297

Índice de Tablas

0. Introducción **10**
1. Metodología inductiva **13**
2. DESCRIPCIÓN DE UNA RED DE DATOS **28**
Tabla 2.1 Características de Estándares para dispositivos inalámbricos 37
Tabla 2.2 Intensidad de la señal 41
Tabla 2.3 Tecnologías de Entrada de Servicios 44
Tabla 2.4 Dispositivos de las redes de datos domésticas 44
Tabla 2.5 Materiales de construcción 47
3. FUNCIONAMIENTO DE INTERNET **50**
Tabla 3.1 Clases de direcciones IPv4 54
Tabla 3.2 Clasificación de direcciones IPv4 54
Tabla 3.3 Extensiones de dominio 58
Tabla 3.4 Código del país 59
Tabla 3.5 Ejemplos de ancho de banda según actividad 70
4. SEGURIDAD **72**
Tabla 4.1 Servicios de seguridad 75
Tabla 4.2 Tipos de amenazas 76
Tabla 4.3 Aspectos atacables en un sistema 80
Tabla 4.4 Elementos de control de acceso a la red 84
Tabla 4.5 Conjunto de estándares de la familia ISO 27000 90
Tabla 4.6 Antivirus 93
Tabla 4.7 Tipos de VLAN 96
Tabla 4.8 Tipos de ataques 104
Tabla 4.9 Tipos de malware 109
5. IMPACTO AMBIENTAL **114**
6. Manual **1**
7. Resultado, impacto y conclusiones **286**
Glosario de Términos **289**
Bibliografía **295**
Mesografía **297**

0. Introducción

El trabajo analiza las redes domésticas, su funcionamiento, seguridad e impacto ambiental, y presenta un manual práctico para que usuarios sin experiencia protejan su red, naveguen de forma segura y gestionen adecuadamente sus dispositivos y la información personal.

En la era digital, las redes domésticas se han convertido en un componente esencial de nuestra vida cotidiana, facilitando la comunicación, el acceso a la información y el funcionamiento de diversas aplicaciones y servicios. Este trabajo tiene como objetivo proporcionar una comprensión integral de las redes domésticas, su funcionamiento, seguridad y el impacto ambiental asociado, además de ofrecer un manual práctico para la protección digital en redes domésticas.

Este estudio se estructura en varios capítulos que abordan distintos aspectos cruciales de las redes domésticas. El primer capítulo se enfoca en la metodología inductiva, utilizada para analizar y resolver problemas mediante la observación e inferencia de soluciones. Se detalla el proceso realizado para la redacción de un manual de seguridad de redes aplicable por usuarios y usuarias con poca o nula experiencia en el tema.

En el segundo capítulo, se ofrece una descripción detallada de las redes domésticas, incluyendo sus propiedades, normas de instalación y los medios de transmisión utilizados. Aquí se analizan aspectos técnicos como la confiabilidad, las características de las tarjetas de red y la configuración de redes según el tamaño y ubicación de los dispositivos con la finalidad de conocer el funcionamiento de las redes y las posibles causas que lo afecten para que sean corregidas.

El tercer capítulo explora el funcionamiento de Internet, cubriendo temas como IP y dominios, redes públicas y privadas, servidores y la conexión global. Abordando las conexiones móviles y la importancia de la velocidad y la banda ancha en el rendimiento de las redes a fin de dar un mejor entendimiento sobre la navegación por Internet, tomando en cuenta su creciente uso.

La seguridad en las redes domésticas es el tema central del cuarto capítulo. Se examinan conceptos fundamentales como el Triunvirato de la Seguridad, el acceso a la red, normas y estándares, y la importancia de los antivirus y las VPNs (Redes Privadas Virtuales). Además, se discuten las amenazas y ataques más comunes, así como las medidas de contingencia y prevención, incluyendo la identificación de sitios fraudulentos y aplicaciones con malware, siendo este el capítulo más importante, dado que sienta las bases para el manual que servirá de guía para que los usuarios y usuarias puedan navegar con seguridad en la red.

El impacto ambiental de las redes domésticas se analiza en el quinto capítulo. Este apartado aborda la contaminación generada por el uso de las redes, el consumo de energía, el deterioro de las infraestructuras y el tiempo de vida útil de los dispositivos. Se ofrecen recomendaciones para prolongar la vida útil de los equipos y estrategias para la actualización y gestión de residuos a través de la reparación y el reciclaje, para contribuir con la reducción de desperdicio tecnológico.

El sexto capítulo presenta un manual práctico para los usuarios y usuarias, con instrucciones detalladas sobre cómo encontrar la dirección IP de los dispositivos, crear y almacenar contraseñas seguras, cambiar la contraseña del módem, actualizar sistemas operativos y realizar limpiezas de archivos en Windows. Además, se incluye una guía para crear copias de seguridad, identificar correos electrónicos con malware y verificar los dispositivos conectados a un módem Telmex. También se aborda el manejo seguro de la información personal en línea.

Finalmente, en las conclusiones se describe lo que se espera lograr una vez el manual sea difundido con el fin de resaltar la importancia de la seguridad en las redes domésticas y el impacto positivo que el conocimiento y la implementación de medidas de protección pueden tener en los usuarios finales.

Este trabajo busca no solo proporcionar un análisis exhaustivo y técnico de las redes domésticas y su seguridad, sino también ofrecer herramientas prácticas y accesibles para los usuarios. Al aumentar la conciencia sobre la seguridad digital y proporcionar recursos educativos, este estudio pretende contribuir a la creación de un entorno digital más seguro y confiable para todos.

1. Metodología inductiva

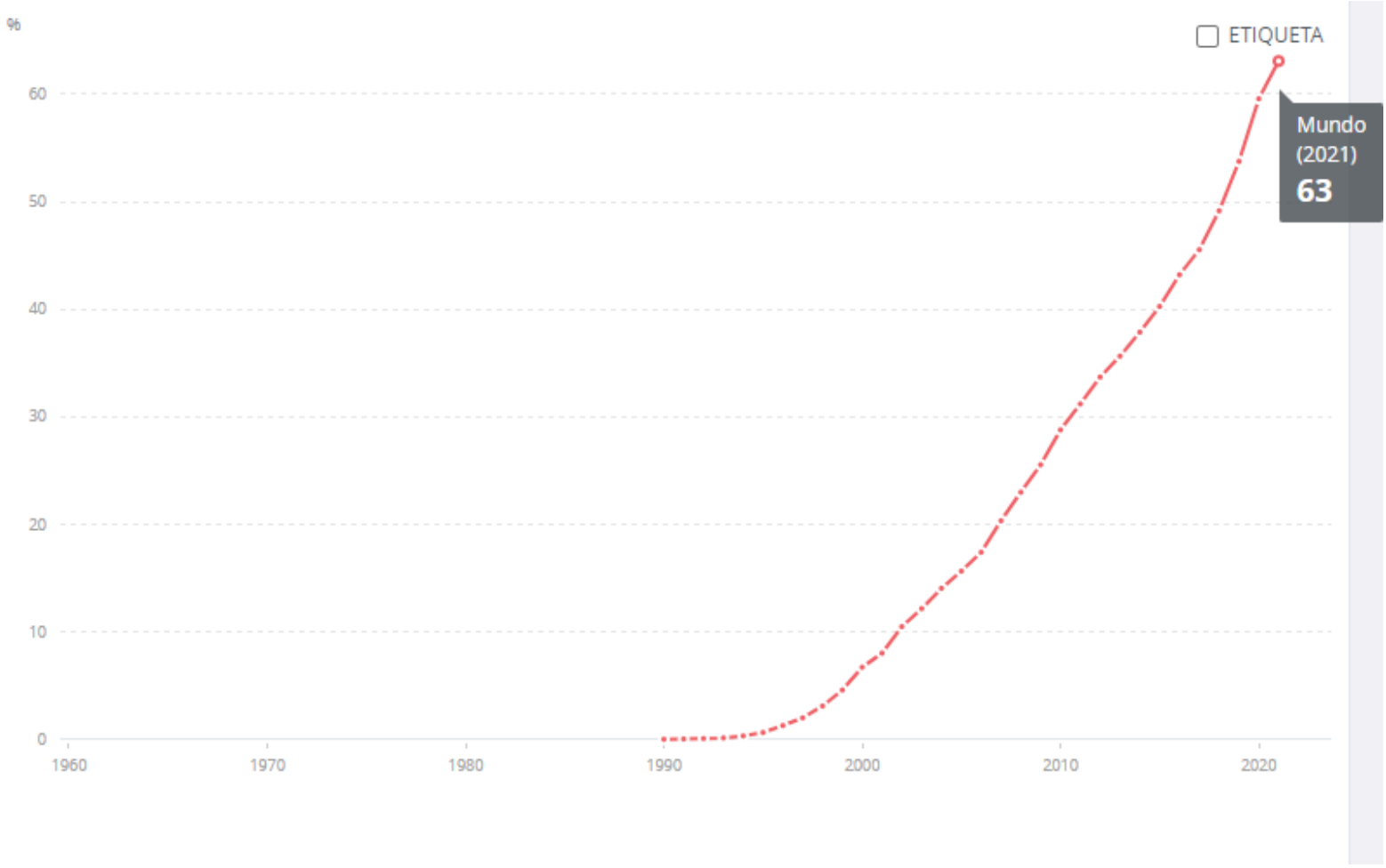
Este tipo de metodología se basa en la observación y experimentación para llegar a una conclusión siendo la más adecuada para el alcance del trabajo. Está conformada por dos tipos de procedimientos inversos: inducción y deducción. Donde la inducción es la forma de razonamiento donde se pasa el conocimiento de casos particulares a un conocimiento general que es el principal propósito de este trabajo.

1.1. Definición del problema

Desde su apertura al público en 1993 como World Wide Web, el internet ha tenido un constante crecimiento de usuarios y usuarias como indica el Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC realizado por la Unión Internacional de Telecomunicaciones del 2022 donde se observa que el 63% de la población mundial utiliza el internet, cifra bastante pronunciada considerando sus poco más de 30 años de desarrollo como se observa en la figura 1.1.

Figura 1.1

Personas que usan internet (% de la población).

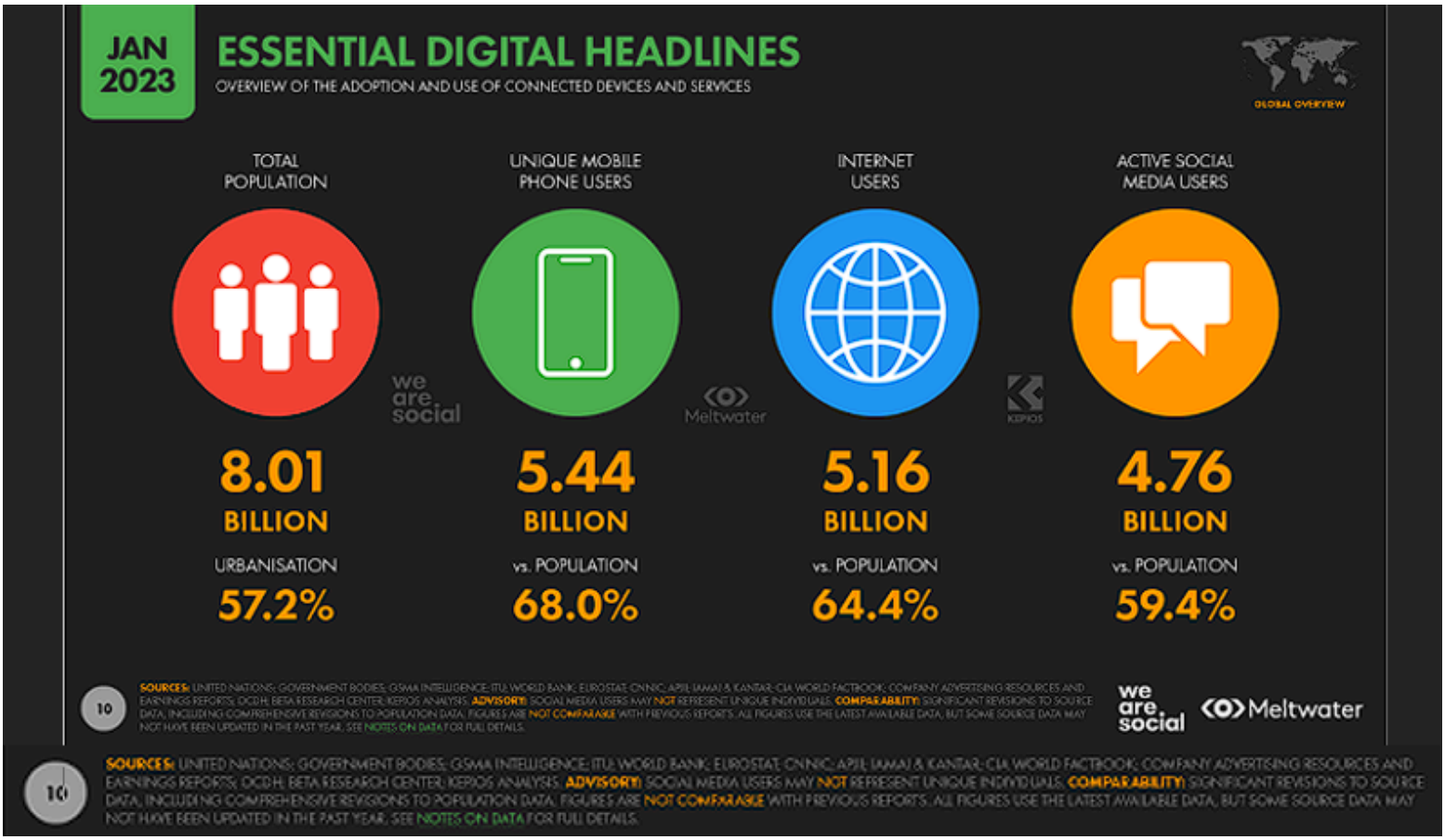


***Nota:** La figura muestra el porcentaje de personas que usan internet a nivel mundial desde 1960 hasta 2021. Tomado de "Global Connectivity Report 2022", por ITU, 2022, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/.*

El Informe General Global Digital 2023 de DATAREPORTAL describe un crecimiento de 1.4% a la cifra del año pasado, reportando 5.16 millones de usuarios y usuarias interconectados a través del internet, información que se aprecia en la figura 1.2.

Figura 1.2

Uso de dispositivos conectados a internet en 2023.



Nota: La figura muestra datos esenciales sobre el uso de dispositivos conectados a internet en 2023, incluyendo la población total, usuarios únicos de teléfonos móviles, usuarios de internet y usuarios activos de redes sociales. Tomado de "Digital 2023 Global Overview Report", por DataReportal, 2023, https://datareportal.com/reports/digital-2023-global-overview-report.

La tendencia de aumento en el consumo del internet y la cantidad de dispositivos utilizados por los usuarios y usuarias para la conexión con el mundo seguirá aumentando conforme su accesibilidad aumente a nivel global; este patrón se presenta de igual manera en México de acuerdo con los resultados obtenidos por el INEGI en su Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) del 2022 como se observa en la figura 1.3.

Figura 1.3

Resultados de la ENDUTIH que muestra el aumento del uso de internet a través de los años.

Disponibilidad y Uso de TIC

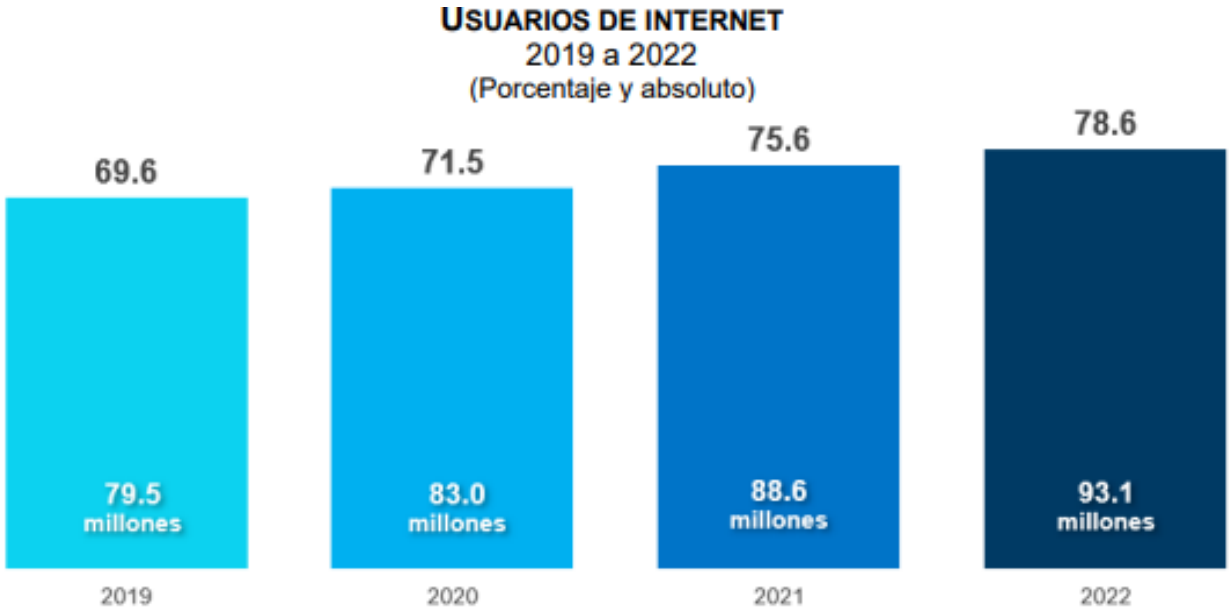
Indicadores sobre Disponibilidad y Uso de TIC	2015	2016	2017	2018	2019	2020	2021	2022 P
Hogares con computadora como proporción del total de hogares	44.9	45.4	45.3	44.7	43.9	43.8	44.8	43.9
Hogares con conexión a Internet como proporción del total de hogares	39.1	46.9	50.7	52.5	55.8	59.9	66.4	68.5
Hogares con televisor como proporción del total de hogares	93.5	93.1	93.2	92.9	92.4	91.4	91.2	90.7
Hogares con televisión de paga como proporción del total de hogares	43.7	52.0	49.4	47.1	45.6	42.6	43.3	41.5
Usuarios de computadora como proporción de la población de seis años o más de edad	51.2	46.8	45.2	44.7	42.4	37.5	37.4	37.0
Usuarios de Internet como proporción de la población de seis años o más de edad	57.4	59.4	63.7	65.5	69.6	71.5	75.6	78.6
Usuarios de computadora que la usan como herramienta de apoyo escolar como proporción del total de usuarios de computadora	51.3	52.2	46.7	46.8	44.5	51.5	46.5	46.8
Usuarios de Internet que han realizado transacciones vía Internet como proporción del total de usuarios de Internet	12.8	14.7	20.4	23.6	27.1	32.5	35.5	36.0
Usuarios de Internet que acceden desde fuera del hogar como proporción del total de usuarios de Internet	29.2	20.7	16.8	13.5	10.9	6.2	4.8	4.6
Usuarios de teléfono celular como proporción de la población de seis años o más de edad	71.4	73.5	72.1	73.3	74.9	75.1	78.3	79.2

Nota: La figura presenta los indicadores sobre disponibilidad y uso de TIC en los hogares mexicanos desde 2015 hasta 2022, mostrando el aumento en el uso de internet y otros dispositivos tecnológicos. Tomado de "Disponibilidad y Uso de TIC", por INEGI, 2023, https://www.inegi.org.mx/temas/ticshogares/.

Con una población de 129 millones de habitantes en 2023, el 78% de usuarios y usuarias en internet en 2022 reportados, equivale a 93.1 millones de mexicanos que utilizan el internet, como se observa en la figura 1.4:

Figura 1.4

Aumento de usuarios en internet.

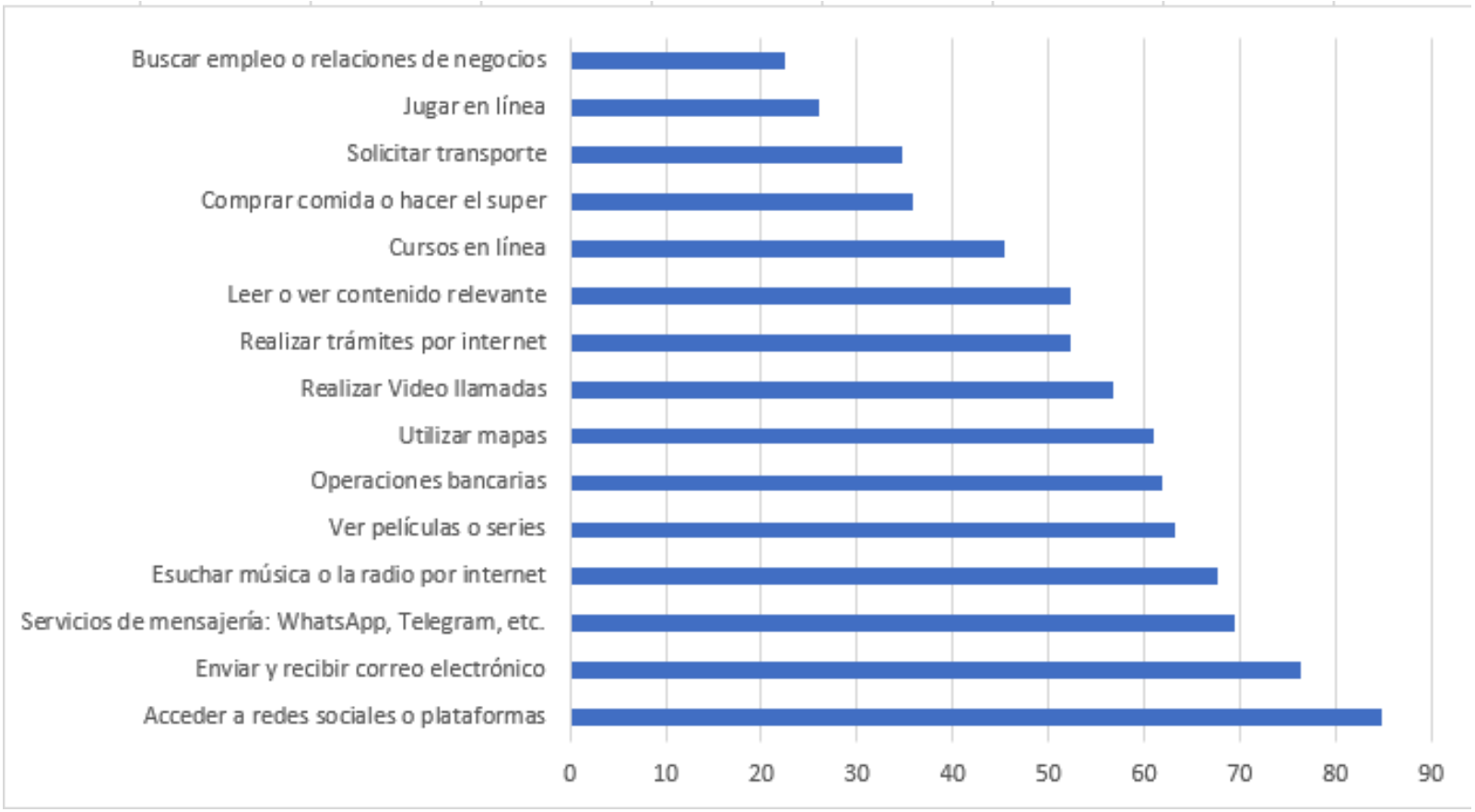


***Nota:** La figura muestra el incremento del número de usuarios de internet en México de 2019 a 2022, tanto en porcentaje como en números absolutos. Tomado de "Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH)", por IFT, 2023, https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/encuesta-nacional-sobre-disponibilidad-y-uso-de-tecnologias-de-la-informacion-en-los-hogares-endutih-0.*

Según el 19° Estudio sobre los Hábitos de Usuarios de Internet en México 2023, el 42.7% de los mexicanos permanece conectado por un tiempo de entre 7 y 9 horas diarias a través de distintos dispositivos y redes, dejando en claro que utilizar internet es algo habitual y constante en la población mexicana, que cada vez se digitaliza más haciendo de este una herramienta indispensable actualmente, y como se observa en la figura 1.5, son cada vez más mexicanos los que tienen mayor acceso a internet para su uso en distintas actividades.

Figura 1.5

Principales actividades que realizan los internautas mexicanos - porcentaje.

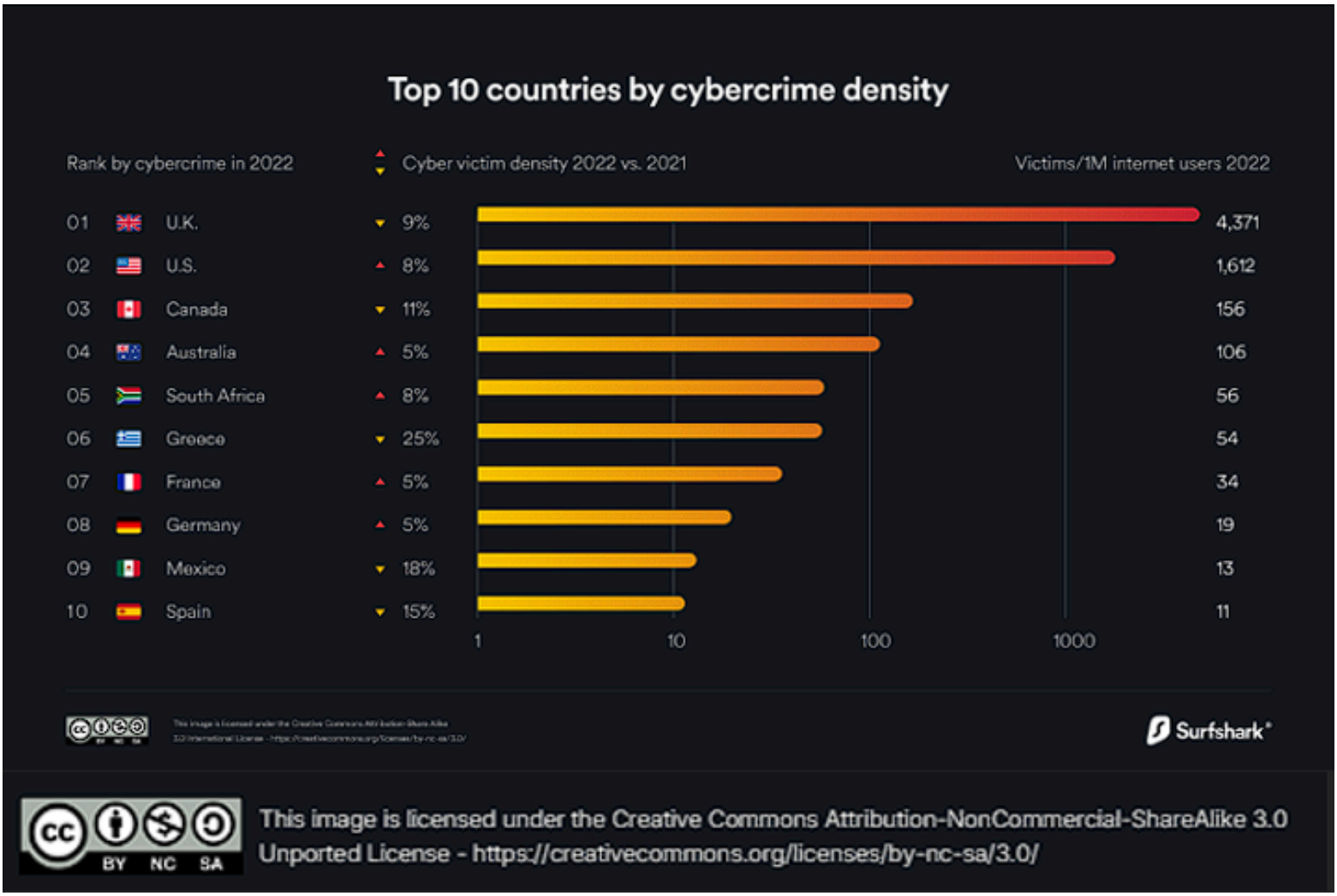


***Nota:** La figura muestra las principales actividades realizadas por los internautas mexicanos, expresadas en porcentaje. Tomado de "Estudio sobre los Hábitos de los Usuarios de Internet en México 2023", por IRP, 2023, https://irp.cdn-website.com/81280eda/files/uploaded/19%20Estudio%20sobre%20los%20Habitos%20de%20Usuarios%20de%20Internet%20en%20Mei-xico%202023%20pptx.pdf.*

Sin embargo, se deben considerar los problemas y riesgos que existen al utilizar el internet que son realmente preocupantes tomando en cuenta que en el ranking sobre los países con mayor tasa de cibercriminalidad reportado por la empresa Surf Shack y dado a conocer a través de su página https://surfshark.com/research/data-breach-impact/statistics en 2022, México entra en el top 10 ocupando la posición número 9 (véase la figura 1.6).

Figura 1.6

Top 10 de países con mayor cibercriminalidad.



***Nota:** La figura muestra los diez países con mayor incidencia de cibercriminalidad según el reporte de 2023. Tomado de "Top 10 de países con mayor cibercriminalidad", por surfshark.com, 2023, https://surfshark.com/research/data-breach-impact/statistics*

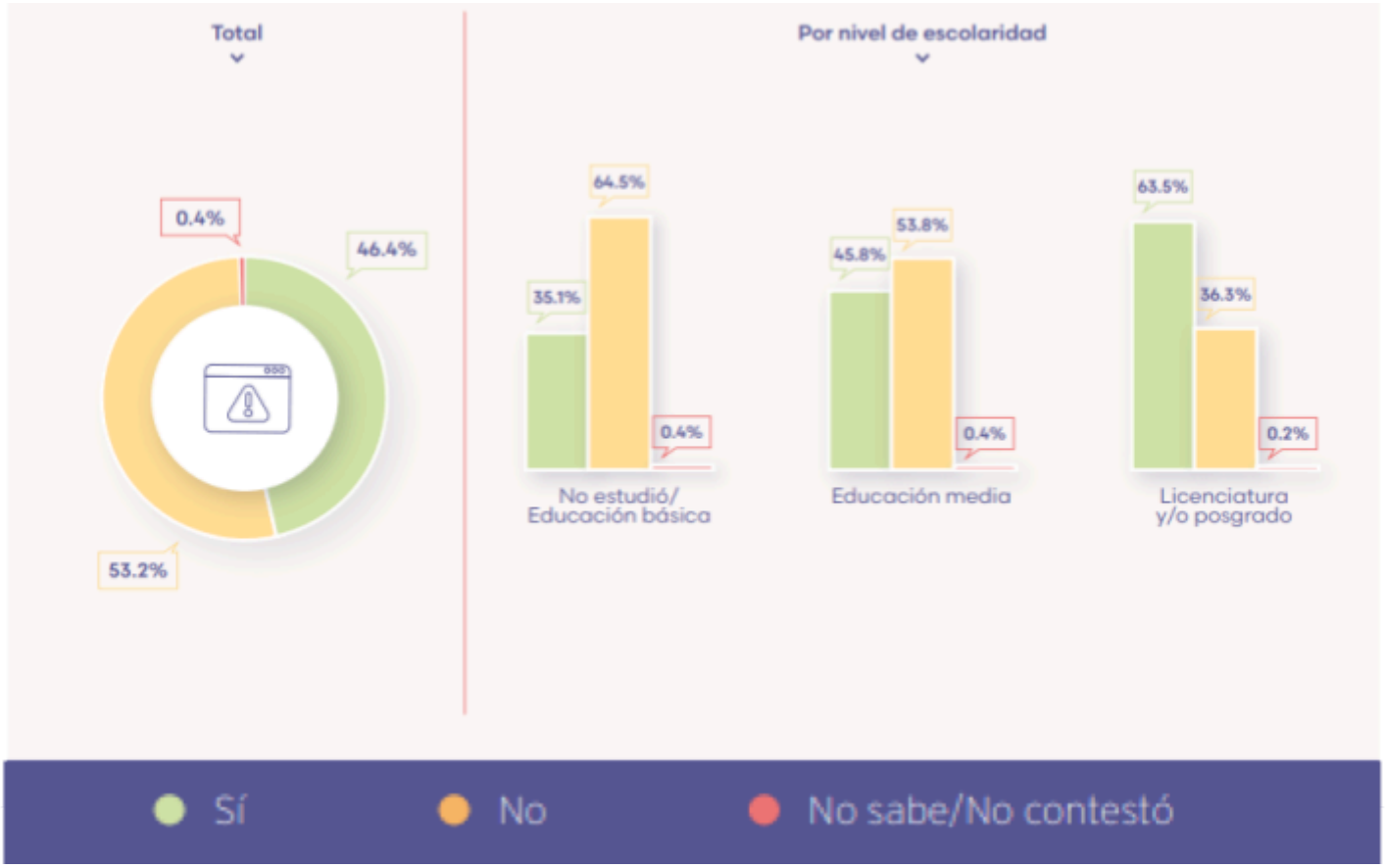
La gráfica mostrada en la figura 1.6, fue realizada en colaboración con en el Reporte de Crímenes de Internet del FBI donde hay 13 ciberataques por cada millón de usuarios en internet en México, sumando 1209 en el año 2022; según Fortinet en su informe semestral sobre el Panorama Global de Amenazas, en 2023, México ha sido objetivo de más de 14,000 millones de intentos de ciberataques en la primera mitad del año por lo que más del 15% de los usuarios y usuarias de internet han sido o son objetivo de algún tipo de ciberataque

y si no se toman acciones para disminuirlos, uno de cada tres internautas será atacado año con año llevando a pérdidas significativas en la población.

A medida que la sociedad se sumerge cada vez más en un mundo conectado en línea, el impacto de la falta de conocimiento sobre los riesgos cibernéticos se vuelve aún más pronunciado debido a que solamente el 46.4% de personas usuarias de internet fijo están informadas sobre riesgos cibernéticos como lo informa la IFT en su encuesta publicada en 2022
https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-466-de-personas-usuarias-de-internet-fijo-estan-informadas-sobre-riesgos-ciberneticos-encuesta donde es preocupante que más de la mitad de usuarios y usuarias no saben sobre el riesgo que implica navegar en internet (véase la figura 1.7).

Figura 1.7

¿En algún momento se ha informado sobre los riesgos cibernéticos (a través de publicaciones, páginas oficiales, redes sociales, búsquedas en Internet, televisión, revistas, etc.)?

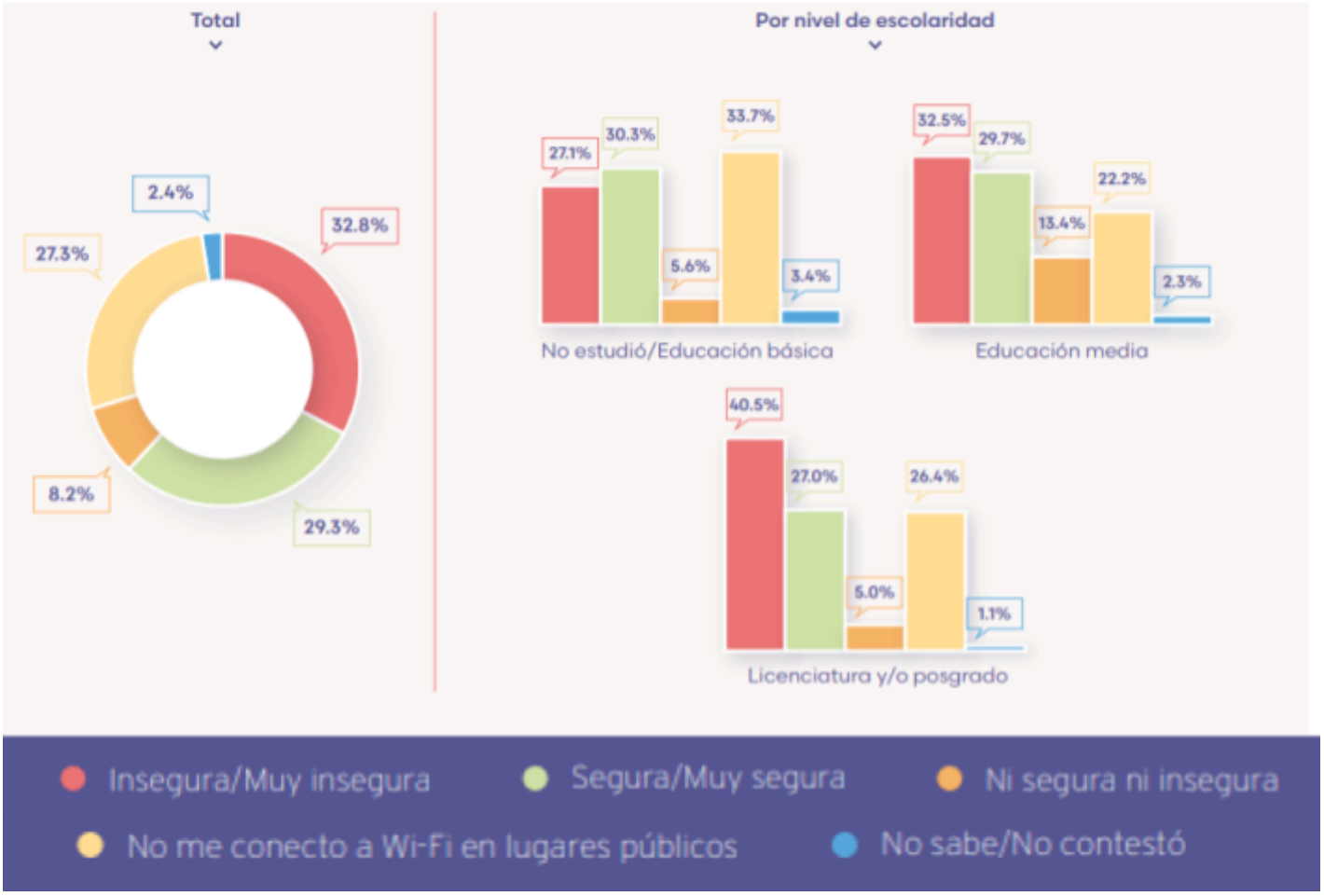


Nota: La figura representa los diferentes medios a través de los cuales las personas han sido informadas sobre los riesgos cibernéticos. Tomado de "El 46.6% de personas usuarias de internet fijo están informadas sobre riesgos cibernéticos", por Instituto Federal de Telecomunicaciones, 2023, https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-466-de-personas-usuarias-de-internet-fijo-estan-informadas-sobre-riesgos-ciberneticos-encuesta.

Al analizar la gráfica mostrada en la figura 1.8, es evidente que la mayoría de los usuarios y usuarias se sienten inseguros al conectarse a redes públicas. Por lo tanto, el objetivo de este trabajo es proporcionar información esencial a estos usuarios y usuarias para que puedan conectarse de manera segura a las redes. Es importante informar a los usuarios sobre las medidas que pueden tomar para mantener un nivel óptimo, en la medida de sus posibilidades, de seguridad al conectarse.

Figura 1.8

¿Qué tan seguras se sienten las personas usuarias cuando se conectan a Internet a través de Wi-Fi en lugares públicos (transporte público, parques, aeropuertos, restaurantes, plazas comerciales, etc.)?



***Nota:** La figura muestra el nivel de seguridad percibido por las personas usuarias al conectarse a Internet mediante Wi-Fi en diversos lugares públicos. Tomado de "El 46.6% de personas usuarias de internet fijo están informadas sobre riesgos cibernéticos", por Instituto Federal de Telecomunicaciones, 2023, https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-466-de-personas-usuarias-de-internet-fijo-estan-informadas-sobre-riesgos-ciberneticos-encuesta.*

Los usuarios y usuarias no solo son en gran medida inconscientes de los peligros que enfrentan en línea, sino que también subestiman la importancia de medidas de seguridad sólidas. Además, esta falta de conciencia no solo afecta a individuos, sino que también implica fallas más amplias en la seguridad cibernética a nivel global. Debido a todo esto necesitan conocer de medidas de seguridad que sean prácticas y fáciles de entender para que las apliquen.

1.2. Hipótesis

Los usuarios y usuarias no son conscientes de los riesgos de utilizar el internet y necesitan conocer medidas de seguridad que sean prácticas y fáciles de entender para que las apliquen.

1.3. Objetivo central

Desarrollar un manual de *Medidas de protección digital en redes de datos* a fin de que los usuarios y usuarias finales mejoren el rendimiento y seguridad en sus redes domésticas.

1.4. Objetivos secundarios

- Conocer y desglosar detalladamente los componentes de las redes domésticas y las configuraciones que se pueden realizar sobre los dispositivos para contar con seguridad.
- Demostrar las principales vulnerabilidades del internet y cómo atentan en la seguridad de las redes domésticas.
- Conocer los hábitos de los usuarios y usuarias en la red: Determinar las poblaciones cuyo uso del internet les vuelve más vulnerables a ataques y su relación con factores como su edad, género, y nivel de estudios.
- Relacionar los efectos de la pandemia con el aumento del tráfico y consumo de internet por parte de los usuarios finales en hogares y el uso de aplicaciones de conexión remota.
- Solucionar los principales tipos de fallas que puedan ocurrir en las redes domésticas.

1.5. Actividades a realizar para alcanzar los objetivos

Para lograr los objetivos planteados anteriormente, es fundamental llevar a cabo una serie de actividades que nos permitirán alcanzarlos. A continuación, se detallan estas actividades:

- Conocer a los usuarios y usuarias de internet.
- Conocer las redes de internet.
- Conocer las redes de los usuarios y usuarias.
- Conocer los dispositivos que están al alcance de los usuarios y usuarias.
- Conocer la interacción de los usuarios y usuarias con la red.
- Conocer la formación de los usuarios y usuarias en los temas de redes.
- Analizar la actividad de los usuarios y usuarias en las redes.
- Encontrar posibles vulnerabilidades de los usuarios y usuarias al navegar en internet.

- Encontrar posibles vulnerabilidades en los dispositivos de los usuarios y usuarias.
- Solventar las fallas que puedan encontrarse.
- Informar a usuarios y usuarias, en un lenguaje coloquial, sobre el funcionamiento de la red.
- Resaltar la importancia de aplicar perfiles de protección y medidas de seguridad en las redes.
- Conocer el internet.
- Mostrar las amenazas que hay dentro del internet.
- Observar los efectos de la pandemia en el consumo de internet.
- Investigar sobre el auge del teletrabajo y home office.
- Conocer las herramientas de conexión remota.
- Investigar sobre la compra de equipos de cómputo con conexión a internet para el trabajo remoto.
- Conocer el software utilizado durante la pandemia y sus políticas y permisos de uso.
- Conocer los ataques realizados y suscitados en las conexiones remotas y los hogares de los usuarios.
- Conocer las fallas que pueden ocurrir en la configuración de las redes y su solución.
- Denotar los errores comunes que se presentan en la configuración de las redes.

1.6. Metodología de trabajo

La metodología de trabajo empleada se centra en la resolución de un problema, para ello los pasos a seguir son:

- Conocer el problema.
- Entender el problema.
- Investigar la magnitud del problema.
- Investigar los informes y estadísticas del problema.
- Analizar las causas del problema.
- Analizar las problemáticas que presenta.
- Conocer los recursos que se tienen para resolver el problema.
- Diseñar una solución.
- Probar la solución.
- Ajustar la solución a los resultados.
- Aplicar correcciones.
- Dar a conocer los resultados.

De manera particular en el problema de falta de aplicación de medidas de seguridad en las redes domésticas, se realizan las siguientes acciones:

- Conocer las redes.
- Conocer la seguridad de las redes.
- Entender las redes y su seguridad.
- Conocer los informes y estadísticas de las redes y su seguridad.
- Conocer a los usuarios y usuarias de las redes y su seguridad.
- Investigar la conformación y seguridad de las redes domésticas.
- Conocer los dispositivos de redes domésticas.
- Conocer la configuración de los dispositivos.
- Investigar los hábitos de los usuarios y usuarias.
- Conocer la seguridad que aplican los usuarios y usuarias.
- Conocer los ataques a la seguridad.
- Conocer las medidas de seguridad apropiadas para las redes.
- Conocer si existen otros manuales de recomendaciones e investigar cómo mejorarlos.
- Dar a conocer la importancia de la seguridad a los usuarios y usuarias.
- Ejemplificar y explicar las redes de forma entendible a los usuarios y usuarias.
- Explicar la configuración de los dispositivos a los usuarios y usuarias.
- Diseñar planes de acción ante los ataques.
- Dar recomendaciones de seguridad a los usuarios y usuarias.
- Ejemplificar las configuraciones de seguridad en los dispositivos.
- Recomendar programas de seguridad.
- Recomendar hábitos de seguridad.
- Recopilar la información en un manual.
- Dar a conocer el manual de seguridad.
- Recopilar resultados de lo que se logró con el manual.
- Analizar los resultados obtenidos y corregir el manual.
- Dar a conocer el manual corregido.

Para poder realizar todas estas actividades es necesario los conocimientos de las siguientes materias:

Inventario de Materias

1. Redes de Datos Seguras.
2. Administración de Redes.
3. Seguridad Informática Básica.
4. Administración de Servicios de Internet.
5. Sistemas de Comunicaciones.
6. Señales y sistemas.
7. Matemáticas avanzadas.

8. Ecuaciones diferenciales.
9. Cálculo integral.
10. Cálculo y Geometría Analítica.
11. Sistemas operativos.
12. Estructura y programación de computadoras.
13. Estructura de Datos y algoritmos I.
14. Estructura de Datos y algoritmos II.
15. Fundamentos de Programación.
16. Programación orientada a objetos.
17. Fundamentos de Estadística.
18. Probabilidad.
19. Algebra Lineal.
20. Algebra.
21. Redacción y exposición de temas de ingeniería.
22. Ética profesional.
23. Recursos y necesidades de México.
24. Dispositivos electrónicos.
25. Electricidad y magnetismo.
26. Administración de proyectos de software.
27. Ingeniería de Software.
28. inteligencia artificial.
29. Lenguajes formales y autónomos.
30. Ciencia, tecnología y sociedad.
31. Bases de datos.
32. Arquitectura cliente servidor..
33. Sistemas embebidos.
34. Computación Gráfica.
35. Finanzas en la ingeniería en computación.
36. Introducción a la economía.
37. Minería de datos.
38. Seguridad informática avanzada.
39. Literatura Hispanoamericana contemporánea.
40. Cultura y comunicación.

1.7. Resultados esperados

Se espera que los usuarios y usuarias con media, poca o nula experiencia en la configuración de las redes de telecomunicaciones adquieran conciencia sobre la importancia de la seguridad en redes domésticas y el uso de internet mediante el uso del manual creado en el trabajo para conocer sobre las medidas de protección digital que

pueden aplicar dentro de sus redes domésticas a fin de mejorar la seguridad y rendimiento de sus equipos.

2. DESCRIPCIÓN DE UNA RED DE DATOS

En este capítulo se abordan las redes de datos y sus componentes como parte integral de las redes de internet domésticas, sus características e instalación atendiendo a la normatividad y reglamentos indicados por los fabricantes y organismos calificados para asegurar un rendimiento óptimo de los dispositivos y una cobertura total en los hogares tomando en cuenta la entrada de servicios, las dimensiones del hogar, la disposición de los equipos, los protocolos con los que operan y las tecnologías disponibles para que las personas puedan realizar la administración de su red con base en sus actividades y uso de internet.

2.1. Propiedades

La composición de las Redes de Datos es variada en elementos y características dependiendo de las operaciones y aplicaciones que llevará a cabo. Una red de datos es un *sistema* cuya definición según la Real Academia Española (RAE) es: “Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto” (Diccionario de la lengua española, 2023); en este trabajo, la definición requiere enfocarse en las redes informáticas o redes de computadoras, por lo que se ajusta la definición a: *Conjunto de dispositivos electrónicos interconectados entre sí, mediante uno o más medios de transmisión que comparten datos, recursos y servicios para llevar a cabo diferentes actividades.* Ambas definiciones comparten la característica de no especificar el objetivo de las redes dado que los usuarios y usuarias que la ocupan serán los que decidan cual es el propósito o propósitos de la red.

De acuerdo con la empresa de administración de Centros de Datos y Servicios de Tecnología e Información KIO (2023): “Un dispositivo de interconexión de redes es un término ampliamente utilizado para cualquier hardware que conecte diferentes recursos de red” por otro lado, la escuela de tecnología y programación Keep Coding (2023) los dispositivos de red son: “los equipos físicos necesarios para la interacción y comunicación del hardware de una red informática” siendo los teléfonos inteligentes (smartphones), las computadoras de escritorio y las laptops los más comunes de acuerdo a la Asociación para la Investigación de Medios de Comunicación. Las características de estos dispositivos, específicamente su tarjeta de red, serán las que determinen su interrelación y operación dentro de la red del hogar así como las configuraciones de seguridad y rendimiento que pueden aplicarse.

La intercomunicación de los dispositivos es la operación más importante que llevan a cabo los dispositivos de red para cumplir con las actividades que solicitan los usuarios y usuarias, para ello requieren de medios de transmisión aéreos y terrestres cuyo propósito es darle una *vía a la información emitida por los dispositivos hacia su receptor*, para lo cual utiliza protocolos específicos que permiten la conexión y sincronización de emisor y receptor.

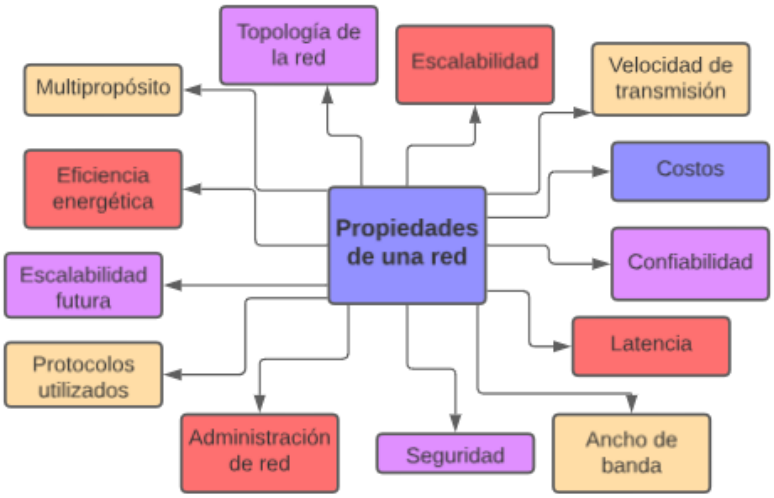
Los usuarios y usuarias de la red asumen roles duales como emisor y receptor, dependiendo de la acción que realicen y se les define como *persona que emplea un producto o servicio de forma ocasional o habitual;* para este trabajo en particular se define al *usuario y usuaria común* como *aquel que no posee los conocimientos necesarios para realizar la configuración de su red de internet y aplicar medidas de seguridad en la misma.* El usuario y usuaria común mantiene la configuración de fábrica de sus dispositivos de red conectándose tan pronto como les es posible, sin considerar las opciones de personalización disponibles, las cuales incluyen medidas de seguridad.

Dentro de este contexto de las redes domésticas, la composición de estos entornos tecnológicos es un factor crucial que determina su funcionamiento y capacidad. Como se ha mencionado anteriormente, las redes domésticas son conjuntos dinámicos de elementos interconectados que facilitan el intercambio de información para alcanzar objetivos específicos.

Para realizar todo esto es necesario considerar algunas de las propiedades (véase figura 2.1) que permiten llevar a cabo el correcto funcionamiento de la red de datos, mismos que se listan a continuación y que más adelante se describen:

- Topología de la red.
- Escalabilidad.
- Velocidad de transmisión.
- Confiabilidad.
- Latencia.
- Ancho de banda.
- Seguridad.
- Administración de red.
- Protocolos utilizados.
- Escalabilidad futura.
- Eficiencia energética.
- Multipropósito.
- Costo.

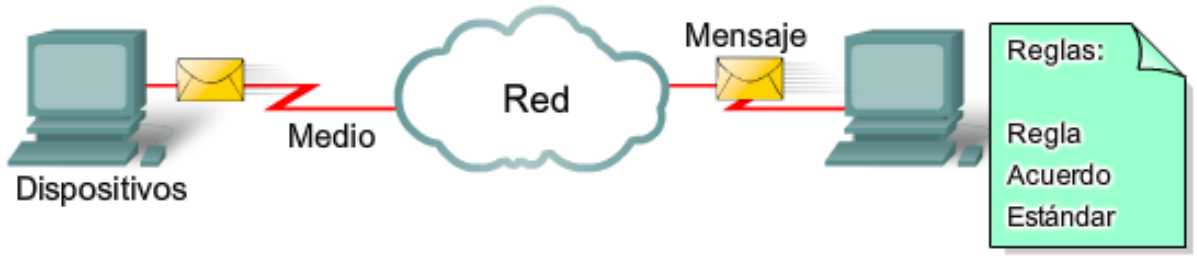
Figura 2.1
Propiedades de una red.



Nota: La figura ilustra las propiedades fundamentales de una red. Elaboración propia.

Dado que el comunicarse de manera confiable con cualquier persona en cualquier lugar es de suma importancia en nuestra vida personal y comercial se debe respaldar el envío inmediato de millones de mensajes a nivel global por lo que confiamos en una red de información interconectada para lograr este cometido. De acuerdo con la Ing. Eugenia Macías, en los Apuntes de la Asignaturas de Redes de Datos I y Redes de Datos II (2009, p.9), estas redes, ya sea de gran escala o más pequeñas, comparten cuatro elementos básicos (véase la figura 2.2):

Figura 2.2
Elementos de una red.



Nota: La figura muestra los diferentes elementos que componen una red. Tomado de "Manual de la Asignatura de Redes de Datos I y II", por Víctor, 2023, http://profesores.fi-b.unam.mx/victor/CCNA/Productos/Notas%20de%20Curso/Manual%20de%20la%20Asignatura%20de%20Redes%20de%20Datos%20I%20y%20II%20%28avance%2050%25%29.pdf.

- Reglas o Acuerdos: Estas normas especifican cómo se envían, dirigen e interpretan los mensajes. Por ejemplo, en la mensajería instantánea Jabber, los protocolos XMPP, TCP e IP son esenciales para la comunicación. En este trabajo se presenta una variedad de mensajes, dispositivos, medios y servicios, así como los protocolos que unen estos elementos de red.
- Mensajes: Unidades de información que viajan entre dispositivos, el inicio de su viaje desde la computadora hacia su destino, los mensajes se convierten en bits, señales digitales codificadas en binario, independientemente de su formato original. Este proceso es esencial para la transmisión efectiva a través de la red, abarcando mensajes de texto, vídeo, voz o datos informáticos.
- Medios de Transmisión: Permiten la interconexión de dispositivos y transportan mensajes. Las redes locales, ya sea con cables o inalámbricas, conectan dispositivos en hogares o empresas. La red inalámbrica amplía la conectividad a zonas exteriores y lugares públicos. Las redes con cables, como Ethernet, son ideales para la transmisión de grandes cantidades de datos a altas velocidades.
- Dispositivos en la Red: Intercambian mensajes entre sí, más allá de las computadoras, otros dispositivos, como teléfonos, cámaras y consolas de juegos, se

conectan a la red para participar en servicios y compartir información. Los routers, componentes críticos, aseguran una transmisión rápida y eficiente entre redes.

- Servicios de red: Programas computacionales distribuidos en la red brindan soporte a herramientas de comunicación en línea, como correos electrónicos, foros y mensajería instantánea, facilitando la interacción humana.

2.2. Normas de instalación

Al trabajar con las redes domésticas y los dispositivos electrónicos, también conocidos como *equipos electrónicos*, es necesario conocer las regulaciones que aseguran su correcto funcionamiento conocidas como normas y estándares.

Estos conceptos suelen ser interpretados como uno solo y lo mismo, dado que ambos dictan especificaciones para reglamentar procesos y productos a fin de garantizar la interoperabilidad, sin embargo, según la Ley de Infraestructura de la Calidad de México un estándar es “un documento técnico que prevé un uso común y repetido de reglas, especificaciones, atributos o métodos de prueba aplicables a un bien, producto, proceso o servicio, asì como aquellas relativas a terminología, simbología, embalaje, marcado, etiquetado o concordaciones.” (Artículo 4, fracción X). Mientras que la norma es definida como “la regulación técnica de observancia obligatoria expedida por las autoridades normalizadoras competentes cuyo fin esencial es el fomento de la calidad para el desarrollo económico y la protección de los objetivos legítimos de interés público mediante el establecimiento de reglas, denominación, especificaciones o características aplicables a un bien, producto, proceso o servicio, asì como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y de información.” (Artículo 4, fracción XVI). La diferencia notable en las definiciones es que el estándar se asegura de que los productos y servicios cubren con determinadas especificaciones y las normas aceptan las especificaciones utilizadas a fin de garantizar que los productos funcionen con otros de diferentes especificaciones; y para ello, la redacción de normas y estándares es realizada por varias organizaciones, en conjunto con los fabricantes de los dispositivos, expertos del área y grandes corporaciones encargadas de la fabricación de los productos y préstamo de los servicios.

En las redes domésticas se aplican las mismas especificaciones que en las grandes corporaciones pero a una menor escala debido a su cobertura, es decir, el área que cubre el servicio de internet. De acuerdo con la Encuesta Nacional de Vivienda (ENVI) del INEGI, los hogares mexicanos tienen entre 45 a 180 metros cuadrados donde un 67% de las viviendas cuentan con menos de 100 metros cuadrados, por lo que entran en el área de cobertura de una *red de área local (LAN)*, la cual cubre un entorno de hasta 200 metros y le confiere características que se profundizan en el apartado 1.3 de este capítulo.

En la instalación de la redes LAN, las normas que más intervienen corresponden al cableado estructurado y para este trabajo, se consideran las normas mexicanas:

1. NMX-I-108-NYCE-2006: Cableado de telecomunicaciones - Cableado estructurado-Conexión a tierra en sistemas de telecomunicaciones.

Esta norma establece las especificaciones técnicas para la puesta de tierra que requieren los sistemas eléctricos de las redes para prevenir daños a sí mismos, al usuario y a los sistemas con los que se encuentre conectado.

2. NMX-I-154-NYCE-2008: Cableado de telecomunicaciones - Cableado estructurado - Cableado residencial general

Esta norma establece las características y especificaciones que debe tener el cableado estructurado para ser utilizado en las residencias de forma segura y confiable.

3. NMX-I-279-NYCE-2009: Cableado de telecomunicaciones - Cableado estructurado - Conducto y espacio para cableado de telecomunicaciones en edificios comerciales

Esta norma establece las características de los conductos, canaletas, escalerillas y vías para la instalación de cableado estructurado, así como los doblamientos, giros y torsiones aplicables al cableado sin dañarlo.

2.2.1. Confiabilidad

En el marco de la implementación y cumplimiento de las normas mencionadas anteriormente, es imperativo contar con la intervención de organizaciones especializadas que respalden y velen por su aplicación integral. Estas entidades desempeñan un papel fundamental al asegurar que las normativas sean correctamente interpretadas y seguidas por los diversos actores involucrados.

Por ello algunas de las principales organizaciones encargadas de respaldar su aplicación y garantizar su adecuado seguimiento son las siguientes:

- TIA - Telecommunications Industry Association: Es la principal asociación que representa el mundo de la información y la comunicación (TIC) a través de la elaboración de normas.
- ANSI - American National Standard institute : Administra y coordina el sistema de estandarizar voluntaria del sector privado
- EIA - Electronic Industries Alliance: Es una organización formada por la asociación de las compañías electrónicas y de alta tecnología cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología

- ISO - International Organization for Standardization : Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación.
- IEEE - Institute of Electrical and Electronics Engineers : Es una asociación técnico-profesional dedicada a la estandarización. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías.

Estas organizaciones desempeñan un papel activo en la validación y supervisión de procesos, productos o servicios, actuando como garantes de la calidad e integridad. A través de auditorías regulares, certificaciones y colaboraciones con otras entidades reguladoras, se aseguran de que las normas establecidas se mantienen y evolucionan según las nuevas necesidades que se presenten .

Su participación no solo brinda un sello de aprobación, sino que también ayuda a promover la confianza con los consumidores y usuarios. Además, al establecer un marco de referencia sólido, estas organizaciones fomentan la innovación y la mejora continua en las redes domésticas.

2.2.2. Características de Tarjeta de red

Dentro de los dispositivos de red se encuentra el componente esencial para realizar la conexión a la red doméstica conocido como *Tarjeta de red*.

Este elemento se encarga de conectar la red doméstica con los componentes internos de los equipos que requieren datos de la red para poder realizar sus tareas. Para ello realizan la traducción de las señales enviadas a través de la red de datos en código de computadora conectándose a través de Ethernet, WiFi, Fibra óptica, Bluetooth entre otros medios a la red y los componentes internos mediante PCI, PCI-E, USB, entre otros conectores.

En el caso de los dispositivos móviles, laptops y algunas computadoras de escritorio, la tarjeta de red se encuentra integrada en lo que se conoce como placa base o motherboard lo que permite un mejor procesamiento de datos resultando en un mayor rendimiento, esto se obtiene gracias a la configuración realizada por los fabricantes de los componentes para asegurar su funcionamiento, conocido como *plug-and-play* que ayuda a los usuarios y usuarias comunes a utilizar sus equipos tan pronto como sean adquiridos o tras pequeños ajustes de configuración regularmente incluidos en un manual de fácil instalación dentro del paquete que contiene al dispositivo. Mientras que esta configuración es conveniente, limita la personalización de la red lo cual puede generar problemas de compatibilidad con dispositivos de mayor antigüedad ya integrados a la red, causa fallas de conexión debido a diferencias entre las configuraciones de fábrica, deja la red expuesta a varias

vulnerabilidades y abre la posibilidad a pérdidas de comunicación debido a estar ubicado fuera del rango efectivo de transmisión, conocido como *cobertura*.

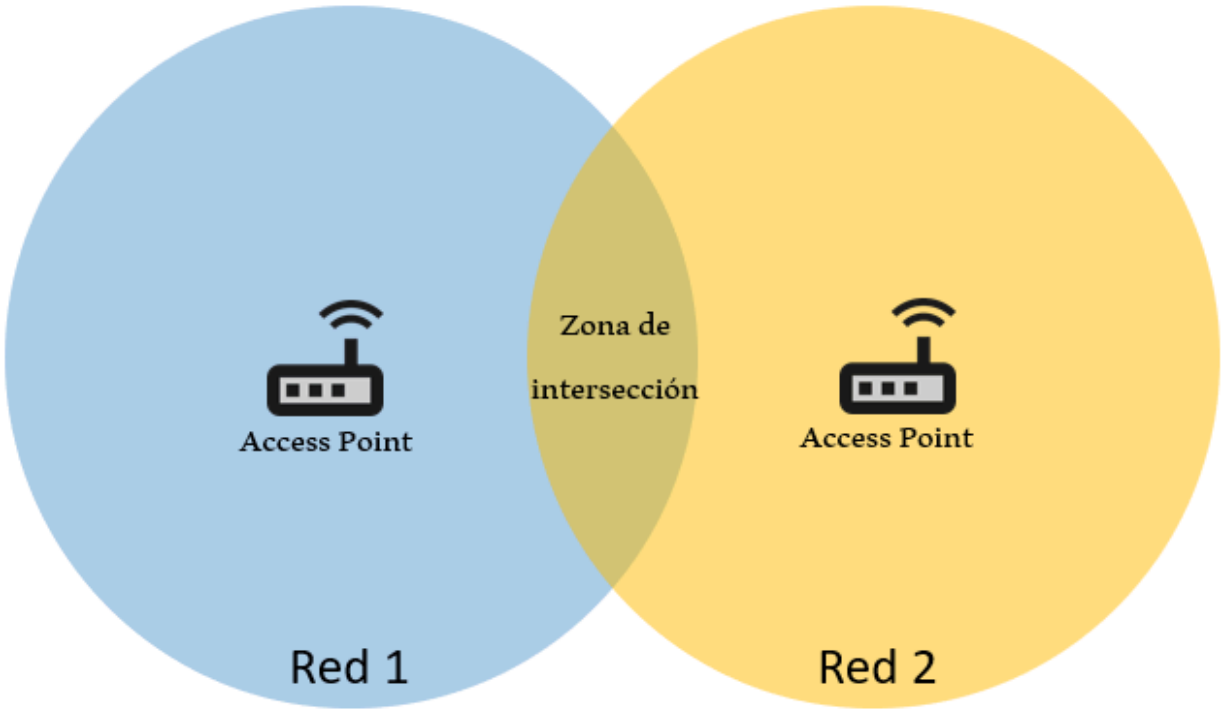
2.2.3. Tamaño y ubicación de la Red

En la instalación de dispositivos de redes, uno de los factores más importantes a considerar es el *espacio físico* que ocupan cada uno y el área a la debe brindar servicio, esto aplica para los componentes tales como Modem, Switches, Routers, Access Points y Repetidores de señal. En el caso de dispositivos finales como computadoras, celulares, tabletas y dispositivos pertenecientes al Internet de las Cosas, su posición determinará cuáles son las ubicaciones óptimas para que puedan conectarse a la red y aprovecharla en su totalidad haciendo importante considerar la interacción que tendrán ambos con el entorno.

De forma física, los dispositivos se pueden conectar utilizando medios terrestres y aéreos, identificados por el uso de cables para el primer caso, y radio-frecuencias para el segundo; ambos con características particulares que se abordan en el capítulo 1.4 y las cuales deben ser utilizadas para decidir en qué parte del hogar colocar los dispositivos, qué tecnología es más conveniente, qué tantos equipos se pueden conectar a la red y la seguridad aplicable a toda la red.

Al conectar un dispositivo de red con tecnología inalámbrica, se crea una zona física de conexión limitada por la intensidad de la señal que pueda generar el dispositivo, a la cual se pueden conectar todos los dispositivos que permita su configuración. Este escenario es conveniente para los usuarios y usuarias dado que solo requieren estar dentro de la zona de conexión para utilizar los servicios de su red, pero también es peligroso dado que la transmisión de sus datos y las operaciones que realizan pueden ser observadas si son captadas, ya que se encuentran viajando en el aire y pueden ser interrumpidas por fluctuaciones del mismo, así mismo los mensajes enviados pueden interferir unos con otros si hay una gran concurrencia de ellos (REDES CISCO: Fundamentos de Networking para el examen de certificación CCNA). Este efecto se presenta de igual manera si dos o más zonas de conexión ocupan un mismo espacio, conocida como zonas de intersección, lo que se puede visualizar en la figura 2.3.

Figura 2.3
Intersección de zona de conexión entre dos redes.



Nota: La figura muestra la intersección entre dos redes, cada una representada por un círculo. Los puntos de acceso (Access Points) se encuentran en cada red, y la zona de intersección indica el área donde las dos redes se superponen y pueden interferir su señal. Elaboración propia.

Otros factores como los materiales del hogar, sean estos las paredes de piedra y estructuras metálicas, al igual que aparatos electrodomésticos de uso común como el horno de microondas, radiadores y lavadoras, así como el agua presente en las tuberías del hogar, causan interferencias en las redes domésticas y son aspectos que afectan el uso de internet por parte de los usuarios y usuarias.

Para solucionar estas fallas, es necesario que los usuarios y usuarias conozcan cuáles son las diferentes tecnologías inalámbricas con las que operan sus dispositivos para tomar decisiones informadas sobre la ubicación geográfica de ellos dentro de sus hogares. Información que se incluye en el Manual realizado durante este trabajo en el cual se adjuntan ejemplos aplicables que funcionan de guía para la instalación de la red.

Como ya se mencionó, la cobertura es el área de rango efectivo de transmisión de datos definido por los fabricantes de ellos, siguiendo los estándares de comunicación dictados por organizaciones especializadas en la materia a fin de asegurar su correcto

funcionamiento e interoperabilidad y se aplican en **conexiones inalámbricas**; el más importante de ellos es el estándar IEEE 802.11.

El estándar 802.11 contiene los protocolos, técnicas y procedimientos para la fabricación de componentes inalámbricos y sus características, de las que destacan su frecuencia, velocidad y rango, que se muestran en la Tabla 2.1, siendo rango el que dicte el área de cobertura, la posición del equipo de redes y la cantidad de dispositivos que se requerirán para cubrir toda el área deseada.

Tabla 2.1

Características de Estándares para dispositivos inalámbricos.

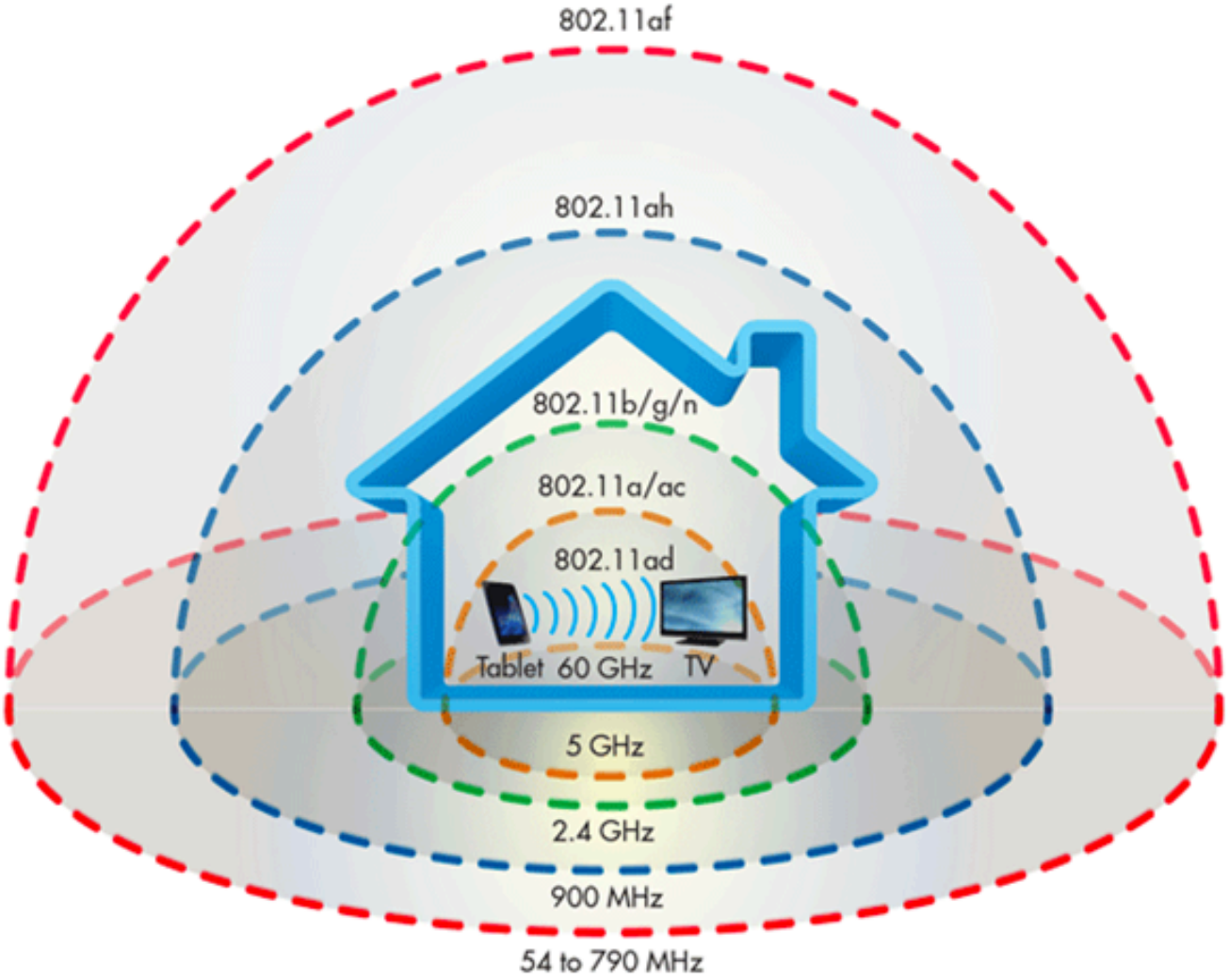
Estándar	Frecuencia (GHz)	Velocidad (Mbps)	Rango (m)
IEEE 802.11	2.4	2	20
Wi-Fi 1 / IEEE 802.11a	5 / 3.7	54	35
Wi-Fi 2 / IEEE 802.11b	2.4	11	35
Wi-Fi 3 / IEEE 802.11g	2.4	54	38
Wi-Fi 4 / IEEE 802.11n	2.4 /5	600	70
Wi-Fi 5 / IEEE 802.11ac	2.4 / 5	450 / 1300	46
IEEE 802.11ad (WiGig)	60	6.7 Gbps	9
IEEE 802.11ah (HaLow)	0.9	347	1 km
IEEE 802.11af (WhiteFi)	54 - 790 MHz	26	> 1 km

Nota: La tabla muestra las características de varios estándares IEEE 802.11 para dispositivos inalámbricos, incluyendo frecuencia de operación, velocidad máxima teórica y rango de cobertura. Elaboración propia.

El área de cobertura de los dispositivos, según el estándar que utilicen, se puede visualizar como un círculo con radio del tamaño del rango, esto se aplica igualmente en sentido vertical como lo muestra la figura 2.4.

Figura 2.4

Cobertura de los estándares 802.11.



Nota: La figura ilustra la cobertura de los diferentes estándares de la serie 802.11, mostrando las frecuencias y el alcance relativo de cada uno dentro de un entorno doméstico. Tomado de "Proyecto IoT", por Andino, 2023, https://uai.edu.ar/ciiti/2023/buenos-aires/certamen-de-trabajos-estudiantiles-del-CIITI/trabajos/Andino%20Proyecto%20IoT.pdf.

Todos estos estándares pueden utilizarse para la conexión de las redes domésticas, pero se debe considerar varios factores para esa decisión; por ejemplo, si se quisiera utilizar WiGig para conectar toda una residencia, a fin de aprovechar lo 6.7 Gigabytes de velocidad, se necesitaría instalar un repetidor de señal cada 5-7 metros para obtener un funcionamiento óptimo, lo cual sería bastante costoso. Además, como se mencionó anteriormente, los

materiales del hogar causan interferencia en la red y puede que la instalación sobre ellos no sea viable haciendo necesario un reajuste lo que aumentaría más su costo.

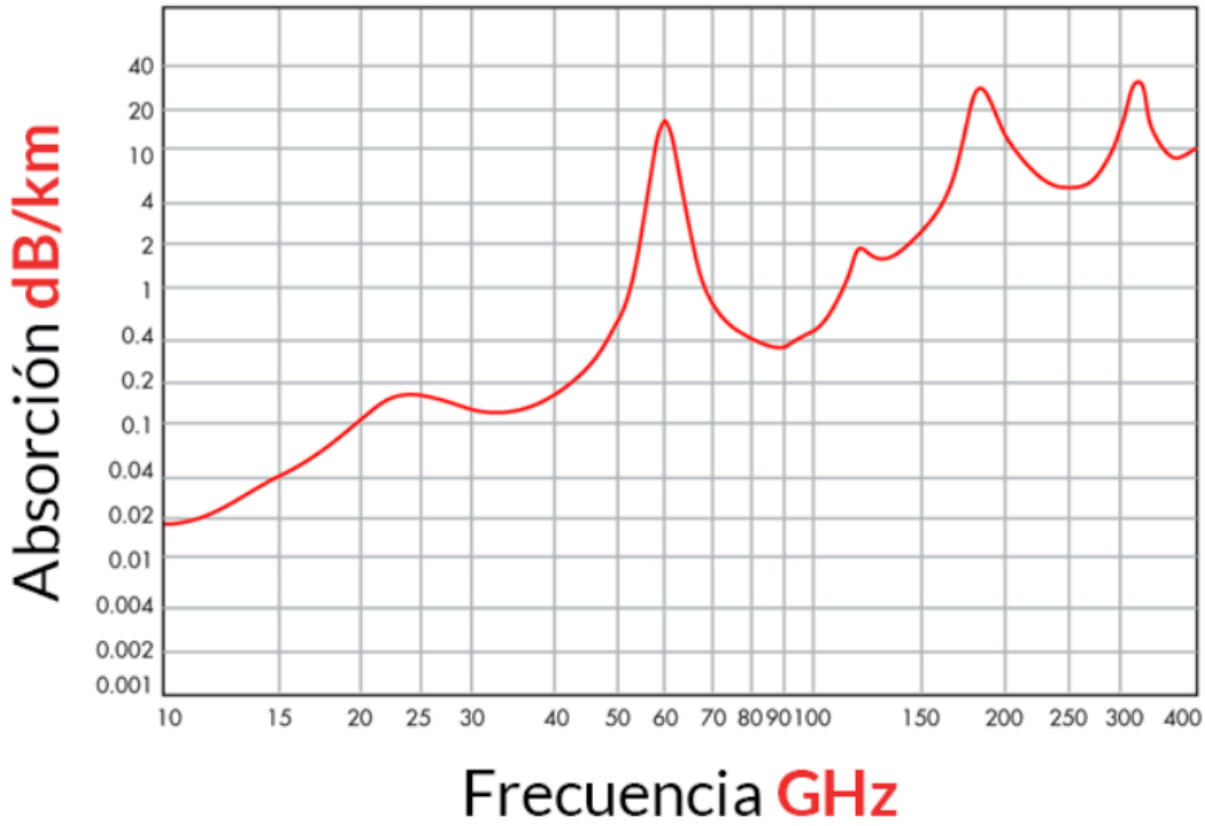
Por otra parte, no todos los dispositivos cuentan con estas tecnologías, tal es el caso del estándar 802.11af que funciona sobre las frecuencias de transmisión de las televisoras, siendo estas las que determinan la viabilidad de su instalación; y el estándar 802.11ah, que no ha sido integrado en los chips de las tarjetas de red por ningún fabricante, haciendo su presencia nula en el mercado actual. De igual manera, el estándar 802.11ax, también conocido como Wi-Fi 6, publicado en el 2020, se encuentra en su proceso de integración al mercado, con escasos modelos de compra para el público en general, siendo esta otra de las situaciones por las que no se consideran en este trabajo como alternativas viables para la instalación de una red doméstica para el usuario y usuaria común, por ello se da un mayor enfoque a los estándares 802.11b/g/n/ac, es decir Wi-Fi 2-5, siendo estos los más disponibles actualmente.

La comunicación inalámbrica consiste de una transmisión realizada por el emisor que envía señales de radiofrecuencia generadas por el paso de energía eléctrica a través de una antena metálica a cierta frecuencia y velocidad para generar pulsos u ondas electromagnéticas que se propagan por el medio en el que se encuentra y del cual el receptor las capta para interpretarlas según la configuración de los circuitos de la tarjeta de red; para lograr esto de forma efectiva, se requiere que exista una vía de transmisión directa y sin obstrucciones, conocida también como libre, entre emisor y receptor. A esta condición se le llama *línea de vista*.

La propagación de las señales electromagnéticas no es infinita, la energía de las señales eventualmente será absorbida por el material que compone al medio por el que se propaga, generalmente el aire. Esta absorción se mide en decibeles por kilómetros (dB/km) y se determina por la frecuencia de la señal como lo muestra la figura 2.5.

Figura 2.5

Absorción de las ondas de radiofrecuencia.



Nota: La figura muestra la absorción de las ondas de radiofrecuencia en función de la frecuencia, expresada en dB/km. Tomado de "La absorción en las ondas y radioenlaces", por Prored, 2023, https://www.prored.es/la-absorcion-en-las-ondas-y-radioenlaces/.

Como se puede observar en la figura 1.5, hay una correlación de aumento en la absorción conforme se aumenta la frecuencia de emisión de las ondas con picos significativos en los 60, 185 y 325 GHz. Estas frecuencias no son consideradas en los estándares mostrados en la Tabla 1, dado que se encuentran en investigación y son parte del desarrollo de la quinta generación de tecnología celular inalámbrica 5G, con poco acceso al público general.

La absorción de los materiales causa que la zona de cobertura de los estándares inalámbricos mostrados en la Tabla 2.1 disminuya, haciendo necesario el uso de Repetidores de señal orientados hacia la ubicación geográfica donde se quiere generar una zona de cobertura, por lo que se deben considerar herramientas tales como mapas de calor WiFi que permiten observar todas las zonas de cobertura de los dispositivos que se tienen en la red y la efectividad de su transmisión, según la posición en la que se encuentra y para la cual se mide la intensidad de la señal y la velocidad de transmisión de esta.

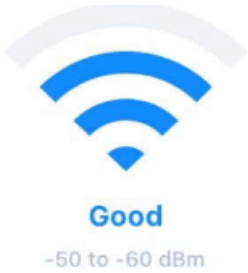
La intensidad de la señal de radiofrecuencia se mide en decibeles por kilómetro (dB/km), lo cual da una descripción físicamente precisa de las propiedades de la señal transmitida a través de un medio. Estos valores se utilizan en el cálculo del margen Señal-Ruido (margen SNR) de la forma:

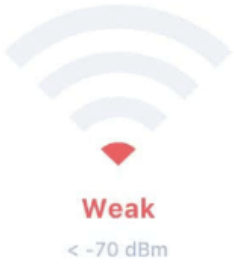
$$\text{Margen SNR} = \text{Señal (dBm)} - \text{Ruido (dBm)}$$

Con el que se determina la calidad de la señal de internet que se está obteniendo generando una relación especificada en el estándar 802.11 conocida como Indicador de señal recibida (RSSI), que ayuda a establecer rangos en los cuales el nivel de energía de señal de radio en el canal excelente, buena, media o mala como se observa en la tabla 2.2.

Tabla 2.2

Intensidad de la señal.

Intensidad de la señal	Calificador	Indicadores	RSSI
–50 dBm	Excelente	Nivel de señal apropiado para todos los usuarios con gran actividad en la red. Los dispositivos deben estar a pocos metros del Access Point o Router para recibir esta intensidad.	
–70 dBm	Buena	Recomendado para dispositivos móviles (smartphones y tablets). Recepción y envío de paquetes confiables, suficiente para streaming y voz sobre IP	
–80 dBm	Media	Intensidad mínima para recepción y envío de paquetes ligeros como navegación web e intercambio de correos electrónicos. Posibles fallos en la conectividad.	

–90 dBm	Mala	El ruido inhibe la mayoría de las transmisiones.	

Nota: La tabla muestra los distintos niveles de intensidad de la señal, sus calificadores, indicadores y la representación gráfica del RSSI (Received Signal Strength Indicator). Elaboración propia.

Como se puede observar en la tabla 1.2, la escala RSSI es subjetiva ya que el estándar 802.11 permite a los fabricantes definir su propio valor máximo y mínimo de señales de radiofrecuencia que pueden procesar los chip de las tarjetas de red que ensamblan, fijando los rangos de calidad de la señal de tal manera que sean entendibles para los usuarios y usuarias.

La distancia física entre los dispositivos conectados inalámbricamente no es la única causa para la pérdida y fallos de comunicación, también lo son diversos elementos denominados **interferencias.** Cuando se cumple el tener una línea de vista y excelente calidad de señal, se debe mantener un espacio libre de interferencias en el área conocida como *Zona de Fresnel,* definida por la familia de ecuaciones:

$$F_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

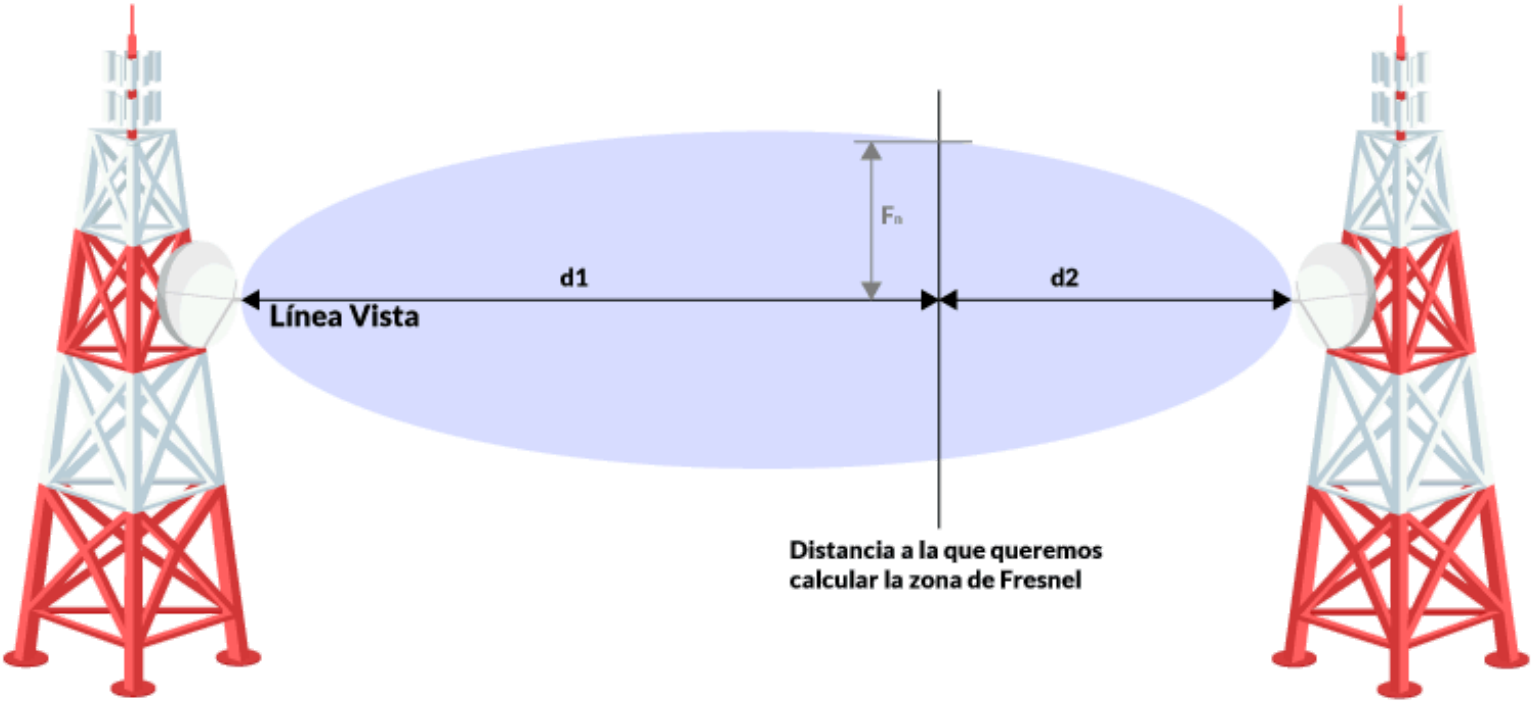
Donde:

- λ: es la longitud de onda de la señal emitida
- d1: es la distancia al punto donde se calcula el valor de la zona de la antena emisora
- d2: es la distancia al punto donde se calcula el valor de la zona de la antena receptora
- *n*: Conjunto de números naturales: 1, 2, 3, 4, ..

La proyección de este grupo de ecuaciones se observa en la figura 2.6. Si se presentan interferencias dentro de las elipses, la señal puede verse afectada, por lo que se recomienda liberar hasta la tercera Zona de Fresnel a fin de conservar una conexión sin interrupciones; sin embargo, es difícil tener un arreglo como este en una LAN debido a su cobertura, especialmente dentro de un hogar, donde la distribución de los objetos y estructuras es bastante densa haciendo necesario el uso de varios repetidores.

Figura 2.6

Diagrama de cálculo para Zonas de Fresnel.



***Nota:** La figura ilustra el cálculo de las Zonas de Fresnel en un enlace de radio, mostrando los componentes esenciales como la línea de vista y las distancias involucradas. Tomado de "Zonas de Fresnel en un radioenlace", por Prored, 2023, https://www.prored.es/zonas-de-fresnel-en-un-radioenlace/.*

2.3. Medios aéreos y terrestres

En la sección Tamaño y Ubicación de la Red se describen varios métodos de transmisión inalámbricos conocidos como *Medios Aéreos* que son los más comunes actualmente, pero también existen los *Medios Terrestres* que operan a través de cableado regulado por la norma ANSI/TIA 568 conectando físicamente a los dispositivos electrónicos.

En las estadísticas del Banco de Información Telecomunicaciones proporcionadas por el Instituto Federal de Telecomunicaciones sobre Servicio Fijo de Acceso a internet, las tecnologías alámbricas que distribuyen a todo México en los últimos 5 años (2019 para este trabajo) son DSL (Digital Subscriber Line - Línea de Abonado Digital), Cable Coaxial, conexión Satelital, conexión Móvil, y Fibra Óptica las cuales se describen en la tabla 2.3 y que componen la entrada de servicios del *cableado estructurado* del hogar.

Tabla 2.3

Tecnologías de Entrada de Servicios.

Tecnología	Descripción	Velocidad (Bitrate)
DSL (Digital Subscriber Line)	Consiste en la transmisión de datos utilizando la conexión de cobre telefónica de los hogares; requiere un módem DSL o decodificador interno para que lo puedan ocupar los dispositivos de red.	De 9 a 52 Mbps
Cable Coaxial	Se envía la señal analógica de internet mediante los cables de CCTV.	De 10 a 300 Mbps
Conexión Satelital	Utiliza un módem especializado para captar la señal de los satélites que dan el servicio.	De 5 a 25 Mbps
Conexión Móvil	El módem de entrada se conecta a una red celular 4.5 G para proporcionar el servicio	De 300 a 1000 Mbps
Fibra Óptica	Consiste de un cable de fibra de vidrio por el cual viajan los datos de internet como pulsos de electricidad, haciéndolo ligero y rápido.	De 100 a 2000 Mbps

Nota: La tabla describe varias tecnologías de entrada de servicios de internet, detallando la descripción y la velocidad (bitrate) de cada tecnología. Elaboración propia.

Para conectar a los distintos dispositivos electrónicos que componen las redes del hogar, véase la tabla 2.4, se requieren tecnologías diferentes a las de la entrada de servicio, las cuales se pueden encontrar en la sección de *Especificaciones* de los dispositivos.

Tabla 2.4

Dispositivos de las redes de datos domésticas.

Estaciones de Trabajo	
También llamados *dispositivos terminales*, es el equipo con el que interactúa directamente el usuario, pueden ser computadoras de escritorio, laptops, smartphones, tablets, entre otros.	Se compone de elementos como procesador, memoria, almacenamiento, controladores y varios dispositivos de entradas y salidas.

Tarjetas de Red	
Es el componente ubicado dentro de los dispositivos terminales que se encarga de comunicarse con la red.	Implementan diversos circuitos electrónicos para la transmisión de bits a través de medios aéreos o terrestres según su tipo.
Modems	
Es el dispositivo que recibe la entrada de internet al hogar y funciona como router repartiendo la señal a los demás dispositivos.	Generalmente lo proporciona e instala el proveedor de servicios. Posee un sistema operativo que permite varias configuraciones para adaptarse a las posibles necesidades de la red.
Switches	
El dispositivo conecta a router o módem hacia las terminales para distribuir mejor el internet mediante cableado. Puede no estar presente en las redes domésticas.	Consiste de varios circuitos que manejan el tráfico de internet de la red doméstica para distribuirla de forma más confiable. Algunos modelos tienen un sistema configurable para implementar mayor seguridad en la red.
Routers	
Se encarga de direccionar el tráfico de internet para que las solicitudes de los usuarios sean respondidas correctamente.	Selecciona la ruta de transmisión de datos más eficiente y evita que distintas transmisiones se mezclen. Su sistema operativo permite la configuración de dichas rutas, así como el filtrado o bloqueo de dispositivos y datos.
Repetidores	
Se presentan sobre todo en redes inalámbricas y se les denomina *Access Point*.	Algunos modelos no digitalizan la señal que reciben por lo que solo tienen el *perfil de seguridad* implementado en los routers por lo que pueden ser inseguros.

Nota: La tabla describe varios dispositivos utilizados en redes de datos domésticas, detallando las funciones y características de estaciones de trabajo, tarjetas de red, módems, switches, routers y repetidores. Elaboración propia.

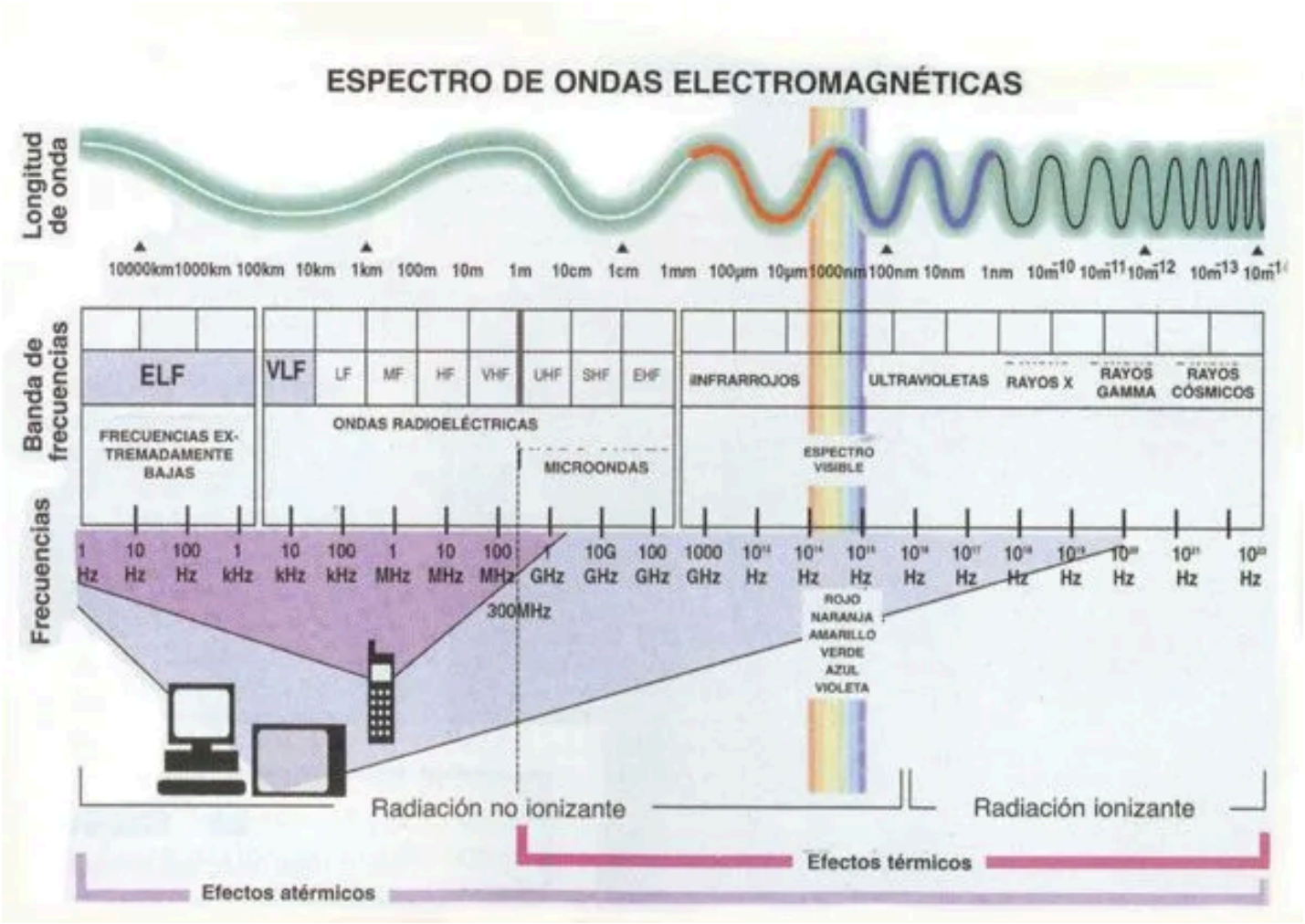
2.4 Interferencias

El Wireless-Fidelity (WiFi) ha revolucionado la conectividad al permitir el acceso a internet de forma inalámbrica. Sin embargo, esta tecnología se ve afectada por diversas interferencias electromagnéticas generadas por dispositivos cotidianos como microondas, radios y otros aparatos eléctricos. Estas interferencias pueden afectar la calidad de la señal WiFi, causando pérdida de conexión o una conexión lenta e inestable.

Como se puede observar en la figura 2.7 el espectro electromagnético se encuentra dividido para cada uno de los aparatos que se utilizan dentro de la vida diaria.

Figura 2.7

Espectro de ondas electromagnéticas.



Nota: La figura muestra el espectro completo de las ondas electromagnéticas, incluyendo las diferentes bandas de frecuencias y sus correspondientes longitudes de onda, desde las frecuencias extremadamente bajas hasta los rayos cósmicos. Tomado de "Espectro electromagnético", por Fandom, 2023, https://ingenieriatopografica.fandom.com/es/wiki/Discusi%C3%B3n:Espectro_electromagn%C3%A9tico.

Gracias a que este espectro electromagnético también se encuentra compartido con varios dispositivos domésticos y de oficina, es necesario tomar en cuenta la ubicación de estos dentro del domicilio para lograr reducir la interferencia que ocasionan estos dispositivos en la red del hogar.

Algunos indicadores de interferencias en el hogar son:

- Los dispositivos se desconectan muy seguido de la red wifi
- La intensidad de la señal disminuye en gran medida dentro de los rangos normales del router
- Menor velocidad de descarga y carga a la normal
- Dificultad para encontrar nuestra red
- Rendimiento lento en un dispositivo cuando se utiliza otro

Estos factores pueden resultar molestos al momento de utilizar la red y en muchas ocasiones no es culpa del proveedor de la red sino de la ubicación de los equipos de red por lo que es importante identificar qué dispositivos que puedan causar interferencias al estar cerca de ellos, tales como:

- Radios.
- Monitores para bebés.
- Cámaras.
- Cables de alimentación.
- Microondas.
- Fuentes eléctricas como líneas de alimentación.
- Televisores.
- Otros dispositivos wifi como routers o teléfonos.
- Altavoces.

Pero no solo estos dispositivos pueden interferir con nuestra red sino que también podemos presentar interferencias por los materiales de construcción utilizados en el edificio como se puede observar en la tabla 2.5.

Tabla 2.5

Materiales de construcción.

Material	Interferencia	Uso de muestra
Panel de madera	Bajo	Dentro de una pared o puerta delantera
Drywall	Bajo	Paredes internas (cada pared entre el enrutador y el dispositivo inalámbrico degrada más la

		señal)
Yeso	Bajo	Paredes internas (sin malla de cables)
Mueble	Bajo	Buzones o particiones de oficina
Vidrio transparente	Bajo	Ventanas
Vidrio resobado	Medio	Ventanas
Personas	Medio	Áreas de tráfico de alto volumen que tienen un tráfico peatonal considerable
Mosaico	Medio	Paredes
Mármol	Medio	Encimeras
Ladrillos	Medio	Paredes
Bloques de concreto	Media/alta	Construcción de pared externa
Espejos	Alta	Vidrio reflectante o de espejo
Metales	Alta	Particiones metálicas de oficina, puertas, muebles metálicos de oficina
Agua	Alta	lluvias, peceras, aguaderas

Nota: La tabla muestra los diferentes materiales de construcción, el nivel de interferencia que generan y los usos comunes de muestra. Tomado de "Cómo identificar y reducir la interferencia de señal inalámbrica", por Dell, 2023,https://www.dell.com/support/kbdoc/es-mx/000150359/c%C3%B3mo-identificar-y-reducir-la-interferencia-de-se%C3%B1al-inal%C3%A1mbrica.

Debido a esta enorme cantidad de interferencias que existen para nuestra red inalámbrica debemos considerar las siguientes recomendaciones antes de llamar a nuestro proveedor de servicios:

- Colocar el router en un lugar elevado de nuestro domicilio sin ningún tipo de obstrucción alrededor de este.
- Mantener el router alejado de paredes gruesas o electrodomésticos.
- Cambiar el canal de transmisión del router si se nota interferencia de otras redes WiFi cercanas.

- Asegurarnos de tener la última versión del firmware de nuestro router para poder mejorar nuestro rendimiento.
- Ajustar las antenas del router para dirigir la señal donde se necesita.
- Utilizar la banda 5GHz si nuestro router nos lo permite.
- Considerar la opción de utilizar repetidores o extensores de la señal wifi para mejorar su alcance en algunas habitaciones.
- Mantener el dispositivo alejado de hornos de microondas o teléfonos inalámbricos.

3. FUNCIONAMIENTO DE INTERNET

En este capítulo, se explorará el funcionamiento de una conexión a Internet en el hogar, un aspecto crucial en la actualidad debido a que Internet se ha convertido en una herramienta influyente en casi todos los aspectos de la vida diaria. El objetivo es brindar una comprensión profunda del funcionamiento de Internet, desde su estructura física hasta los protocolos y tecnologías que hacen posible su operación.

3.1. IP y dominios

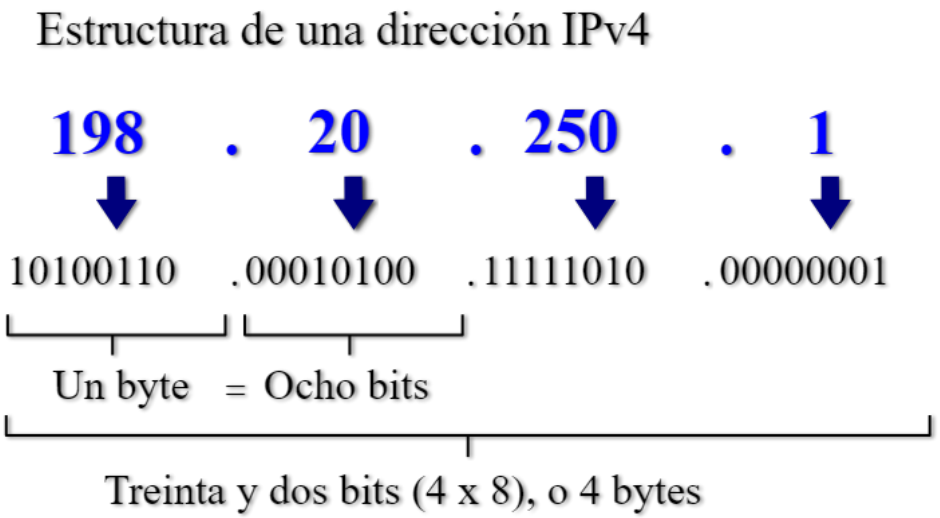
Como lo dice AVG en su página https://www.avg.com/es/signal/what-is-an-ip-address "Una dirección IP (dirección de protocolo de Internet) es una serie de números asignados a cada dispositivo conectado a una red informática o a Internet. Las direcciones IP identifican y diferencian los miles de millones de dispositivos en línea, incluidos los ordenadores y los teléfonos móviles, y ayudan a esos dispositivos a comunicarse entre sí." De esta definición podemos determinar que dispositivos como impresoras, altavoces inteligentes, refrigeradores inteligentes y cámaras de vigilancia cuentan con una dirección IP al poderse conectar a una red por lo que saber el funcionamiento de esta es muy importante.

Las direcciones IP pueden compararse con los números telefónicos: al igual que necesitamos un número para que alguien nos llame, un dispositivo conectado a una red necesita una dirección IP para poder comunicarse. Esta dirección asegura que los datos enviados lleguen al equipo correcto. Así como un número telefónico identifica de manera única un teléfono, una dirección IP identifica de manera única un dispositivo en una red. Es esencial para el enrutamiento efectivo de datos en Internet y otras redes, garantizando que la información llegue a su destino correcto.

Existen 2 tipos de direcciones IP:

- IPv4: Es el estándar de direccionamiento IP predominante que facilita la comunicación entre equipos dentro de redes, ya sean privadas o públicas. Se compone de una secuencia de 32 bits, representada por números decimales del 0 al 255, dispuestos en cuatro grupos separados por puntos. La estructura se puede observar en la figura 3.1.

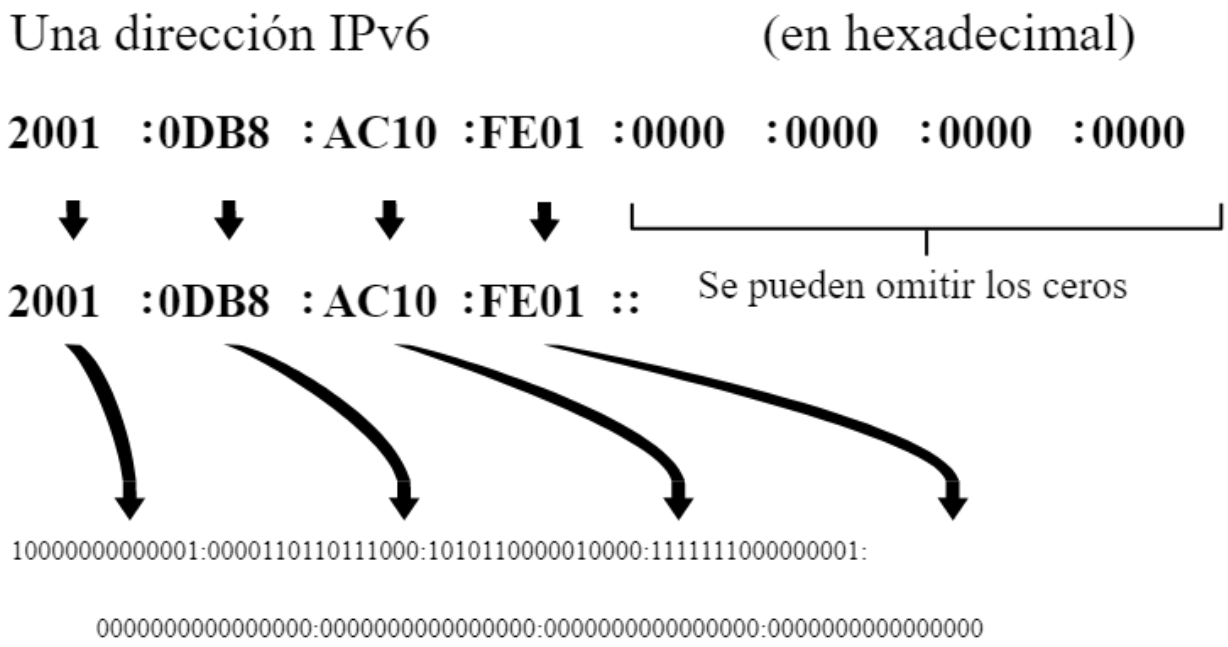
Figura 3.1
Estructura de una dirección IPv4.



Nota: La figura muestra la estructura de una dirección IPv4, desglosando cada octeto en su representación binaria y explicando la equivalencia en bytes y bits. Tomado de "IPv4 e IPv6", por Trustnet, 2023, https://trustnet.com.mx/ipv4-e-ipv6/.

- IPv6: Representa una evolución en el estándar de identificación de computadoras en Internet. Al igual que su predecesor, IPv4, otorga una identificación única a cada dispositivo. Sin embargo, IPv6 ha sido diseñado para hacer frente al creciente número de dispositivos conectados a Internet en la actualidad, ofreciendo un espacio de direcciones considerablemente más amplio y otras mejoras en la gestión y seguridad de la red. La estructura se puede observar en la figura 3.2

Figura 3.2
Estructura de una dirección IPv6.



Nota: La figura muestra la estructura de una dirección IPv6, desglosando cada segmento en su representación hexadecimal y binaria, y explicando la posibilidad de omitir ceros en la notación abreviada. Tomado de "IPv4 e IPv6", por Trustnet, 2023, https://trustnet.com.mx/ipv4-e-ipv6/.

El protocolo IPv4 se agotó en términos de disponibilidad en los registros de la Internet Assigned Numbers Authority (IANA) el 3 de febrero de 2011, cuando IANA asignó los últimos bloques de direcciones IPv4 a los cinco registros regionales de Internet. Desde entonces, se ha estado realizando una transición gradual hacia IPv6 debido al aumento exponencial de dispositivos conectados a redes y a la creciente demanda de servicios en Internet. Es probable que el hogar sea uno de los últimos en llevar a cabo este cambio, ya que requiere una actualización de la infraestructura y de los dispositivos para ser compatible con IPv6. En un futuro cercano, es inevitable que IPv6 se adopte como el estándar principal de direccionamiento IP, debido a su espacio de direcciones sustancialmente más amplio, que garantiza una capacidad suficiente para soportar el crecimiento continuo de la red global.

En IPv4 las direcciones se dividen en clases, que determinan el rango de direcciones disponibles y la cantidad de hosts que pueden haber en una red. Las clases de direcciones IP más comunes son A, B, C, D y E, cada una con características y usos específicos los cuales se pueden observar en la tabla 3.1

Tabla 3.1

Clases de direcciones IPv4.

Clase	Rango de direcciones	Máscara de subred	Número de redes	Número de Host por red
A	1.0.0.0 - 126.255.255.255	255.0.0.0	126 redes	16,777,214
B	128.0.0.0 - 191.255.255.255	255.255.0.0	16,384 redes	65,534
C	192.0.0.0 - 223.255.255.255	255.255.255.0	2,097,152 redes	254
D	224.0.0.0 - 239.255.255.255	No aplica	No aplica	No aplica
E	240.0.0.0 - 255.255.255.255	No aplica	No aplica	No aplica

Nota: La tabla muestra las diferentes clases de direcciones IPv4, incluyendo el rango de direcciones, la máscara de subred, el número de redes y el número de hosts por red. Elaboración propia.

Las direcciones IP se clasifican en diferentes tipos según su uso y alcance, lo que facilita la organización y gestión de las direcciones en redes informáticas. En el subtema de redes públicas y privadas, se analizará con mayor detalle el funcionamiento de estas, como se detalla en la tabla 3.2.

Tabla 3.2

Clasificación de direcciones IPv4.

Tipo de dirección	Rango	Uso
Direcciones Públicas	1.0.0.0 - 126.255.255.255 128.0.0.0 - 191.255.255.255 192.0.0.0 - 223.255.255.255	Utilizadas en Internet y son únicas en todo el mundo.
Direcciones Privadas	10.0.0.0 - 10.255.255.255 172.16.0.0 - 172.31.255.255 192.168.0.0 - 192.168.255.255	Reservadas para redes locales y no se enrutan en Internet.
Direcciones de Loopback	127.0.0.0 - 127.255.255.255	Se utilizan para las comunicaciones internas de

		un dispositivo.
Direcciones de Enlace Local	169.254.0.0 - 169.254.255.255	Se asignan automáticamente cuando no hay un servidor DHCP disponible.
Direcciones de Difusión (Broadcast)	Dirección de red con todos los bits de host establecidos en 1.	Utilizadas para enviar un mensaje a todos los dispositivos en una red.

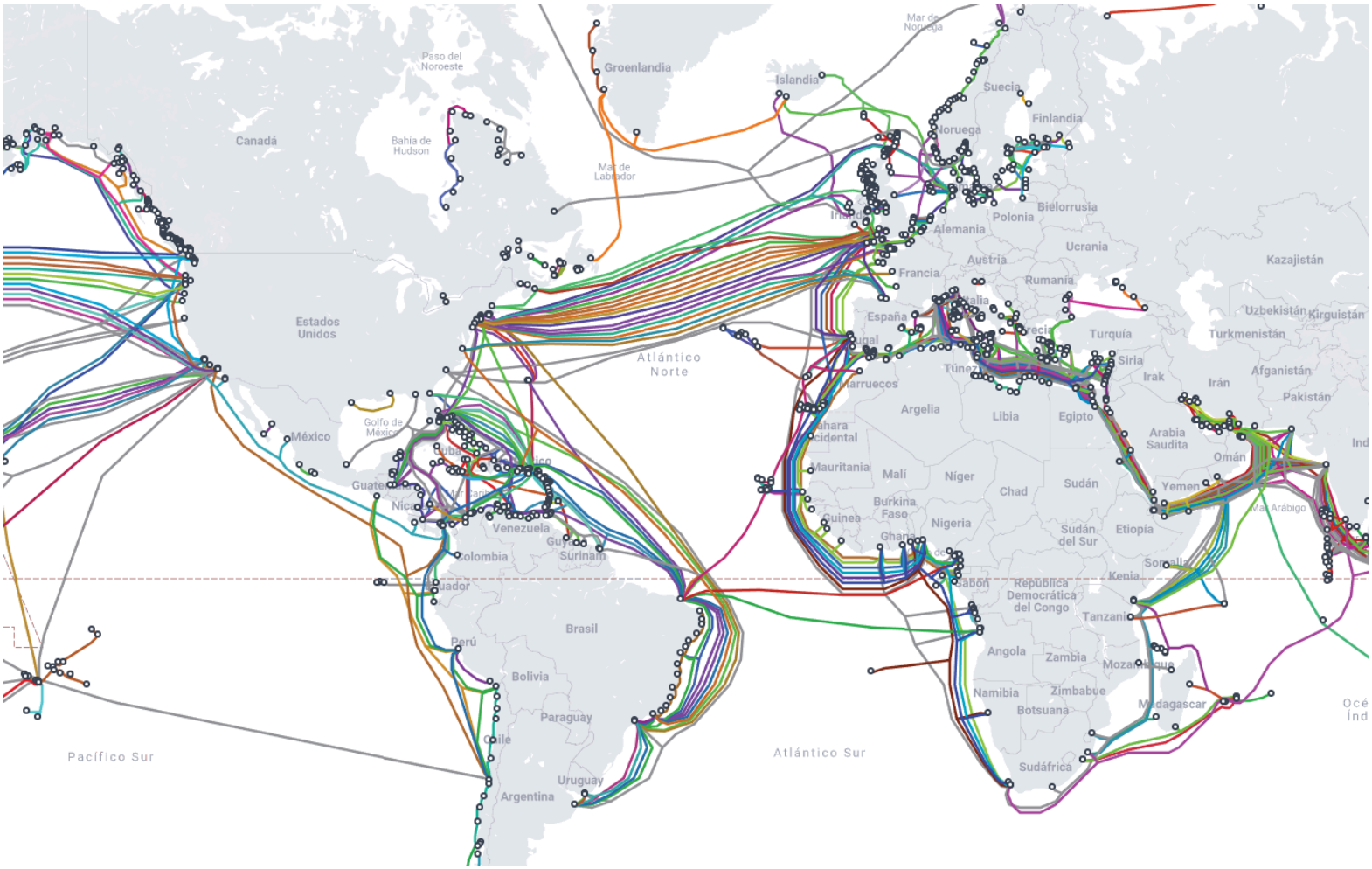
Nota: La tabla muestra la clasificación de las direcciones IPv4, incluyendo el tipo de dirección, el rango de direcciones y el uso correspondiente. Elaboración propia.

Las direcciones internas, por convención, se encuentran en el rango de 192.168.1.0 a 192.168.255.255 y pueden ser utilizadas para configurar los dispositivos de los hogares. Estas direcciones son solo visibles para los dispositivos conectados en la misma red generada por un *Traductor de Direcciones de Internet* (Network Address Translation - NAT en inglés) proporcionado por el módem del proveedor de servicios de internet que tiene un dirección asignada por la empresa que administra el servicio.

La configuración de redes internas con redes externas a otras redes externas se presenta en todo el mundo y por ello es que al Internet se le considera una red de redes interconectadas, lo cual es posible de visualizar en la página Submarine Cable Map de TeleGeography https://www.submarinecablemap.com/ (observe la figura 3.3) donde se pueden consultar todo el cableado físico que conecta a los continentes y por los cuales viajan nuestros datos al salir del país.

Figura 3.3

Mapa de Cableado Submarino.



Nota: La figura muestra un mapa global de los cables submarinos de telecomunicaciones, destacando las rutas y conexiones internacionales. Tomado de "Mapa de Cableado Submarino", por Submarine Cable Map, 2023, https://www.submarinecablemap.com/.

Cada uno de los NAT por los que pasan datos de internet, tienen una dirección IP, que varía según donde se ubique y quien lo administre, por lo que requieren ser registrados y organizados a nivel global. De acuerdo con el sitio IP2LOCATION, en México hay 29,840,896 direcciones IP visibles en todo el mundo correspondientes a diversas dependencias de gobierno, instituciones varias y otros proveedores de servicio que las utilizan para llevar a cabo sus operaciones.

Existen dos métodos principales para asignar direcciones IP a los equipos en una red:

- Asignación estática: En este método, quien administra la red configura manualmente la información de red para cada dispositivo. Esto implica asignar direcciones IP específicas a cada host de manera fija.
- Asignación dinámica: Este método implica la asignación automática de direcciones IP por parte del servicio DHCP (Protocolo de Configuración Dinámica de Host) dentro del router. El DHCP permite la asignación automática de información como la dirección IP, la máscara de subred y otros parámetros de configuración de red a los dispositivos conectados a la red, simplificando así el proceso de administración de la red.

La problemática de las direcciones IP es que consisten en largas secuencias de números, lo que puede resultar poco práctico y difícil de recordar para los usuarios. Para abordar esta complejidad, surgieron los nombres de dominio, una solución más amigable y fácil de recordar. Los dominios son los nombres asociados a las páginas web en Internet, los cuales aparecen en forma de URL o enlaces en la barra de direcciones de nuestros navegadores. Estos nombres resuelven el problema de las complicadas secuencias de direcciones IP, sustituyéndolas por palabras o frases que los usuarios pueden recordar más fácilmente, lo que facilita la navegación y el acceso a los sitios web.

Un dominio está compuesto por dos partes fundamentales y una que no siempre está presente:

- Nombre de dominio: Esta es la parte principal y distintiva del dominio. Es el nombre que elegimos para identificar nuestro sitio web de manera única en Internet. Por ejemplo, en el dominio "Google.com", "Google" es el nombre de dominio. Observe la figura 3.4
- Extensión de dominio: También conocida como dominio de nivel superior (TLD, por sus siglas en inglés), es la parte final del dominio que sigue al nombre de dominio. La extensión de dominio proporciona información adicional sobre la naturaleza, propósito o ubicación del sitio web. Por ejemplo, en "Google.com", ".com" es la extensión de dominio. Observe la tabla 3.3 para más ejemplos.
- Código del país : Es una abreviatura asignada por la normativa internacional para identificar a qué país pertenece un dominio y no siempre puede estar presente. Por ejemplo “.mx” para México, “.us” para Estados Unidos o “.jp” para Japón. Observe la tabla 3.4 para más ejemplos.

Figura 3.4
Estructura de un dominio.

***Nota:** La figura muestra la estructura de un dominio de Internet, desglosando los componentes de dominio, extensión y código del país. Tomado de "¿Qué es un dominio en Internet?", por Hostgator, 2023, https://www.hostgator.mx/blog/que-es-un-dominio-en-internet/.*

Tabla 3.3
Extensiones de dominio.

Tipos de dominio	Uso
.com	Empresas
.org	Organizaciones sin fines de lucro
.net	Empresas relacionadas con redes
.edu	Instituciones educativas
.gov	Entidades gubernamentales
.mil	Entidades militares
.io	Territorios británicos en el océano Índico
.info	Sitios informativos
.biz	Sitios comerciales
.mobi	Sitios optimizados para dispositivos móviles
.travel	Sitios relacionados con viajes
.name	Sitios personales
.coop	Cooperativas

.int	Organizaciones internacionales
.pro	Profesionales
.cat	Comunidad catalana
.tv	Sitios relacionados con televisión

Nota: La tabla muestra las diferentes extensiones de dominio y sus respectivos usos. Elaboración propia.

Tabla 3.4

Código del país.

Código	País	Código	País
.ar	Argentina	.gt	Guatemala
.br	Brasil	.hk	Hong Kong
.ca	Canadá	.jm	Jamaica
.ch	Suiza	.jp	Japón
.cl	Chile	.mx	México
.cn	China	.pa	Panamá
.co	Colombia	.pe	Perú
.de	Alemania	.pr	Puerto Rico
.do	República Dominicana	.uk	Reino Unido
.es	España	.uy	Uruguay
.fr	Francia	.ws	Samoa Occidental
.gr	Grecia	.au	Australia

Nota: La tabla muestra los códigos de país y sus respectivas asignaciones, indicando el código correspondiente a cada país. Elaboración propia.

El DNS (Domain Name System) es fundamental para el funcionamiento de los dominios en Internet. Actúa como un traductor automático, convirtiendo los nombres de dominio que los usuarios y usuarias ingresan en sus navegadores en direcciones IP correspondientes, sin que necesiten saber los detalles técnicos de este proceso. Esta operación se realiza mediante una red de servidores DNS distribuidos globalmente. Estos servidores trabajan para traducir el nombre de dominio a la dirección IP correspondiente. Una vez completada

esta traducción, la resolución se envía al servidor DNS de nuestro proveedor de servicios, permitiendo que los recursos de la página web sean finalmente cargados en nuestro dispositivo, lo que nos permite visualizar la página deseada.

3.2. Redes públicas y privadas

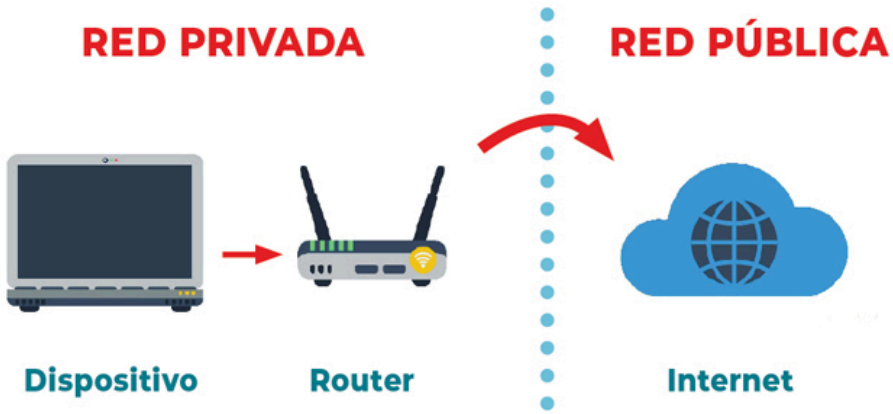
Dentro de las redes domésticas, un aspecto crucial es determinar si la red es pública o privada, lo cual se define según quiénes tengan acceso a ella. La profesora Ma. Jaquelina López Barrientos proporcionó la siguiente definición de estos tipos de redes:

- Pública: El tipo de red pública es aquella a la que cualquier persona tenga acceso siempre y cuando tenga un dispositivo que sea compatible con la red. Un ejemplo puede ser el internet.
- Privada: El tipo de red privada es accesible únicamente por un cierto número de personas seleccionadas dentro de una organización u hogar. Un ejemplo es la red dentro de tu casa sin tomar en cuenta la salida a internet.

Para poder distinguir de una mejor forma la diferencia entre estos 2 tipos de redes se puede observar en la figura 3.5 que la red privada en este caso pertenece a la conexión que existe únicamente entre los dispositivos dentro del hogar debido a que las personas que tienen acceso son limitadas por los propios usuarios de la red, por el contrario la red pública ya se encuentra fuera del hogar, es la conexión que tiene el módem con el proveedor de servicios y a su vez la salida que tiene este último a internet donde los usuarios que posean una conexión pueden acceder a toda la información que se encuentra dentro de esta.

Figura 3.5

Red pública y privada.



***Nota:** La figura ilustra la diferencia entre una red privada y una red pública, mostrando cómo un dispositivo se conecta a Internet a través de un router. Tomado de "Perfiles de red en Windows", por RedUsers, 2023, https://www.redusers.com/noticias/publicaciones/perfiles-de-red-en-windows/.*

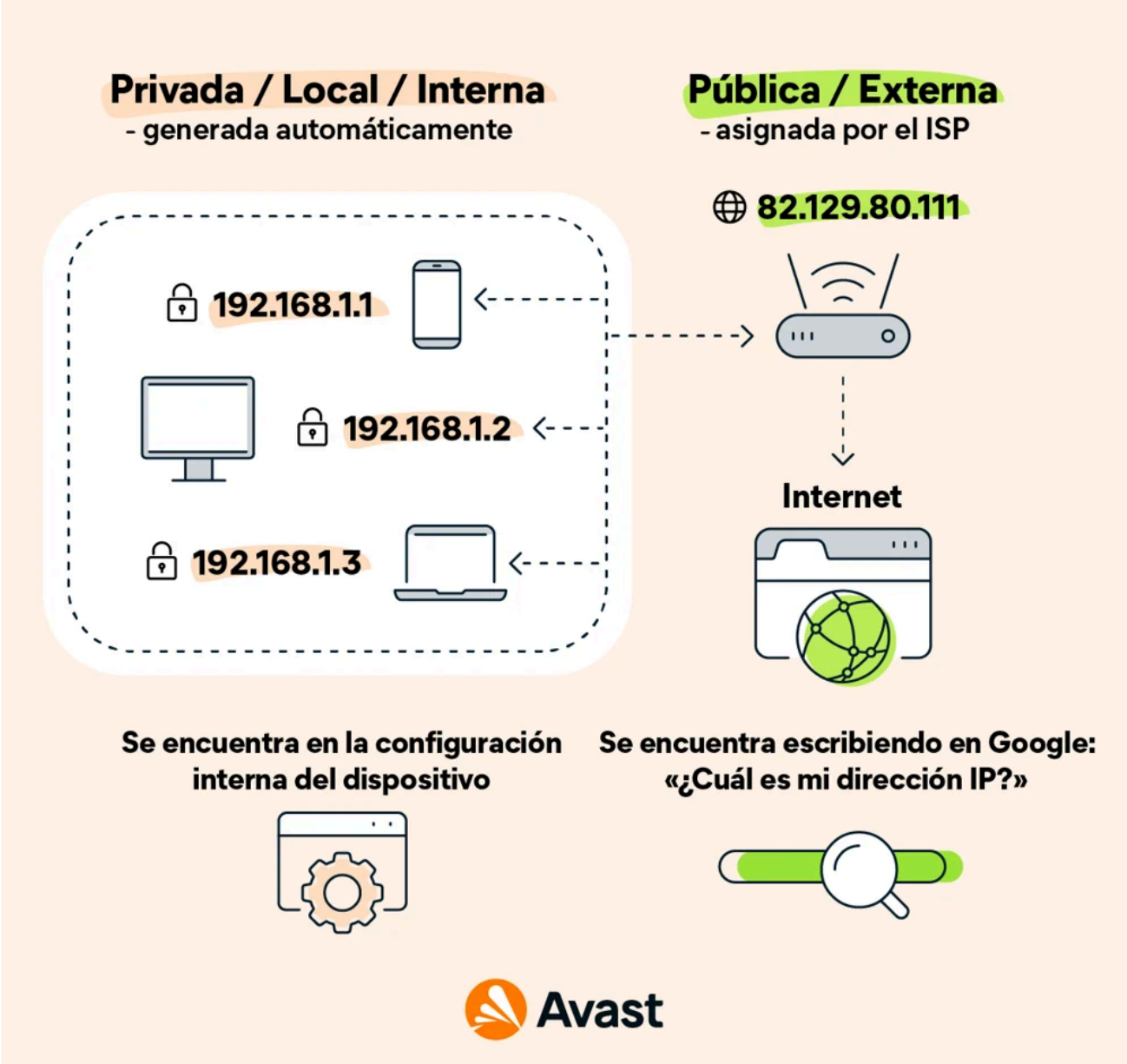
Una característica importante de las redes privadas es que estas permiten el uso de alguna tecnología determinada y no permitir el uso de alguna otra, además permiten discriminar usuarios, protocolos y el tipo de tráfico dentro de la red, configuraciones que las redes públicas, al ser utilizadas por cualquier usuario o usuaria, deben mantener una neutralidad en cuanto a las tecnologías utilizadas.

Además de la clasificación por tipos de direcciones IP que se observa en la tabla 3.2 del subtema “IP y dominios”, es posible determinar si una red es pública o privada según el rango de direcciones que utiliza. Las direcciones IP públicas suelen caer en rangos específicos asignados por la Autoridad de Números Asignados de Internet (IANA, por sus siglas en inglés). Estos rangos incluyen direcciones que van desde 1.0.0.0 hasta 126.255.255.255, 128.0.0.0 hasta 191.255.255.255, y 192.0.0.0 hasta 223.255.255.255. Por otro lado, las redes privadas utilizan rangos reservados que no se enrutan en Internet, como 10.0.0.0 hasta 10.255.255.255, 172.16.0.0 hasta 172.31.255.255, y 192.168.0.0 hasta 192.168.255.255. Estos rangos permiten a los administradores de red distinguir entre redes públicas y privadas, facilitando así la configuración y gestión de la infraestructura de red.

Como se puede ver en la figura 3.6, las direcciones IP privadas/locales/internas se encuentran dentro de los dispositivos en nuestro hogar mientras que las direcciones públicas/externas van desde el punto de conexión del router que se comunica hacia internet a través de la dirección que es proporcionada por el proveedor de servicios.

Figura 3.6

Direcciones IP públicas frente a privadas.



***Nota:** La figura compara las direcciones IP privadas (locales/internas) generadas automáticamente con las direcciones IP públicas (externas) asignadas por el proveedor de servicios de Internet (ISP). Tomado de "Direcciones IP públicas frente a privadas", por Avast, 2023, https://www.avast.com/es-es/c-ip-address-public-vs-private.*

3.3. Servidores y conexión global

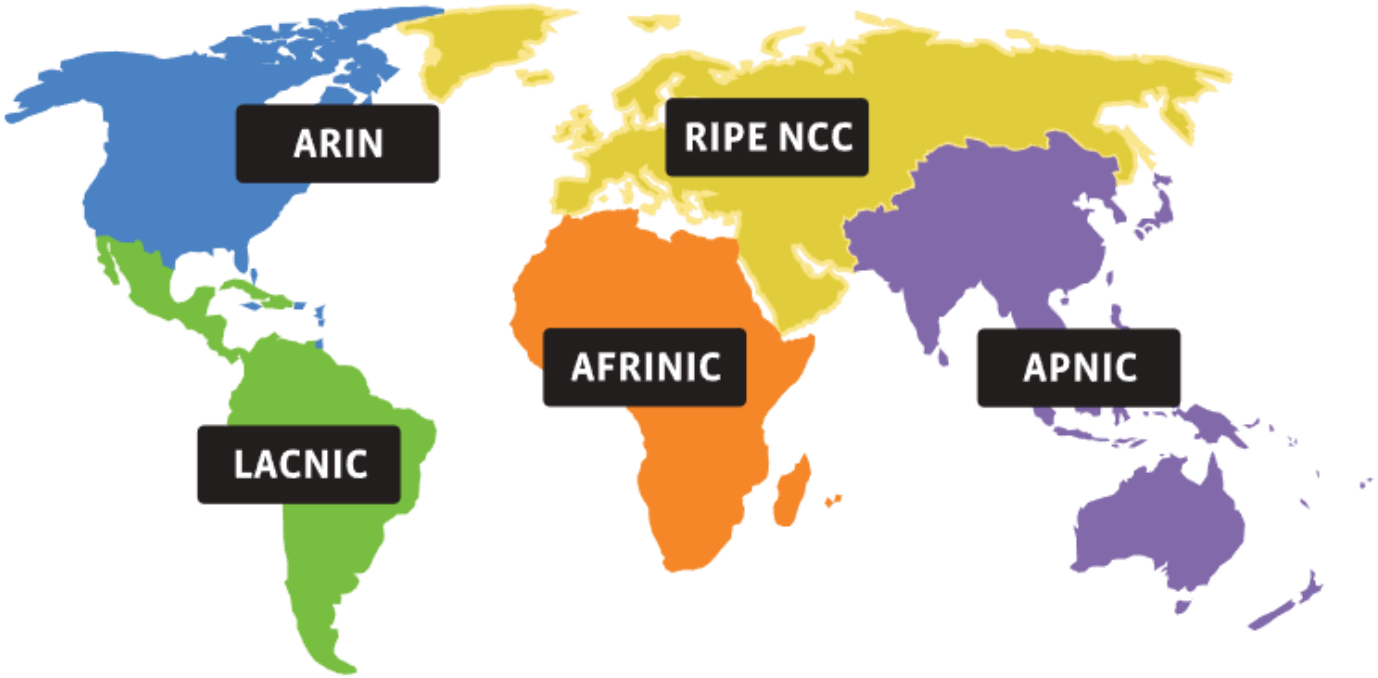
La Autoridad de Números Asignados de Internet - IANA - es la encargada de administrar las direcciones IP a través del mundo, para ello divide al mundo en cinco áreas a las que les asigna un organismo encargado de registrar a los dispositivos de red, específicamente, a

aquellas instituciones, organizaciones, entidades y empresas que brindan un servicio mediante internet. Estas organizaciones son:

- AFRINIC: Región Africana
- APINIC: Región Asia/Pacífico
- ARIN: Canadá, Estados Unidos de América y algunas islas del Caribe
- LACNIC: América Latina y algunas islas del Caribe
- RIPE NCC: Europa, Oriente Medio y Asia Central

Y el área que administran se observa en la figura 3.7.

Figura 3.7
Registro de Internet Regional.



***Nota:** La figura muestra los registros de Internet regionales que administran la asignación de recursos de numeración de Internet, incluyendo direcciones IP y números de sistemas autónomos, y sus respectivas áreas de cobertura en el mundo. Tomado de "Números", por IANA, 2023, https://www.iana.org/numbers.*

Dentro de los registros de cada organismo, se encuentra la información necesaria para interconectar todas las áreas, así como la ruta que deben seguir los paquetes que se envían por internet para alcanzar su destino, comúnmente un servidor físico alojado en algún área, y regresar hasta el dispositivo de red que envió su solicitud y/o paquetes atravesando distintos NAT y DNS en el proceso.

Al navegar por internet se utilizan los nombres de dominio que identifican las páginas visitadas, pero estos nombres son difíciles de recordar además de cambiar dinámicamente según las operaciones que realicen las páginas de internet, por ello se utilizan los *buscadores*, que son servidores que recopilan información de todo el internet para filtrarlos en las búsquedas de los usuarios, de acuerdo a una diversa cantidad de parámetros y configuraciones. A través del uso de Localizadores de Recursos Uniforme (o URL por sus siglas en inglés), los navegadores pueden acceder a los recursos de las páginas web, como configuración de texto, bases de datos, recursos gráficos y todo lo que necesite la página para funcionar y realizar las operaciones que requiera el usuario sin la necesidad de ingresar las direcciones web de las páginas que se visitan.

3.4. Conexiones móviles

La telefonía móvil, también conocida como conexiones móviles, es un servicio que permite a los usuarios acceder a la red de Internet de forma inalámbrica. Además de realizar y recibir llamadas telefónicas, los usuarios y usuarias pueden navegar por Internet, enviar mensajes de texto y utilizar diversas aplicaciones y servicios en sus dispositivos móviles.

Para habilitar la conexión de dispositivos móviles, los proveedores de servicios instalan antenas de telefonía móvil (observe la figura 3.8) en áreas donde desean ofrecer cobertura. Estas antenas suelen colocarse en lugares altos, como torres, edificios altos o estructuras especiales diseñadas para este propósito, con el fin de proporcionar una mejor señal y cobertura. Las torres de telefonía móvil suelen tener una altura que varía entre 30 y 200 metros, dependiendo de varios factores como la densidad poblacional, el terreno y las regulaciones locales. Estas torres están equipadas con antenas direccionales que emiten señales de radio en diferentes direcciones para cubrir un área específica. Las antenas también pueden tener equipos adicionales, como amplificadores de potencia y equipos de transmisión, para garantizar una cobertura efectiva y una calidad de señal óptima. Las características específicas de las torres, como la altura exacta y la ubicación, suelen ser determinadas por los proveedores de servicios en función de sus necesidades operativas y las regulaciones locales.

Estas antenas tienen la función principal de recibir las señales de radiofrecuencia de los dispositivos móviles, procesarlas y enviarlas a través de la red móvil utilizando enlaces de cable o fibra óptica. Finalmente, transmiten la respuesta de vuelta al dispositivo móvil. Durante este proceso las antenas también se encargan de gestionar toda la información que se está recibiendo para poder mantener una conexión estable y de esa forma optimizar la calidad de comunicación para todos los usuarios.

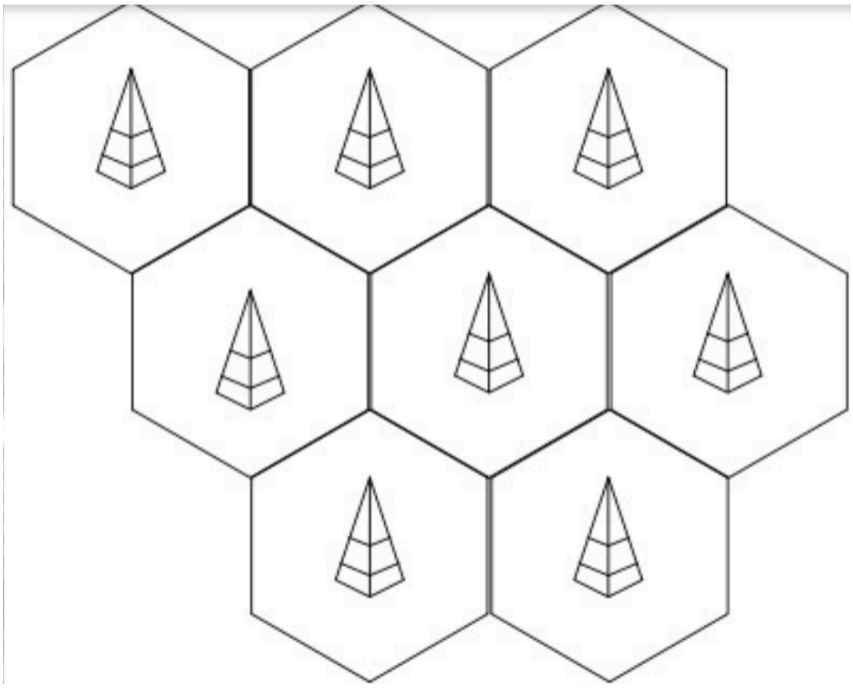
Figura 3.8

Antenas de telefonía móvil.

Nota: La figura muestra una variedad de antenas de telefonía móvil utilizadas para la transmisión de señales de comunicación. Tomado de "Aprobarán NOM de antenas de telefonía", por IDET, 2023, https://www.idet.org.mx/noticias/aprobaran-nom-antenas-telefonia/.

Estas antenas funcionan mediante celdas, cada una ajustada a un rango específico de frecuencias y distribuida a través de múltiples celdas (observe la figura 3.9) físicamente separadas mediante conmutadores y multiplexores. Esta separación permite reutilizar las frecuencias entre celdas adyacentes, optimizando el uso del espectro, pero requiere la instalación de miles de estaciones base. Para garantizar una transición fluida al moverse, se realiza un cambio de frecuencia de radio en cada celda, en un proceso conocido como hand-off hand-over, que debe ser imperceptible para el usuario.

Figura 3.9
Antenas de telefonía móvil.



Nota: La figura muestra un diagrama de la disposición de antenas de telefonía móvil en una configuración de celdas hexagonales, que es común en las redes celulares para maximizar la cobertura y la capacidad. Tomado de "Aprobarán NOM de antenas de telefonía", por IDET, 2023, https://www.idet.org.mx/noticias/aprobaran-nom-antenas-telefonia/.

Actualmente en México, existen dos modalidades para obtener el servicio de telefonía móvil: prepago y pospago. En el caso del prepago, los usuarios recargan saldo en sus cuentas para utilizar el servicio y lo hacen de manera flexible, según sus necesidades de comunicación. En cambio, en el pospago, los usuarios pagan una cantidad fija cada cierto tiempo, generalmente de manera mensual, por una cantidad predeterminada de datos y horas de telefonía.

Las conexiones móviles han experimentado una evolución significativa a lo largo del tiempo, con la introducción de cinco generaciones distintas hasta la fecha. Cada generación ha supuesto una mejora notable con respecto a la anterior, ofreciendo nuevas capacidades y funcionalidades. Sus principales características de cada una de estas generaciones son:

- Primera generación 1G: Utilizaba transmisión analógica y sólo admitía servicios de voz, con capacidad limitada para usuarios simultáneos.

- Segunda generación 2G y 2.5G: Utilizaba transmisión digital, ofreciendo mayor capacidad para usuarios simultáneos, mejor calidad de comunicación, mayor seguridad y velocidades de 9.6 a 65 Kbps.
- Tercera generación 3G: Ofrecía mayor ancho de banda en comparación con las generaciones anteriores, mayor eficiencia y velocidades superiores a 144 Kbps.
- Cuarta generación 4G: Proporcionó mejoras significativas en términos de velocidad, capacidad y calidad de la conexión, permitiendo velocidades de datos más altas que las generaciones anteriores.
- Quinta generación 5G: Es el estándar más reciente y está siendo impulsado por el 3GPP (3rd Generation Partnership Project). Ofrece baja latencia (4 ms), está diseñado para el Internet de las cosas (IoT) y alcanza velocidades de hasta 20 Gbps. Continúa en desarrollo para mejorar aún más sus capacidades.

Cada una de estas generaciones tuvo su propio estándar de identificación en los dispositivos móviles. Algunos de los identificadores más reconocidos son:

- G/GPRS
- E
- 1X
- 3G
- H
- H+
- 4G/LTE
- 4G+/LTE+
- VoLTE
- 5G

- GPRS
- EDGE
- CDMA 2000 1x
- UMTS/EV-DO
- HSPA
- HSPA+
- LTE
- LTE Advanced
- Voice over LTE
- 5G/5GUWB/5G UW

Dependiendo del dispositivo, los identificadores pueden aparecer de diversas formas. Algunos ejemplos de dónde podemos encontrarlos se muestran en la figura 3.10.

Figura 3.10

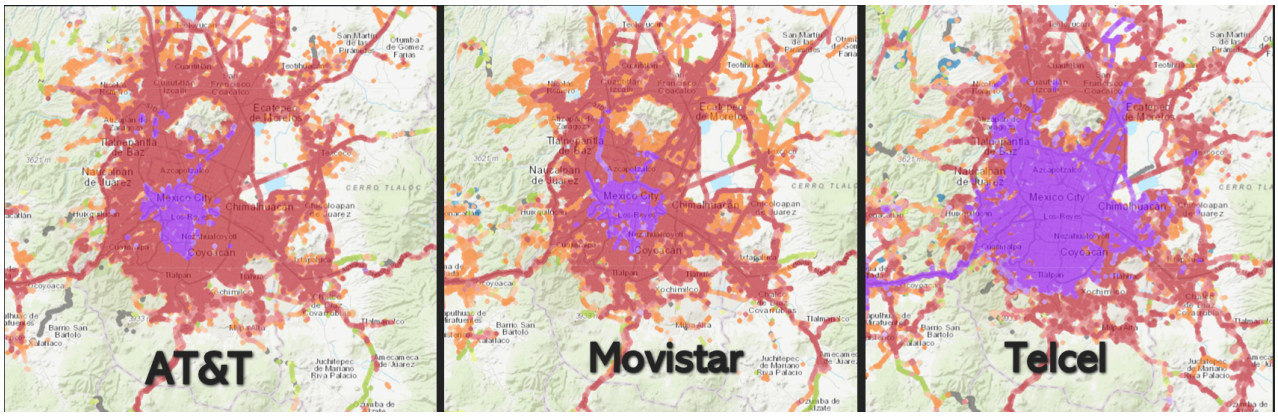
Identificación red móvil.

Nota: La figura muestra la identificación de diferentes tipos de redes móviles (4G, LTE, 5G) en la pantalla de un dispositivo móvil, destacando los iconos y etiquetas utilizadas para indicar la conexión de red. Elaboración propia.

La infraestructura de redes móviles en México ha sido construida principalmente por tres empresas líderes: Telcel, Movistar y AT&T. Estas empresas han desplegado redes 4G y 5G que ofrecen una cobertura casi total en la ciudad de México y a lo largo del país, como se puede observar en la figura 3.11 y la figura 3.12 respectivamente :

Figura 3.11

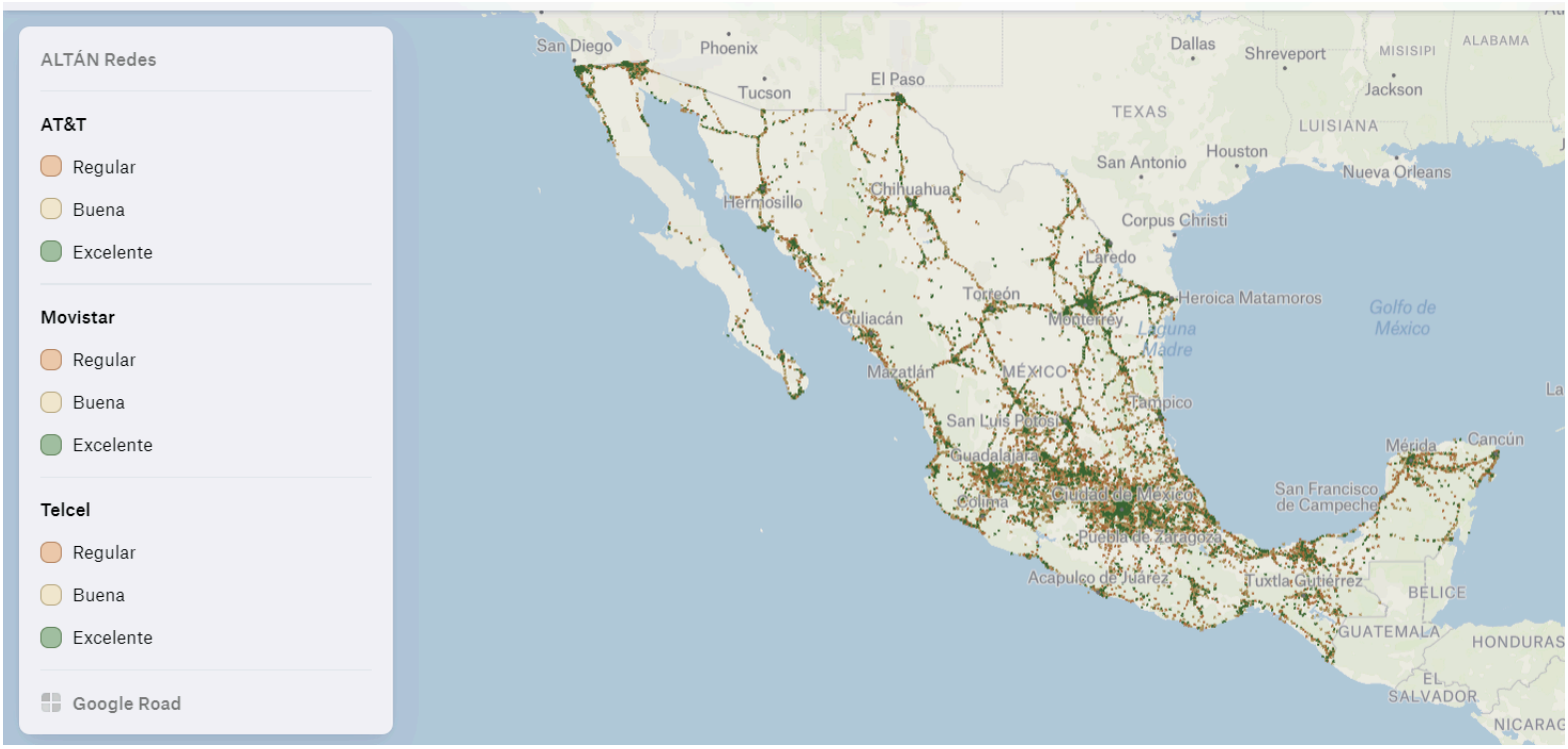
Cobertura móvil en la Ciudad de México.



Nota: La figura muestra la cobertura móvil de los operadores AT&T, Movistar y Telcel en la Ciudad de México, destacando las áreas de cobertura en diferentes colores. Tomado de "Mapa interactivo de cobertura 4G", por Felt, 2023, https://felt.com/map/Mapa-interactivo-de-cobertura-4G-RCLj9C9CutSVmct11kT4tnjC?loc=22.38,-102.2,5z.

Figura 3.12

Cobertura móvil en México.



***Nota:** La figura muestra la cobertura móvil de los operadores AT&T, Movistar y Telcel en México, destacando las áreas de cobertura con diferentes niveles de calidad (regular, buena, excelente) en un mapa del país. Tomado de "Mapa interactivo de cobertura 4G", por Felt, 2023, https://felt.com/map/Mapa-interactivo-de-cobertura-4G-RCLj9C9CutSVmct11kT4tnjC?loc=22.38,-102.2,5z.*

3.5. Velocidad y banda ancha

La calidad de la comunicación en una red no solo depende del área de cobertura y la ubicación de los dispositivos, sino también de la amplitud de banda ancha disponible. La banda ancha permite a los usuarios acceder a información en internet mediante diversas tecnologías de transmisión. Los datos, como imágenes, audios, videos e información, se transmiten en forma de bits a través de la red, y la calidad de esta transmisión depende en gran medida de la velocidad de subida/bajada que ofrece la banda ancha en los hogares.

La velocidad que se necesite dentro del hogar depende tanto de las necesidades que se tienen así como el número de usuarios que van hacer uso de esta simultáneamente, por ello en la tabla 3.5 se puede observar cuánto ancho de banda se necesitará para las actividades más comunes que realizan los usuarios.

Tabla 3.5

Ejemplos de ancho de banda según actividad.

Actividad en línea	Ancho de banda necesario para 1-2 usuarios (unidades en Mbps)	Ancho de banda necesario para 3-4 usuarios (unidades en Mbps)
Streaming de música	1	2
Navegación web general, email, redes sociales	1.5	3
Video chat personal HD (Skype, FaceTime, Zoom, etc.)	3	6
Transmisión de videos en SD (definición estándar)	4	8
Juegos en línea (multijugador)	4	8
Transmisión de videos en HD (alta definición)	5-8	10-16
Videoconferencia en HD	6	12
Descarga de archivos grandes	10	20
Transmisión de videos en ultra HD 4K	25	45
Trabajo/educación a distancia	25	45

Nota: La tabla muestra ejemplos de ancho de banda necesario según la actividad en línea, para distintos números de usuarios. Tomado de "¿Qué velocidad de Internet necesito?", por CenturyLink, 2023, https://espanol.centurylink.com/home/help/internet/what-internet-speed-do-i-need.html.

Las siguientes son opciones de tecnologías para servicios de banda ancha:

- Línea Digital de Suscriptor (Digital Subscriber Line, conocida como DSL en inglés): Esta tecnología ofrece la posibilidad de acceder a Internet a través de las infraestructuras telefónicas existentes, lo que permite una conectividad rápida y eficiente, incluso en áreas donde otros medios de conexión pueden no estar disponibles. En función de la velocidad requerida, existen tres variantes principales de tecnología DSL:

    - Línea de Suscriptor Digital Asimétrica (ADSL): Esta tecnología, como su nombre sugiere, ofrece velocidades de descarga más rápidas que las de carga, lo que la hace ideal para actividades como navegación web.
    - Línea de Suscriptor Digital Síncrona (SDSL): En contraste con el ADSL, esta tecnología es simétrica, lo que significa que proporciona las mismas velocidades tanto en descarga como en carga. Es especialmente útil para aplicaciones que requieren una alta capacidad de carga.
    - Línea de Suscriptor Digital de Muy Alta Velocidad (VDSL): Similar al ADSL pero con una capacidad de transferencia de datos considerablemente mayor, el VDSL ofrece un rendimiento mejorado en comparación con las tecnologías más antiguas, aunque no alcanza las velocidades ofrecidas por las tecnologías más recientes.
- Fibra óptica: Como dice la CITEL (Comisión Interamericana de Telecomunicaciones) “La fibra óptica es una guía de onda en forma de hilo de material altamente transparente diseñado para transmitir información a grandes distancias utilizando señales ópticas.”
- Inalámbrica: Ampliamente conocida como Wi-Fi, esta tecnología brinda la capacidad de conectar los dispositivos a Internet en el hogar sin depender de cables físicos, gracias al uso de señales de radio electromagnéticas.
- Satélite: Se refiere a una conexión bidireccional a Internet, establecida a través de satélites en órbita terrestre. Este método es especialmente útil en áreas remotas o de difícil acceso donde la instalación de medios terrestres, como cables o fibra óptica, resulta poco práctica o imposible.

La selección de la tecnología de banda ancha dependerá de diversos factores, tales como la modalidad de acceso a Internet de banda ancha (que en ocasiones se combina con otros servicios como telefonía de voz y entretenimiento en el hogar), así como el costo y la disponibilidad del servicio.

4. SEGURIDAD

En el ámbito de la conectividad digital, la seguridad de las redes desempeña un papel fundamental en la protección y preservación de la información sensible y privada que circula a través de Internet. En este capítulo, se verá la importancia de implementar medidas de seguridad robustas en las redes, las cuales tienen el objetivo primordial de salvaguardar la integridad y confidencialidad de los datos manejados por las y los usuarios en el vasto y dinámico entorno virtual particularmente en las redes domésticas. Además de explorar los diversos organismos encargados de otorgar estándares de calidad a las empresas, es importante profundizar en la importancia y el impacto que estos estándares tienen en el desempeño y la reputación de las organizaciones con las y los usuarios.

4.1. Triunvirato de la Seguridad

La seguridad es mucho más que un simple conjunto de protecciones. Se trata de un conjunto de medidas diseñadas para brindar confianza y resguardar los activos más valiosos, sean datos, sistemas o infraestructuras, con el fin de preservar su integridad, disponibilidad y confidencialidad en todo momento (observe la figura 4.1). Esta perspectiva se debe a que la seguridad siempre debe considerar la protección del bien, el entorno y a quienes la manipulan.

Figura 4.1
Triada de la seguridad.

Nota: La figura muestra la triada de la seguridad de la información, que incluye la confidencialidad, integridad y disponibilidad. Tomado de "Seguridad de la información: historia, terminología y campo", por DesdeLinux, 2023, https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/.

En el entorno actual, la seguridad es un aspecto que se encuentra presente en cualquier contexto:

- Social
- Económico
- Cultural
- Nacional
- Internacional
- Educativo

Es esencial que las medidas de seguridad proporcionen una protección integral y generen confianza tanto para las y los usuarios individuales como para las organizaciones, que dependen cada vez más de la tecnología para llevar a cabo sus actividades diarias. La

seguridad, por sí sola, abarca un enfoque completo para proteger todos los activos que son valiosos y deben ser protegidos. Por tanto, es fundamental definir qué se entiende por "seguridad de la información".

La seguridad de la información engloba un conjunto de medidas diseñadas para brindar confianza y salvaguardar la integridad, disponibilidad y confidencialidad de la información, ya sea en su forma física o digital. Partiendo de esta premisa, se puede decir que la seguridad informática, es la que se encarga de proteger específicamente la información en forma digital, asegurando su integridad, disponibilidad y confidencialidad en todo momento. Es este tipo de seguridad la que concierne directamente a las y los usuarios al gestionar y proteger la red de datos del hogar.

Antes de iniciar la implementación de medidas de seguridad, es fundamental plantear las siguientes preguntas y responderlas en ese orden :

1. ¿Qué quiero proteger?
2. ¿De qué los quiero proteger?
3. ¿Cómo los quiero proteger?

Para responder la primera pregunta “¿Qué quiero proteger?” , dentro del ámbito de la seguridad, se considera a la información como un bien o activo, que constituye todo aquello de valor para una persona, entidad o grupo. Esta puede ser clasificada en:

- Bienes tangibles: Engloban todos aquellos activos que son físicamente tangibles y visibles, tales como: automóviles, vivienda, teléfonos, equipos de cómputo, entre otros.
- Bienes intangibles: Comprende aquellos activos que no tienen una forma física pero poseen un alto valor y requieren protección, como la reputación, la identidad personal, datos personales, recursos financieros, accesos a diversas aplicaciones, contactos, entre otros aspectos.

El principio de profundidad, también conocido como defensa en profundidad, es una estrategia de seguridad que implica la implementación de múltiples capas de defensa para proteger los bienes y activos de una organización. Este enfoque reconoce que no existe una solución de seguridad única que pueda ofrecer protección total contra todas las amenazas posibles. En lugar de ello, se utilizan varias medidas de seguridad que trabajan juntas para crear una barrera más robusta y resistente.

Las diferentes capas pueden incluir firewalls, sistemas de detección de intrusos, antivirus, controles de acceso, cifrado de datos y políticas de seguridad, entre otras. Cada capa tiene su propia función específica y fortalezas, lo que permite abordar diferentes tipos de amenazas de manera efectiva. Si una capa de defensa es superada o comprometida, otras

capas siguen proporcionando protección. Esto reduce la probabilidad de una brecha de seguridad catastrófica, ya que no se depende de una sola línea de defensa.

Cada capa debe tener un responsable que conozca ampliamente al bien e identifique las medidas que mejor se adapten a la situación específica del bien, sin obstruir en su funcionamiento y/o propósito, tomando en cuenta el valor que se le atribuye, ya sea en términos económicos, de tiempo, esfuerzo o valor sentimental. Para comprender las necesidades de seguridad, es fundamental considerar los servicios de seguridad, los cuales mejoran la protección de un bien y su flujo dentro de una organización. Estos servicios se observan en la tabla 4.1 :

Tabla 4.1

Servicios de seguridad.

Servicio	Descripción
Control de acceso	Solo las personas, sistemas o procesos autorizados pueden acceder a la información.
Autenticación	Se refiere a la acción de "verificar" la identidad de una persona, sistema o proceso, y confirmar que en efecto es quien afirma ser.
Confidencialidad	Cualidad de la información que impide su divulgación a personas, sistemas o procesos no autorizados. Esencialmente, se trata de la propiedad que garantiza que dicha información solo sea accesible con la autorización adecuada y debidamente verificada.
Integridad	Cualidad de la información de no haber sido modificada, manteniendo sus datos exactamente como fueron generados, sin manipulaciones ni alteraciones por parte de terceros. La integridad se ve comprometida si la información es modificada o si una parte de ella es eliminada.
No repudio	Previene la negación de envío o recepción, así como la modificación o manipulación de información.
Disponibilidad	Capacidad de garantizar que tanto el sistema como los datos estarán accesibles en todo momento para las personas, sistemas o procesos que los requieran, y tan frecuentemente como sea necesario.

Nota: La tabla describe varios servicios de seguridad, incluyendo control de acceso, autenticación, confidencialidad, integridad, no repudio y disponibilidad, junto con sus respectivas descripciones. Elaboración propia.

Para los bienes, existen riesgos que representan la posibilidad de sufrir algún tipo de daño o pérdida. Por ello, es importante mencionar qué tipos de pérdidas se pueden presentar:

- Pérdidas nulas: Son tan insignificantes que apenas tienen impacto, siendo casi como si no hubiera ocurrido ningún incidente.
- Pérdidas parciales: Son aquellas problemáticas de las que la recuperación es posible de alguna manera.
- Pérdidas notables: Son aquellas que afectan al bien de tal manera que se requiere una inversión significativa para recuperarlo.
- Pérdidas totales: Se refieren a situaciones donde no hay forma de recuperar el bien, o si existe alguna posibilidad, no será en las mismas condiciones en las que se encontraba previamente.

Para responder a la segunda pregunta "¿De qué los quiero proteger?", es crucial abordar el tema de las amenazas, las cuales pueden ser cualquier actividad, evento, circunstancia o fenómeno que intenta o pretende causar algún daño a la información o cualquier bien. En este sentido, es primordial identificar y examinar qué tipos de amenazas pueden afectar al bien, estimar la frecuencia con la que estas amenazas podrían presentarse y, finalmente, determinar cuál sería la pérdida si dichas amenazas se materializaran.

Existen cinco tipos principales de amenazas que pueden afectar la seguridad de los bienes y se pueden ver en la tabla 4.2:

Tabla 4.2

Tipos de amenazas.

Amenaza	Descripción
Factor humano	Esta amenaza proviene de acciones inadvertidas o malintencionadas por parte de personas dentro de una organización. Esto puede incluir errores humanos, descuidos, falta de conciencia de seguridad, o acciones intencionales com o el robo de información o la divulgación no autorizada.
Factor de hardware	Se refiere a las amenazas relacionadas con los componentes físicos de los sistemas informáticos, como equipos de cómputo, dispositivos de almacenamiento, servidores y dispositivos de red. Estas amenazas pueden incluir fallos de hardware, pérdida o robo de dispositivos, o compromisos de la integridad física de los equipos.

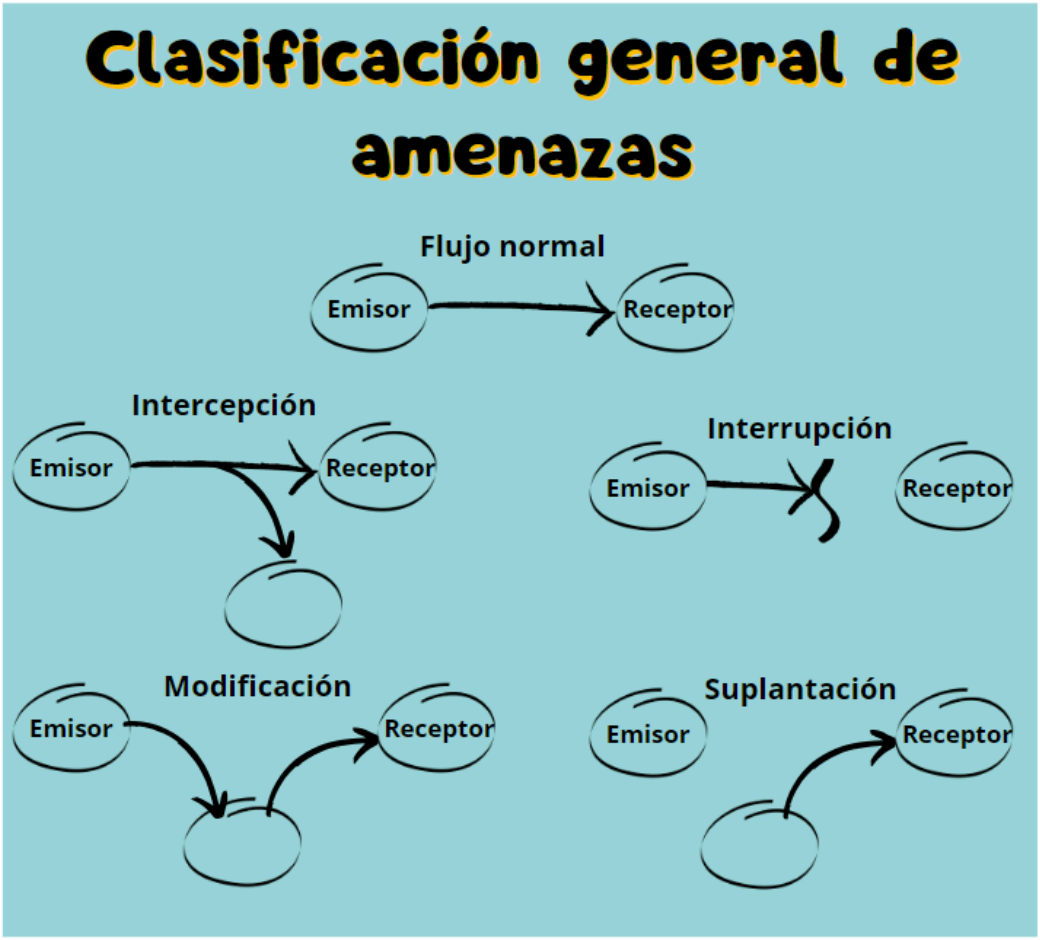
Fallas de software	Este tipo de amenaza se origina en vulnerabilidades o defectos en el software utilizado en los sistemas informáticos. Estas vulnerabilidades pueden ser explotadas por atacantes para comprometer la seguridad de los sistemas, lo que puede llevar a la ejecución de código malicioso, robo de información o interrupción del funcionamiento normal de los sistemas.
Problemas en la Red	Las amenazas de red se refieren a los riesgos asociados con la comunicación de datos a través de redes informáticas, como Internet o redes locales. Esto puede incluir ataques de intercepción de datos, ataques de denegación de servicio (DDoS), intrusiones en la red, y el robo de información transmitida a través de la red.
Desastres naturales	Estas amenazas son eventos catastróficos de origen natural, como terremotos, inundaciones, incendios forestales o tormentas, que pueden causar daños físicos a los sistemas informáticos y la infraestructura de tecnología de la información, así como la pérdida de datos o interrupción de servicios.

Nota: La tabla describe diferentes tipos de amenazas, incluyendo factor humano, factor de hardware, fallas de software, problemas en la red y desastres naturales, junto con sus respectivas descripciones. Elaboración propia.

Adicionalmente, las amenazas pueden observarse a través de la clasificación general que se muestra en la figura 4.2:

Figura 4.2

Clasificación general de amenazas.



Nota: La figura ilustra la clasificación general de amenazas en el flujo de comunicación, incluyendo la intercepción, interrupción, modificación y suplantación, además del flujo normal entre emisor y receptor. Elaboración propia.

- Intercepción: Ocurre cuando un agente externo, ajeno al receptor, captura la información transmitida a través de la red, comprometiendo la confidencialidad de los datos.
- Interrupción: Se produce cuando el mensaje enviado no alcanza al receptor debido a diversas circunstancias, lo que afecta la disponibilidad de la comunicación.
- Modificación: Consiste en que un agente externo intercepta el archivo antes de que llegue al receptor, lo modifica y luego lo reenvía, poniendo en riesgo la integridad de la información.
- Suplantación: Implica que un agente externo se hace pasar por el emisor legítimo, enviando información al receptor en nombre de otro, comprometiendo así la autenticación del remitente.

Sin embargo, esta no es la única manera de clasificar las amenazas. También es posible categorizarlas según el objetivo de la amenaza o según la ubicación del bien o activo en riesgo.

- Objetivo de la amenaza:
    - Intencionada: Estas amenazas son llevadas a cabo por usuarios con la intención expresa de causar daño al bien desde su origen. Pueden ser provocadas por personas que abusan de su autoridad o por usuarios no autorizados que acceden indebidamente a la información.
    - No intencionada: Este tipo de amenazas suele ser resultado de descuidos o falta de conocimiento por parte de los usuarios, sin tener la intención de dañar el bien. Suelen ser más comunes dentro de una organización y pueden pasar desapercibidas.
- Ubicación:
    - Internas: Estas amenazas se originan dentro del entorno físico donde se encuentra el activo en cuestión. Son causadas por desinformación y descuidos de los propietarios del bien, así como de omisiones en las medidas de seguridad debido a un análisis poco extensivo. Los agentes externos de amenaza pueden volverse internos si logran ingresar a la ubicación del bien, o cuando obtienen credenciales de acceso al sistema.
    - Externas: Estas amenazas provienen de fuera del entorno físico donde se encuentra el bien en cuestión. Incluyen cualquier actividad maliciosa llevada a cabo por individuos o grupos que no tienen acceso autorizado al área protegida. Las amenazas externas suelen ser más fáciles de identificar y prevenir a través de medidas de seguridad perimetral, vigilancia, y sistemas de detección de intrusiones, pero aún representan un riesgo significativo para la seguridad del bien en cuestión.

Finalmente, la pregunta "¿Cómo deseo protegerlos?" Se relaciona con la identificación de las vulnerabilidades que puedan afectar a los bienes donde el nivel de riesgo se determina mediante el análisis de la relación entre las amenazas y las vulnerabilidades. Una vulnerabilidad se define como una debilidad en los procedimientos de seguridad, diseño, implementación o control interno que podría ser explotada de manera intencionada o no intencionada, resultando en una brecha de seguridad o una violación de la política de seguridad de los sistemas.

A diferencia de las amenazas que cuentan con 5 tipos , las vulnerabilidades se componen de seis aspectos atacables en un sistema, aunque presentan similitudes y se pueden ver en la tabla 4.3:

Tabla 4.3

Aspectos atacables en un sistema.

Aspecto	Descripción
Humano	Se refiere a las debilidades que ocurren debido a las acciones o errores de las personas en casa. Por ejemplo, ser engañado por un estafador que llama por teléfono, dejar las contraseñas anotadas en lugares visibles, o no saber cómo proteger los dispositivos conectados a la red del hogar.
Hardware	Estas debilidades afectan a los dispositivos físicos en el hogar, como las computadoras, routers, y otros equipos electrónicos. Pueden deberse a problemas en su diseño, fabricación o configuración, así como a la falta de actualizaciones necesarias para mantenerlos seguros. Por ejemplo, un router que no se ha actualizado puede ser vulnerable a ataques.
Red	Se refiere a las debilidades en la red doméstica, como el router Wi-Fi. Estas debilidades pueden ser explotadas para llevar a cabo ataques como robar información personal o interrumpir la conexión a internet. Un ejemplo es no cambiar la contraseña predeterminada del router, lo que facilita el acceso a intrusos.
Software	Son las debilidades que afectan a los programas y aplicaciones que usamos en casa. Pueden incluir errores de programación, falta de validación de los datos que se ingresan o la presencia de accesos ocultos que los atacantes podrían usar para entrar al sistema. Por ejemplo, una aplicación de la computadora que no se ha actualizado podría tener fallos de seguridad.
Natural	Estas debilidades se relacionan con eventos naturales que pueden afectar el hogar, como terremotos, inundaciones o tormentas. Aunque no son causados por personas, pueden afectar seriamente los dispositivos y la seguridad del hogar. Por ejemplo, una tormenta puede causar un corte de energía que dañe los dispositivos electrónicos.
Físico	Se refiere a las debilidades relacionadas con el entorno físico del hogar, como la ubicación de los dispositivos electrónicos y su protección. Estas debilidades pueden incluir acceso no autorizado a áreas del hogar, robo de dispositivos, o daños por agua o fuego. Por ejemplo, dejar una

	computadora portátil sin supervisión en una habitación accesible puede llevar a que sea robada.

Nota: La tabla describe los diferentes aspectos de un sistema que pueden ser vulnerables a ataques, incluyendo humano, hardware, red, software, natural y físico, junto con sus respectivas descripciones. Elaboración propia.

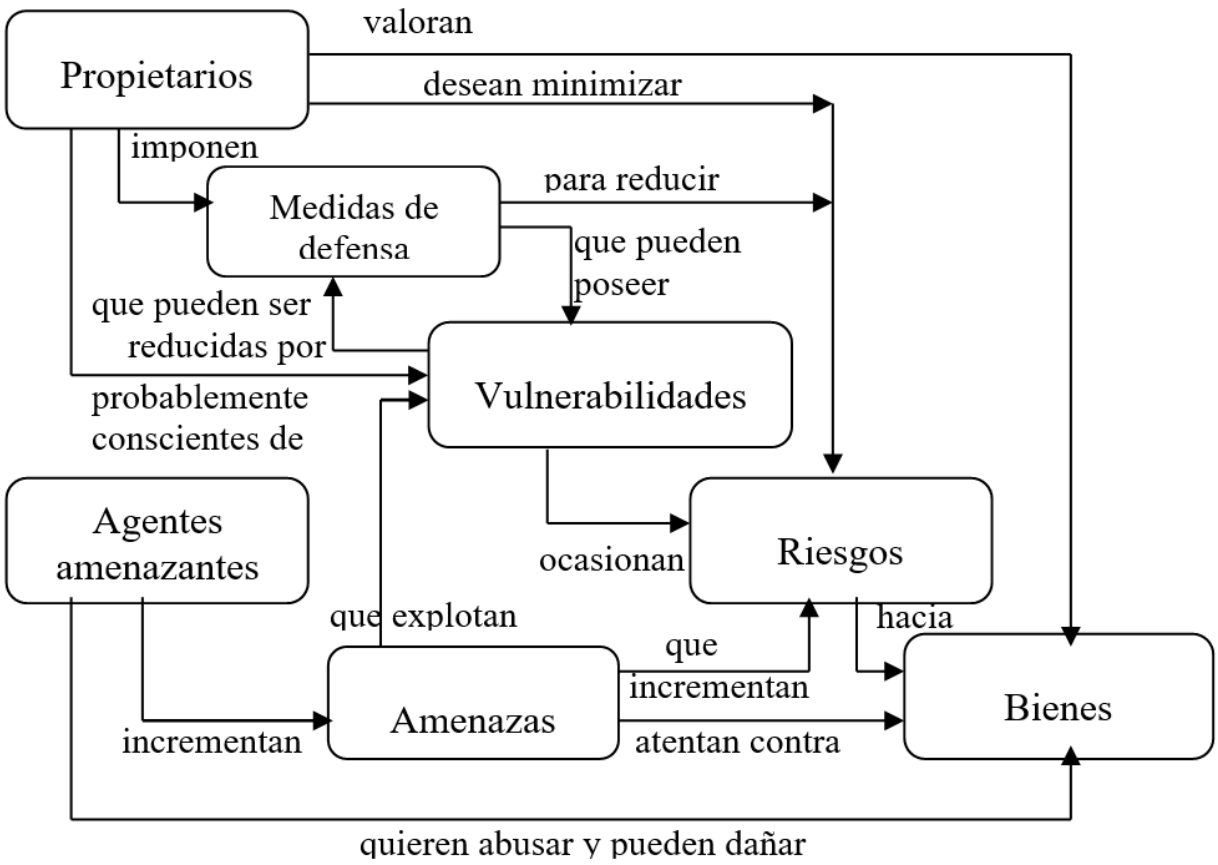
Para identificar vulnerabilidades, es crucial preguntarse lo siguiente:

- ¿Qué ha faltado o falta en el sistema?: Se trata de identificar cualquier aspecto que esté ausente en el sistema y que pueda representar una vulnerabilidad potencial. Esto podría incluir la falta de medidas de seguridad, controles de acceso insuficientes o actualizaciones no aplicadas.
- ¿Qué no se ha implementado o considerado adecuadamente?: Se busca identificar aquellas medidas de seguridad que no se han aplicado correctamente o que no se han tenido en cuenta durante el diseño o la implementación del sistema. Esto podría incluir políticas de seguridad no definidas, configuraciones incorrectas o falta de cifrado de datos.
- ¿Qué elementos faltan en el sistema? Se enfoca en identificar cualquier componente o recurso que debería estar presente en el sistema para garantizar su seguridad. Puede referirse a la ausencia de firewalls, sistemas de detección de intrusos, copias de seguridad regulares o procedimientos de respuesta a incidentes.
- ¿Qué aspectos han sido omitidos o descuidados?: Aquí se busca identificar cualquier aspecto de la seguridad que haya sido pasado por alto o descuidado durante el proceso de diseño, implementación o mantenimiento del sistema. Esto podría incluir la falta de capacitación del personal en seguridad, la ausencia de políticas de seguridad claras o la falta de actualizaciones regulares del software.

Debido a estas 3 preguntas en el contexto de la seguridad, tenemos varios elementos involucrados que se encuentran relacionados entre sí, como se puede observar en la figura 4.3:

Figura 4.3

Contexto de la seguridad y sus relaciones



Nota: La figura ilustra los elementos clave involucrados en la seguridad, incluyendo hardware, software, datos, procedimientos y personas. Tomado de "Contexto de la seguridad y sus relaciones", por UNAM, 2020, Recuperado el 15 de octubre de 2023 de http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/915/4/A4.pdf.

Donde:

- Propietarios: Personas que poseen un bien.
- Agentes de amenaza: Son individuos o entidades que tienen la capacidad de realizar acciones dañinas.
- Amenazas: Son situaciones, eventos o acciones que tienen el potencial de causar daño o pérdida a los bienes.
- Medidas de defensa: Son los métodos y acciones que se emplean para proteger los bienes.
- Vulnerabilidades: Son debilidades en los sistemas o fallas en los procedimientos de seguridad que pueden ser explotadas por amenazas para causar daño o pérdida.
- Riesgos: Representan la posibilidad de que ocurra un daño o pérdida en los bienes debido a amenazas y vulnerabilidades.

- Bienes: Son todos aquellos activos que son importantes para un individuo, entidad o grupo.

Pese a todos los esfuerzos, es crucial recordar que ***la seguridad al 100% no existe***. A pesar de implementar medidas exhaustivas para proteger los bienes, siempre existe alguna vulnerabilidad por mínima que sea, que podría poner en riesgo la seguridad de los mismos.

4.2. Acceso a la Red

En el mundo altamente interconectado y digitalizado de hoy, el acceso a la red se ha convertido en una necesidad fundamental tanto para individuos como para organizaciones. Desde la comunicación y el intercambio de información hasta el acceso a recursos compartidos, la red es esencial en la vida cotidiana y en el funcionamiento de las empresas. Sin embargo, con este acceso también vienen desafíos significativos en términos de seguridad y protección de datos. Por ello, es vital comprender y gestionar adecuadamente el control de acceso a la red para garantizar la integridad, confidencialidad y disponibilidad de la información.

Al definir el acceso a la red es importante saber qué tantos recursos van a utilizar los usuarios y de qué naturaleza son estos. Para conocer esto es importante autenticar a todo el personal que ingrese a la red, a fin de administrar los permisos y las actividades que pueden realizar dentro de la red, de tal manera que no se genere una amenaza interna y que el acceso no sea aprovechado por un amenaza externa.

La seguridad de la red del hogar es de suma importancia, y un aspecto crucial para asegurarla es el control de acceso. Este proceso permite restringir el acceso de usuarios y dispositivos a la información contenida en la red. Análogamente a cómo protegemos al hogar con candados y puertas para evitar el acceso no autorizado, el control de acceso también previene que intrusos físicos accedan a los dispositivos, como computadoras, teléfonos celulares y módems. Es una barrera fundamental para salvaguardar la integridad y privacidad de los datos, garantizando que solo aquellos con permisos adecuados puedan acceder a ellos.

Además de los aspectos mencionados, es importante tener en cuenta el protocolo WPS (Wi-Fi Protected Setup), una característica que muchos routers incluyen para facilitar la conexión de dispositivos a la red WiFi. Sin embargo, aunque es conveniente, WPS puede ser un punto débil si no se utiliza adecuadamente, ya que puede permitir que intrusos accedan a la red a través de métodos de fuerza bruta. Por lo tanto, se recomienda desactivar WPS para fortalecer la seguridad de la red, ya que esta función, si no se controla, puede ser explotada por atacantes.

El control de acceso a la red es esencial por varias razones fundamentales:

- Seguridad: Establece barreras que protegen los recursos de posibles manipulaciones o robos perpetrados por usuarios malintencionados. Es una capa de defensa vital para preservar la integridad de los datos y sistemas dentro de la red.
- Privacidad: Al restringir el acceso a la información contenida en los hogares, se garantiza que esta no se divulgue indiscriminadamente. Esto es especialmente crucial en la protección de datos personales y confidenciales que pueden ser sensibles o privados.
- Cumplimiento: En muchas organizaciones, el control de acceso es un requisito para cumplir con estándares y regulaciones específicas. Esto no solo asegura el cumplimiento legal, sino que también brinda a los usuarios y usuarias una mayor confianza al utilizar los servicios de la organización, sabiendo que se han implementado medidas robustas de seguridad y protección de datos.

Para una comprensión mejor sobre cómo se controla el acceso, es esencial desglosar los elementos que lo componen. En este sentido, HPE Aruba Networking ofrece una guía que se visualiza en la Tabla 4.4:

Tabla 4.4

Elementos de control de acceso a la red.

Capacidades	Función
Visibilidad	Saber quién y qué está en la red en cada momento.
Autenticación	Determinar con confianza que un usuario o dispositivo es quien/lo que declara ser.
Definición de políticas	Definición de normas para usuarios y dispositivos en relación con los recursos a los que pueden acceder y cómo se puede acceder a los recursos.
Autorización	Determinación de las reglas apropiadas para el usuario o dispositivo autenticado.
Cumplimiento	Permitir, denegar o revocar el acceso de un usuario o dispositivo autenticado a un recurso en función de la política correspondiente.

Nota: La tabla muestra las capacidades y funciones de los elementos de control de acceso a la red, incluyendo visibilidad, autenticación, definición de políticas, autorización y cumplimiento. Tomado de "¿Qué es el control de acceso a la red (NAC)?", por Aruba Networks, 2023, https://www.arubanetworks.com/latam/faq/que-es-control-de-acceso-a-la-red-nac/.

Entre estos controles, el más común y fácil de implementar es el uso de contraseñas de acceso, esta será la primer restricción que impedirá a los usuarios no deseados entrar a la red, esta se encuentra configurada previamente en los modem pero se sugiere cambiarla de forma inmediata tomando en cuenta las siguientes consideraciones:

- La contraseña debe tener un mínimo de 8 caracteres para tener una mayor resistencia a ataques de prueba y error.
- Debe incluir una combinación de letras mayúsculas, letras minúsculas, símbolos o caracteres especiales y números para aumentar su complejidad.
- Se recomienda cambiar la contraseña periódicamente, esto es por ejemplo cada 30, 60 días u otro periodo, idealmente que no exceda de un año.
- Evitar contraseñas sencillas como "12345" o "1111" que sean fáciles de adivinar.
- Utilizar una contraseña distinta en cada uno de los dispositivos o servicios que se tengan.
- Se sugiere el uso de gestores de contraseñas para mantener un registro seguro y no olvidarlas.
- En caso de guardar las contraseñas en un documento electrónico, es importante cifrarlo para proteger la información.
- Si se anotan las contraseñas en un cuaderno o papel, asegurarse de que esté en un sitio resguardado donde nadie más pueda acceder a él.
- Evitar que en las contraseñas se utilice información personal, como nombres o fechas de nacimiento.
- En absoluto pegar las contraseñas al monitor o debajo del teclado, lugares comunes y fácilmente accesibles para los intrusos.
- No compartir la contraseña con cualquier persona, incluso si son familiares o amigos, para mantener la seguridad de la red.

Otro aspecto importante de la seguridad de la red inalámbrica es el cifrado. Se recomienda utilizar WPA3 (Wi-Fi Protected Access 3), el estándar más reciente, que proporciona un mayor nivel de protección frente a ataques comunes como el descifrado de contraseñas y ataques de diccionario. Si tu router o dispositivos no son compatibles con WPA3, al menos asegúrarse de utilizar WPA2, que sigue siendo seguro, aunque menos robusto comparado con WPA3.

Existen varios protocolos de seguridad para redes WiFi, cada uno con diferentes niveles de seguridad:

- WEP (Wired Equivalent Privacy): Fue el primer protocolo de seguridad WiFi, introducido en 1997. Utiliza claves estáticas de 64 o 128 bits, pero está gravemente

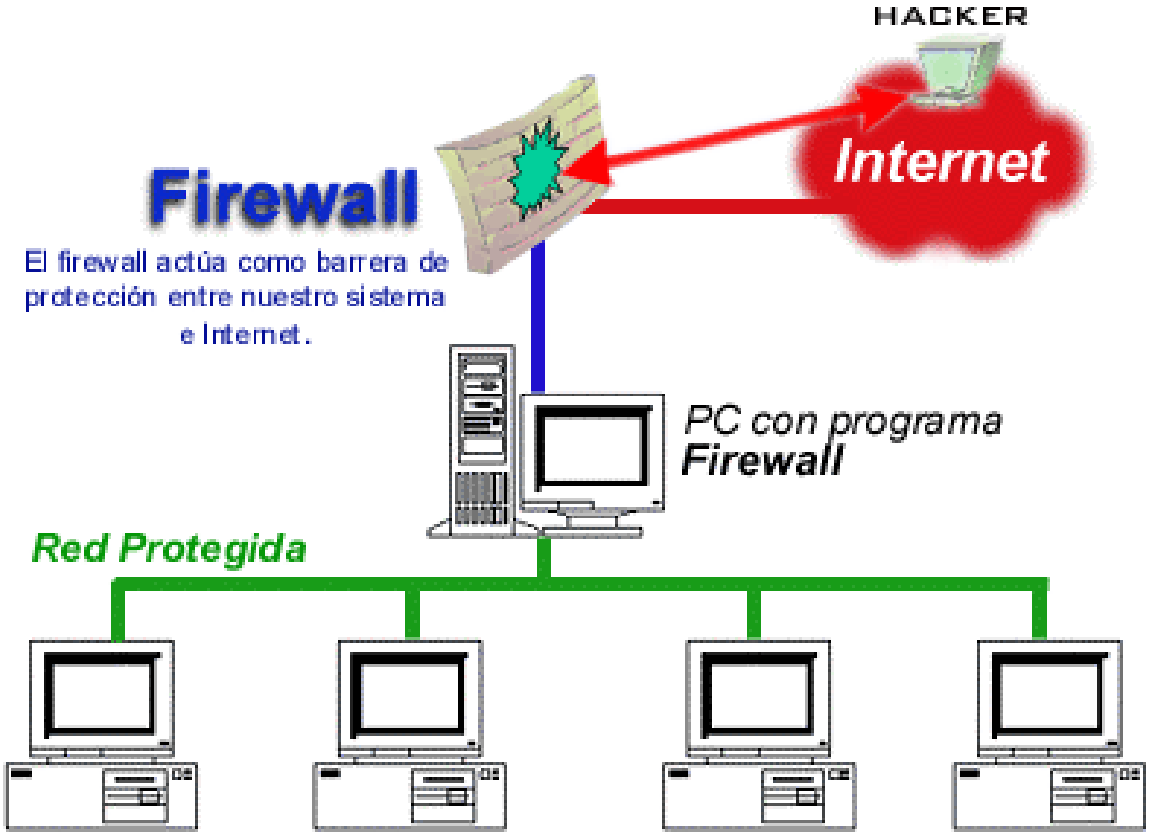
desactualizado y es vulnerable a ataques que pueden romper la clave de cifrado en minutos. No se recomienda su uso en absoluto.

- WPA (Wi-Fi Protected Access): Introducido en 2003 como una solución temporal para mejorar la seguridad de WEP antes del lanzamiento de WPA2. Utiliza el protocolo TKIP (Temporal Key Integrity Protocol), que mejora el cifrado, pero también tiene vulnerabilidades conocidas y no se recomienda su uso.
- WPA2 (Wi-Fi Protected Access 2): Introducido en 2004, es una mejora significativa sobre WPA y usa el protocolo de cifrado AES (Advanced Encryption Standard), mucho más seguro que TKIP. Aunque sigue siendo ampliamente utilizado, WPA2 tiene algunas vulnerabilidades frente a ciertos tipos de ataques, como el ataque KRACK, pero sigue siendo seguro si se configura adecuadamente con AES.
- WPA3 (Wi-Fi Protected Access 3): Introducido en 2018, es la versión más avanzada y segura. Ofrece mejoras frente a ataques de fuerza bruta y proporciona una mejor cifrado, incluso cuando se usan contraseñas débiles. Implementa un método llamado SAE (Simultaneous Authentication of Equals) para proteger contra ataques de diccionario y es ideal para redes públicas y domésticas.
- WPA2-Enterprise y WPA3-Enterprise: Estas versiones están diseñadas para entornos corporativos y proporcionan una autenticación más robusta a través de servidores RADIUS, además de un control más detallado sobre los dispositivos que se conectan a la red. Se diferencian de las versiones estándar (WPA2/WPA3-Personal) por permitir autenticación basada en certificados en lugar de contraseñas compartidas.

Al cambiar la contraseña de tu red, asegúrate también de seleccionar el protocolo de cifrado adecuado para mantener la red protegida contra accesos no autorizados. WPA3 es la opción más recomendada, pero si no está disponible, WPA2 con AES sigue siendo una buena alternativa. Evita usar WPA o WEP, ya que son estándares obsoletos y vulnerables.

Otro control de acceso muy común es el firewall, una herramienta fundamental en el arsenal de seguridad de redes. Cisco lo describe como: “un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.” Observe la figura 4.4.

Figura 4.4
Firewall.



Nota: La figura muestra cómo un firewall actúa como una barrera de protección entre un sistema y la Internet, bloqueando el acceso de posibles atacantes y protegiendo la red interna. Tomado de "Firewall", por TicoNologia, 2023, https://ticnologia.fandom.com/es/wiki/Firewall.

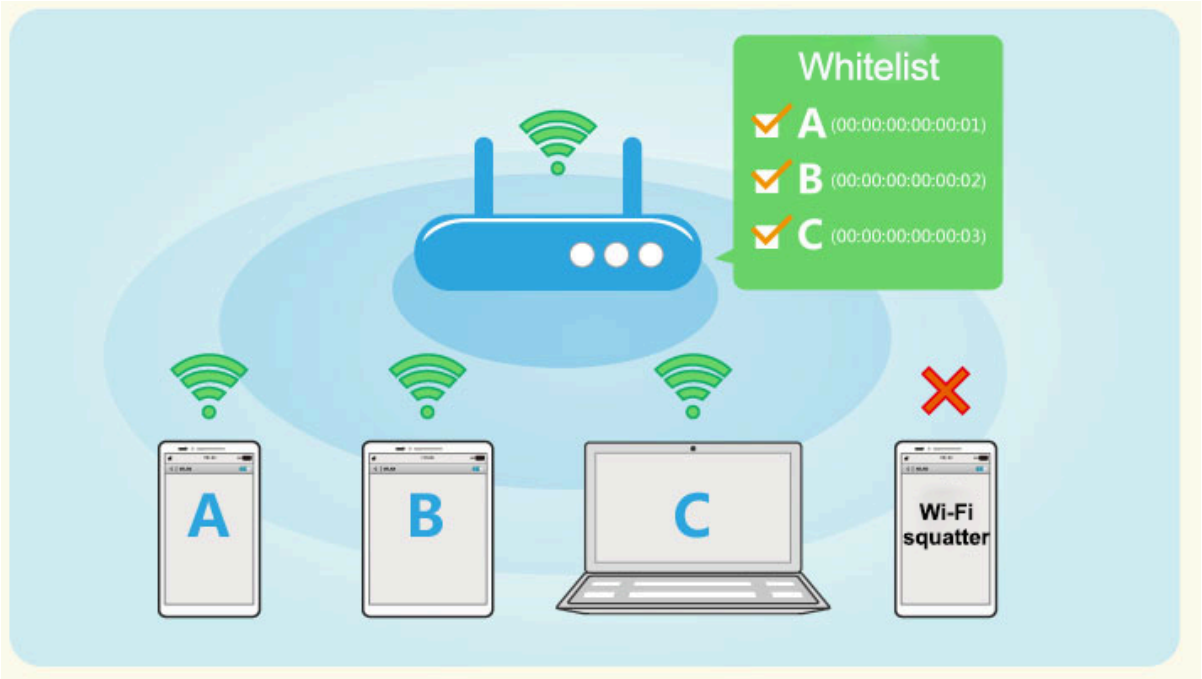
Hay diversos tipos de firewalls, cada uno con sus propias características y funciones específicas:

- Firewall Proxy: Este tipo de firewall actúa como un intermediario entre redes, funcionando como un gateway. Además de filtrar el tráfico, puede ofrecer funciones adicionales como seguridad y almacenamiento en caché de contenido, evitando conexiones directas desde el exterior.
- Firewall de Inspección Activa: Conocido como firewall "tradicional", este dispositivo monitorea y controla el tráfico dentro de la red. Desde la apertura hasta el cierre de una conexión, los administradores pueden definir reglas para determinar qué tráfico se permite o bloquea.

- Firewall de Administración Unificada de Amenazas (UTM): Este tipo de firewall, a menudo administrado a través de la nube, combina de manera flexible funciones de inspección activa con prevención de intrusiones y antivirus.
- Firewall de Próxima Generación (NGFW): Además de ofrecer las funcionalidades de los tipos anteriores, este tipo de firewall está diseñado para enfrentar amenazas más actuales, como los ataques de capa de aplicación y el malware avanzado. Según Gartner, Inc., un NGFW debe incluir:
    - Funcionalidades de firewall estándar, como la inspección activa.
    - Prevención de intrusiones integrado.
    - Control y reconocimiento de aplicaciones para identificar y bloquear aplicaciones riesgosas.
    - Actualizaciones regulares para adaptarse a nuevas amenazas.
    - Técnicas para hacer frente a amenazas de seguridad en constante evolución.
- NGFW Centrado en Amenazas: Este tipo de NGFW va más allá, ofreciendo funciones avanzadas de detección y corrección de amenazas. Puede:
    - Identificar activos de alto riesgo mediante un reconocimiento completo del contexto.
    - Responder rápidamente a los ataques con automatización inteligente de seguridad.
    - Detectar actividad sospechosa o evasiva mediante la correlación de eventos de endpoints y la red.
    - Reducir el tiempo necesario para eliminar amenazas con seguridad retrospectiva que monitorea continuamente la actividad sospechosa.
    - Simplificar la administración con políticas unificadas que brindan protección en todas las etapas del ataque.

El filtrado de direcciones MAC es una medida de control de acceso que se puede implementar fácilmente en el hogar para reforzar la seguridad de la red. Consiste en crear una lista de las direcciones MAC de los dispositivos autorizados que pueden conectarse a la red (observe la figura 4.5). De esta manera, el enrutador o módem sabe exactamente qué dispositivos están permitidos para acceder a la información en la red.

Figura 4.5
Filtrado MAC.



***Nota:** La figura muestra el funcionamiento del filtrado de direcciones MAC, donde solo los dispositivos con direcciones MAC específicas (en la lista blanca) pueden conectarse a la red, mientras que otros dispositivos son bloqueados. Tomado de "Fundamentos sobre ONT: Botones de la ONT de la parte frontal", por Huawei Forum, 2023, https://forum.huawei.com/enterprise/es/fundamentos-sobre-ont-botones-de-la-ont-de-la-parte-frontal/thread/667223987203227648-667212890693840896.*

Esta medida también brinda la capacidad de controlar qué recursos de la red pueden acceder los dispositivos, según las necesidades específicas de la red del hogar. En resumen, el filtrado MAC garantiza que sólo los dispositivos cuyas direcciones MAC están en la lista autorizada puedan conectarse a la red, incluso si tienen la contraseña correcta para establecer la conexión.

Aunque existen diversas medidas de control de acceso para proteger las redes, aquellas que implican el filtrado de direcciones MAC son, sin duda, las más accesibles para implementar en los hogares. No requieren un conocimiento técnico profundo y pueden proporcionar una capa adicional de seguridad significativa. Es esencial tener en cuenta las recomendaciones para establecer contraseñas seguras, como se mencionó anteriormente, ya que estas medidas de control de acceso no son infalibles por sí solas. La combinación de ambas estrategias puede fortalecer significativamente la seguridad de la red doméstica, protegiendo los datos y dispositivos contra accesos no autorizados.

Además, es importante destacar que la seguridad de la red no debe considerarse como un proceso estático. Se recomienda revisar y actualizar regularmente las medidas de

seguridad implementadas, así como estar al tanto de las nuevas amenazas y vulnerabilidades que puedan surgir. Esto nos permitirá mantener nuestra red protegida de manera efectiva a medida que evolucionan las tecnologías y los métodos de ataque.

4.3. Normas y Estándares

La seguridad en las redes se ha convertido en un aspecto crucial en la era actual. A medida que la tecnología avanza, también surgen vulnerabilidades, lo que aumenta la cantidad de amenazas y ataques. Esta dinámica hace imperativa la implementación de controles de seguridad eficaces para garantizar la protección de los dispositivos. Por consiguiente, han surgido diversas organizaciones que han desarrollado normativas y estándares destinados a regular el trabajo en redes. Entre estas, destacan las siguientes:

- ISO 27000: Conjunto de estándares creado y administrado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Establecen pautas y requisitos detallados para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Se conforma de diversos estándares y los más importantes se encuentran detallados en la tabla 4.5:

Tabla 4.5

Conjunto de estándares de la familia ISO 27000

Norma Iso	Descripción
ISO 27001	Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Es la norma más importante de la familia y es certificable.
ISO 27002	Define un conjunto de buenas prácticas para la implantación del SGSI, a través de 93 controles, estructurados en 4 grandes dominios.
ISO 27005	Define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información, orientado en cómo establecer la metodología a emplear.
ISO 27032	Facilita la identificación de las líneas generales para fortalecer el estado de la ciberseguridad en una compañía.
ISO 27033	Establece las pautas de seguridad de la administración, operación y uso de las redes.

ISO 27034	Proporciona orientación en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación.
ISO 27035	Define un conjunto de mejores prácticas relacionadas con la gestión de incidentes de seguridad haciendo hincapié en la detección, reporte y evaluación de incidentes de seguridad.
ISO 27037	Ofrece directrices para la identificación, recolección, adquisición y preservación de evidencias digitales.
ISO 27040	Determina las pautas para proteger la seguridad de los sistemas de almacenamiento, así como para la protección de los datos contenidos en los mismos.
ISO 27701	Define directrices para la implementación de la ISO/IEC-27002 en la industria de la salud.
ISO 27799	Ofrece requisitos para gestionar la seguridad de la información para los proveedores de servicios de confianza de infraestructura de clave pública (PKI).

Nota: La tabla muestra los principales estándares de la familia ISO 27000, incluyendo ISO 27001, ISO 27002, ISO 27005, entre otros. Estos estándares definen las mejores prácticas y pautas para la gestión de la seguridad de la información. Tomado de "La familia de normas ISO 27000", por GlobalSuite Solutions, 2023, https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/.

De entre todos estos estándares, se utiliza como referencia certificable el ISO 27001. Este estándar proporciona los requisitos necesarios para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), basado en el ciclo Deming o PDCA (Planificar, Hacer, Verificar, Actuar), que se ilustra en la figura 4.6.

Figura 4.6
Ciclo Deming.

Nota: La figura muestra el Ciclo Deming, también conocido como el ciclo PDCA (Plan-Do-Check-Act), que es un método iterativo para la mejora continua de procesos y productos. Tomado de "Normas ISO para mejorar la ciberseguridad", por GlobalSuite Solutions, 2023, https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/#La_ciberseguridad_y_las_normas_ISO.

- NIST (Instituto Nacional de Normas y Tecnología): El NIST es una institución gubernamental de los Estados Unidos que desempeña un papel fundamental en el establecimiento de estándares y directrices para la seguridad de la información y las redes. Sus documentos, como el NIST SP 800-53, proporcionan un catálogo completo de controles de seguridad que abarcan desde la gestión de riesgos hasta la protección de sistemas y datos. Por otro lado, el NIST SP 800-171 se enfoca en la protección de información no clasificada pero controlada por el gobierno, estableciendo requisitos específicos para salvaguardar estos datos.
- GDPR (Reglamento General de Protección de Datos): Aunque su enfoque principal es la protección de la privacidad de los datos personales en la Unión Europea, el GDPR también influye en la seguridad de redes al exigir a las organizaciones medidas técnicas y organizativas adecuadas para proteger estos datos. Esto incluye la implementación de controles de acceso, cifrado, monitoreo de seguridad y respuesta a incidentes, entre otros aspectos relacionados con la seguridad de la red.
- HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico): Este estándar es de vital importancia para las organizaciones de atención médica en los Estados Unidos, ya que establece requisitos específicos para proteger la privacidad y seguridad de la información de salud protegida (PHI). HIPAA aborda aspectos clave de la seguridad de la red en entornos de atención médica, como la protección de la integridad de los datos, la autenticación de usuarios, el control de acceso y la

seguridad de la transmisión de datos electrónicos de salud (ePHI). Esto garantiza que los datos médicos sensibles estén protegidos contra accesos no autorizados y posibles amenazas cibernéticas.

4.4. Antivirus

Un antivirus es una herramienta de software diseñada para identificar, bloquear y eliminar archivos maliciosos que pueden comprometer la seguridad de los equipos de red. No solo detecta virus, sino también otros tipos de amenazas como malware, ransomware, troyanos y spyware que pueden infiltrarse en nuestros sistemas. Además de proteger los dispositivos, los antivirus también desempeñan un papel crucial en la prevención de la propagación de estas amenazas a través de la red, ya que pueden detectar y bloquear la transmisión de archivos infectados.

Con el continuo crecimiento de Internet y el constante avance tecnológico, la importancia de mantener actualizados los antivirus es crucial. Esta actualización constante garantiza que los antivirus se encuentren equipados para hacer frente a la creciente sofisticación de las actividades maliciosas en línea. Entre estas actividades se incluyen el robo de información confidencial, el espionaje, la cifrado de archivos con fines de rescate (ransomware), la distribución de troyanos para el control remoto de dispositivos, el envío masivo de correos no deseados (spam) y diversas formas de estafas en línea. Mantener los antivirus actualizados permite una protección efectiva contra estas amenazas, ayudando a mantener la seguridad y la privacidad de los usuarios en el entorno digital.

La continua actualización por parte de las empresas desarrolladoras de antivirus implica que la mayoría de estos programas deben ser adquiridos. En la siguiente tabla (Tabla 4.6), se muestran algunos de los antivirus más efectivos, indicando si son de pago o no.

Tabla 4.6
Antivirus

Antivirus	Pago/Gratuito	Características
Windows Defender	Gratuito	Protección integral contra virus, malware, ransomware y amenazas en línea, integrado en el sistema operativo Windows.

ESET NOD32	Pago	Protección en tiempo real contra virus, malware, ransomware y phishing, escaneo de archivos adjuntos de correo electrónico.
Bitdefender	Pago	Protección avanzada contra malware, firewall, protección de ransomware, análisis de vulnerabilidades, VPN incluida.
Avast	Gratuito	Protección básica contra virus, malware y ransomware, escaneo de Wi-Fi, análisis de seguridad del navegador.
Kaspersky	Pago	Protección en tiempo real contra virus, malware, ransomware y phishing, firewall, protección de pagos seguros
AVG Antivirus	Gratuito	Protección esencial contra virus y malware, escaneo de PC en tiempo real, protección de navegación web segura
Norton Antivirus	Pago	Protección avanzada contra virus, malware, ransomware y estafas en línea, firewall, protección de identidad

Nota: La tabla presenta una lista de antivirus, especificando si son de pago o gratuitos y describiendo sus características principales, como la protección contra virus, malware, ransomware y otras amenazas. Tomado de "Guía de los mejores antivirus para 2023", por TechRadar, 2023, https://www.techradar.com/best/best-antivirus.

De todos estos, Windows Defender viene preinstalado en todas las computadoras con sistema operativo Windows, proporcionando una capa adicional de seguridad desde el primer momento. Sin embargo, es crucial tener en cuenta que si se desea instalar otro antivirus, se debe desactivar Windows Defender, aunque esto debería ocurrir automáticamente, es recomendable verificarlo por precaución.

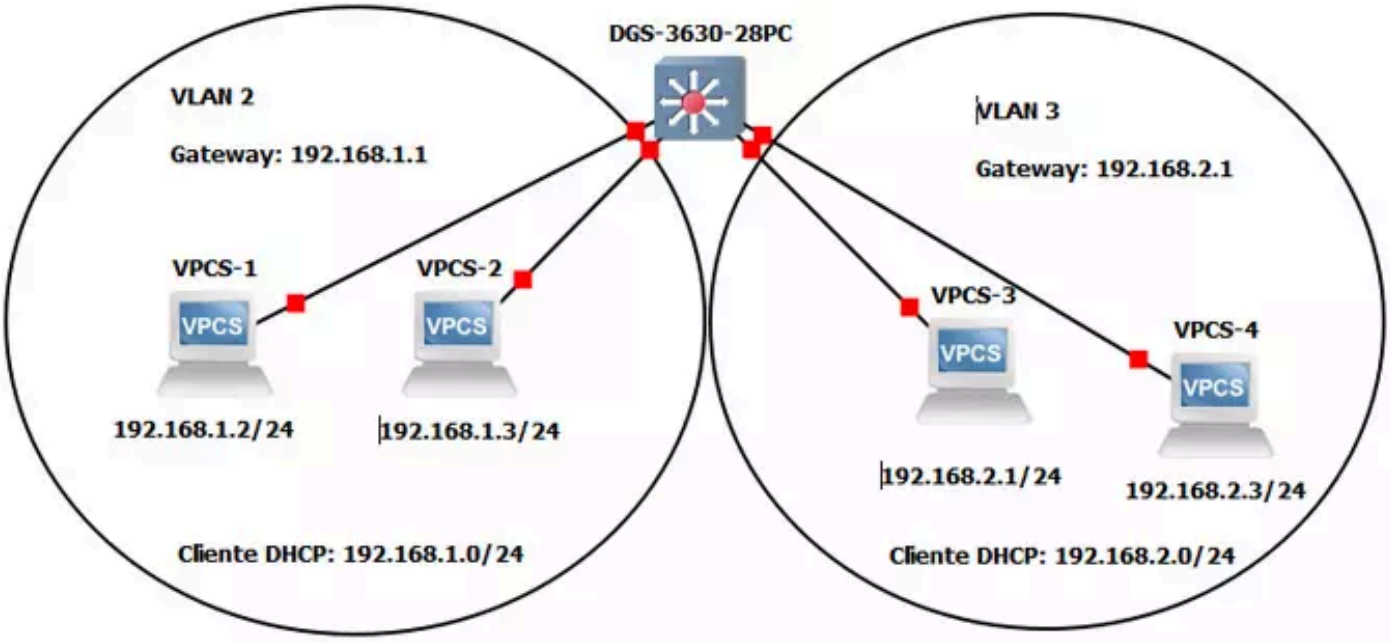
Lo mismo ocurre si ya se tiene instalado un antivirus y se considera instalar otro para reforzar la seguridad. Esta acción podría ser perjudicial para el equipo de red, ya que mantener dos antivirus activos consumirá recursos significativos y podría resultar en escaneos simultáneos que ralenticen el sistema. Además, existe el riesgo de que los ambos antivirus se detecten mutuamente como aplicaciones maliciosas y traten de eliminarse

entre sí, lo que podría causar fallos en el dispositivo. En el peor de los casos, esta interferencia entre los programas antivirus podría llevar a la omisión de detección de archivos realmente maliciosos. Por lo tanto, es recomendable elegir un solo antivirus confiable y mantenerlo actualizado regularmente para garantizar una protección óptima sin comprometer el rendimiento del sistema.

4.5. VLANs - VPN

Las VLAN (Redes de Área Local Virtuales) son una tecnología que posibilita la creación de redes lógicas dentro de una infraestructura física compartida. Esto significa que, en lugar de implementar redes físicas separadas cada vez que se necesite segmentar el tráfico, las VLAN permiten dividir y organizar el tráfico en grupos lógicos, sin necesidad de una infraestructura física adicional y permiten un filtrado de IP 's como medida de seguridad adicional. Es importante tener en cuenta que la capacidad de configuración de VLAN en el router es esencial para su funcionamiento. Si el enrutador no admite esta funcionalidad, no será posible implementarlas correctamente, ya que se encargará de denegar la comunicación entre las distintas redes lógicas.

Figura 4.7
Red VLAN.



Nota: La figura muestra una configuración de red VLAN, ilustrando dos VLANs con sus respectivos gateways y dispositivos conectados. Tomado de "Qué son las VLAN: Tipos y configuración", por RedesZone, 2023, https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/#446967-que-son-las-vlan.

Al configurar VLAN, es esencial realizar una segmentación de la red para determinar cómo se dividirán las subredes según su uso y la cantidad de usuarios que se conectarán. Por ejemplo, al observar la figura 4.7,se observa la presencia de dos VLAN denominadas vlan2 y vlan3. Estas VLAN están clasificadas como tipo C, según lo indicado en la tabla 3.1 del capítulo 3 "Funcionamiento de internet" subtema "IP y dominios", lo que sugiere que el número de usuarios no supera los 254 en cada una. Sin embargo, lo más significativo es que ambas VLAN están representadas por círculos separados, lo que indica que, a pesar de estar en la misma red física, están segregadas. Este enfoque asegura una gestión eficiente del tráfico y una mejor organización de la red.

Una parte crucial para comprender las VLAN implica familiarizarse con los diferentes tipos disponibles y comprender cómo se aplican en diversos entornos de red. Esto nos permite determinar cuál de ellos sería más útil para nuestras necesidades específicas. Para facilitar esta comprensión, observar la tabla 4.7, que resume los tipos de VLAN junto con sus respectivas descripciones:

Tabla 4.7

Tipos de VLAN

Tipo de VLAN	Descripción
VLAN basada en puertos	Asigna puertos específicos en un switch a una VLAN, lo que permite agrupar dispositivos conectados a esos puertos en la misma red lógica.
VLAN basada en direcciones MAC	Agrupa dispositivos en una VLAN según sus direcciones MAC, lo que puede ser útil para aplicar políticas de red basadas en la identidad de los dispositivos.
VLAN basada en protocolos	Divide el tráfico de red en VLAN según el protocolo de red utilizado, como IP, IPX o IPv6. Esto puede ayudar a optimizar el rendimiento y la seguridad de la red.
VLAN de voz	Diseñada específicamente para el tráfico de voz sobre IP (VoIP), esta VLAN prioriza el tráfico de voz para garantizar una calidad de llamada óptima.
VLAN de gestión	Reservada para la administración y supervisión de dispositivos de red, como switches, routers y puntos de acceso inalámbrico.
VLAN nativa	Esta VLAN predeterminada se utiliza para el tráfico que no está

	etiquetado con una VLAN específica, como el tráfico que proviene de dispositivos que no admiten VLAN.
VLAN de invitados	Diseñada para aislar el tráfico de los invitados de la red principal, proporcionando acceso limitado a Internet sin comprometer la seguridad de la red corporativa.

Nota: La tabla presenta una clasificación de diferentes tipos de VLAN (Red de Área Local Virtual), incluyendo VLAN basadas en puertos, direcciones MAC, protocolos, voz, gestión, nativas y de invitados, detallando sus descripciones y usos. Tomado de múltiples fuentes sobre tecnología de redes y administración de sistemas, 2023.

El uso de VLAN conlleva una serie de beneficios significativos:

- Seguridad: Al separar a los usuarios en VLAN, es posible administrar de manera más eficiente y precisa qué recursos y servicios pueden acceder. Esto significa que podemos aplicar políticas de acceso más específicas, lo que aumenta la seguridad al reducir el riesgo de accesos no autorizados o maliciosos.
- Segmentación: La segmentación de la red mediante VLAN permite dividir el tráfico en grupos lógicos, lo que facilita la gestión y el control de la red. Cada VLAN puede representar diferentes departamentos, funciones o niveles de acceso, lo que mejora la organización y la claridad en la administración de la red.
- Optimización de la red: Utilizar VLAN puede ayudar a optimizar el rendimiento de la red al reducir el tráfico innecesario. Al dirigir el tráfico únicamente a los destinos relevantes en lugar de inundar toda la red, se reduce la congestión y se mejora la eficiencia general del sistema.
- Flexibilidad: La implementación de VLAN proporciona una mayor flexibilidad en la administración de la red. Puede adaptarse fácilmente a cambios en la organización, como la adición de nuevos equipos o la reorganización de departamentos, sin necesidad de reconfigurar toda la infraestructura física de red. Esto permite una mayor agilidad y capacidad de respuesta a las necesidades cambiantes de la empresa.
- Optimización de la red: Al posibilitar la creación de múltiples subredes en un entorno con varios dispositivos conectados, se logra un mejor rendimiento. Esto se debe a que los mensajes no tienen que pasar a través de tantos dispositivos ni llegar hasta el router, lo que reduce la congestión y mejora la eficiencia del tráfico de datos.

- Reducción de costos: Esta ventaja puede ser una de las más significativas, ya que elimina la necesidad de adquirir nuevo equipo o realizar actualizaciones frecuentes. Esto se traduce en un ahorro considerable para la empresa, ya que evita gastos innecesarios en la expansión o modernización de la infraestructura de red.

Como se ha visto, las VLAN pueden ofrecer numerosas ventajas para mejorar la eficiencia de la red. Sin embargo, como ocurre con cualquier tecnología, también tienen algunas limitaciones. Las principales desventajas que pueden brindar son:

- Equipos y software específicos: No todos los routers son compatibles con la implementación de VLAN, lo que podría requerir la adquisición de nuevo equipo si el existente no cumple con este requisito.
- Aislamiento: Aunque la segmentación de la red mediante VLAN ofrece un alto nivel de aislamiento entre diferentes grupos de usuarios o dispositivos, esto puede generar complejidad adicional en la administración y configuración de la red.
- Congestión: El aumento en la cantidad de información que un solo router debe manejar, puede llevar a una reducción en la velocidad de transferencia de datos. Esta congestión puede mitigarse con una configuración adecuada, pero aún así puede ser un desafío gestionarla eficazmente.
- Seguridad: Aunque las VLAN pueden mejorar la seguridad al limitar el acceso a recursos específicos, también pueden introducir nuevas vulnerabilidades. Si un virus logra ingresar a la red, su dispersión puede ser más fácil entre los distintos segmentos de VLAN, aumentando así el riesgo de propagación y daño.
- Latencia: La implementación de VLAN puede introducir una ligera latencia adicional en la red debido al procesamiento adicional requerido para dirigir el tráfico entre las distintas VLAN. Aunque este aumento suele ser mínimo, puede afectar el rendimiento de aplicaciones sensibles a la latencia.

En general, las VLAN ofrecen una amplia gama de beneficios que mejoran la eficiencia operativa, la seguridad y la flexibilidad de una red. Sin embargo, es importante reconocer que también pueden presentar desafíos, como la necesidad de contar con equipos y software compatibles, la complejidad en la administración y configuración, así como posibles problemas de congestión, seguridad y latencia. A pesar de estas limitaciones, cuando se implementan adecuadamente y se gestionan de manera eficiente, las VLAN siguen siendo una herramienta invaluable para la gestión de redes modernas, permitiendo a las organizaciones adaptarse ágilmente a las cambiantes demandas del entorno empresarial y optimizar el rendimiento de sus infraestructuras de red.

Las VLAN no son las únicas tecnologías que operan redes de forma virtual; también existen las VPN (Redes Privadas Virtuales), que crean un entorno de red virtual seguro y cifrado entre dos computadoras ubicadas en diferentes lugares. A través de Internet, las VPN permiten a los usuarios establecer conexiones remotas seguras, facilitando el acceso a recursos que pueden estar restringidos geográficamente. Por ejemplo, al conectarse a través de una VPN, los usuarios pueden acceder a servicios en línea que pueden no estar

disponibles en su país de origen, ya que el sitio web reconoce la ubicación de la VPN como la ubicación desde la que se realizó la conexión.

Las VPN se encargan de cifrar los datos que se envían entre dos dispositivos, lo que garantiza la seguridad de la información de los usuarios. Este cifrado dificulta la intercepción y lectura de los datos por parte de usuarios malintencionados, proporcionando una capa adicional de protección para la privacidad y la seguridad en línea. Es por ello que existen diversos tipos de VPN, diseñados para adaptarse a las diferentes necesidades y preferencias de los usuarios:

- VPN de Acceso Remoto: Permite a los usuarios conectarse de forma segura a una red privada a través de Internet desde cualquier ubicación, accediendo a los recursos de esa red. Por ejemplo, un usuario en un café puede acceder a su computadora doméstica desde cualquier lugar.
- VPN de Sitio a Sitio: Similar a la VPN de acceso remoto, pero permite la conexión de múltiples redes, permitiendo que varios usuarios se conecten simultáneamente a los recursos de una misma red. Por ejemplo, los empleados pueden acceder a los recursos de la red empresarial desde sus computadoras domésticas.
- VPN Personal: Conecta a los usuarios desde sus hogares a una VPN y es ampliamente utilizada para acceder a recursos de sitios web no disponibles en su país. Por ejemplo, permite el acceso a contenido geo-restringido o la protección de la privacidad en línea.
- VPN Móvil: Diseñada especialmente para dispositivos móviles, permite a los usuarios conectarse a redes mientras están en movimiento. Por ejemplo, los trabajadores pueden acceder a la red de la empresa desde sus teléfonos mientras se desplazan a reuniones u otros lugares.

Para proteger los datos importantes cuando se establece una conexión a través de Internet, las VPN integran diversos protocolos que, entre sus funciones principales, cifran los datos. A continuación, se presentan algunos de estos protocolos:

- SSTP (Secure Socket Tunneling Protocol): Desarrollado por Microsoft específicamente para su plataforma Windows, SSTP se destaca por su enfoque en la seguridad. Utiliza el cifrado SSL/TLS para garantizar la confidencialidad y la integridad de los datos transmitidos a través del túnel VPN. Debido a su integración nativa en Windows, SSTP es una opción conveniente para usuarios de este sistema operativo que buscan una conexión VPN segura.
- L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security): L2TP/IPsec ofrece una combinación de dos protocolos para proporcionar una conexión VPN segura y confiable. Aunque puede considerarse menos seguro en comparación con otros protocolos, como OpenVPN, L2TP/IPsec es ampliamente utilizado debido a su

facilidad de configuración y compatibilidad con una amplia gama de dispositivos y sistemas operativos. Es una opción popular para aquellos que buscan una solución VPN fácil de implementar y que funcione en diversos entornos.

- PPTP (Point-to-Point Tunneling Protocol): PPTP es uno de los primeros protocolos VPN desarrollados y, a menudo, se elige por su simplicidad y compatibilidad. Sin embargo, su seguridad ha sido cuestionada en los últimos años debido a vulnerabilidades conocidas. Aunque puede ser rápido y fácil de configurar, se recomienda precaución al usar PPTP debido a sus limitaciones de seguridad.
- OpenVPN (Open Virtual Private Network): OpenVPN es un protocolo de código abierto que se destaca por su alto nivel de seguridad y flexibilidad. Utiliza tecnologías de cifrado sólidas y es altamente configurable, lo que lo convierte en una opción popular para aquellos que priorizan la seguridad y la privacidad en sus conexiones VPN. OpenVPN es compatible con una variedad de sistemas operativos y dispositivos, lo que lo hace versátil y ampliamente utilizado en entornos empresariales y domésticos por igual.
- IKEv2 (Internet Key Exchange versión 2): IKEv2 es un protocolo de intercambio de claves que se utiliza junto con IPsec para establecer conexiones VPN seguras. Es conocido por su capacidad para restablecer rápidamente la conexión en caso de pérdida de conectividad, lo que lo hace ideal para dispositivos móviles que cambian frecuentemente entre redes Wi-Fi y datos móviles. IKEv2 ofrece una combinación de seguridad y rendimiento, lo que lo convierte en una opción popular para usuarios que requieren conexiones VPN estables y confiables.

En conclusión, las VPN ofrecen una herramienta indispensable para garantizar la seguridad, la privacidad y la accesibilidad en el mundo digital actual. Con una amplia variedad de protocolos disponibles y opciones de configuración, las VPN permiten a los usuarios proteger sus datos mientras acceden a recursos en línea desde cualquier lugar del mundo. Ya sea para uso personal o empresarial, las VPN continúan desempeñando un papel crucial en la protección de la información confidencial y en la creación de conexiones seguras en Internet.

4.6. Respaldos - Limpieza de archivos

La importancia de los respaldos de información en la seguridad de los dispositivos no puede ser subestimada. Estas copias de seguridad ofrecen una red de seguridad vital que permite recuperarse de diversos contratiempos que puedan surgir en el mundo digital. Desde fallos de hardware que pueden dejar inoperativos a los dispositivos, hasta ataques de malware que cifra o eliminan datos, los respaldos son la salvaguarda contra la pérdida catastrófica de información.

Es fundamental prepararse para enfrentar estos escenarios, ya que la pérdida de información puede tener repercusiones que van desde mínimas hasta significativas, incluso con impacto económico. Por esta razón, contar con una estrategia robusta de respaldo permite reducir el impacto de tales eventualidades hasta el punto de que su efecto se minimiza considerablemente, e incluso se puede restaurar la normalidad sin apenas percibir el contratiempo.

Además de realizar respaldos, es recomendable cifrar los discos de los dispositivos donde se almacena información sensible. El cifrado protege tus datos, asegurando que, incluso si un atacante accede a tu dispositivo, no podrá leer la información sin la clave de cifrado. Esto añade una capa adicional de seguridad que es especialmente importante en caso de robo o pérdida del dispositivo.

Estos respaldos deben realizarse en algún medio de almacenamiento, como se observa en la figura 4.8, donde se muestran algunos de los más utilizados. Por esta razón, es importante tener en cuenta las siguientes consideraciones al momento de adquirir uno:

- Asegurarse de que el almacenamiento sea mayor al espacio ocupado por tus archivos actuales, para permitir el crecimiento futuro de tus datos.
- Si se opta por el almacenamiento en la nube, verificar si se requiere un plan de pago o si un plan gratuito satisface las necesidades de almacenamiento.
- Asegurarse de tener suficiente espacio físico para guardar el dispositivo de respaldo una vez completado el proceso.
- Utilizar el dispositivo únicamente para el respaldo de la información y evitar realizar más actividades en el almacenamiento para disminuir el riesgo de pérdida de datos.
- Verificar la velocidad de lectura/escritura del dispositivo para garantizar que no se demore más de lo necesario en guardar la información.
- Comparar los costos del almacenamiento con otros dispositivos o servicios que puedan ofrecer funcionalidades similares.
- Considerar la portabilidad del dispositivo si se planea guardarlo en un lugar diferente al del dispositivo principal o en un sitio externo.
- Asegurarse de que el dispositivo de respaldo sea compatible con la forma de conexión de los equipos de cómputo, especialmente en el caso de dispositivos como DVD o discos duros internos que requieren una conexión específica, como USB o SATA.
- Verificar la durabilidad y confiabilidad del medio de almacenamiento para garantizar que los datos estén protegidos contra posibles fallas o deterioro con el tiempo.

- Considerar la posibilidad de utilizar una combinación de almacenamiento local y en la nube para aumentar la redundancia y la seguridad de los datos.

Figura 4.8

Medios de almacenamiento.

***Nota:** La figura muestra diversos medios de almacenamiento, incluyendo disco duro portátil, DVD, USB, tarjeta SD, almacenamiento en la nube y disco duro interno. Autoría propia. Elaboración propia.*

Antes de realizar copias de seguridad, es crucial llevar a cabo una limpieza periódica de archivos en los dispositivos. En ocasiones, se almacena información no esencial o archivos basura, como cookies descargadas de sitios web, que ocupan espacio innecesario. AVG recomienda realizar esta limpieza al menos una vez cada seis meses. Aunque Windows realiza automáticamente una limpieza cada 30 días, eliminando principalmente cookies, no se debe depender únicamente de esta función automática. Es importante eliminar manualmente archivos como descargas que ya no son necesarias, así como aquellos que se hayan creado pero que ya no son relevantes.

Considerando estos aspectos, las copias de seguridad generadas ocuparan menos espacio y se almacenarán de forma más rápida. Además, se podrá gestionar la información de manera más efectiva en los dispositivos de red, facilitando la detección de posibles aplicaciones o archivos maliciosos. Esto se debe a que al reducir la cantidad de datos almacenados, el antivirus tendrá menos información que analizar, lo que aumentará la eficiencia de sus escaneos y mejorará la seguridad del sistema.

4.7. Ataques, amenazas y planes de contingencia

Según la definición de IBM, “un ataque se refiere a cualquier intento deliberado de sustraer, exponer, alterar, inhabilitar o destruir datos, aplicaciones u otros activos a través de un acceso no autorizado a una red, sistema informático o dispositivo digital”. Partiendo de esta premisa y lo explorado en el subtema de ″Triunvirato de la Seguridad″ sobre amenazas, se puede distinguir que las amenazas representan los posibles peligros o riesgos que acechan a los sistemas. Estas amenazas pueden provenir de diversas fuentes y adoptar múltiples formas, como malware, ingeniería social, o fallos de seguridad. Por otro lado, los ataques son las acciones específicas que se ejecutan con el objetivo de aprovechar estas amenazas para comprometer la seguridad de los sistemas. En resumen, mientras que las amenazas son los potenciales riesgos a los que nos enfrentamos, los ataques son los medios concretos mediante los cuales estos riesgos pueden materializarse y causar daño.

Principalmente, los atacantes tienen como objetivo perjudicar a las personas, ya sea económicamente o moralmente. Desde una perspectiva económica, muchos ataques buscan obtener beneficios monetarios directos, como el rescate en los casos de ransomware, donde los atacantes exigen un pago para restaurar el acceso a los archivos secuestrados. Por otro lado, desde una perspectiva moral, algunos atacantes pueden buscar dañar la reputación o el bienestar emocional de la víctima. Por ejemplo, al eliminar archivos valiosos, los atacantes esperan que la persona afectada se sienta obligada a intentar recuperarlos, generando estrés y ansiedad. Por lo que las motivaciones detrás de los ataques pueden variar, pero suelen estar vinculadas a obtener algún tipo de ventaja, ya sea económica o emocional, a expensas de la víctima.

Al igual que las amenazas, los ataques presentan una variedad de tipos y su nivel de peligro está determinado por la naturaleza de la acción que ejecutan. Este nivel de peligro se detalla en la tabla 4.8.

Tabla 4.8

Tipos de ataques

Tipo de Ataque	Descripción	Nivel de Peligro
Malware	El malware es un software malicioso que puede volver inutilizables a los sistemas infectados. Puede destruir datos, robar información o borrar archivos indispensables para el funcionamiento del sistema operativo. Se presenta en muchas formas, como troyanos, ransomware, scareware, spyware, rootkits y gusanos.	Alto
Ingeniería Social	Los ataques de ingeniería social manipulan a las personas para que realicen acciones no deseadas, como compartir información confidencial o descargar software malicioso. Incluyen phishing, spear phishing, whale phishing y estafas de vulneración de correo electrónico empresarial (BEC).	Alto
Ataques de Denegación del Servicio (DoS/DDoS)	Estos ataques inundan los recursos de un sistema con tráfico fraudulento, evitando respuestas a solicitudes legítimas y reduciendo la capacidad del sistema para funcionar. Pueden ser un fin en sí mismo o una distracción para otros ataques. Los DDoS, en particular, pueden ser llevados a cabo utilizando botnets, lo que aumenta su efectividad y dificulta su mitigación.	Alto
Cuenta Comprometida	Resultado de ataques en los que los hackers se apropian de la cuenta de un usuario legítimo para realizar actividades maliciosas. Pueden obtener credenciales a través de phishing, ataques de fuerza bruta o mediante el uso de herramientas para descifrar contraseñas.	Alto
Ataques de Intermediario	Un hacker intercepta secretamente las comunicaciones entre dos partes, lo que les permite leer, modificar o inyectar datos en tiempo real. Pueden llevarse a cabo a través de redes wifi no seguras o utilizando técnicas como el secuestro de sesiones.	Alto

Ataque a la Cadena de Suministro	Los hackers violan a una empresa dirigiendo sus ataques a sus proveedores de software, materiales u otros servicios. Esto les permite a los hackers acceder a múltiples objetivos a la vez, como se vio en el ataque a SolarWinds en 2020.	Muy Alto
Scripts en Sitios Cruzados (XSS)	Insertan código malicioso en páginas web o aplicaciones web legítimas, que se ejecutan en el navegador del usuario. Pueden robar información confidencial o redirigir al usuario a sitios maliciosos.	Medio
Inyección SQL	Envían comandos maliciosos a la base de datos de un sitio web o aplicación, permitiendo a los hackers acceder y robar datos confidenciales.	Alto
Tunelización del DNS	Ocultan tráfico malicioso dentro de paquetes DNS, eludiendo así medidas de seguridad y permitiendo a los hackers extraer datos o establecer conexiones entre el malware y un servidor de comando y control.	Alto
Ataques de Día Cero	Aprovechan vulnerabilidades no corregidas, lo que permite a los hackers lanzar ataques antes de que se desarrollen parches de seguridad.	Muy Alto
Ataques Sin Archivos	Utilizan vulnerabilidades en programas legítimos para inyectar código malicioso en la memoria de una computadora. Pueden cambiar configuraciones o robar contraseñas.	Alto
Falsificación del DNS	Editan registros de DNS para redirigir a los usuarios a sitios web maliciosos en lugar de los legítimos. Pueden robar datos o distribuir malware.	Alto

Nota: La tabla detalla los tipos de ataques cibernéticos, incluyendo malware, ingeniería social, ataques de denegación de servicio, cuentas comprometidas, ataques de intermediario, ataques a la cadena de suministro, scripts en sitios cruzados, inyección SQL, tunelización del DNS, ataques de día cero, ataques sin archivos y falsificación del DNS. Tomado de "Tipos de ataques cibernéticos", por IBM, 2023, https://www.ibm.com/mx-es/topics/cyber-attack#:~=Un%20ataque%20cibern%C3%A9tico%20es%20cualquier,sistema%20inform%C3%A1tico%20o%20dispositivo%20digital.

Considerando la distinción entre amenazas y ataques, es importante recordar que la seguridad absoluta al 100% no es alcanzable. Sin embargo, es posible implementar

medidas preventivas para mitigar el impacto de estos ataques o evitarlos por completo desde el principio.

4.7.1. Identificación de sitios fraudulentos

Uno de los primeros y más útiles métodos de defensa es aprender a identificar sitios web fraudulentos. Dado que gran parte de la actividad de los usuarios se centra en la navegación por la red, corren el riesgo de toparse con páginas web que intenten robar información personal o financiera, o que engañen con descargas gratuitas que, en realidad, pueden ser dañinas. Es esencial estar alerta a señales como URL sospechosas, certificados de seguridad ausentes, solicitudes inusuales de información personal o redirecciones constantes a otras páginas. Estar atentos a estos indicadores puede ayudar a evitar ser víctima de estafas en línea.

Considerando todo lo expuesto, se pueden tomar las siguientes medidas:

- Revisión del nombre de dominio: Esta es una medida muy sencilla de llevar a cabo. Cada vez que se accede a un sitio web, es crucial verificar si la URL coincide con la habitual. Las empresas no suelen cambiar su nombre de dominio de forma repentina y sin previo aviso. Se puede realizar esta comprobación de manera fácil al observar la URL en la barra de direcciones del navegador (como se observa en la Figura 4.9). Si se nota alguna discrepancia o si la URL es diferente de la conocida, es posible que se haya ingresado a un sitio creado por terceros con el propósito de suplantar la identidad del sitio oficial.

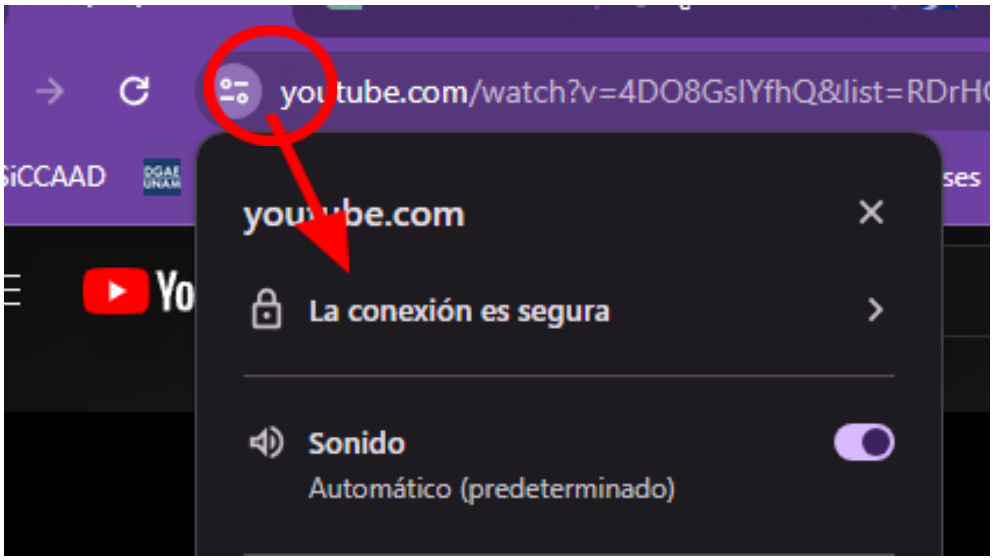
Figura 4.9

Sitio fraudulento.

Nota: La figura muestra la comparación entre un sitio web legítimo de Facebook y un sitio web fraudulento que imita su apariencia. La diferencia principal radica en la URL, que en el caso del sitio fraudulento no corresponde al dominio oficial de Facebook. Elaboración propia.

- Método de pago: La elección del método de pago dentro de un sitio web es crucial. Es recomendable evitar las operaciones bancarias directas, como depósitos o transferencias, ya que estas pueden dificultar la recuperación del dinero en caso de problemas. En su lugar, es preferible utilizar aplicaciones de pago intermedias que ofrezcan mayor seguridad y protección al consumidor. Ejemplos de estas aplicaciones incluyen Mercadopago o PayPal, las cuales actúan como intermediarios para mantener el dinero seguro hasta que se reciba el producto esperado. Además, es aconsejable limitar el tiempo que se pasa en aplicaciones bancarias o de pago para reducir la exposición a posibles ataques o fraudes. Al finalizar tus operaciones, cierra sesión y evita dejar aplicaciones abiertas innecesariamente, lo que puede ayudar a proteger tu información personal y financiera.
- Buscar en internet: Si estamos visitando un sitio por primera vez y no podemos verificar su URL, es prudente buscar el sitio en la web. Algunos sitios se dedican a recopilar listas de páginas web fraudulentas, lo que puede ayudar a determinar si el sitio en cuestión es legítimo o no. Una de las fuentes más confiables para esto es la proporcionada por el gobierno de México en el siguiente enlace: https://www.gob.mx/indep/documentos/sitios-apocrifos.
- Tener una conexión segura: Este método es uno de los más efectivos para verificar la autenticidad de un sitio web, ya que la mayoría de los sitios oficiales cuentan con certificaciones que garantizan su seguridad y cumplimiento de medidas de protección de datos. Se puede verificar esto fácilmente al observar la barra de direcciones del navegador y hacer clic en el icono de "más" como se muestra en la Figura 4.10. Si el sitio cuenta con esta certificación, veremos un icono de candado y el texto "La conexión es segura". Sin embargo, es importante tener en cuenta que estos certificados pueden expirar con el tiempo, por lo que el sitio puede tardar en renovar la verificación.

Figura 4.10
Conexión segura.



***Nota:** La figura muestra un ejemplo de una conexión segura en un navegador web, destacando el icono de candado y la indicación de que la conexión es segura. Elaboración propia.*

4.7.2. Identificación de aplicaciones con malware

Un malware es un software malicioso diseñado para dañar o infiltrarse en un sistema sin el consentimiento del usuario. A menudo, se disfraza como una aplicación legítima para engañar a los usuarios y lograr que la instalen. Por esta razón, es posible que se tenga malware en los dispositivos de la red sin ser conscientes de su presencia y resulta necesario saber o tener medidas de precaución contra estos.

Existen diferentes tipos de malware y Microsoft los ha clasificado en 14 tipos los cuales se pueden observar en la tabla 4.9:

Tabla 4.9
Tipos de malware

Tipo de malware	Descripción	Nivel de peligro
Backdoor	Un tipo de malware que proporciona a los hackers malintencionados acceso remoto y control del dispositivo.	Alto
Comando y control	Un tipo de malware que infecta el dispositivo y establece la comunicación con el servidor de comandos y control de	Alto

	los hackers para recibir instrucciones. Una vez establecida la comunicación, los hackers pueden enviar comandos que pueden robar datos, apagar y reiniciar el dispositivo e interrumpir los servicios web.	
Depositador	Un tipo de malware que descarga otro malware en el dispositivo. Debe conectarse a Internet para descargar archivos.	Moderado
Cuentagotas	Un tipo de malware que instala otros archivos de malware en el dispositivo. A diferencia de un descargador, un cuentagotas no tiene que conectarse a Internet para eliminar archivos malintencionados. Los archivos eliminados normalmente se insertan en el propio cuentagotas.	Moderado
Explotar	Un fragmento de código que usa vulnerabilidades de software para obtener acceso al dispositivo y realizar otras tareas, como instalar malware.	Alto
Hackeo-Herramienta	Un tipo de herramienta que se puede usar para obtener acceso no autorizado al dispositivo.	Alto
Virus de macro	Un tipo de malware que se propaga a través de documentos infectados, como Microsoft Word o documentos de Excel. El virus se ejecuta al abrir un documento infectado.	Moderado
Ofuscador	Un tipo de malware que oculta su código y propósito, lo que dificulta la detección o eliminación del software de seguridad.	Moderado
Roba contraseñas	Un tipo de malware que recopila su información personal, como nombres de usuario y contraseñas. A menudo funciona junto con un keylogger, que recopila y envía información sobre las teclas que presiona y sitios web que visita.	Alto
Ransomware	Un tipo de malware que cifra los archivos o realiza otras modificaciones que pueden impedir que se use el dispositivo. Luego, aparece una nota de rescate que indica	Muy Alto

	que debe pagar o realizar otras acciones para poder volver a usar el dispositivo.	
Software de seguridad no autorizado	Malware que pretende ser software de seguridad, pero no proporciona ninguna protección. Este tipo de malware suele mostrar alertas sobre amenazas inexistentes en el dispositivo. También intenta convencerle de que pague por sus servicios.	Moderado
Troyano	Un tipo de malware que intenta parecer inofensivo. A diferencia de un virus o un gusano, un troyano no se propaga por sí mismo. En su lugar, intenta parecer legítimo para engañar a los usuarios para que lo descarguen e instalen. Una vez instalados, los troyanos realizan diversas actividades malintencionadas, como robar información personal, descargar otro malware o dar acceso a los atacantes al dispositivo.	Moderado
Clicker Troyano	Un tipo de troyano que hace clic automáticamente en botones o controles similares en sitios web o aplicaciones. Los atacantes pueden usar este troyano para hacer clic en anuncios en línea. Estos clics pueden sesgar sondeos en línea u otros sistemas de seguimiento e incluso pueden instalar aplicaciones en el dispositivo.	Moderado
Gusano	Un tipo de malware que se propaga a otros dispositivos. Los gusanos pueden propagarse por correo electrónico, mensajería instantánea, plataformas de uso compartido de archivos, redes sociales, recursos compartidos de red y unidades extraíbles. Los gusanos más sofisticados aprovechan las vulnerabilidades de software para propagarse.	Alto

Nota: La tabla detalla los tipos de malware, incluyendo backdoor, comando y control, downloader, cuentagotas, explotar, hacktool, virus de macro, ofuscador y roba contraseñas. Tomado de "Microsoft Criteria for Classifying Malware", por Microsoft, 2023, https://learn.microsoft.com/es-es/microsoft-365/security/defender/criteria?view=o365-worldwide.

Como se puede observar, la gran mayoría de este malware intenta ocultarse para evitar ser eliminado. Por esta razón, es importante estar atentos a ciertos signos que pueden indicar la presencia de este tipo de aplicaciones en los dispositivos. Algunos de estos signos son los siguientes:

- Aparición de publicidad de forma espontánea en los dispositivos, sin estar dentro de una aplicación, o el aumento de esta dentro de aplicaciones que antes no la tenían.
- La duración de la batería del dispositivo es más corta de lo normal.
- El dispositivo se vuelve más lento de repente.
- El almacenamiento del dispositivo disminuye de forma inusual.
- El dispositivo se apaga de forma espontánea o se bloquea mientras se utiliza.
- La velocidad de la red es más lenta de lo normal debido al aumento del tráfico de datos del dispositivo.
- Algunos archivos empiezan a dañarse o eliminarse periódicamente.
- Aparecen nuevos archivos o carpetas que no fueron creados por el usuario.
- El dispositivo muestra un comportamiento inusual, como abrir aplicaciones o enviar mensajes sin que el usuario lo haya iniciado.
- Se detectan transacciones no autorizadas en cuentas bancarias o en plataformas de pago desde el dispositivo.
- La configuración del dispositivo cambia sin la intervención del usuario, como cambios en el fondo de pantalla, tonos de llamada o configuraciones de aplicaciones.
- Se experimentan problemas de rendimiento, como bloqueos frecuentes de aplicaciones o reinicios inesperados del dispositivo.
- Se reciben mensajes de texto o correos electrónicos sospechosos, especialmente con enlaces o archivos adjuntos desconocidos.
- La navegación por internet se redirige a sitios web no deseados o de dudosa reputación.
- Se observan actividades sospechosas en la red, como tráfico saliente inusualmente alto o conexiones a servidores desconocidos.

Si se sospecha que un dispositivo está infectado con malware 0 se quiere prevenir de futuras infecciones, se pueden tomar las siguientes medidas:

- Instalar y mantener actualizado un software antivirus: Utilizar un antivirus confiable y actualizado para detectar y eliminar malware.
- Actualizar regularmente el software: Mantener actualizado el sistema operativo y todas las aplicaciones para protegerse contra vulnerabilidades conocidas.
- Descargar aplicaciones solo de fuentes confiables: Utilizar tiendas de aplicaciones oficiales como Google Play Store o Apple App Store para descargar aplicaciones, ya que tienen políticas de seguridad más estrictas.
- Revisar regularmente las aplicaciones instaladas: Eliminar las aplicaciones que ya no se utilicen o que no se reconozcan para reducir el riesgo de malware.

- Utilizar contraseñas seguras: Crear contraseñas complejas y cambiarlas regularmente para proteger las cuentas en línea.
- Realizar copias de seguridad: Crear copias de seguridad de los datos importantes regularmente en caso de que el dispositivo se vea comprometido.
- Evitar hacer clic en enlaces o archivos adjuntos sospechosos: Mantenerse alerta ante correos electrónicos, mensajes o sitios web sospechosos y evitar hacer clic en enlaces o abrir archivos adjuntos no solicitados.
- Configurar el firewall: Utilizar un firewall para bloquear el tráfico no autorizado y proteger la red y el o los dispositivos.
- Educar sobre seguridad cibernética: Mantenerse informado sobre las últimas amenazas de seguridad y compartir buenas prácticas con amigos y familiares.
- Utilizar una red VPN: Para una capa adicional de seguridad en línea, considerar utilizar una red privada virtual (VPN) al conectarse a internet, especialmente en redes públicas.

5. IMPACTO AMBIENTAL

En la actualidad, el impacto ambiental de la tecnología es un tema de gran relevancia, y las redes de datos no son una excepción. A medida que estas redes se actualizan constantemente, es fundamental considerar la repercusión que tienen en el medio ambiente, desde el cableado estructurado hasta otros componentes. Es por esto que en México se han establecido diversas Normas Oficiales Mexicanas (NOMs) e implementado las normas ISO con el objetivo de reducir cada vez más el impacto ambiental de estas tecnologías. Estas normativas buscan regular el manejo adecuado de los desechos electrónicos, promover la eficiencia energética y fomentar prácticas sostenibles en la industria de las telecomunicaciones. Es importante seguir avanzando en la implementación de medidas que contribuyan a preservar nuestro entorno y promover un desarrollo tecnológico más sustentable.

5.1. Contaminación por uso de las redes

La infraestructura tecnológica, especialmente la instalación de redes domésticas, tiene un impacto ambiental significativo. A continuación se describen algunos aspectos clave relacionados con este impacto:

- Consumo de energía: Los dispositivos de red, como servidores, conmutadores, enrutadores y equipos de almacenamiento, consumen una cantidad considerable de energía eléctrica. Este consumo puede tener un impacto en la emisión de gases de efecto invernadero y afectar al cambio climático.
- Uso de recursos naturales: La fabricación de componentes de infraestructura tecnológica implica la extracción de recursos naturales, como minerales, metales y materiales plásticos. La extracción y procesamiento de estos recursos pueden tener consecuencias ambientales negativas, como la degradación del suelo, la contaminación del agua y la destrucción de ecosistemas.
- Generación de residuos electrónicos: Con el tiempo, los equipos de red se vuelven obsoletos y requieren ser reemplazados o actualizados. Esto genera una gran cantidad de residuos electrónicos, como cables, tarjetas de circuitos impresos y dispositivos de red entre otros. El manejo inadecuado de estos residuos puede resultar en la liberación de sustancias tóxicas al medio ambiente y causar contaminación del suelo y del agua.
- Refrigeración y gestión térmica: Los centros de datos y las salas de servidores requieren una refrigeración adecuada para mantener los equipos funcionando correctamente. Esto implica el uso de sistemas de aire acondicionado y refrigeración, que consumen grandes cantidades de energía y pueden tener un impacto significativo en las emisiones de gases de efecto invernadero.
- Huella de carbono: La infraestructura tecnológica contribuye a la huella de carbono de una organización debido al consumo de energía y las emisiones asociadas. Esto incluye las emisiones de CO2 provenientes de la generación de electricidad utilizada para alimentar los dispositivos de red y los sistemas de enfriamiento.
- Agotamiento de recursos hídricos: La infraestructura tecnológica, especialmente los centros de datos, requiere de grandes cantidades de agua para la refrigeración y otros fines operativos. El uso intensivo de agua puede agotar los recursos hídricos locales, especialmente en áreas propensas a la escasez de agua.
- Contaminación electromagnética: Las redes domésticas generan campos electromagnéticos que pueden tener efectos negativos en la salud humana y la vida silvestre. Si bien los estándares y regulaciones están en vigor para mitigar este impacto, es importante tenerlo en cuenta al diseñar y ubicar la infraestructura tecnológica.

- Impacto durante la fase de construcción: La construcción de infraestructura tecnológica, como centros de datos o torres de comunicación, puede implicar la deforestación de áreas naturales, la alteración de ecosistemas y la generación de residuos de construcción. Es necesario minimizar y mitigar estos impactos durante la fase de construcción.

Para mitigar el impacto ambiental de la infraestructura tecnológica, se pueden tomar diversas medidas:

- Eficiencia energética: Utilizar dispositivos de red con mayor eficiencia energética, como servidores y equipos de red con certificación energética, y optimizar la gestión del consumo de energía en los centros de datos.
- Virtualización y consolidación: Consolidar los servicios y aplicaciones en menos servidores físicos mediante la virtualización, reduce el consumo de energía y los requerimientos de hardware.
- Reciclaje y disposición adecuada de residuos electrónicos: Implementar programas de reciclaje y garantizar que los residuos electrónicos se gestionen de manera adecuada, cumpliendo con las regulaciones ambientales y evitando la contaminación.
- Uso de energías renovables: Transicionar hacia fuentes de energía renovables para alimentar los centros de datos y la infraestructura tecnológica, permite reducir las emisiones de gases de efecto invernadero.
- Diseño eficiente de centros de datos: Construir centros de datos con diseños eficientes en términos de energía y refrigeración, utilizando tecnologías como enfriamiento por agua o enfriamiento por inmersión líquida.
- Menor uso de recursos hídricos: Eficientar el uso del agua reutilizándola a través de procesos de enfriamiento, filtrado, limpieza y disposición en zonas de tratamiento y áreas verdes.
- Revisar especificaciones: Conocer las características de los equipos electrónicos e identificar las tecnologías integradas que cuidan al medio ambiente, así como las regulaciones de eficiencia para que el consumo de recursos de los equipos sea el óptimo.
- Aplicación de tecnologías verdes en la construcción: Utilizar materiales no tóxicos con el ambiente, biodegradables, materiales de reciclaje, permeables hacia el suelo y diseños arquitectónicos que permitan aprovechar la ventilación e iluminación natural.
- Ciclo de vida de los equipos: Además del impacto ambiental durante la fase de instalación y operación, es importante considerar el ciclo de vida completo de los equipos de infraestructura tecnológica. Esto incluye la extracción de materiales, la fabricación, el transporte y la eliminación adecuada de los equipos al final de su

vida útil. Es recomendable estar al pendiente de campañas de colecta de equipos electrónicos para su correcta disposición.

Es importante fomentar la conciencia y la educación ambiental entre los usuarios, usuarias y operadores de la infraestructura tecnológica ya que ayuda a promover prácticas más sostenibles y responsables. Esto incluye medidas como la optimización del uso de recursos, la adopción de políticas de reducción de residuos y el fomento de la responsabilidad ambiental en todas las etapas del ciclo de vida de las redes.
Asimismo, es indispensable destacar que la adopción de prácticas sostenibles y la consideración del impacto ambiental en la infraestructura tecnológica no solo son beneficiosas para el medio ambiente, sino también para la eficiencia operativa y la reducción de costos a largo plazo.

5.2. Consumo de energía

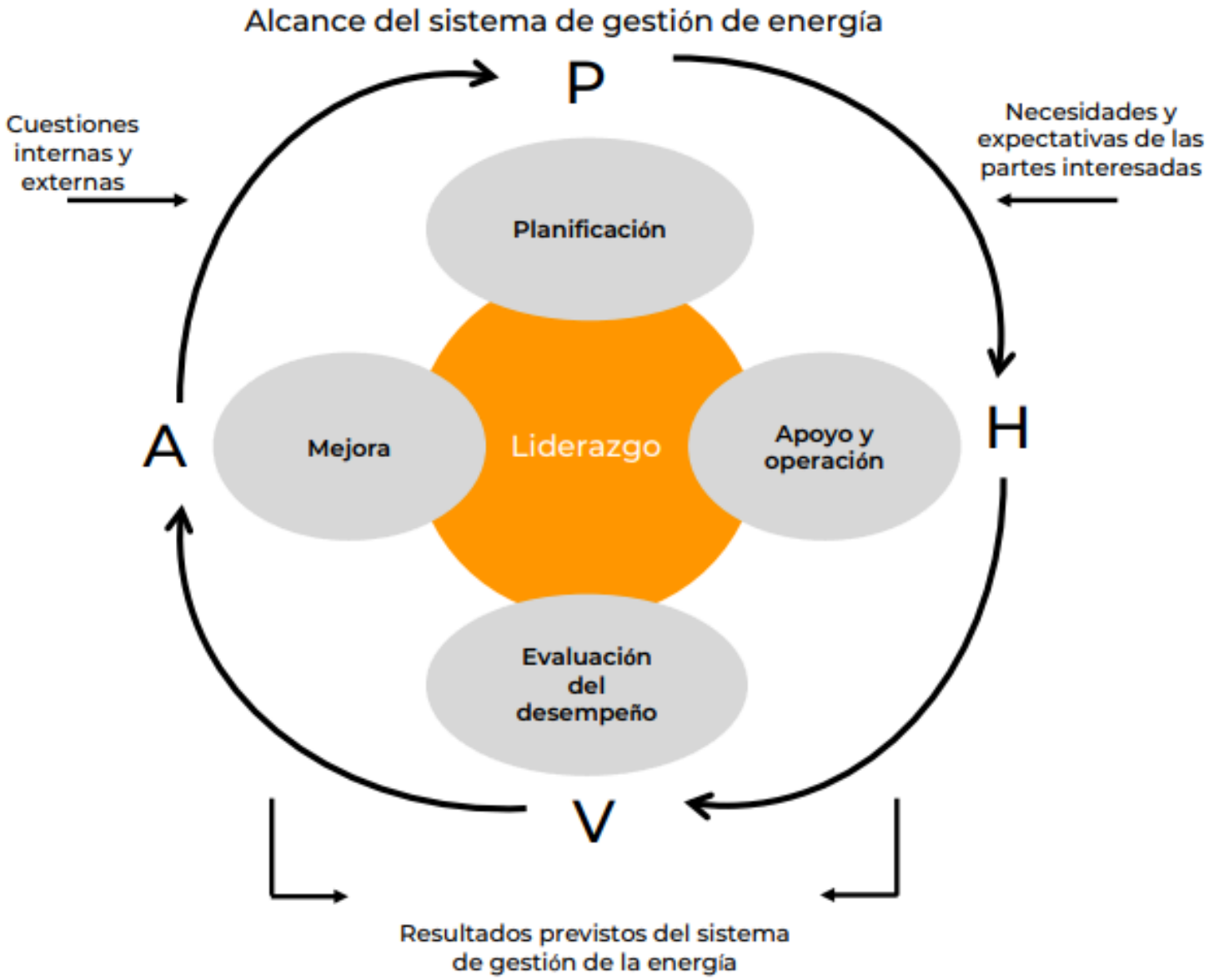
Las redes de datos demandan un alto consumo de energía debido a que están conformadas por dispositivos electrónicos como routers, servidores, computadoras, entre otros, que deben estar funcionando constantemente para garantizar el correcto funcionamiento de la red y evitar fallas. Para abordar este desafío, la norma ISO 50001 proporciona un sistema de gestión de energía que ayuda a las redes de datos a reducir significativamente sus costos operativos al optimizar el uso de la energía. Esto no solo beneficia económicamente a las empresas, sino que también contribuye a reducir su impacto en el consumo de recursos energéticos no renovables.

Algunas de las características principales de la ISO 50001 son:

- Establece un marco para que las organizaciones desarrollen políticas energéticas, establezcan objetivos y metas energéticas, y tomen acciones para mejorar su desempeño energético de manera continua.
- Se basa en el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PHVA) para garantizar que las organizaciones establezcan, implementen, mantengan y mejoren un sistema de gestión de energía eficaz. (Véase figura 5.1)

Figura 5.1

Ciclo de mejora continua.



***Nota:** La figura muestra el ciclo de mejora continua aplicado a un sistema de gestión de energía, destacando las fases de Planificación (P), Hacer (H), Verificación (V) y Actuar (A) junto con el liderazgo en el centro. Este ciclo, conocido como Ciclo PHVA o Ciclo de Deming, es una metodología que promueve la mejora continua en la eficiencia energética. Tomado de "Norma ISO 50001, la encargada del Sistema de Gestión Energética", por Restauración de Ecosistemas, 2023, https://www.restauraciondeecosistemas.com*

- Ayuda a las organizaciones a identificar y gestionar de manera proactiva los riesgos energéticos, incluidas las fluctuaciones de precios, la disponibilidad de recursos y los requisitos legales y reglamentarios.

- Facilita la integración con otros sistemas de gestión, como ISO 9001 (gestión de la calidad) e ISO 14001 (gestión ambiental), para una gestión más eficaz y coherente de los aspectos energéticos.
- Proporciona un marco para la mejora de la eficiencia energética en todos los aspectos de las operaciones de una organización, desde la planificación y el diseño hasta la operación y el mantenimiento.
- Promueve la cultura de la eficiencia energética y la sensibilización del personal en todos los niveles de la organización, involucrando a todos los empleados en la mejora del desempeño energético.
- Permite a las organizaciones demostrar su compromiso con la sostenibilidad y la responsabilidad social corporativa al reducir su impacto ambiental y mejorar su eficiencia operativa.

Aunque está principalmente pensado para empresas se pueden aplicar algunos de estos puntos para mejorar la eficiencia energética en las redes domésticas, como el ciclo de mejora continua, también conocido como el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Este enfoque permite identificar oportunidades de mejora y aplicar medidas que reduzcan el consumo de energía y los costos asociados.

- En la etapa de Planificar, es necesario establecer objetivos claros de eficiencia energética para la red, como reducir el consumo de energía de los dispositivos conectados. Se deben identificar también los puntos de mayor consumo y planificar acciones específicas para mejorar la eficiencia.
- En la etapa de Hacer, se implementan las medidas planificadas, como apagar dispositivos cuando no se están utilizando, utilizar dispositivos con certificación energética eficiente, o programar tiempos de uso para optimizar el consumo.
- En la etapa de Verificar, se monitorea el consumo de energía de la red del hogar para asegurarse de que las medidas implementadas están teniendo el efecto deseado. Se pueden utilizar dispositivos de medición de energía o herramientas de monitoreo en línea para este fin.
- Finalmente, en la etapa de Actuar, se evalúan los resultados obtenidos y se toman decisiones para mejorar aún más la eficiencia energética de la red del hogar. Podemos ajustar lo realizado, establecer nuevos objetivos y continuar el ciclo de mejora continua para seguir reduciendo nuestro impacto ambiental y nuestros costos energéticos.

5.3. Deterioro de las redes

El deterioro de las redes es un proceso constante, impulsado por avances en tecnologías de transmisión de datos y mejoras en seguridad. Por esta razón, es crucial considerar desde el principio el uso previsto para nuestra red y si se planea expandirse en un futuro cercano.

Es fundamental que la red sea diseñada con una visión a largo plazo, ya que según las normas ISO/IEC, se espera que una red bien planificada tenga una vida útil de al menos 10 años.

Para asegurar la durabilidad y eficacia de la red, es esencial seguir las mejores prácticas de diseño y gestión de redes. Esto incluye la selección de equipos y tecnologías adecuadas, la implementación de medidas de seguridad robustas y la planificación de la capacidad y escalabilidad de la red para adaptarse a futuras necesidades.

Algunos puntos clave para prevenir el deterioro rápido de una red son:

- Selección de cableado: Utilizar cableado de categoría 6 (Cat 6) o superior, que proporciona mayor ancho de banda y capacidad de transmisión, asegurando un rendimiento óptimo y una vida útil más larga para la red.
- Equipos de red de calidad: Utilizar equipos de red de alta calidad y fiabilidad, que cumplan con los estándares actuales y tengan capacidad para soportar futuras tecnologías y demandas de tráfico de datos.
- Planificación de la capacidad: Diseñar la red con suficiente capacidad para manejar el tráfico actual y futuro, evitando congestiones y asegurando un rendimiento constante.
- Seguridad de red: Implementar medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones y políticas de acceso seguro, para proteger la red contra amenazas externas e internas.
- Actualizaciones regulares: Mantener actualizados los equipos y software de la red para aprovechar las últimas tecnologías y parches de seguridad, garantizando un funcionamiento óptimo y protegido.
- Monitoreo y mantenimiento: Realizar un monitoreo regular de la red para identificar posibles problemas o puntos de congestión, y llevar a cabo mantenimiento preventivo para evitar fallos y garantizar un funcionamiento eficiente.

Además, es importante realizar mantenimiento regular y actualizaciones según sea necesario para mantener la funcionalidad y seguridad de la red a lo largo del tiempo. Una red bien mantenida y diseñada con visión de futuro no solo garantiza un rendimiento óptimo, sino que también reduce los costos y el impacto ambiental asociados con cambios frecuentes o actualizaciones innecesarias.

5.4. Tiempo de vida de los dispositivos

Una red generalmente se espera que dure al menos 10 años, por lo que es importante seleccionar dispositivos que puedan mantenerse operativos durante este período. Sin

embargo, esto no siempre es posible, ya que los dispositivos pueden experimentar degradación con el uso o tener problemas de compatibilidad y seguridad debido a la falta de mantenimiento del software por parte del proveedor. Cuando esto sucede, se denomina "obsolescencia técnica". Además, los fabricantes a veces lanzan actualizaciones que limitan el funcionamiento de los dispositivos existentes para fomentar la compra de nuevos dispositivos, a lo que se conoce como "obsolescencia programada".

Cuando un dispositivo llega al final de su vida útil debido a estos problemas, se considera que ha concluido su "fase de uso". Este escenario puede resultar en gastos innecesarios para la organización u hogar, ya que se requiere la adquisición de nuevos dispositivos para reemplazar los obsoletos. Por esta razón, una vez que el usuario ya no necesita el dispositivo, es importante limpiar sus datos, es decir, restaurar el dispositivo a los valores de fábrica, para proteger la seguridad y la confidencialidad de la información. Una vez hecho esto, se pueden considerar las siguientes opciones:

- Verificar con el fabricante si ofrece algún programa de reciclaje de dispositivos para devolverlo.
- Donar o vender el dispositivo a una organización que pueda reacondicionarlo.
- Buscar una organización cercana que se dedique al reciclaje de aparatos electrónicos, para recuperar materiales y partes que aún puedan funcionar, y desechar correctamente la basura electrónica.

En cuanto al módem que se encuentra dentro de un hogar es un componente esencial de la red doméstica. Con el tiempo, este dispositivo experimenta desgaste y su rendimiento tiende a disminuir, lo que puede manifestarse en fallas como apagones intermitentes o una calidad de conexión reducida. Por esta razón, se recomienda considerar su reemplazo cada 4 o 5 años. (Estar al pendiente de programas de actualización del proveedor de servicios) .

Aunque el módem parezca estar funcionando correctamente, es crucial tener en cuenta los siguientes puntos:

- Actualizaciones de firmware: Verificar que el módem continúe recibiendo actualizaciones por parte del fabricante es fundamental en el mundo de la tecnología. Las actualizaciones de seguridad son especialmente importantes para proteger la red contra nuevas amenazas y vulnerabilidades. Un módem desactualizado puede dejar la red expuesta a riesgos de seguridad.
- Adopción de nuevas tecnologías: Los módems más recientes suelen integrar nuevas tecnologías que pueden mejorar significativamente la experiencia de conexión. Estos dispositivos pueden ofrecer rangos de conexión más amplios, velocidades de transferencia más rápidas y una mejor estabilidad de la red. Al actualizar el módem,

se pueden aprovechar estas mejoras y garantizar que la red esté preparada para satisfacer las crecientes demandas de conectividad en el futuro.

- Compatibilidad con estándares emergentes: Con la evolución de las tecnologías de red, suelen surgir nuevos estándares y protocolos para mejorar el rendimiento y la seguridad. Al adquirir un nuevo módem, es importante asegurarse de que sea compatible con los estándares más recientes, como el Wi-Fi 6, para garantizar una conectividad óptima y estar preparados para futuras actualizaciones.
- Rendimiento y estabilidad: Aunque el módem pueda seguir funcionando, es posible que no esté aprovechando al máximo las capacidades de la conexión a Internet. Los módems más antiguos pueden limitar la velocidad y la estabilidad de la red, especialmente en entornos donde se utilizan múltiples dispositivos simultáneamente. Actualizar a un módem más nuevo puede mejorar significativamente el rendimiento de la red doméstica y proporcionar una experiencia de usuario más fluida.

Al considerar el reemplazo del módem cada cierto tiempo, se puede garantizar una conectividad confiable, segura y eficiente en el hogar, adaptada a las demandas actuales y futuras de conectividad.

5.5. Recomendaciones para aumentar la vida útil de los dispositivos de red

La eficacia de una red depende en gran medida de dispositivos clave como routers, módems, switches y computadoras. Por tanto, es fundamental cuidarlos adecuadamente para prolongar su vida útil y evitar gastos innecesarios en reparaciones o reemplazos. A continuación, se presentan algunas recomendaciones para lograr este objetivo:

- Limpieza continua: Es crucial para mantener el dispositivo funcionando correctamente. El polvo puede obstruir las rejillas de ventilación, impidiendo que el dispositivo reciba la ventilación adecuada. Además, el polvo puede acumularse en los ventiladores, haciendo que se vuelvan más pesados y reduciendo su velocidad de giro.
- Monitoreo de temperaturas: Es complementario a la limpieza. Permite detectar si el dispositivo necesita limpieza o si el lugar donde está ubicado no tiene la ventilación adecuada. Por ejemplo, si el dispositivo se encuentra en un lugar cerrado donde el aire no circula correctamente, es probable que se sobrecaliente con el tiempo, incluso si está limpio.
- Actualizaciones de software y firmware: Son esenciales para prevenir la explotación de vulnerabilidades por parte de atacantes o errores que puedan dejar el dispositivo inutilizable. Mantener actualizado el software garantiza un funcionamiento óptimo del dispositivo.

- Apagado correcto del dispositivo: Es fundamental para evitar daños al dispositivo. Desenchufar los dispositivos de la corriente o presionar el botón de apagado mientras están en funcionamiento puede interrumpir las operaciones, causando daños en los archivos o en el sistema. Utilizar un no break proporciona unos minutos adicionales de energía en caso de cortes de luz, permitiendo apagar los equipos adecuadamente.
- Protector contra sobretensiones: Ayuda a proteger los dispositivos en caso de aumentos de tensión eléctrica, evitando daños en los componentes internos del dispositivo.
- Realizar un tendido de cable óptimo: Es esencial para evitar daños en la conexión de los dispositivos con la red. El cableado no debe estar tirado por el suelo ni pasar por lugares húmedos, y debe estar fuera del alcance de mascotas, ya que esto puede dañar los cables y afectar la conexión. Utiliza canaletas o tubos de protección para guiar y organizar los cables, evitando enredos y reduciendo el riesgo de daño físico. Además, asegúrate de que los cables no estén estirados ni tensos, ya que esto puede comprometer su integridad y causar desconexiones o fallas en la señal. Un tendido adecuado no solo mejora la estética del espacio, sino que también garantiza un rendimiento óptimo y una mayor durabilidad de la infraestructura de red.

- Mantenimiento preventivo: Realizar un mantenimiento regular puede ayudar a detectar problemas antes de que se conviertan en fallas importantes. Esto incluye la verificación de conexiones sueltas y la inspección visual de posibles daños.
- Respaldo de datos: Realizar copias de seguridad periódicas de los datos almacenados en los dispositivos ayuda a proteger la información en caso de fallas o problemas con los dispositivos. Se recomienda utilizar servicios de almacenamiento en la nube o dispositivos de almacenamiento externo para respaldar los datos de forma segura.
- Protección contra malware: Utilizar programas de antivirus y antimalware actualizados ayuda a proteger los dispositivos de posibles amenazas en línea que puedan comprometer su funcionamiento. Es importante realizar escaneos periódicos para detectar y eliminar cualquier software malicioso.
- Optimización de la configuración: Ajustar la configuración de los dispositivos para que se adapten mejor a las necesidades de la red puede mejorar su rendimiento y prolongar su vida útil. Esto incluye configurar correctamente la calidad de servicio (QoS) para priorizar el tráfico de red y evitar la congestión.
- Reemplazo de componentes defectuosos: Si se detecta algún componente defectuoso en un dispositivo, es importante reemplazarlo de inmediato para evitar daños adicionales al dispositivo y a la red en general. Es recomendable utilizar

componentes de repuesto originales o de alta calidad para garantizar un funcionamiento óptimo.

- Traslado de equipo: Al mover dispositivos electrónicos, es fundamental hacerlo con cuidado para evitar daños. Antes de trasladar cualquier equipo, asegúrate de apagarlo correctamente y desconectar todos los cables para evitar cortocircuitos o daños por movimientos bruscos. Utiliza cajas de transporte adecuadas, preferiblemente con material de acolchado, para proteger los dispositivos de golpes o caídas. Si es posible, mantén los dispositivos en posición vertical y evita apilarlos, ya que esto puede causar daños a componentes internos. Además, si se trata de equipos sensibles como discos duros, asegúrate de que sean manejados con especial cuidado, ya que son más vulnerables a daños físicos. Realizar un inventario de los equipos antes y después del traslado te ayudará a asegurarte de que todo ha llegado en buen estado.

Al seguir estas recomendaciones, se puede prolongar la vida útil de los dispositivos de red y garantizar un funcionamiento eficiente de la red en general.

5.6. Actualización de las redes

Como se ha mencionado previamente, la vida útil de los equipos es de alrededor de 5 años tras los cuales es recomendable cambiar el equipo. Durante este tiempo, mucho del software involucrado en el manejo y consumo de la red pasa a través de diversos cambios y correcciones enfocados en mejorar la experiencia durante su uso y la seguridad que ofrecen, así como adaptación a nuevas políticas y estándares de calidad, por lo que es necesario mantener todas estas aplicaciones y sistemas actualizadas para mantener los dispositivos de cómputo en óptimas condiciones.

Sin embargo es importante tomar en cuenta el estado en el que los equipos operan, ya que muchas veces las actualizaciones dejan de tener retrocompatibilidad con otros programas o son de una beta inestable, lo que puede entorpecer las actividades realizadas en internet. Por ello se recomienda tener un historial de versiones y conocer los ajustes en los que el software funciona apropiadamente según las necesidades del usuario.

También se debe considerar el espacio disponible de almacenamiento para las nuevas actualizaciones y los recursos de operación que tienen los equipos ya que las actualizaciones tienden a requerir mayor capacidad de procesamiento, lo que puede exigir demasiado para los equipos con mayor antigüedad y en varios casos provoca que el equipo se sobrecaliente causando fallas hasta la pérdida total del equipo.

5.7. Gestión de Residuos : Reparación y Reciclaje

La constante actualización de las redes de datos genera una gran cantidad de equipos electrónicos que deben ser desechados. En México, se estableció la Norma Oficial Mexicana NOM-161-SEMARNAT-2011, la cual es definida por la secretaría de medio ambiente y recursos naturales como los criterios para clasificar los residuos como manejo especial y determina cuáles están sujetos a un plan de manejo. Esta norma también establece el listado de dichos residuos, el procedimiento para su inclusión o exclusión en el listado, así como los elementos y procedimientos para la formulación de los planes de manejo.

Dentro de esta norma se encuentra el Plan de Manejo de Residuos de Aparatos Electrónicos y Eléctricos (RAEE), donde los residuos eléctricos y electrónicos considerados dentro del plan están clasificados en tres grupos, los cuales son:

a) Residuos tecnológicos de las industrias de la informática y fabricantes de productos electrónicos:
    - Computadoras personales de escritorio y sus accesorios.
    - Computadoras personales portátiles y sus accesorios.
    - Teléfonos celulares.
    - Monitores con tubos de rayos catódicos (incluyendo televisores).
    - Pantallas de cristal líquido y plasma (incluyendo televisores).
    - Reproductores de audio y video portátiles.
    - Cables para equipos electrónicos.
    - Impresoras, fotocopiadoras y multifuncionales.
b) Residuos de fabricantes de vehículos automotores:
    - Vehículos al final de su vida útil.
c) Otros que al transcurrir su vida útil requieren de un manejo específico y que sean generados en una cantidad mayor a 10 toneladas por año y por residuo:
    - Refrigeradores.
    - Aires acondicionados.
    - Lavadoras.
    - Secadoras.
    - Hornos de microondas.

Para el reciclaje en las redes de datos, se deben tener en cuenta especialmente los siguientes puntos de la RAEE:

- Computadoras personales de escritorio y portátiles, así como sus accesorios, debido a la rápida obsolescencia y la constante renovación de equipos en entornos informáticos.

- Teléfonos celulares, dado el alto índice de renovación de dispositivos en el mercado y la necesidad de gestionar adecuadamente los componentes electrónicos.
- Monitores con tubos de rayos catódicos y pantallas de cristal líquido y plasma, ya que estos dispositivos representan una parte significativa de los residuos electrónicos y requieren un tratamiento especializado debido a sus componentes.
- Impresoras, fotocopiadoras y multifuncionales, que son dispositivos comunes en entornos de redes de datos y pueden generar una cantidad considerable de residuos tecnológicos.
- Cables para equipos electrónicos, que suelen acumularse en entornos de redes de datos y pueden ser reciclados para recuperar materiales como el cobre.

Estos puntos son importantes para el reciclaje en las redes de datos debido a la frecuencia con la que se reemplazan estos dispositivos y la necesidad de gestionar adecuadamente los residuos tecnológicos para reducir el impacto ambiental. Dentro de esta norma se incluyen diversos aspectos relacionados con el reciclaje de estos dispositivos. Algunos de los puntos importantes que se abordan en esta normativa son:

- Clasificación de los residuos: La normativa establece los criterios para identificar qué residuos se consideran de manejo especial, es decir, aquellos que requieren un tratamiento específico debido a su composición o peligrosidad. Esto permite diferenciarlos de otros tipos de residuos y gestionarlos de manera adecuada.
- Listado de residuos: Se incluye un listado detallado de los dispositivos eléctricos y electrónicos que están sujetos al plan de manejo de RAEE. Esto proporciona claridad sobre qué productos deben ser gestionados de acuerdo con la normativa.
- Procedimiento de inclusión o exclusión: La norma establece un procedimiento claro y transparente para incluir o excluir residuos del listado establecido. Esto garantiza que la lista se mantenga actualizada y se ajuste a las necesidades y avances tecnológicos.
- Formulación de planes de manejo: Define los elementos que deben incluirse en los planes de manejo de los RAEE, como objetivos, acciones a realizar, responsabilidades, recursos necesarios y mecanismos de evaluación. Esto permite una gestión integral y efectiva de los residuos, asegurando su adecuado tratamiento y disposición final.

Estos aspectos son fundamentales para establecer un marco regulatorio sólido que promueva la correcta gestión de los residuos electrónicos en México, garantizando la protección del medio ambiente y la salud de la población.

6. Manual Medidas de protección digital en redes de datos

Este manual se realiza para dar a conocer diversas configuraciones aplicables a casi todos los dispositivos de cómputo que se utilizan diariamente a fin de dar herramientas que las personas con poco conocimiento de redes puedan aplicar medidas de seguridad funcionales en sus dispositivos y con ello mejorar la operación de los mismos

Manual
Medidas de protección digital en redes de datos

Guía práctica para usuarios sin conocimientos previos

Elaborado por:
Angel David Rea Aparicio
Diego Jair Crisantos Martinez
27/05/2024
Version: 1.0

Índice

6.0. Introducción....134
6.1. Cómo encontrar la dirección IP de tu dispositivo....135
6.2. Creación de contraseñas seguras....149
6.3. Almacenamiento seguro de contraseñas....153
6.4. Cómo cambiar la contraseña del módem telmex....163
6.5. Cómo configurar IP Estática en tu Módem Telmex....174
6.6. Cómo configurar una VPN en tu Módem....184
6.7. Cómo actualizar mi sistema operativo....192
6.8. Limpieza de archivos en Windows....210
6.9. Cómo crear una copia de seguridad con Windows....233
6.10. Cómo Identificar Correos Electrónicos con malware....250
6.11. Verificar qué dispositivos están conectados a un módem Telmex....266
6.12. Manejo Seguro de Información Personal en Redes Sociales....275
6.13. Manejo Seguro de Información Personal en Línea....278
6.14. Recomendaciones....282

Índice de figuras

6.0. Introducción..... 134
6.1. Cómo encontrar la dirección IP de tu dispositivo..... 135
Figura 6.1 Dirección IP en Windows paso 1..... 137
Figura 6.2 Dirección IP en Windows paso 2..... 138
Figura 6.3 Dirección ip en Windows paso 3..... 139
Figura 6.4 Dirección ip en Windows paso 4..... 140
Figura 6.5 Dirección ip en Windows paso 5..... 141
Figura 6.6 Dirección ip en samsung paso 1..... 142
Figura 6.7 Dirección ip en samsung paso 2..... 142
Figura 6.8 Dirección ip en samsung paso 3..... 143
Figura 6.9 Dirección ip en samsung paso 4..... 143
Figura 6.10 Dirección ip en samsung paso 5..... 144
Figura 6.11 Dirección ip en motorola paso 1..... 145
Figura 6.12 Dirección ip en motorola paso 2..... 145
Figura 6.13 Dirección ip en motorola paso 3..... 146
Figura 6.14 Dirección ip en motorola paso 4..... 146
Figura 6.15 Dirección ip en motorola paso 5..... 147
6.2. Creación de contraseñas seguras..... 149
6.3. Almacenamiento seguro de contraseñas..... 153
Figura 6.16 LastPass paso 1..... 154
Figura 6.17 LastPass paso 2..... 155
Figura 6.18 LastPass paso 3..... 156
Figura 6.19 LastPass paso 4..... 156
Figura 6.20 LastPass paso 5..... 157
Figura 6.21 LastPass paso 6..... 158
Figura 6.22 LastPass paso 7..... 159
Figura 6.23 LastPass paso 8..... 160
Figura 6.24 LastPass paso 9..... 161
6.4. Cómo cambiar la contraseña del módem telmex..... 163
Figura 6.25 Cambiar contraseña modem telmex paso 1..... 164
Figura 6.26 Cambiar contraseña modem Telmex paso 2..... 165
Figura 6.27 Cambiar contraseña modem telmex paso 3..... 166
Figura 6.28 Cambiar contraseña modem telmex paso 4..... 167
Figura 6.29 Cambiar contraseña modem telmex paso 5..... 168
Figura 6.30 Cambiar contraseña modem telmex paso 6..... 169

Figura 6.31 Cambiar contraseña modem Telmex paso 7..... 170
Figura 6.32 Cambiar contraseña modem Telmex paso 8..... 171
Figura 6.33 Cambiar contraseña modem Telmex paso 9.....172
6.5. Cómo configurar IP Estática en tu Módem Telmex.....174
Figura 6.34 Cambiar contraseña modem Telmex paso 1..... 176
Figura 6.35 Cambiar contraseña modem Telmex paso 2.....177
Figura 6.36 Cambiar contraseña modem Telmex paso 3.....178
Figura 6.37 Cambiar contraseña modem Telmex paso 4.....179
Figura 6.38 Cambiar contraseña modem Telmex paso 5..... 180
Figura 6.39 Cambiar contraseña modem Telmex paso 6..... 181
Figura 6.40 Cambiar contraseña modem Telmex paso 7..... 182
Figura 6.41 Cambiar contraseña modem Telmex paso 8..... 182
Figura 6.42 Cambiar contraseña modem Telmex paso 9.....183
6.6. Cómo configurar una VPN en tu Módem.....184
Figura 6.43 Configurar una VPN en tu módem paso 1.....185
Figura 6.44 Configurar una VPN en tu módem paso 2..... 186
Figura 6.45 Configurar una VPN en tu módem paso 3..... 187
Figura 6.46 Configurar una VPN en tu módem paso 4..... 188
Figura 6.47 Configurar una VPN en tu módem paso 5.....189
Figura 6.48 Configurar una VPN en tu módem paso 6..... 190
6.7. Cómo actualizar mi sistema operativo..... 192
Figura 6.49 Actualización de sistema operativo Windows paso 1.....194
Figura 6.50 Actualización de sistema operativo Windows paso 2..... 195
Figura 6.51 Actualización de sistema operativo Windows paso 3..... 196
Figura 6.52 Actualización de sistema operativo Windows paso 4.....197
Figura 6.53 Actualización de sistema operativo Windows paso 5.....198
Figura 6.54 Actualización de sistema operativo Windows paso 6..... 199
Figura 6.55 Actualización de sistema operativo Windows paso 7..... 200
Figura 6.56 Actualización de sistema operativo Windows paso 8..... 201
Figura 6.57 Actualización de sistema operativo samsung paso 1.....202
Figura 6.58 Actualización de sistema operativo samsung paso 2..... 202
Figura 6.59 Actualización de sistema operativo samsung paso 3..... 203
Figura 6.60 Actualización de sistema operativo samsung paso 4.....203
Figura 6.61 Actualización de sistema operativo samsung paso 5.....204
Figura 6.62 Actualización de sistema operativo samsung paso 6.....204
Figura 6.63 Actualización de sistema operativo samsung paso 7..... 205
Figura 6.64 Actualización de sistema operativo motorola paso 1..... 206
Figura 6.65 Actualización de sistema operativo motorola paso 2.....206

Figura 6.66 Actualización de sistema operativo motorola paso 4.....207
Figura 6.67 Actualización de sistema operativo motorola paso 5.....207
Figura 6.68 Actualización de sistema operativo motorola paso 6.....208
Figura 6.69 Actualización de sistema operativo motorola paso 7.....208
6.8. Limpieza de archivos en Windows.....210
Figura 6.70 Limpieza de archivos temporales paso 1.....212
Figura 6.71 Limpieza de archivos temporales paso 2.....213
Figura 6.72 Limpieza de archivos temporales paso 3.....214
Figura 6.73 Limpieza de archivos temporales paso 4.....215
Figura 6.74 Limpieza de archivos temporales paso 5.....216
Figura 6.75 Liberar espacio en disco paso 1.....217
Figura 6.76 Liberar espacio en disco paso 2.....218
Figura 6.77 Liberar espacio en disco paso 3.....219
Figura 6.78 Liberar espacio en disco paso 4.....220
Figura 6.79 Liberar espacio en disco paso 5.....221
Figura 6.80 Liberar espacio en disco paso 6.....222
Figura 6.81 Desinstalar programas innecesarios paso 1.....223
Figura 6.82 Desinstalar programas innecesarios paso 2.....224
Figura 6.83 Desinstalar programas innecesarios paso 3.....225
Figura 6.84 Desinstalar programas innecesarios paso 4.....226
Figura 6.85 Desinstalar programas innecesarios paso 5.....227
Figura 6.86 Desinstalar programas innecesarios paso 6.....228
Figura 6.87 Herramienta para limpieza de disco paso 1.....229
Figura 6.88 Herramienta para limpieza de disco paso 2.....230
Figura 6.89 Herramienta para limpieza de disco paso 3.....231
Figura 6.90 Herramienta para limpieza de disco paso 4.....232
6.9. Cómo crear una copia de seguridad con Windows.....233
Figura 6.91 Copia de seguridad con Windows paso 1.....234
Figura 6.92 Copia de seguridad con Windows paso 2.....235
Figura 6.93 Copia de seguridad con Windows paso 3.....236
Figura 6.94 Copia de seguridad con Windows paso 4.....237
Figura 6.95 Copia de seguridad con Windows paso 5.....238
Figura 6.96 Copia de seguridad con Windows paso 6.....239
Figura 6.97 Copia de seguridad con Windows paso 7.....240
Figura 6.98 Copia de seguridad con Windows paso 8.....241
Figura 6.99 Copia de seguridad con Windows paso 9.....242
Figura 6.100 Copia de seguridad con Windows paso 10.....243
Figura 6.101 Copia de seguridad con Windows paso 11.....244

Figura 6.102 Copia de seguridad con Windows paso 12..... 245
Figura 6.103 Copia de seguridad con Windows paso 13..... 246
Figura 6.104 Copia de seguridad con Windows paso 14..... 247
Figura 6.105 Copia de seguridad con Windows paso 15..... 248
6.10. Cómo Identificar Correos Electrónicos con malware..... 250
Figura 6.106 verificar remitente..... 251
Figura 6.107 Correo con remitente correcto..... 252
Figura 6.108 Correo con remitente incorrecto..... 253
Figura 6.109 Correo con nombre real..... 254
Figura 6.110 Correo sin nombre..... 255
Figura 6.111 Correo con nombre del e-mail..... 256
Figura 6.112 Correo sin errores..... 257
Figura 6.113 Correo con errores gramaticales..... 258
Figura 6.114 Correo con URL correcta..... 259
Figura 6.115 Correo con URL falsa..... 260
Figura 6.116 Correo con archivos maliciosos..... 261
Figura 6.117 Correo de urgencia..... 262
Figura 6.118 Correo con datos reales..... 263
Figura 6.119 Correo con información genérica..... 264
6.11. Verificar qué dispositivos están conectados a un módem Telmex..... 266
Figura 6.120 Dispositivos conectados a mi red paso 1..... 267
Figura 6.121 Dispositivos conectados a mi red paso 2..... 268
Figura 6.122 Dispositivos conectados a mi red paso 3..... 269
Figura 6.123 Dispositivos conectados a mi red paso 4..... 270
Figura 6.124 Dispositivos conectados a mi red paso 5..... 271
Figura 6.125 Dispositivos conectados a mi red paso 6..... 272
Figura 6.126 Dispositivos conectados a mi red paso 7..... 273
6.12. Manejo Seguro de Información Personal en Redes Sociales..... 275
6.13. Manejo Seguro de Información Personal en Línea..... 278
Figura 6.127 Conexión segura..... 280
6.14. Recomendaciones..... 282

Introducción

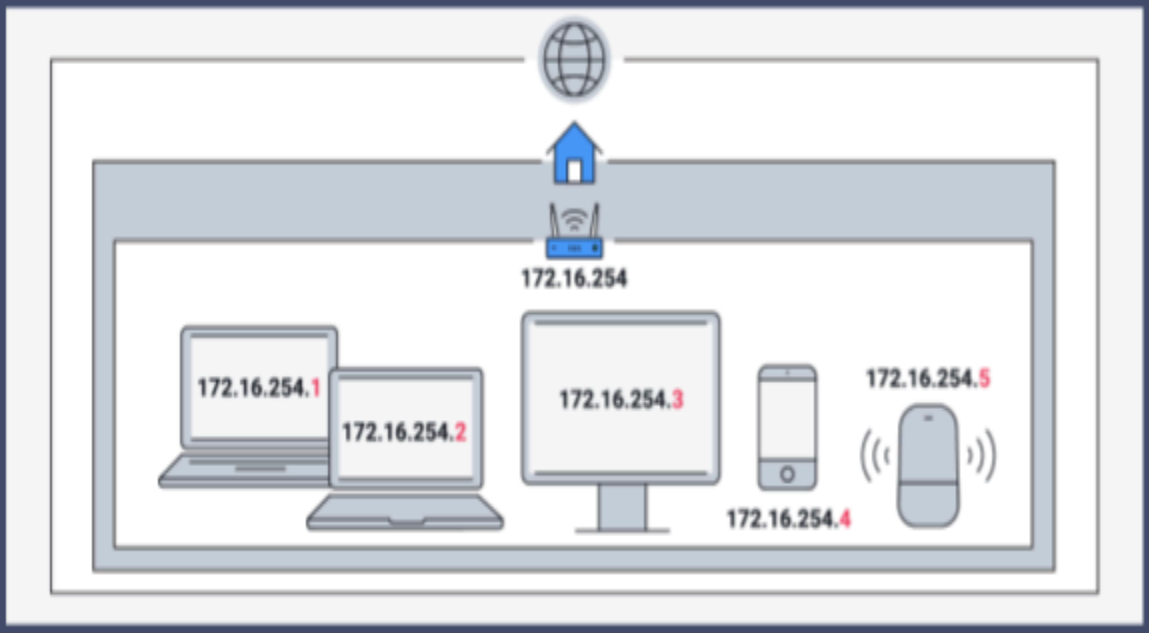
Las redes de datos se han convertido en un componente indispensable de la vida moderna, permitiendo la conexión y el acceso a la información de manera inmediata y constante. Sin embargo, junto con esta creciente dependencia de las redes, también han surgido numerosos riesgos relacionados con la seguridad cibernética. Desde usuarios individuales hasta grandes organizaciones, todos estamos expuestos a amenazas que pueden comprometer la integridad de nuestra información y la estabilidad de nuestras redes.

Por ello, este manual de Medidas de protección digital en redes de datos está diseñado, con la colaboración del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería de la UNAM, para ayudar a los usuarios a comprender los conceptos clave sobre la seguridad de las redes domésticas y a implementar estrategias prácticas para proteger su información. A lo largo del documento, se abordan temas cruciales como la creación de contraseñas seguras, la identificación de amenazas cibernéticas y el uso responsable de los recursos de red. Además, se proporcionan explicaciones accesibles para llevarlo a cabo, con el objetivo de mejorar tanto el rendimiento como la seguridad.

Con un enfoque en la facilidad de uso, este manual está dirigido a personas con poco o ningún conocimiento técnico previo, ofreciendo recomendaciones sencillas de seguir y que se pueden aplicar de inmediato. Al seguir estas medidas, los usuarios estarán mejor preparados para enfrentarse a las amenazas de seguridad que caracterizan el entorno digital contemporáneo, garantizando una experiencia más segura y eficiente en sus redes personales.

6.1

Cómo encontrar la dirección IP de tu dispositivo



Saber cómo encontrar la dirección IP de tu dispositivo es una tarea fundamental para gestionar y mantener la seguridad de tu red. La dirección IP es esencial para la comunicación entre dispositivos, y aunque a primera vista puede parecer algo complicado, localizarla es un proceso sencillo. A continuación, te mostramos cómo hacerlo en sistemas Windows y Android de manera rápida y eficaz.

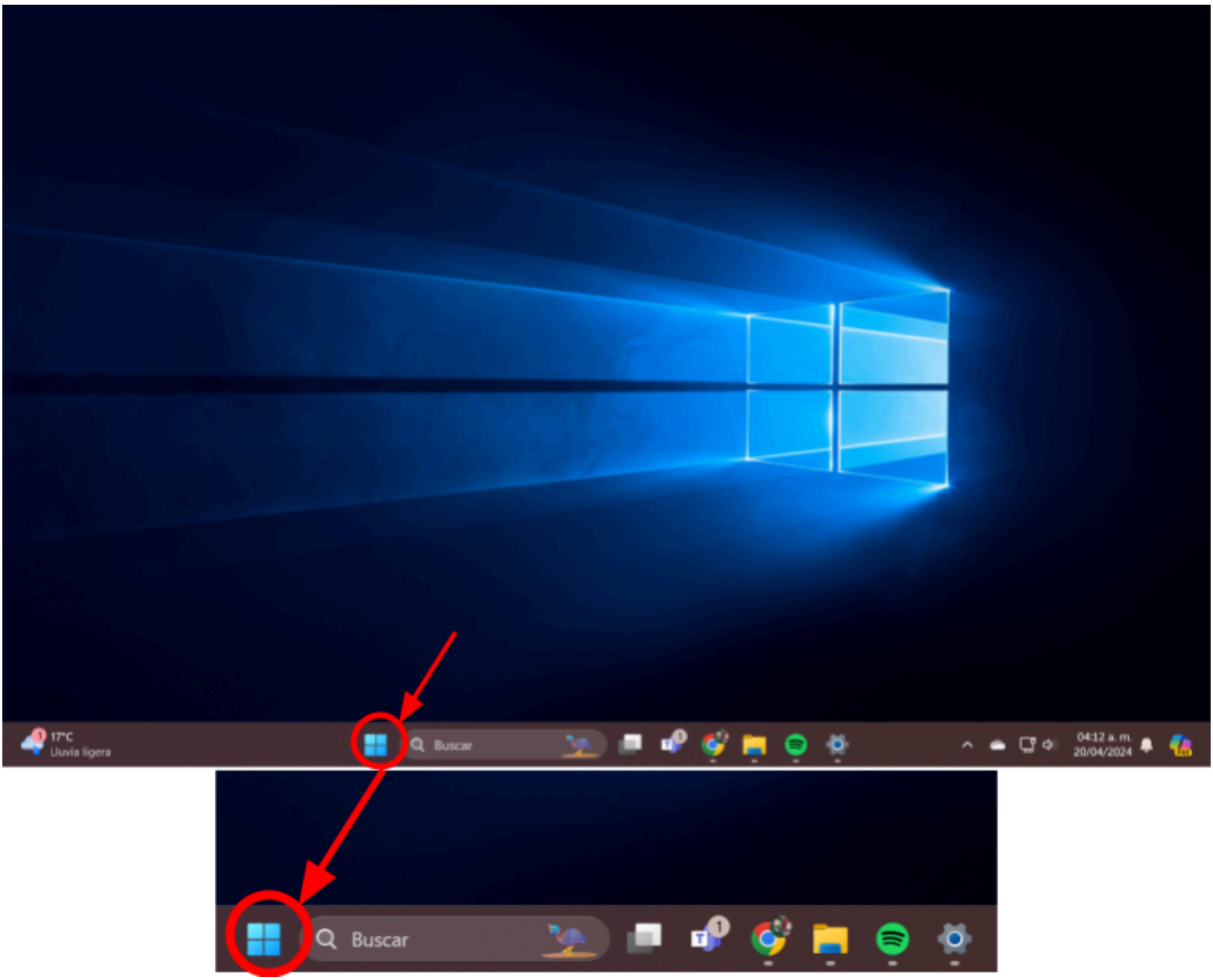
Windows

A través de las siguientes 5 imagenes se podrá observar el proceso para encontrar la dirección IP en Windows :

1. Abre el menú Inicio: Haz clic en el botón de inicio en la esquina inferior izquierda de la pantalla.

Figura 6.1

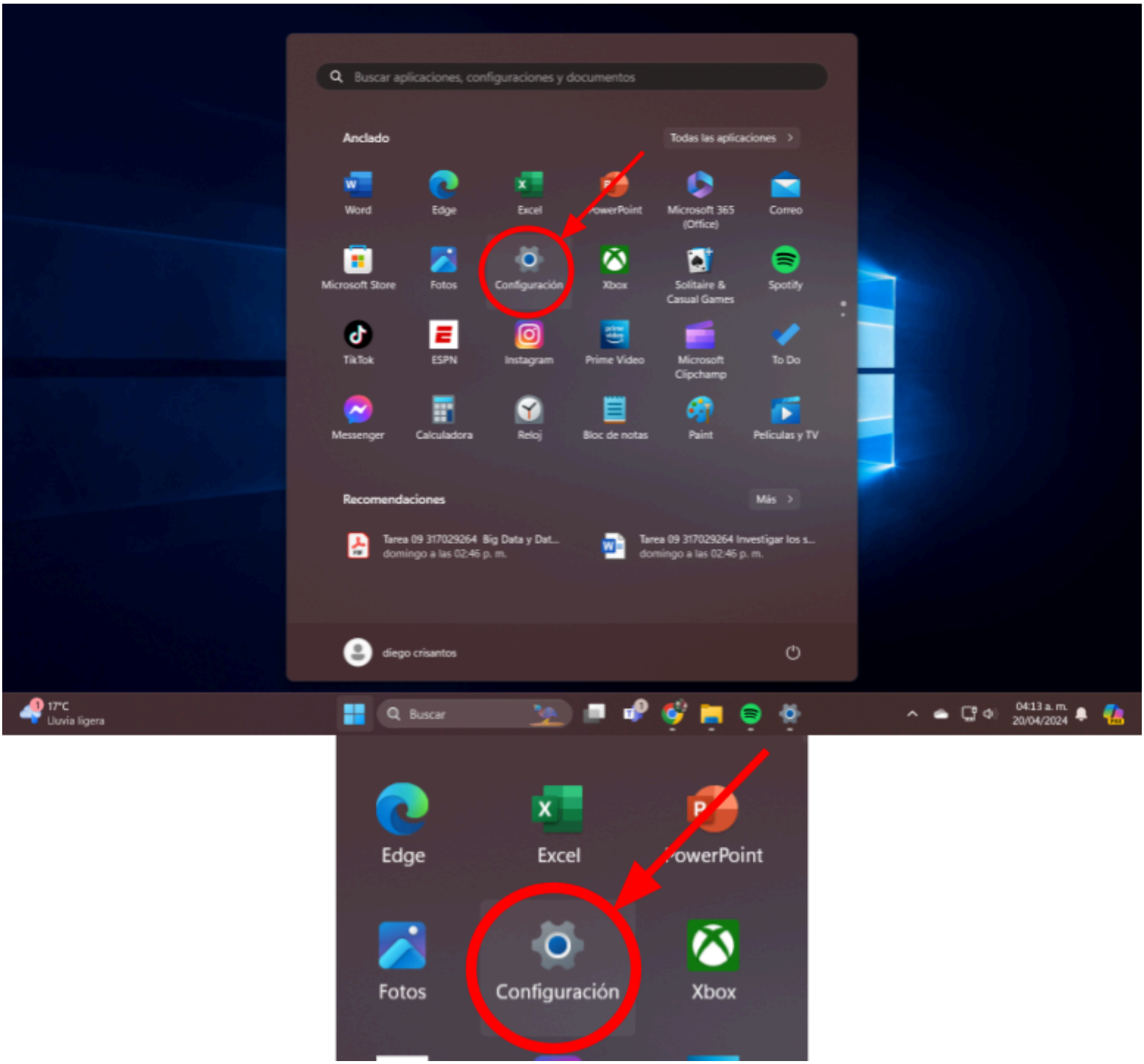
Dirección IP en Windows paso 1



2. Selecciona "Configuración": En el menú de inicio, selecciona el icono de engranaje que dice "Configuración" para abrir la configuración de Windows.

Figura 6.2

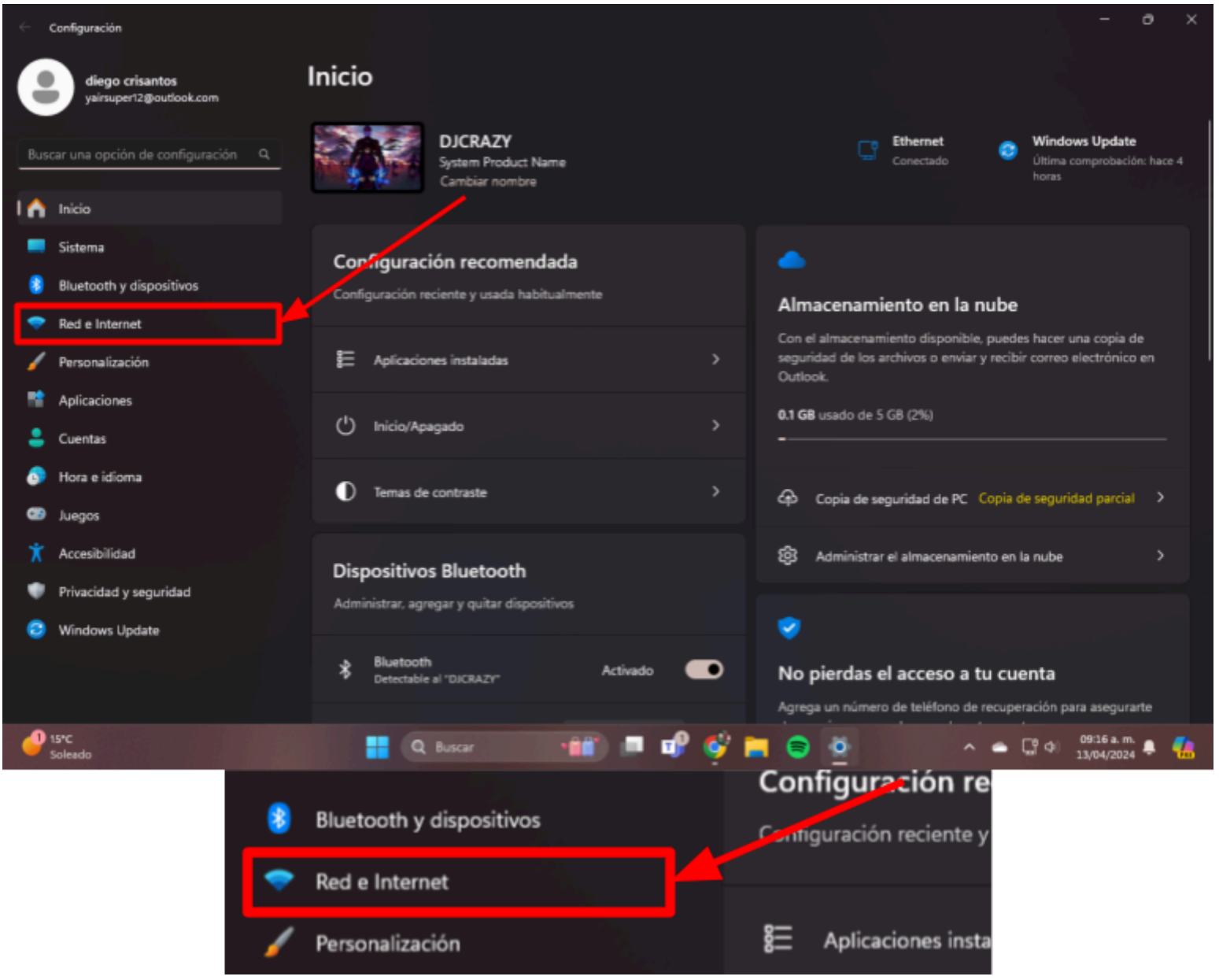
Dirección IP en Windows paso 2



3. Selecciona "Red e Internet": Dentro de la configuración, haz clic en "Red e Internet" en la parte izquierda de la pantalla.

Figura 6.3

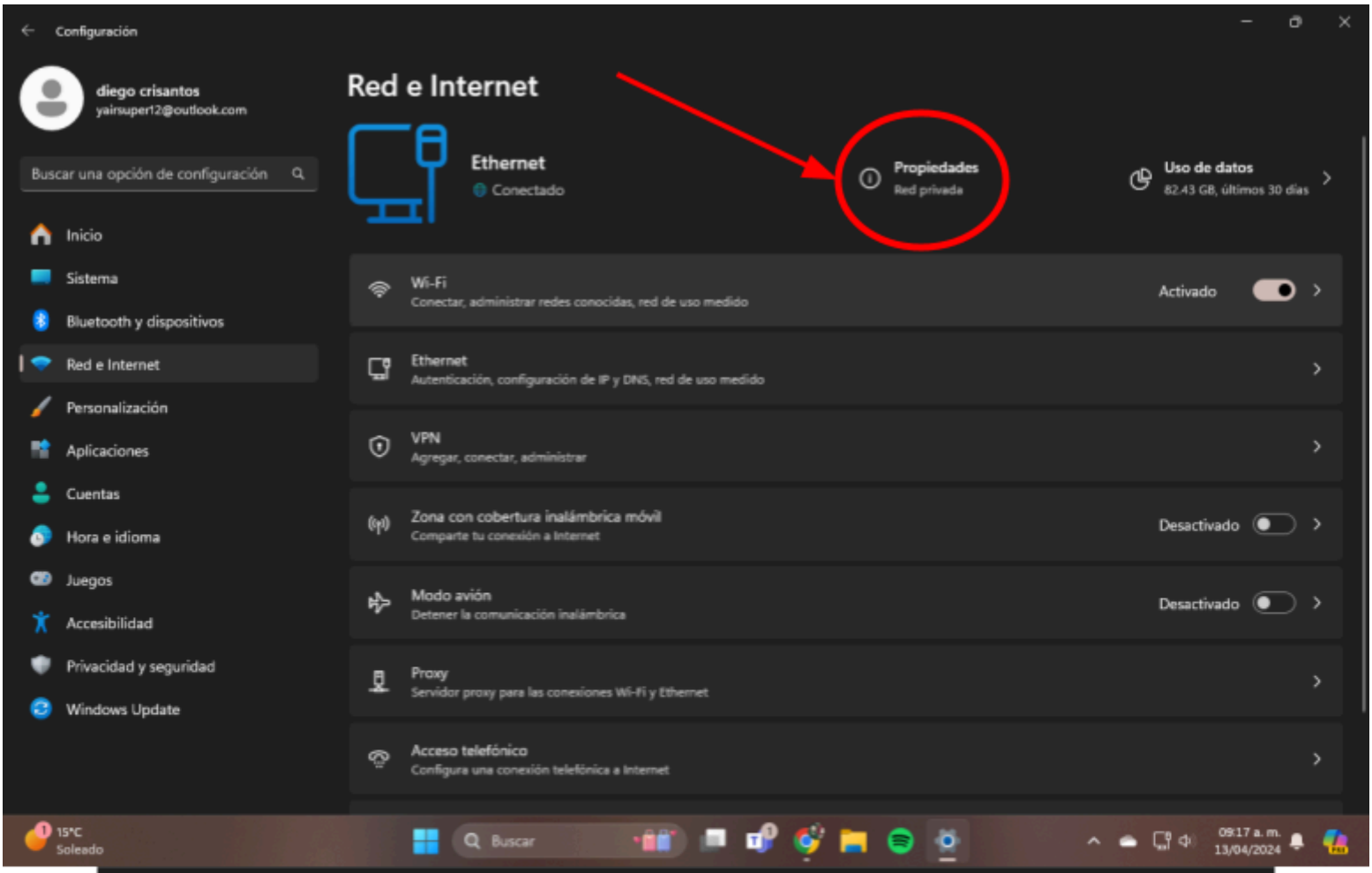
Dirección ip en Windows paso 3

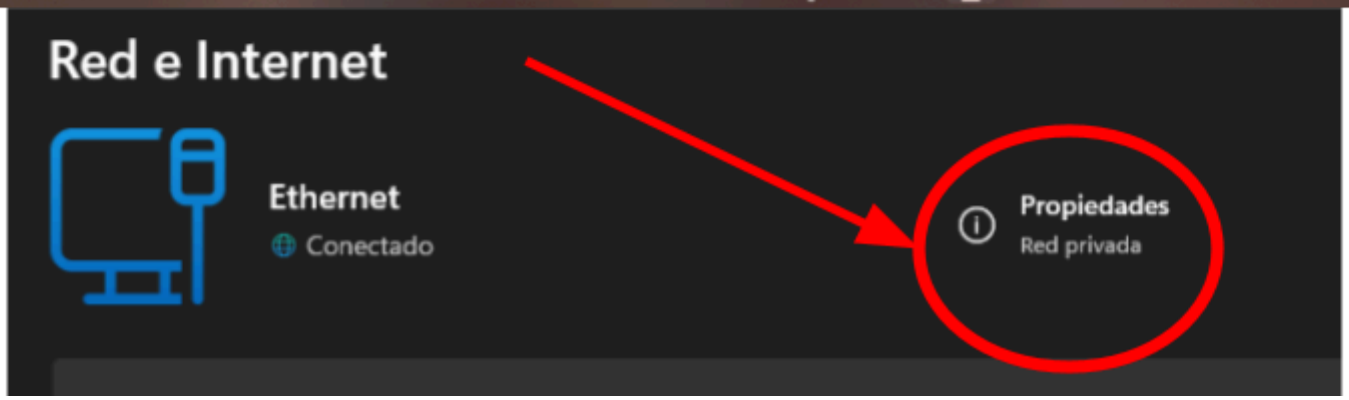


4. Accede a "Propiedades": En la parte superior de la pantalla, selecciona "Propiedades" para ver información sobre la red actual.

Figura 6.4

Dirección ip en Windows paso 4

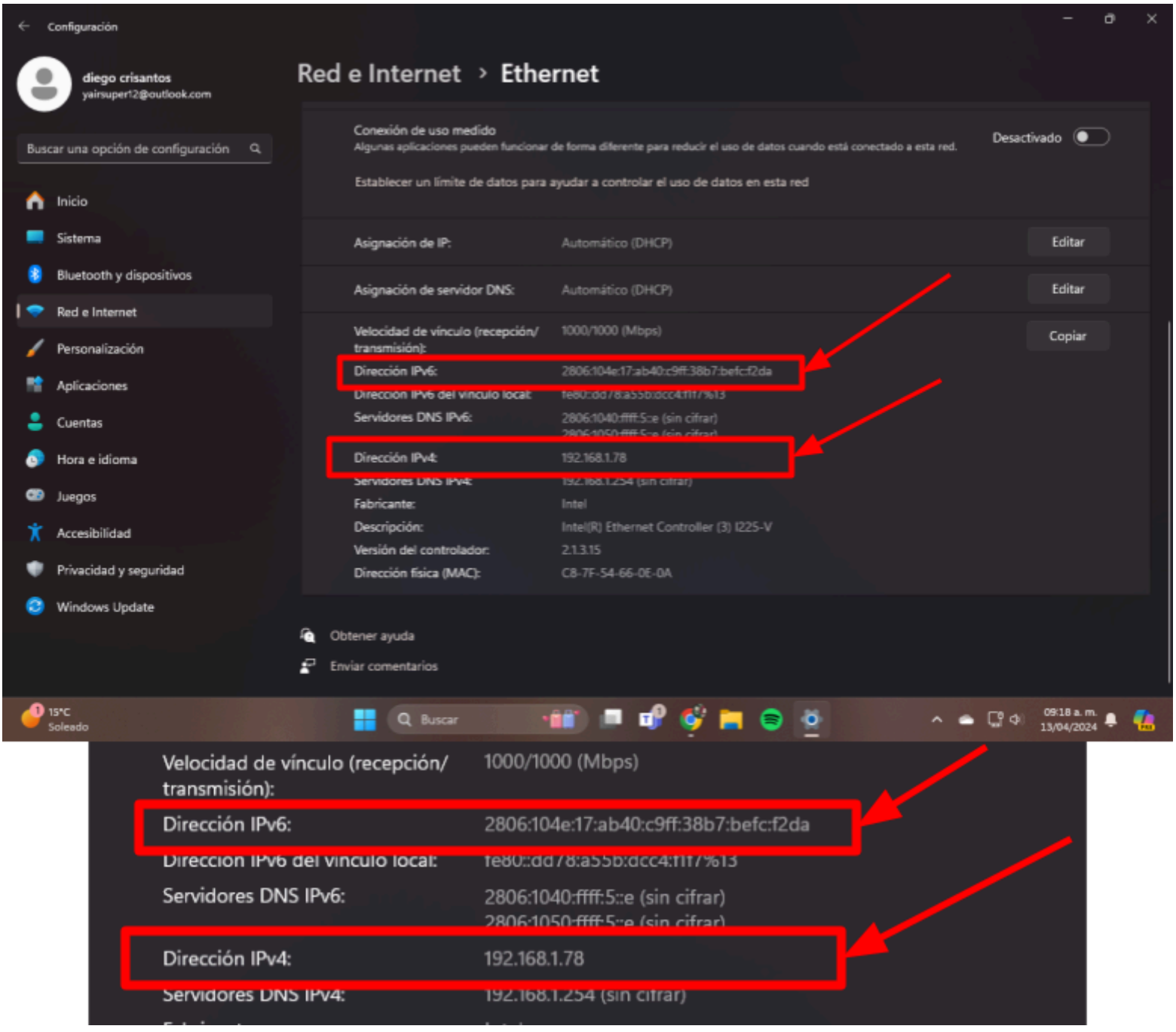




5. Encuentra tu dirección IP: En la sección de Propiedades de la red, busca la información que dice "Dirección IPv4" o “Dirección IPv6”. Esta es la dirección IP de tu dispositivo en la red.

Figura 6.5

Dirección ip en Windows paso 5



Android

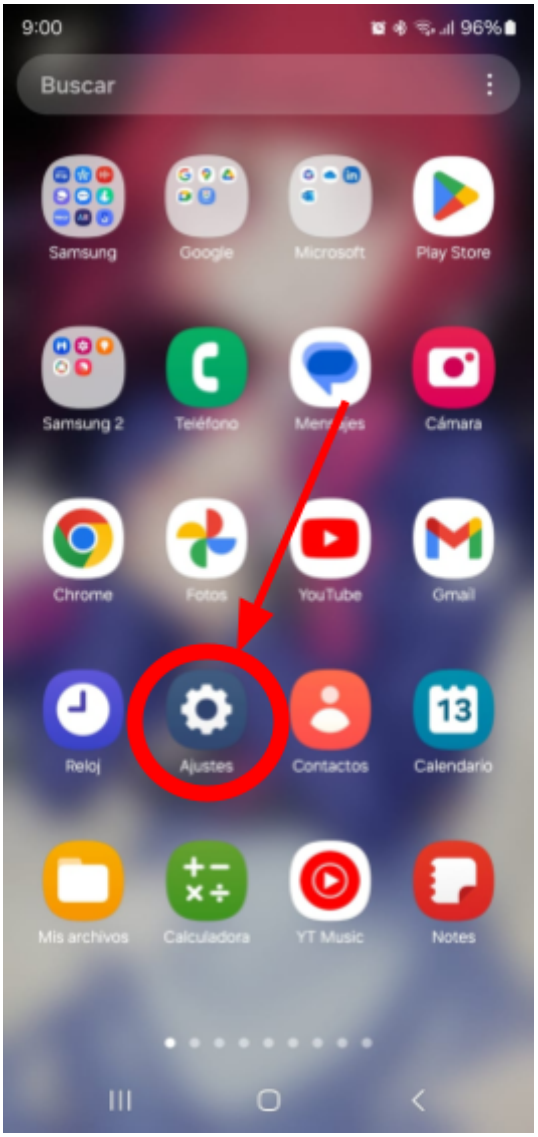
Samsung

A través de las siguientes 5 imagenes se podrá observar el proceso para encontrar la dirección IP en un dispositivo android de la marca samsung:

1. Abre la aplicación Configuración: Toca el icono de la aplicación "Configuración" o "Ajustes" en el menú principal de tu teléfono.

Figura 6.6

Dirección ip en samsung paso 1



2. Selecciona "Conexiones": Dentro de la configuración, selecciona "Conexiones".

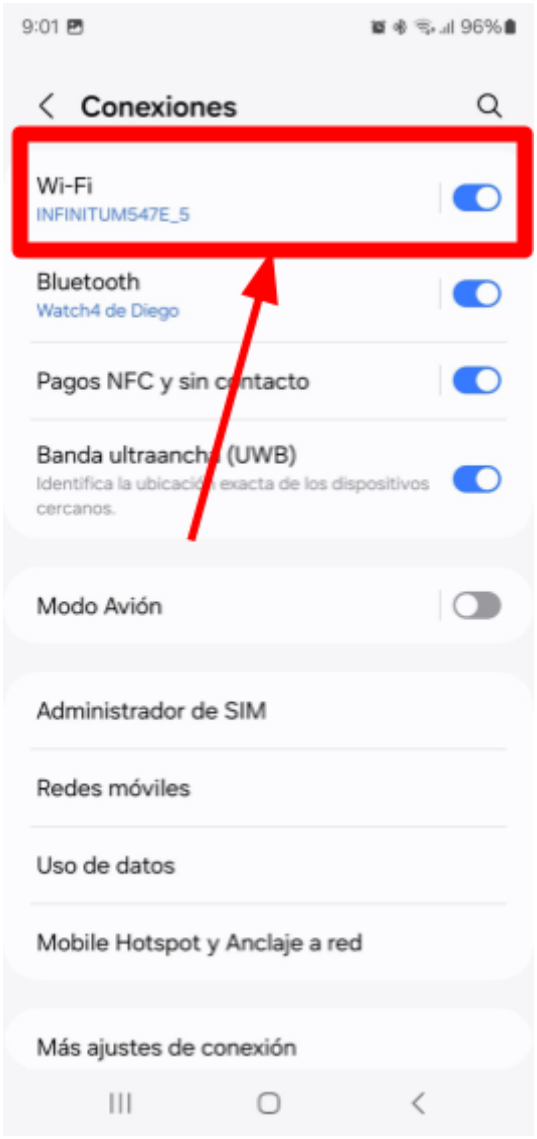
Figura 6.7

Dirección ip en samsung paso 2

3. Accede a "Wi-Fi": Dentro de las opciones de conexión, elige "Wi-Fi".

Figura 6.8

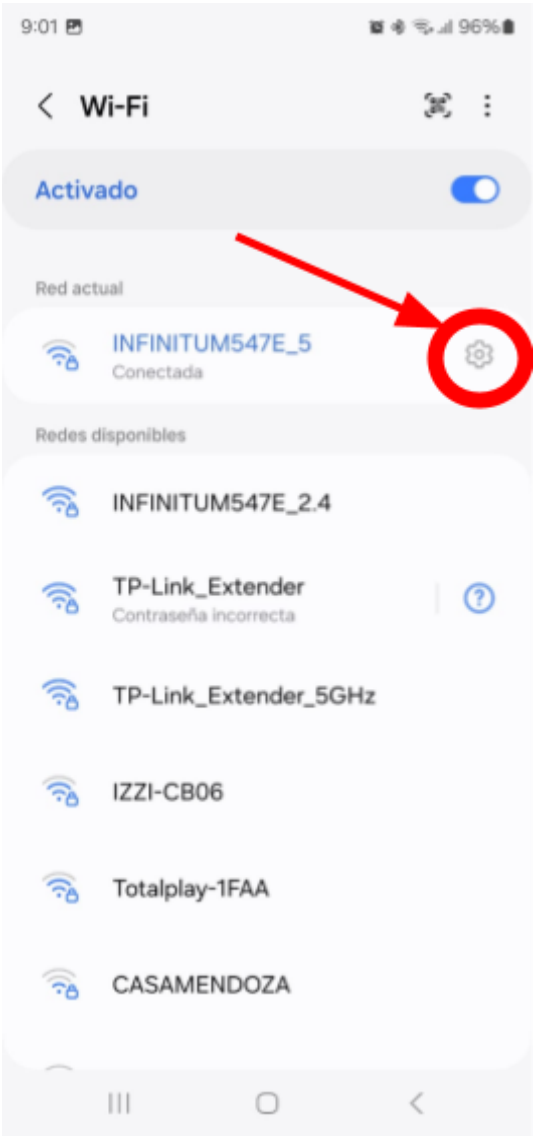
Dirección ip en samsung paso 3



4. Haz clic en "Propiedades de la red": Junto a la red a la que estás conectado, toca el icono de engranaje o la opción que te permita acceder a las propiedades de la red.

Figura 6.9

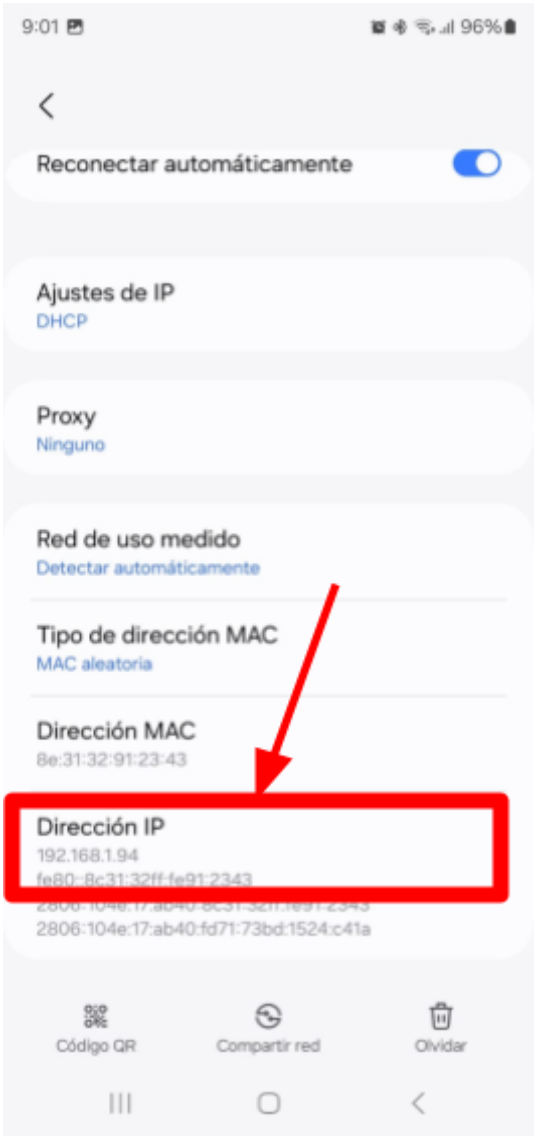
Dirección ip en samsung paso 4



5. Encuentra tu dirección IP: En la sección de Propiedades de la red, busca la información que dice "Dirección IPv4". Esta es la dirección IP de tu dispositivo en la red.

Figura 6.10

Dirección ip en samsung paso 5



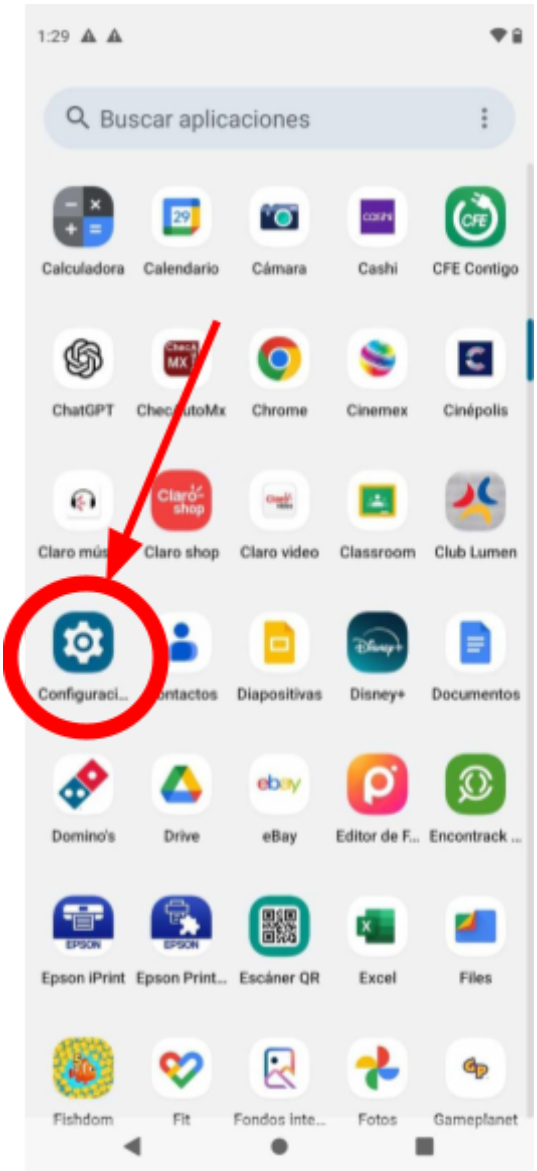
Motorola

A través de las siguientes 5 imagenes se podrá observar el proceso para encontrar la dirección IP en un dispositivo android de la marca Motorola:

1. Abre la aplicación Configuración: Toca el icono de la aplicación "Configuración" o "Ajustes" en el menú principal de tu teléfono.

Figura 6.11

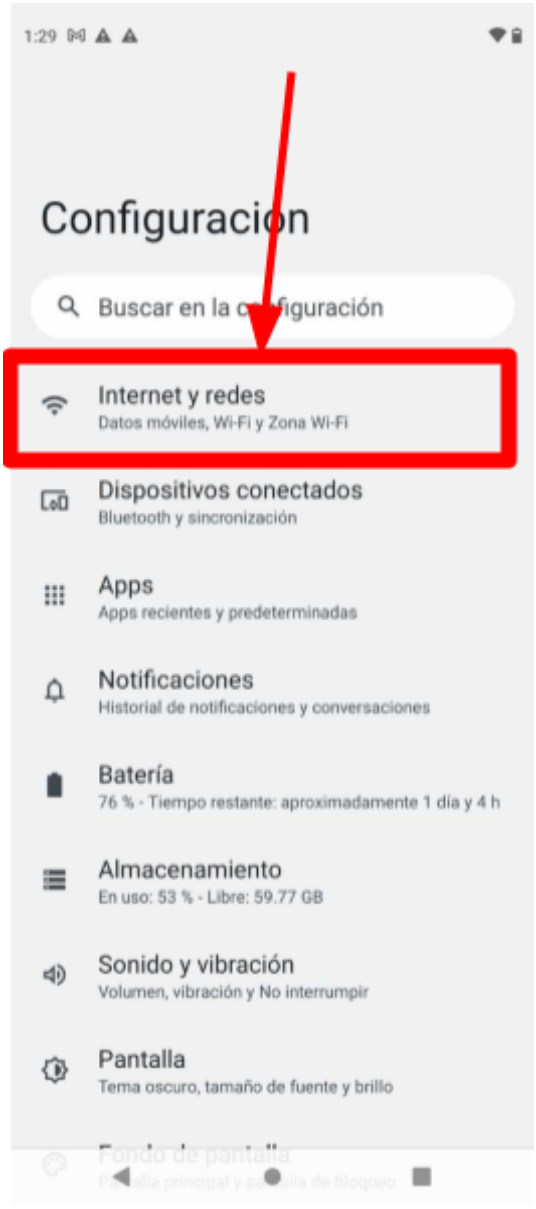
Dirección ip en motorola paso 1



2. Selecciona "Conexiones": Dentro de la configuración, selecciona "Conexiones".

Figura 6.12

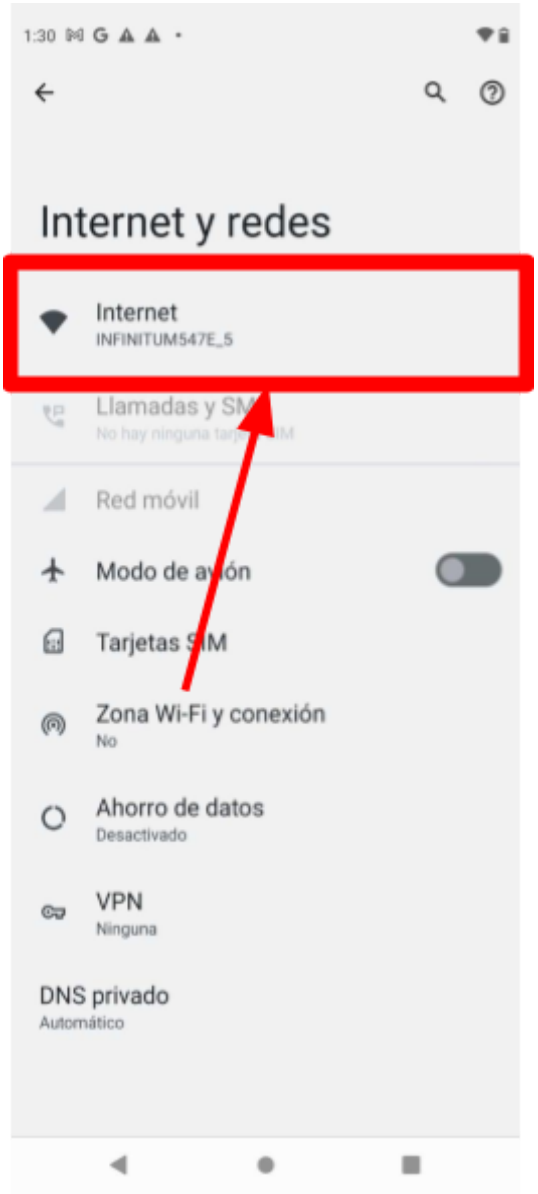
Dirección ip en motorola paso 2



3. Accede a "Wi-Fi": Dentro de las opciones de conexión, elige "Wi-Fi".

Figura 6.13

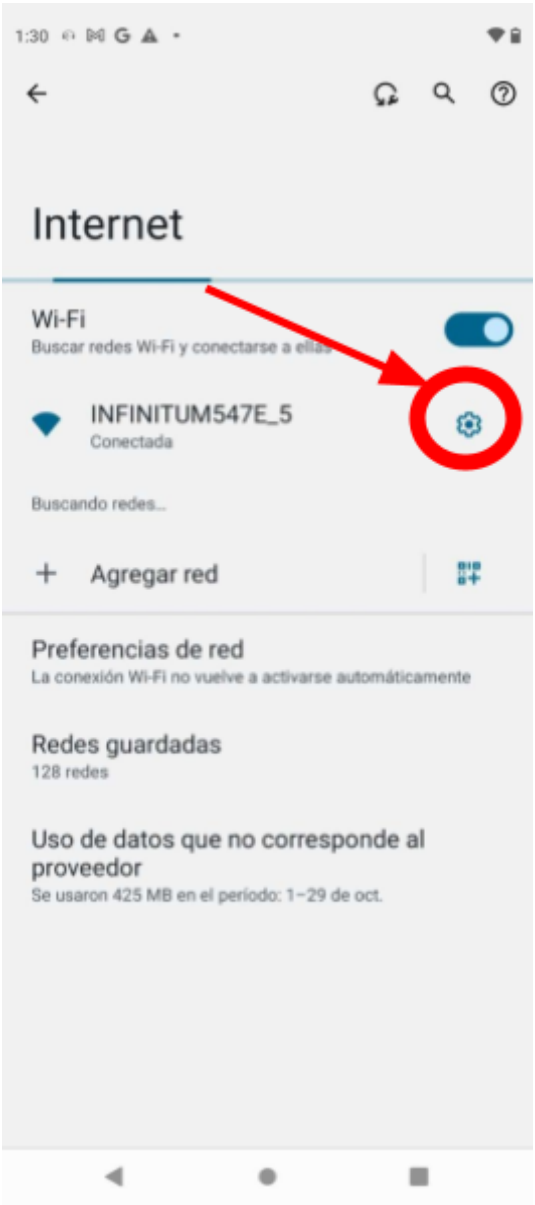
Dirección ip en motorola paso 3



4. Haz clic en "Propiedades de la red": Junto a la red a la que estás conectado, toca el icono de engranaje o la opción que te permita acceder a las propiedades de la red.

Figura 6.14

Dirección ip en motorola paso 4



5. Encuentra tu dirección IP: En la sección de Propiedades de la red, busca la información que dice "Dirección IPv4". Esta es la dirección IP de tu dispositivo en la red.

Figura 6.15

Dirección ip en motorola paso 5

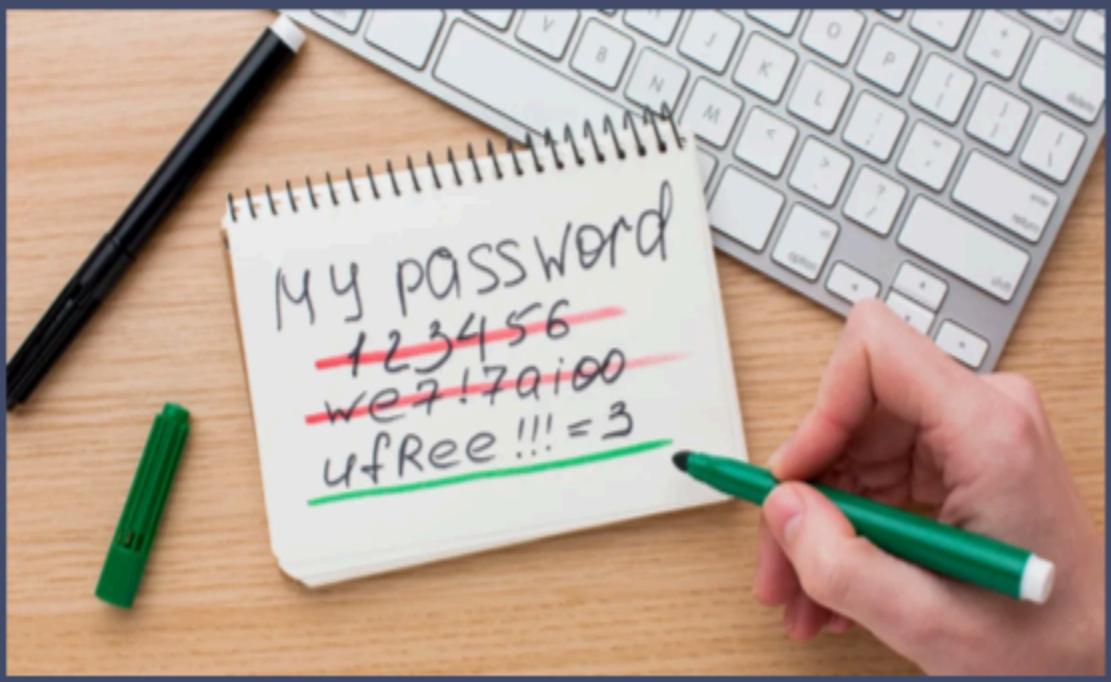
Consideraciones Adicionales:

- Diferencia entre IP Pública e IP Privada: La dirección IP configurada será la IP privada del dispositivo en la red local. La IP pública, asignada por el proveedor de internet, es diferente y puede consultarse en sitios como whatismyip.com.
- IP Estática vs. IP Dinámica: En redes locales, las IP suelen ser dinámicas, cambiando cada vez que un dispositivo se conecta. Configurar una IP estática garantiza que el dispositivo mantenga la misma dirección IP, lo cual es útil para equipos que requieren una conexión constante, como impresoras de red o servidores. Consulta el punto 5, "*Cómo configurar IP estática en tu módem telmex*", de este manual para obtener instrucciones detalladas.
- Conflictos de IP: Al asignar una IP estática, asegúrate de que no se repita con otra en la red, ya que los conflictos de IP pueden causar problemas de conectividad. Selecciona una IP fuera del rango que asigna el DHCP del módem para evitar este tipo de conflictos.
- Identificación de Dispositivos: Lleva un registro de las direcciones IP estáticas asignadas a cada dispositivo. Esto facilita la gestión de la red y permite identificar rápidamente los dispositivos conectados.
- Conexión a través de VPN: Si utilizas una VPN, la dirección IP visible será la asignada por la VPN, no la IP local de la red. Esto es importante si necesitas acceder a recursos específicos de la red local mientras usas la VPN. Consulta el punto 6, "*Cómo configurar una VPN en tu Módem*", de este manual para obtener instrucciones detalladas.
- Solución de Problemas de Conectividad: Ante problemas de conexión, verifica la IP del dispositivo para asegurarte de que esté dentro del rango de la red y libre de conflictos. La dirección IP es un punto inicial para diagnosticar y resolver problemas de red.
- Acceso a la Configuración de Módem o Router: Familiarízate con la configuración del módem o router, ya que es allí donde puedes ver las direcciones IP de los dispositivos conectados y ajustar la configuración de IP estáticas para un mejor control de la red.

Nota: Recuerda que la dirección IP puede aparecer como una serie de números separados por puntos, como por ejemplo "192.168.1.1" en formato IPv4.

6.2

Creación de Contraseñas Seguras



Hoy en día, donde prácticamente todas nuestras actividades diarias están vinculadas a Internet, la seguridad de nuestras cuentas en línea es más crucial que nunca. Una contraseña segura es tu primera línea de defensa contra ciberdelincuentes y protege tus datos personales y financieros de ser comprometidos. Seguir los pasos para crear una contraseña segura es seguir una política de contraseñas seguras, lo que ayuda a garantizar que tu información esté bien protegida de intentos de acceso no autorizado.

Las contraseñas débiles o fáciles de adivinar son una invitación abierta para los hackers, quienes pueden utilizar programas automatizados para probar miles de combinaciones en cuestión de segundos. Una contraseña segura, en cambio, es como una cerradura sólida que dificulta enormemente cualquier intento de intrusión no autorizada. Una contraseña segura no solo protege tu información personal, sino que también ayuda a proteger a otros. En muchas plataformas en línea, una cuenta comprometida puede ser utilizada para enviar spam, distribuir malware o incluso realizar actividades ilegales en tu nombre.

Por todas estas razones, es crucial que tomes en serio la creación y gestión de tus contraseñas. Una contraseña segura es un paso fundamental para proteger tu identidad en línea y mantener tus datos seguros y por ello a continuación puedes ver los pasos para Crear una Contraseña Segura:

1. Longitud Adecuada:

Importancia: Utilizar al menos 12 caracteres hace que la contraseña sea más difícil de adivinar mediante ataques de fuerza bruta, donde se prueban todas las combinaciones posibles. Cuanto más larga sea la contraseña, más tiempo llevará a un atacante descifrarla.

Ejemplo: "Contraseña12"

2. Combinación de Caracteres:

Importancia: Incluir letras mayúsculas, minúsculas, números y símbolos especiales aumenta la complejidad de la contraseña, haciendo que sea más resistente a los ataques de diccionario y fuerza bruta.

Ejemplo: "C0ntr4$eñA12"

3. Evita Información Personal:

Importancia: Evitar información personal como nombres propios o fechas de nacimiento hace que la contraseña sea menos predecible para alguien que conozca tu vida personal.

Ejemplo: "MiPerroFiru123"

4. No uses Palabras del Diccionario:

Importancia: Evitar palabras comunes que puedan encontrarse en un diccionario

reduce la probabilidad de que la contraseña sea descifrada mediante un ataque de diccionario.

Ejemplo: "Investigacion"

5. No uses Secuencias o Patrones Obvios:

Importancia: Evitar secuencias simples o patrones en el teclado hace que la contraseña sea menos predecible y más segura contra ataques de fuerza bruta.

Ejemplo: "QWERTY1234"

6. Contraseñas Únicas y diferentes:

Importancia: Utilizar contraseñas diferentes para cada cuenta o servicio además de evitar el uso de una base común para todas ellas esto impide que si una contraseña se ve comprometida, todas tus cuentas corran el mismo riesgo.

Ejemplo: "jorgeoficina"

"jorgecasa"

7. Actualiza Regularmente:

Importancia: Cambiar tus contraseñas periódicamente (al menos una vez al año) reduce el riesgo de que una contraseña comprometida se use para acceder a tus cuentas en el futuro.

Ejemplo: "Nuev@C0ntr@123"

Consideraciones Adicionales:

- Revisa las Políticas de Contraseña: Asegúrate de seguir las políticas de contraseña establecidas por los servicios o plataformas que utilizas, ya que algunas pueden tener requisitos específicos en términos de longitud y complejidad. Consulta el punto 2, "*Creación de contraseñas seguras*", de este manual para obtener instrucciones detalladas.
- Desconfía de Correos y Mensajes Sospechosos: Nunca ingreses tu contraseña en respuesta a correos electrónicos o mensajes sospechosos que soliciten tus credenciales. Estos pueden ser intentos de phishing. Consulta el punto 10, "*Cómo identificar correos electrónicos con malware*", de este manual para obtener instrucciones detalladas.

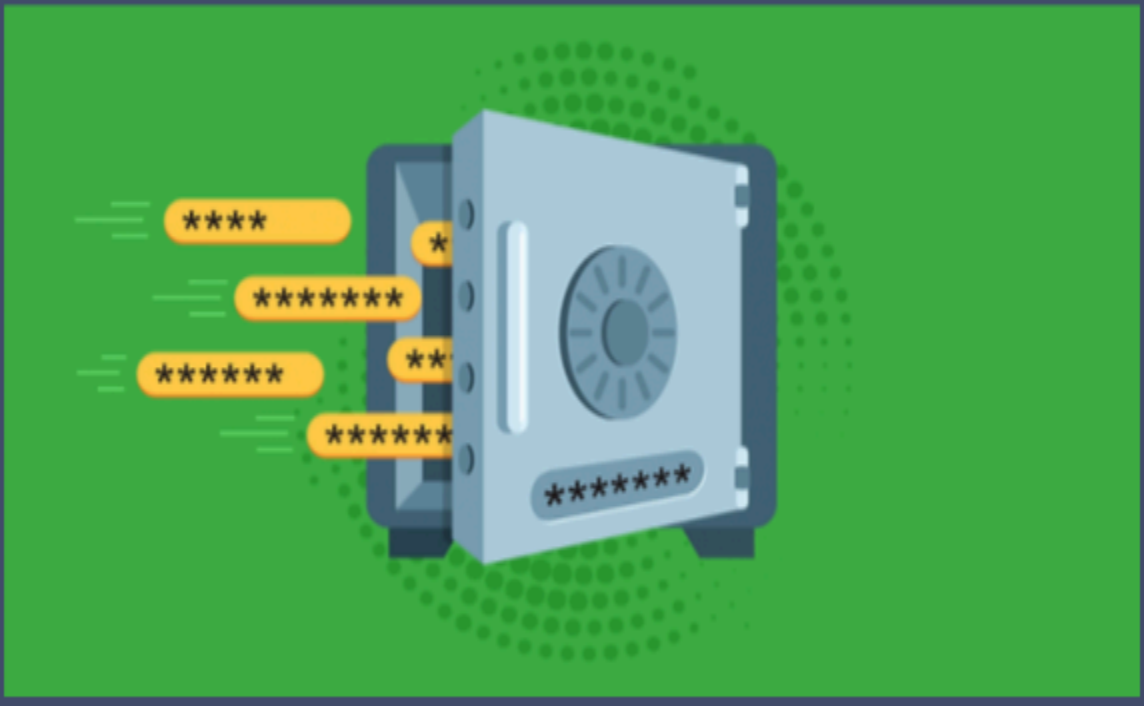
- Cerrar sesiones al cambiar contraseña y al no utilizar la cuenta: Después de cambiar tu contraseña, cierra sesión en todos los dispositivos para evitar que personas no autorizadas accedan con la contraseña anterior. Si no planeas usar una cuenta por un tiempo, también es recomendable cerrar sesión en dispositivos compartidos o públicos para reducir el riesgo de accesos no deseados.

Nota: Utiliza frases o acrónimos que te sean fáciles de recordar pero difíciles de

adivinar para otros.

6.3

Almacenamiento Seguro de Contraseñas



El almacenamiento seguro de contraseñas es una parte fundamental de la seguridad digital. Con el aumento de las cuentas en línea y las amenazas cibernéticas, es crucial proteger nuestras contraseñas para evitar accesos no autorizados y el robo de identidad. Utilizar métodos seguros para almacenar y gestionar contraseñas ayuda a mantener la integridad de nuestras cuentas y datos personales. Por ello a continuación te detallamos cómo puedes instalar y utilizar correctamente un gestor de contraseñas:

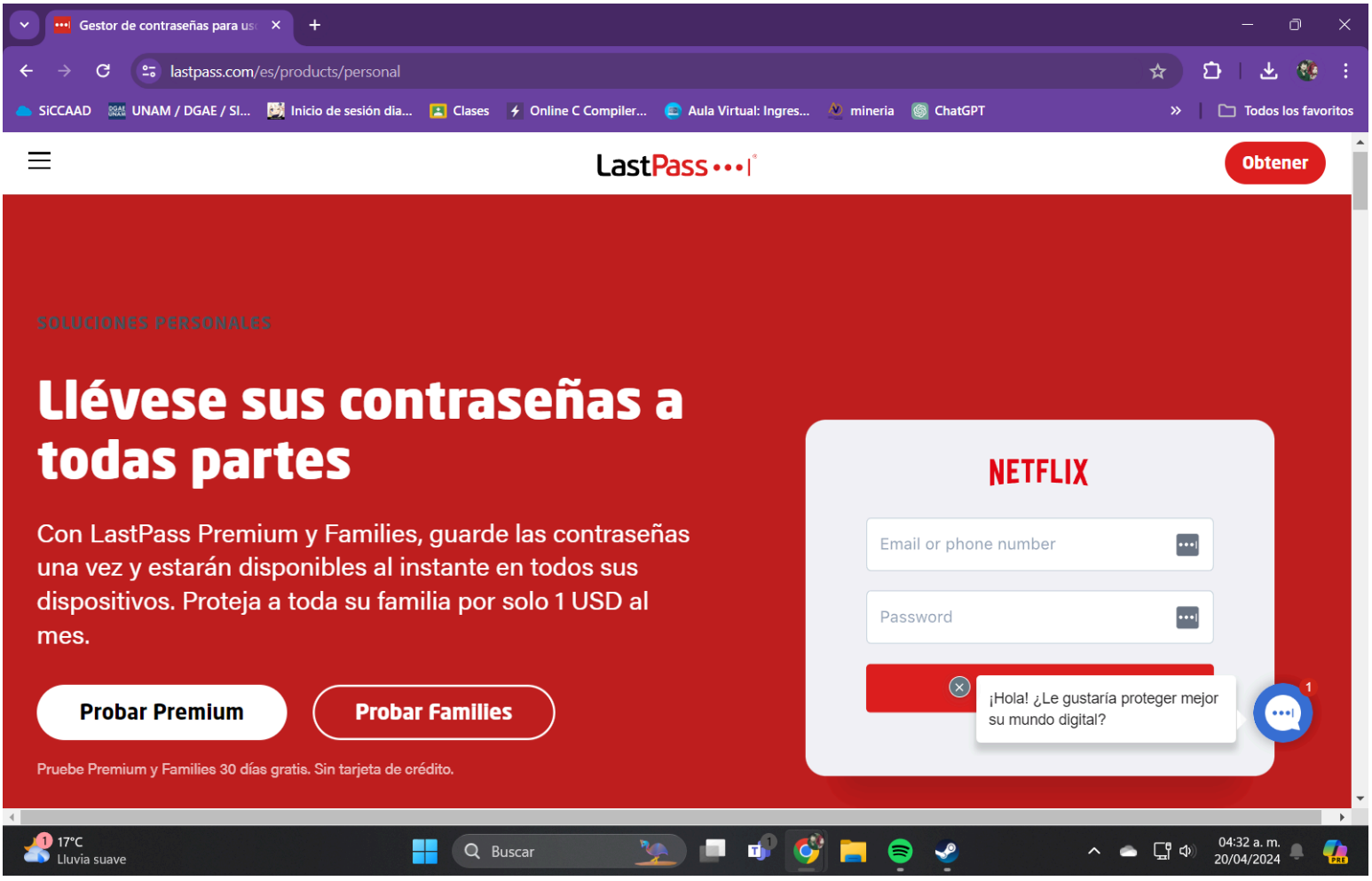
1. Gestores de contraseñas: Utiliza un gestor de contraseñas confiable. Estas aplicaciones almacenan de forma segura tus contraseñas y las cifran para protegerlas de accesos no autorizados.

   Gestor de Contraseñas (LastPass):

   - Descarga e Instalación: Descarga e instala LastPass desde su sitio web oficial (https://www.lastpass.com/es) o desde la tienda de aplicaciones de tu dispositivo.

Figura 6.16

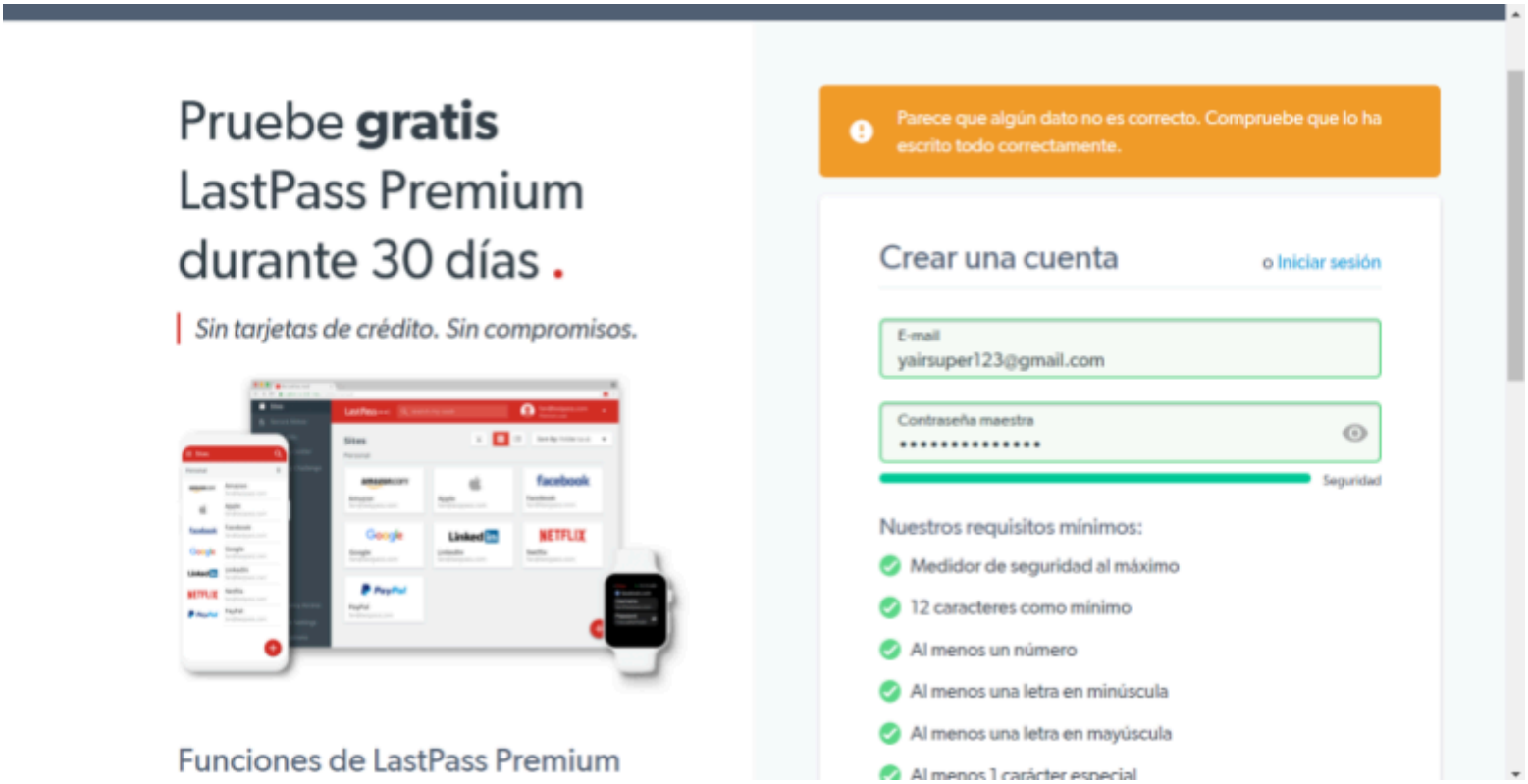
LastPass paso 1



- Creación de una Cuenta Maestra: Al abrir LastPass por primera vez, se te pedirá que crees una cuenta maestra. Esta será la contraseña principal que utilizarás para acceder a tus contraseñas almacenadas en LastPass.

Figura 6.17

LastPass paso 2



- Almacenamiento de contraseñas: Cuando inicies sesión en un sitio web o servicio y LastPass detecte una nueva contraseña, te ofrecerá guardarla en tu bóveda segura. Puedes aceptar guardarla para que LastPass la recuerde por ti.

Figura 6.18
LastPass paso 3

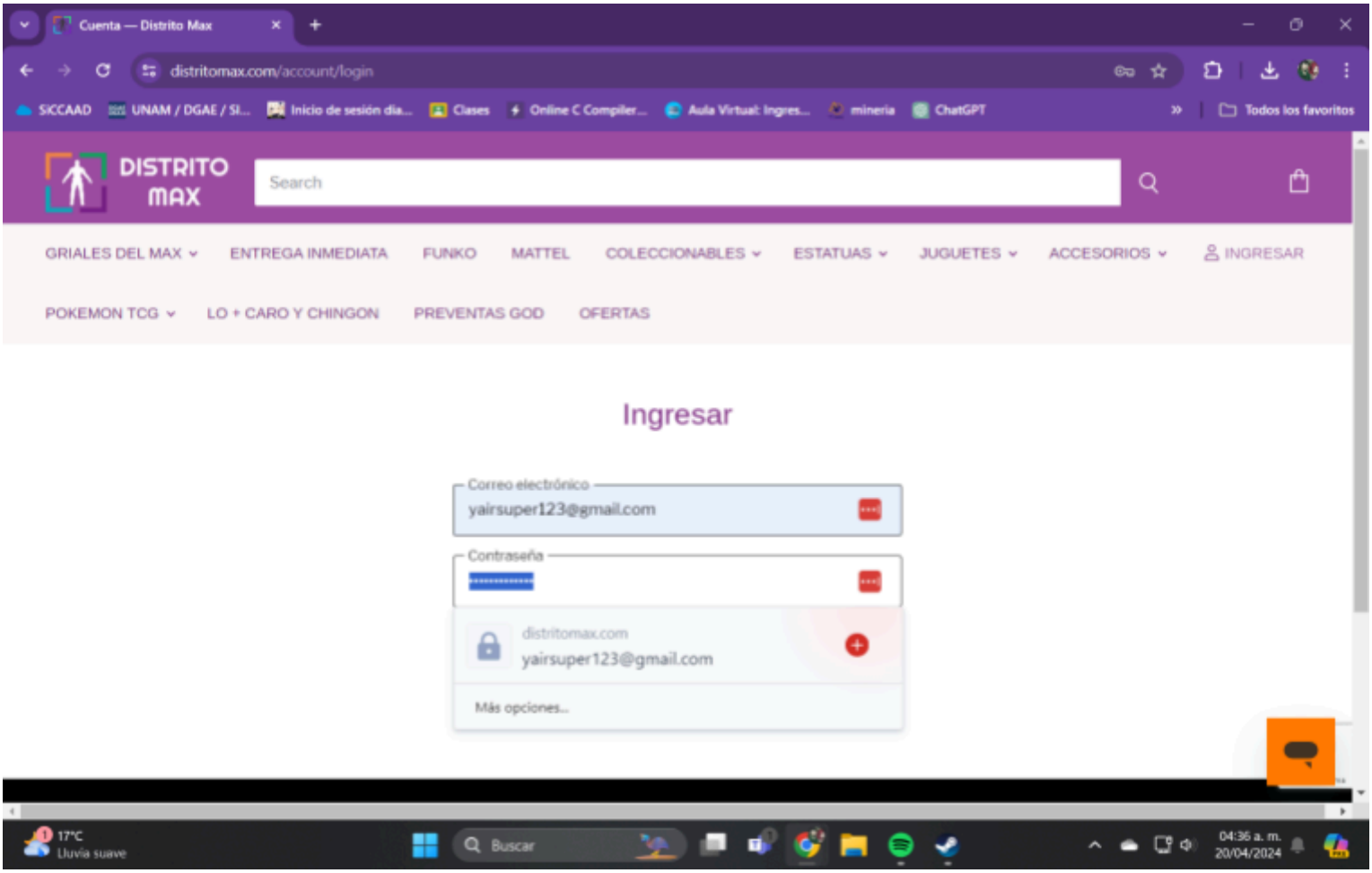
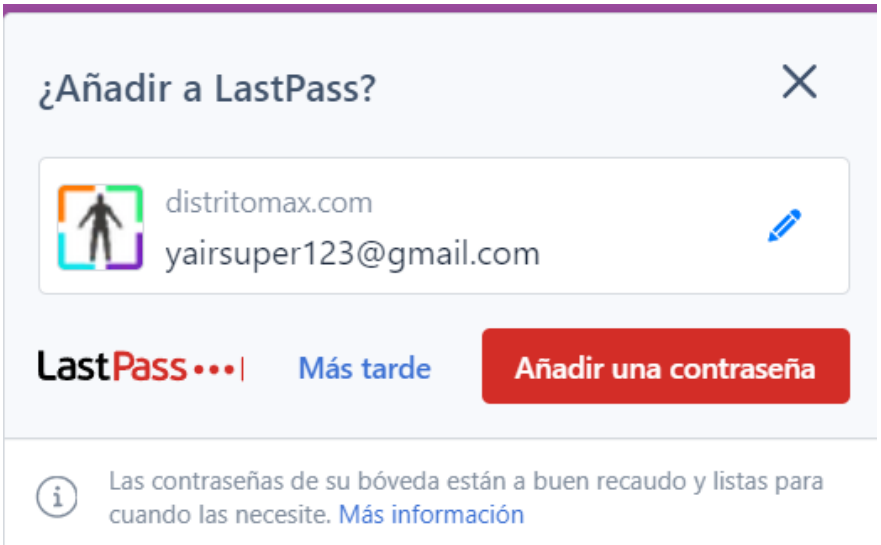
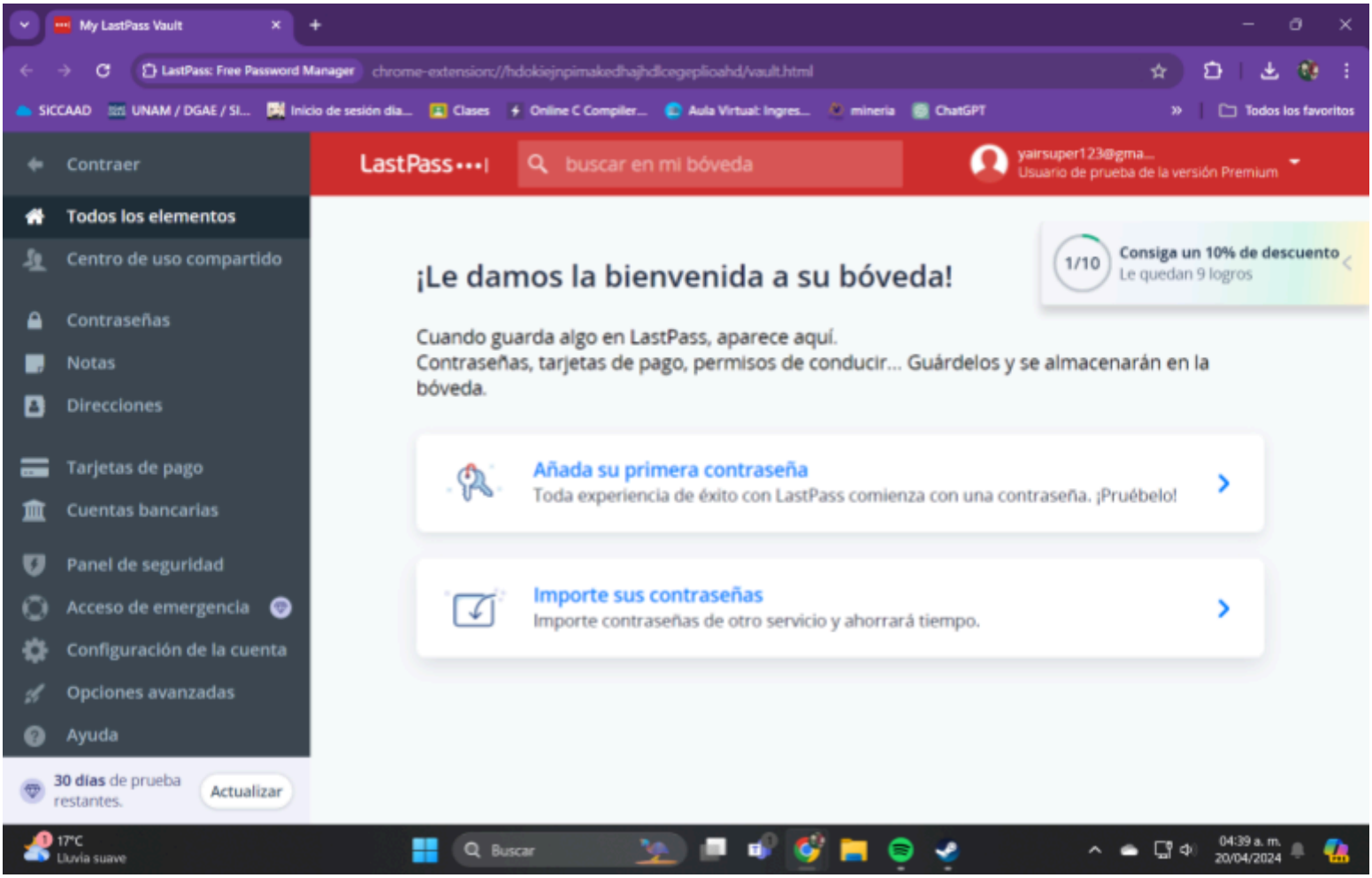


Figura 6.19
LastPass paso 4



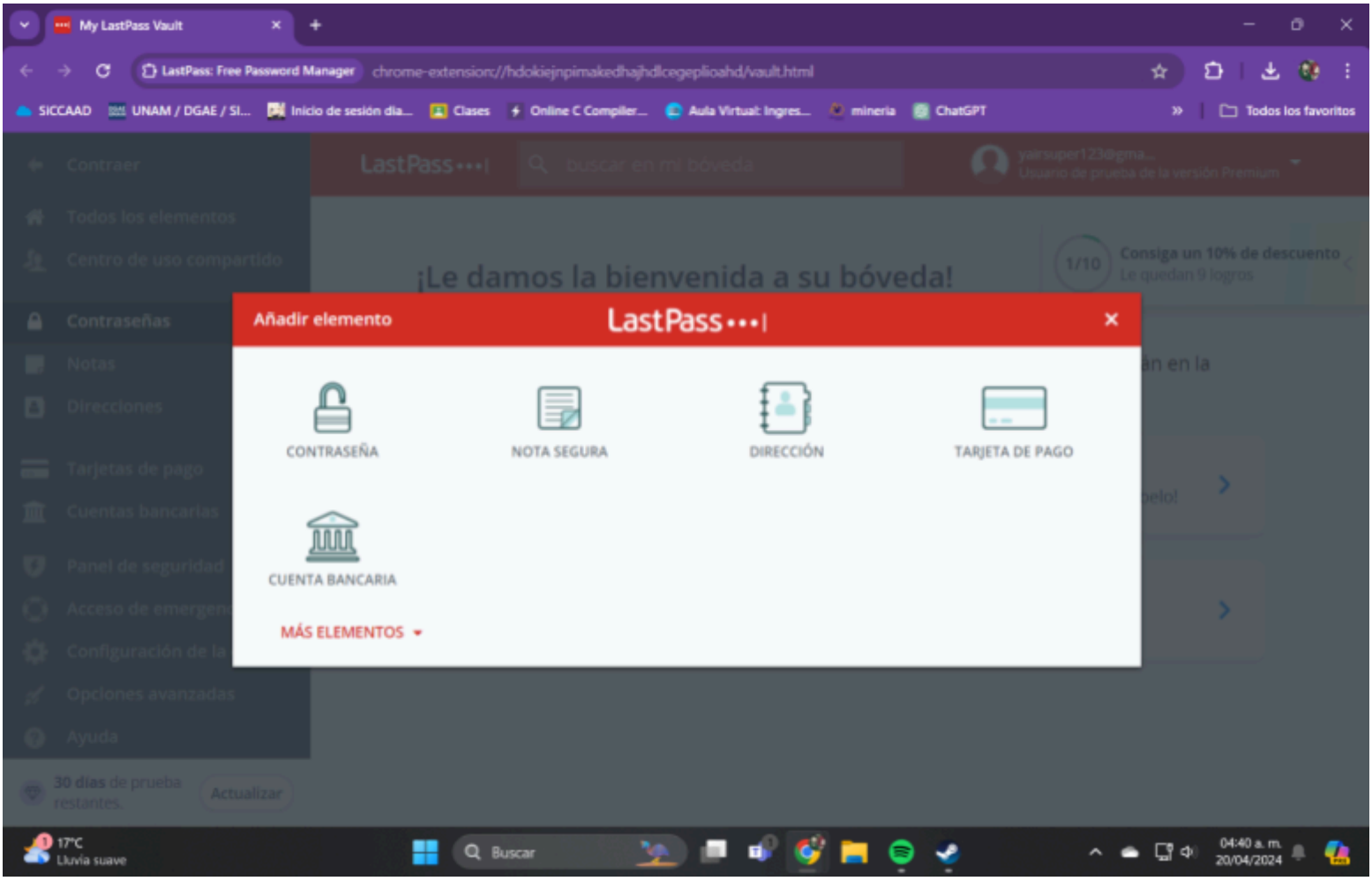
- Guarda contraseña manualmente:
  a) Abre la aplicación y busca la opción "Añadir contraseña" en la pantalla principal. Esta opción puede aparecer como "Añade tu primera contraseña" si es la primera vez que utilizas la aplicación, o cómo "Añadir contraseña" si ya tienes contraseñas almacenadas.

Figura 6.20
LastPass paso 5



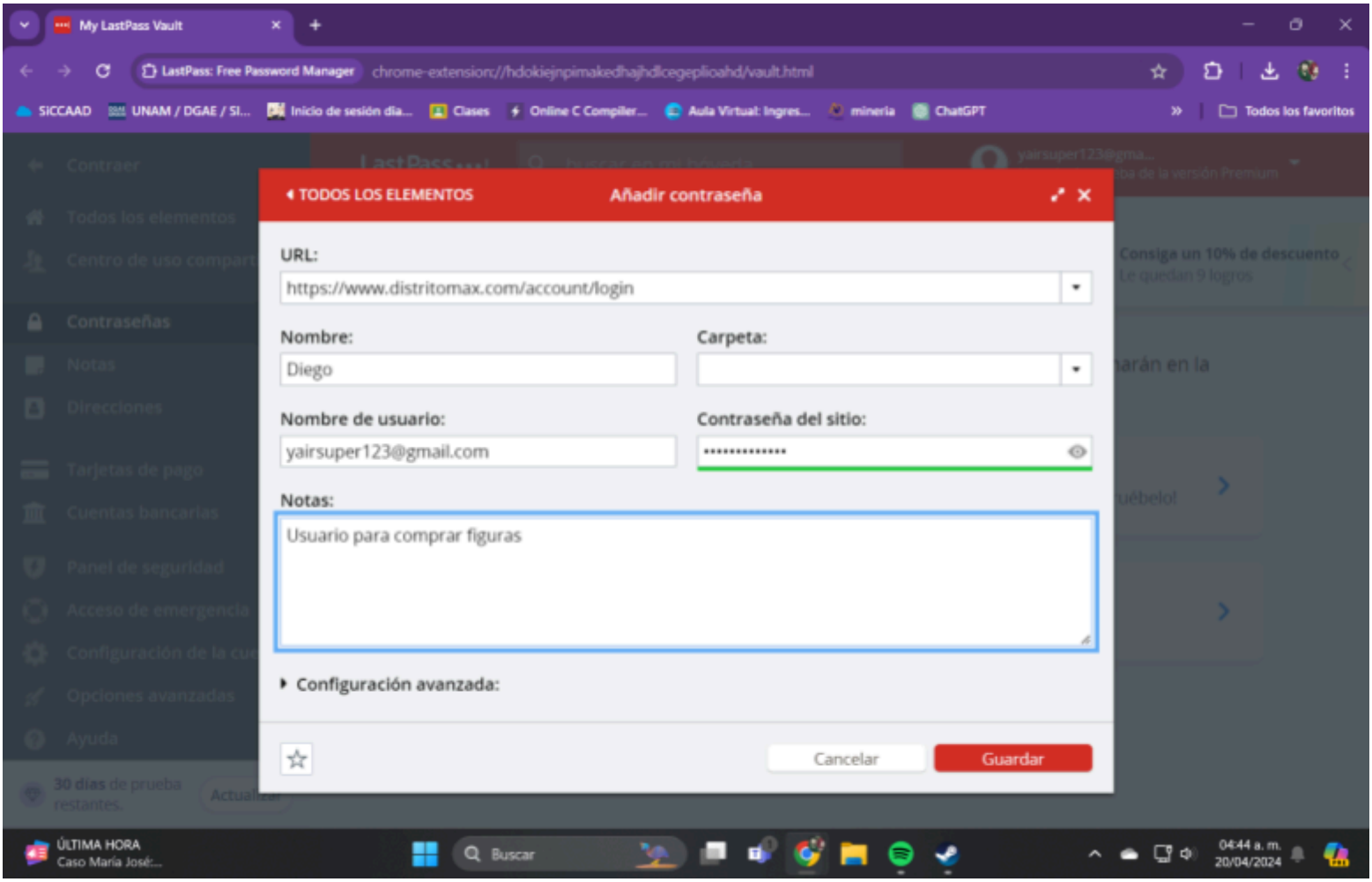
b) Selecciona el tipo de dato que deseas guardar, en este caso, la contraseña.

Figura 6.21
LastPass paso 6



c) En la siguiente pantalla, ingresa la URL del sitio web al que pertenece la cuenta. Esto te ayudará a recordar a qué cuenta pertenece la contraseña. Luego, escribe un nombre para identificar la cuenta dentro de la aplicación. Si deseas organizar tus contraseñas en carpetas, también puedes crear una nueva carpeta e ingresar su nombre. A continuación, completa los campos con el nombre de usuario y la contraseña de la cuenta que deseas almacenar.Si lo deseas, puedes añadir una nota que te ayude a recordar algún detalle específico sobre la cuenta. Por ejemplo, puedes escribir el propósito de la cuenta o cualquier otra información relevante.Una vez completados todos los campos, haz clic en "Guardar" para almacenar la contraseña. La aplicación guardará la información de forma segura y cifrado.

Figura 6.22
LastPass paso 7



d) Una vez guardada la cuenta, podrás acceder a ella fácilmente. Solo haz clic en la cuenta guardada en la lista de contraseñas de la aplicación y luego en "Iniciar sesión". La aplicación te dirigirá automáticamente al sitio web correspondiente, donde podrás ingresar la contraseña y el nombre de usuario para acceder a tu cuenta.

Figura 6.23
LastPass paso 8

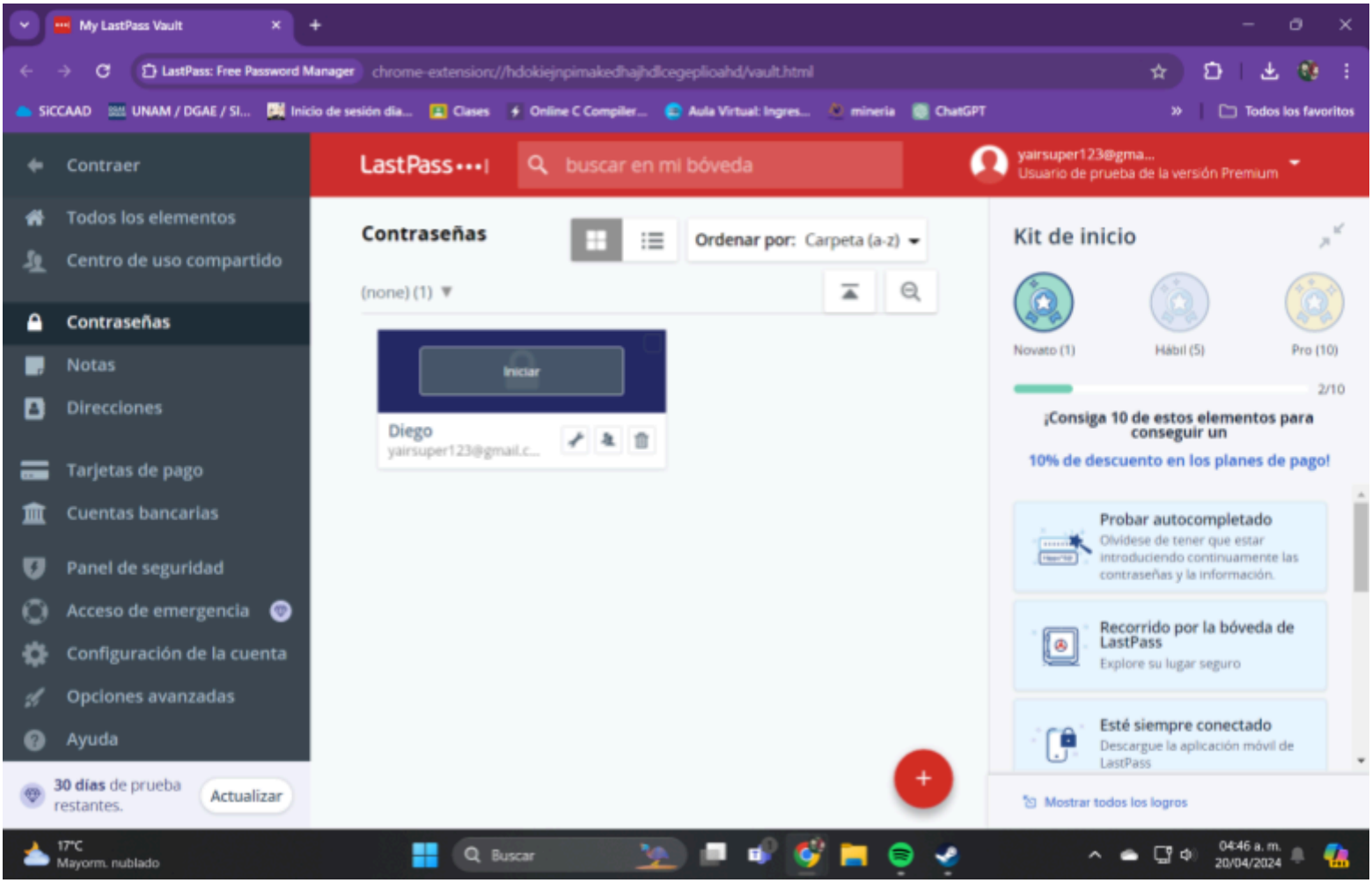
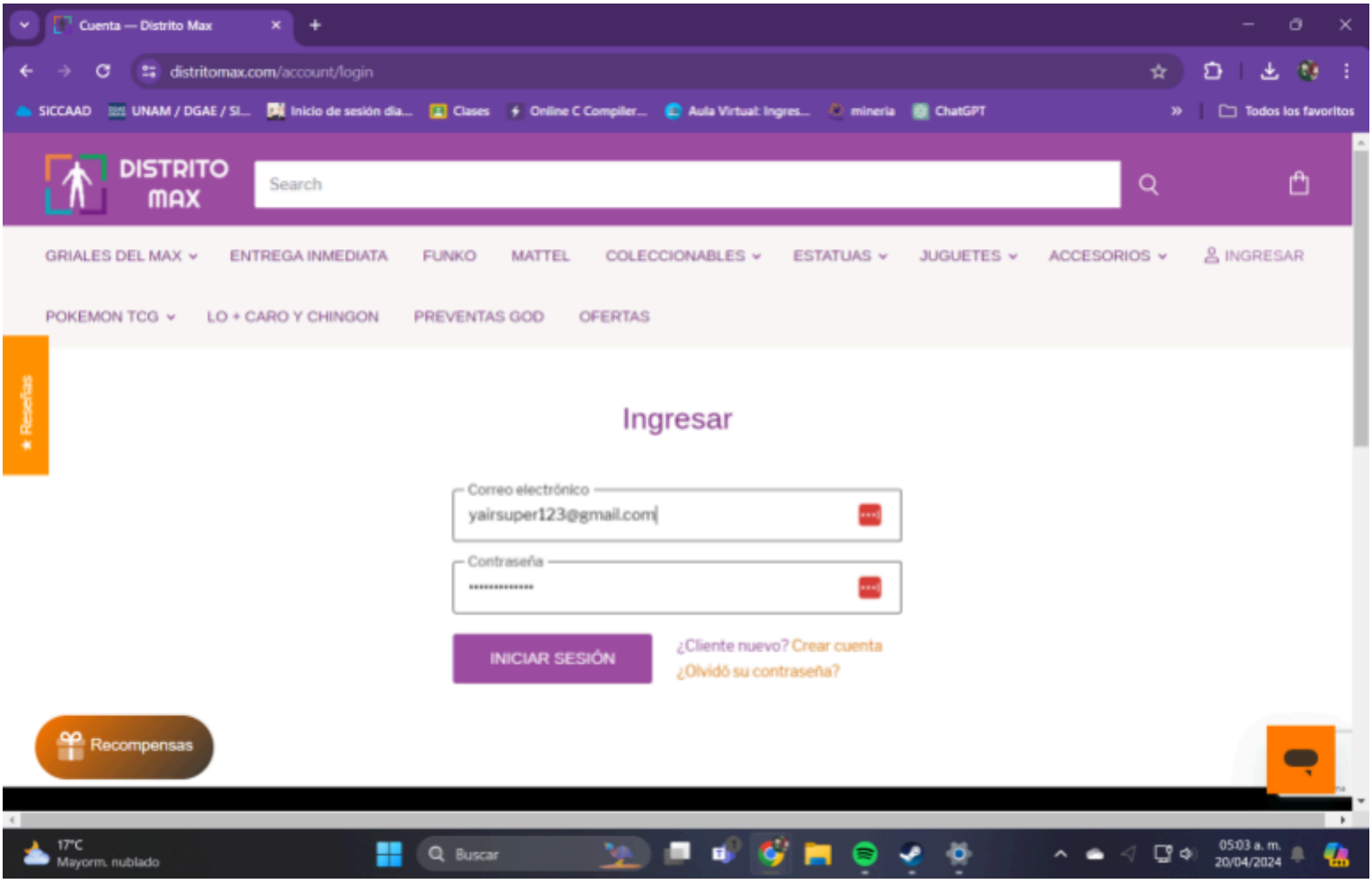


Figura 6.24

LastPass paso 9



2. Almacenamiento Local Seguro: Si prefieres no utilizar un gestor de contraseñas, guarda tus contraseñas en un archivo cifrado en tu dispositivo. Utiliza software de cifrado confiable para proteger el archivo.

3. No las Guardes en Navegadores Web: Evita guardar tus contraseñas en los navegadores web, ya que estos no proporcionan la misma seguridad que los gestores de contraseñas o el almacenamiento cifrado . Además, si alguien accede a tu dispositivo (ya sea móvil o computadora), tus contraseñas quedan disponibles para esa persona.

4. Copia de Seguridad: Asegúrate de hacer copias de seguridad periódicas de tus contraseñas almacenadas en gestores de contraseñas o archivos cifrados. Guarda estas copias en un lugar seguro y fuera de línea. Si necesitas ayuda para realizar este proceso, consulta el manual de usuario del gestor de contraseñas correspondiente, ya que los pasos pueden variar según la aplicación.

5. Autenticación de Dos Factores (2FA): Utiliza la autenticación de dos factores siempre que esté disponible para añadir una capa adicional de seguridad a tus

cuentas. Incluso, si alguien obtiene acceso a tus contraseñas, esta medida de seguridad adicional puede proteger tu cuenta. Si necesitas ayuda para habilitar la autenticación de dos factores, consulta la sección de preguntas frecuentes o el soporte técnico de la página correspondiente, ya que los pasos pueden variar según la aplicación.

6. Evita guardar tus contraseñas en papel o en hojas físicas: Tus contraseñas quedan expuestas a cualquier persona que tenga acceso al lugar donde se guardaron. Siempre que sea posible, utiliza métodos digitales más seguros para almacenar tus contraseñas. En caso de que sea absolutamente necesario escribir tus contraseñas, considera utilizar algún tipo de codificación para que la contraseña no quede expuesta tal como debe ser utilizada.

6.4

Cómo Cambiar la Contraseña del módem Telmex

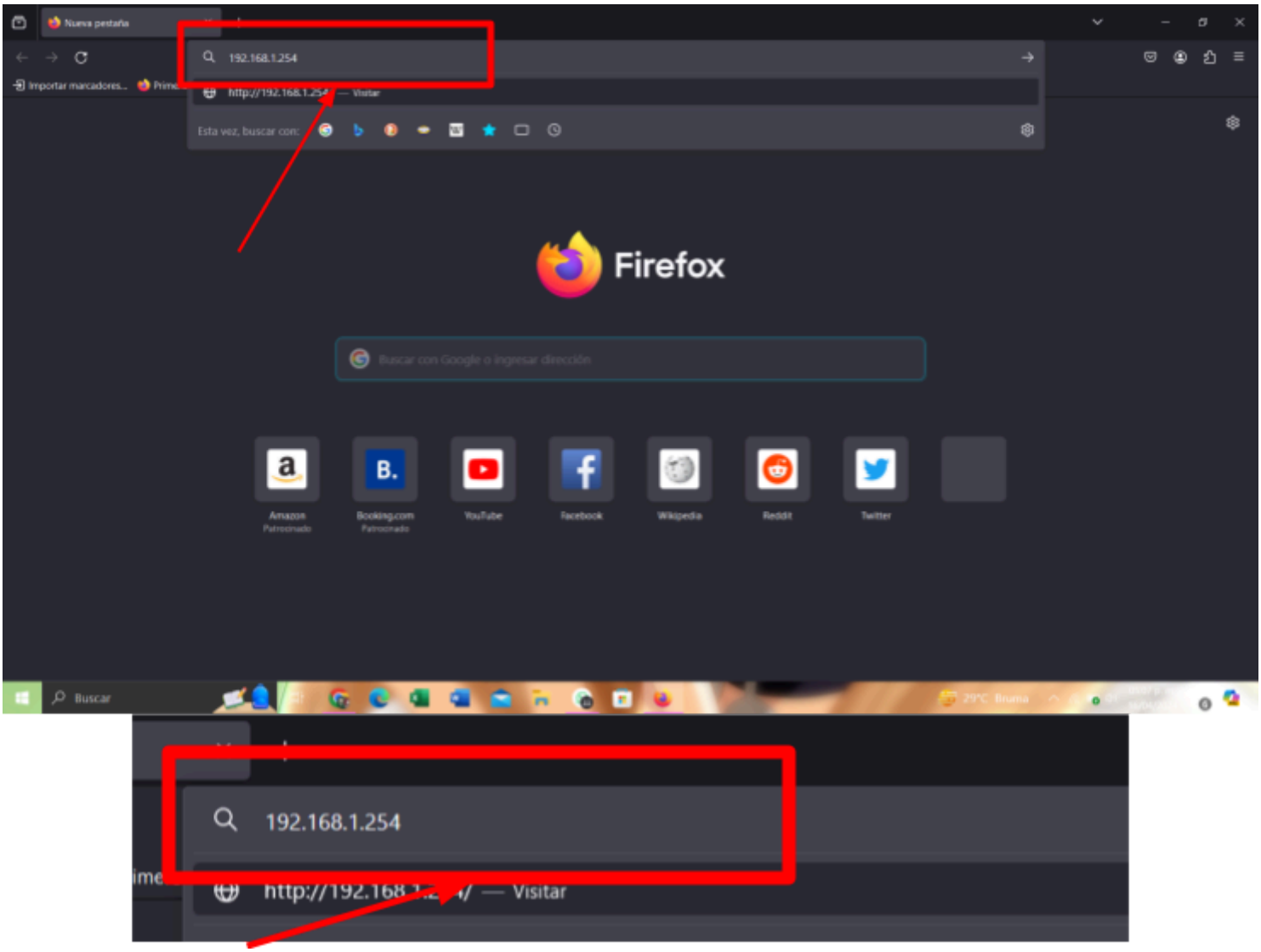
Cambiar la contraseña de tu módem Telmex es una medida de seguridad esencial para proteger tu red doméstica. Una contraseña segura ayuda a prevenir accesos no autorizados, protege tu información personal y asegura que sólo los dispositivos autorizados puedan conectarse a tu red Wi-Fi. A continuación, se detallan los pasos para cambiar la contraseña de tu módem Telmex:

1. Acceder a la Interfaz de Configuración del Módem.

- Conecta tu computadora al módem Telmex mediante un cable Ethernet o a través de una conexión Wi-Fi.
- Abre un navegador web e ingresa la siguiente dirección en la barra de direcciones: http://192.168.1.254/. Presiona Enter.

Figura 6.25

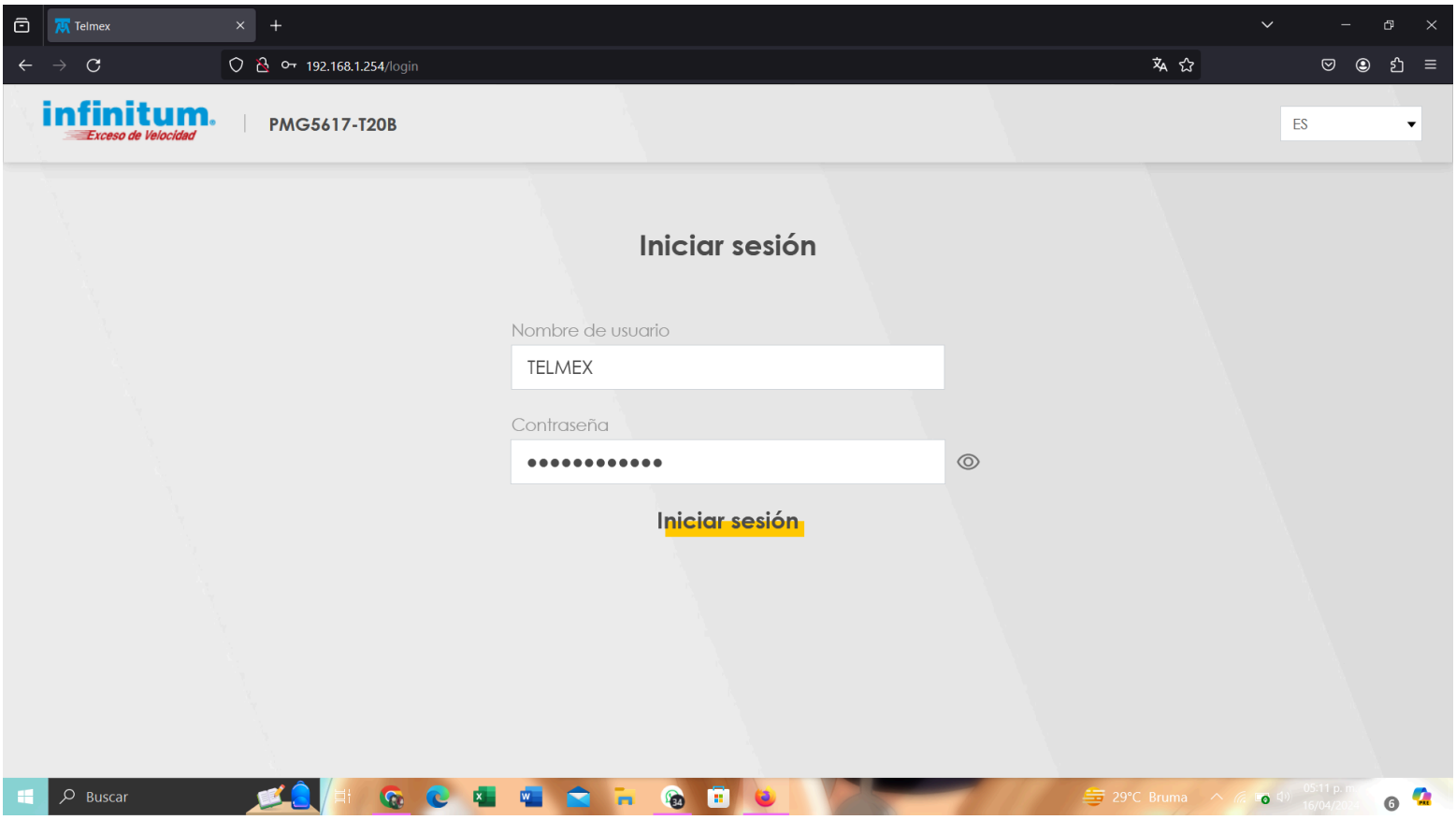
Cambiar contraseña modem telmex paso 1



- Se abrirá la página de inicio de sesión del módem. Ingresa el nombre de usuario y la contraseña y da click en “iniciar sesión”. Por lo general, el nombre de usuario es Telmex y la contraseña es Telmex o está en la etiqueta del módem.

Figura 6.26

Cambiar contraseña modem Telmex paso 2



2. Cambiar la Contraseña

- Una vez que hayas iniciado sesión, busca la sección de configuración de la red inalámbrica y selecciona Wi-Fi.

Figura 6.27

Cambiar contraseña modem telmex paso 3

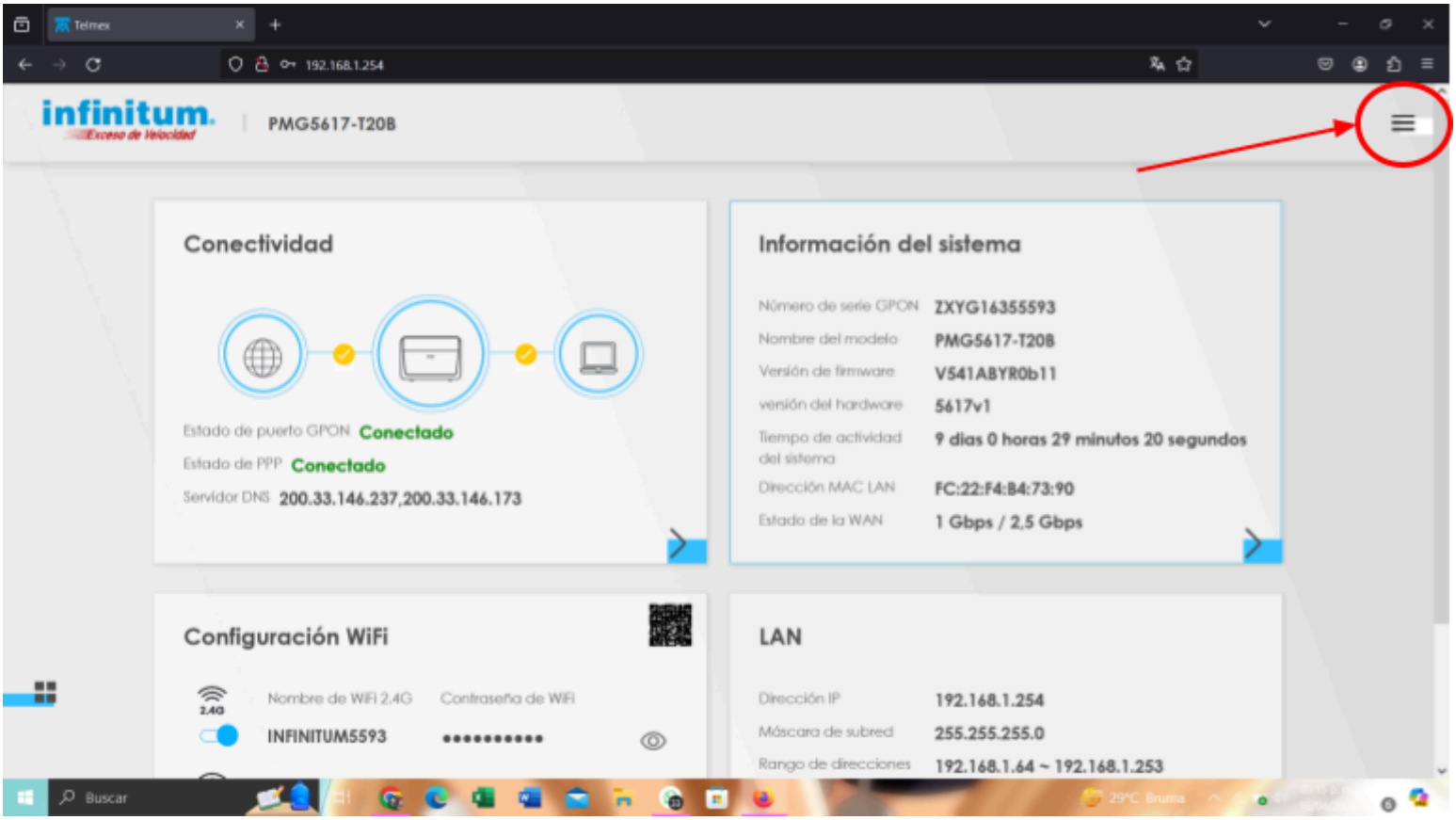


Figura 6.28

Cambiar contraseña modem telmex paso 4

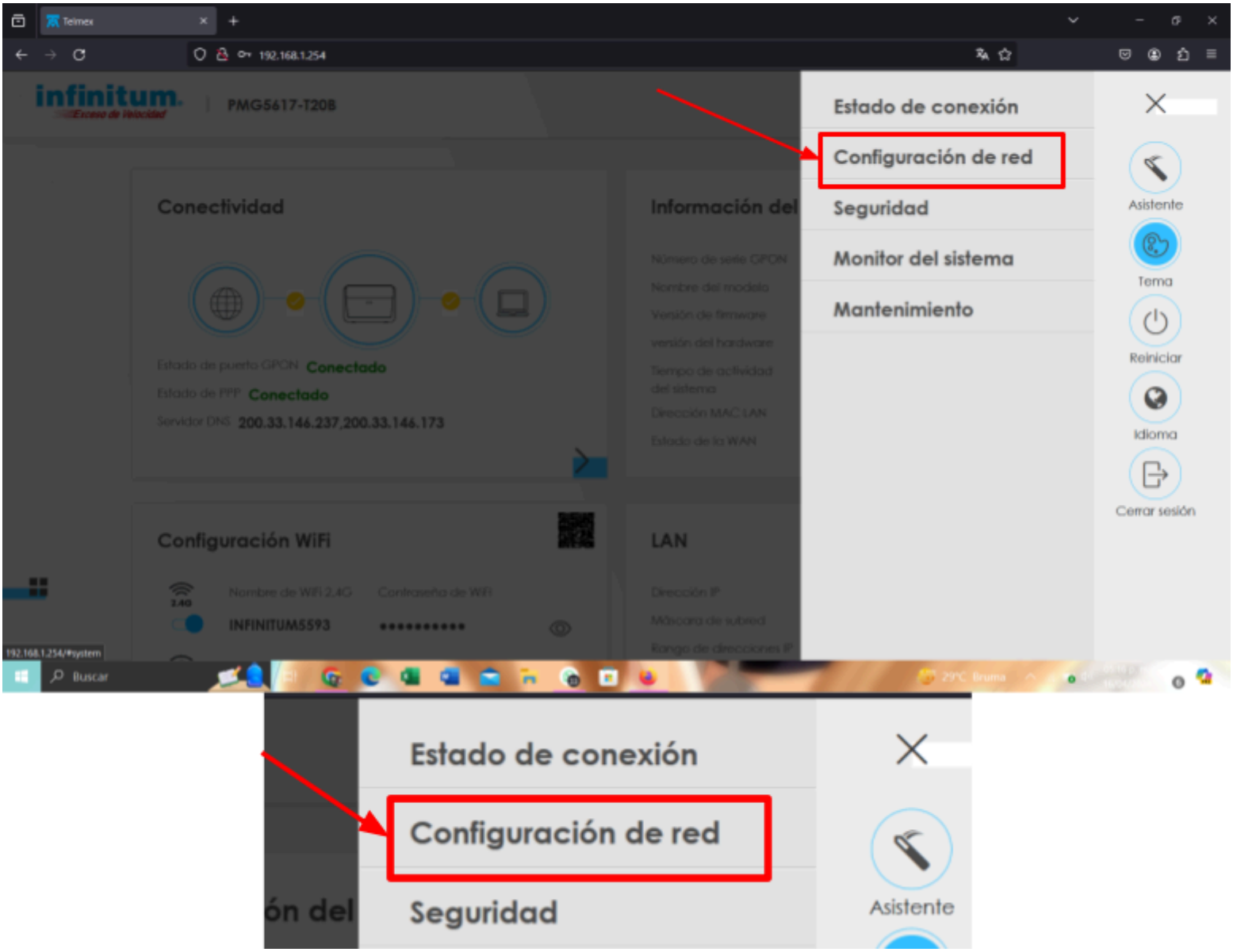
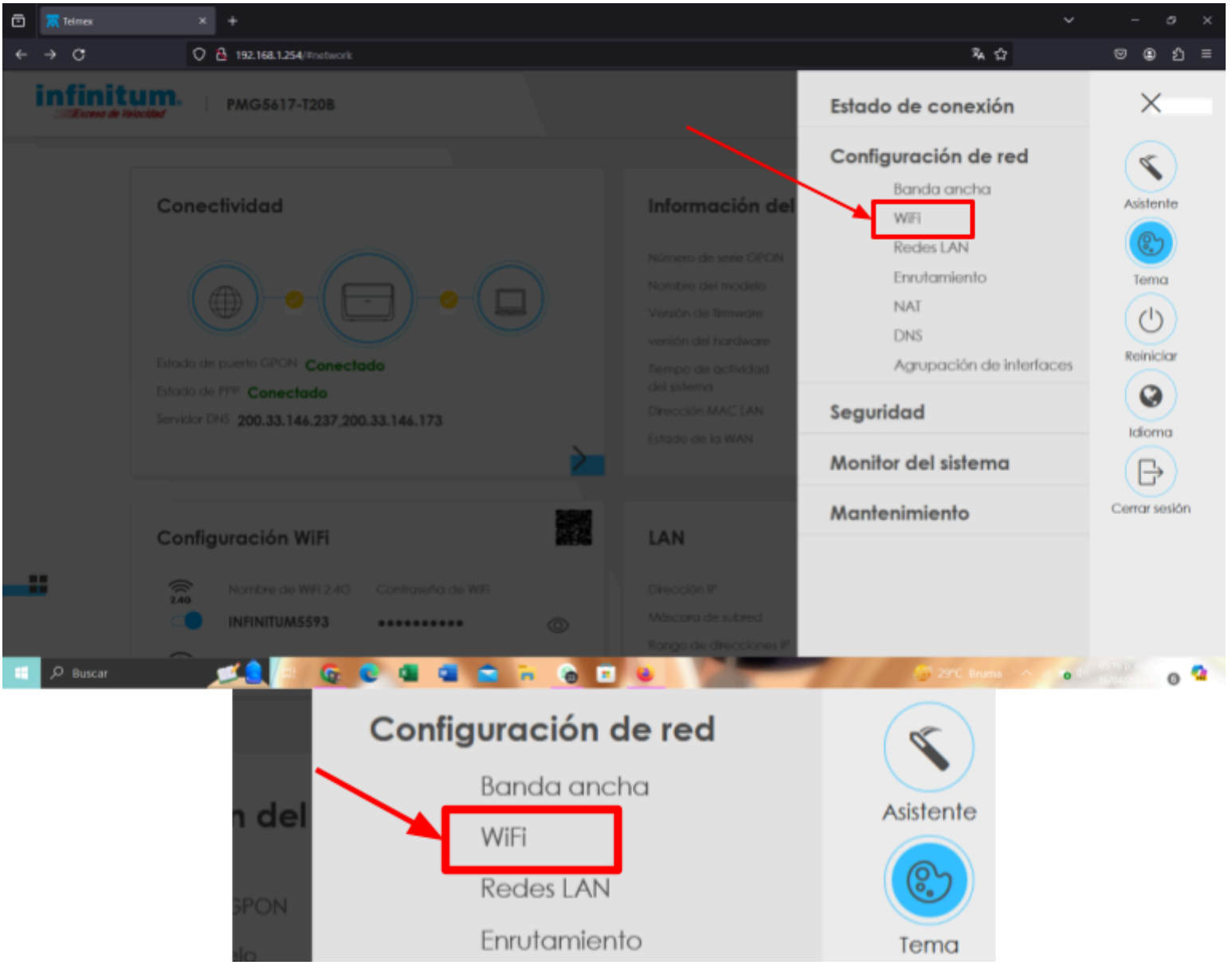


Figura 6.29

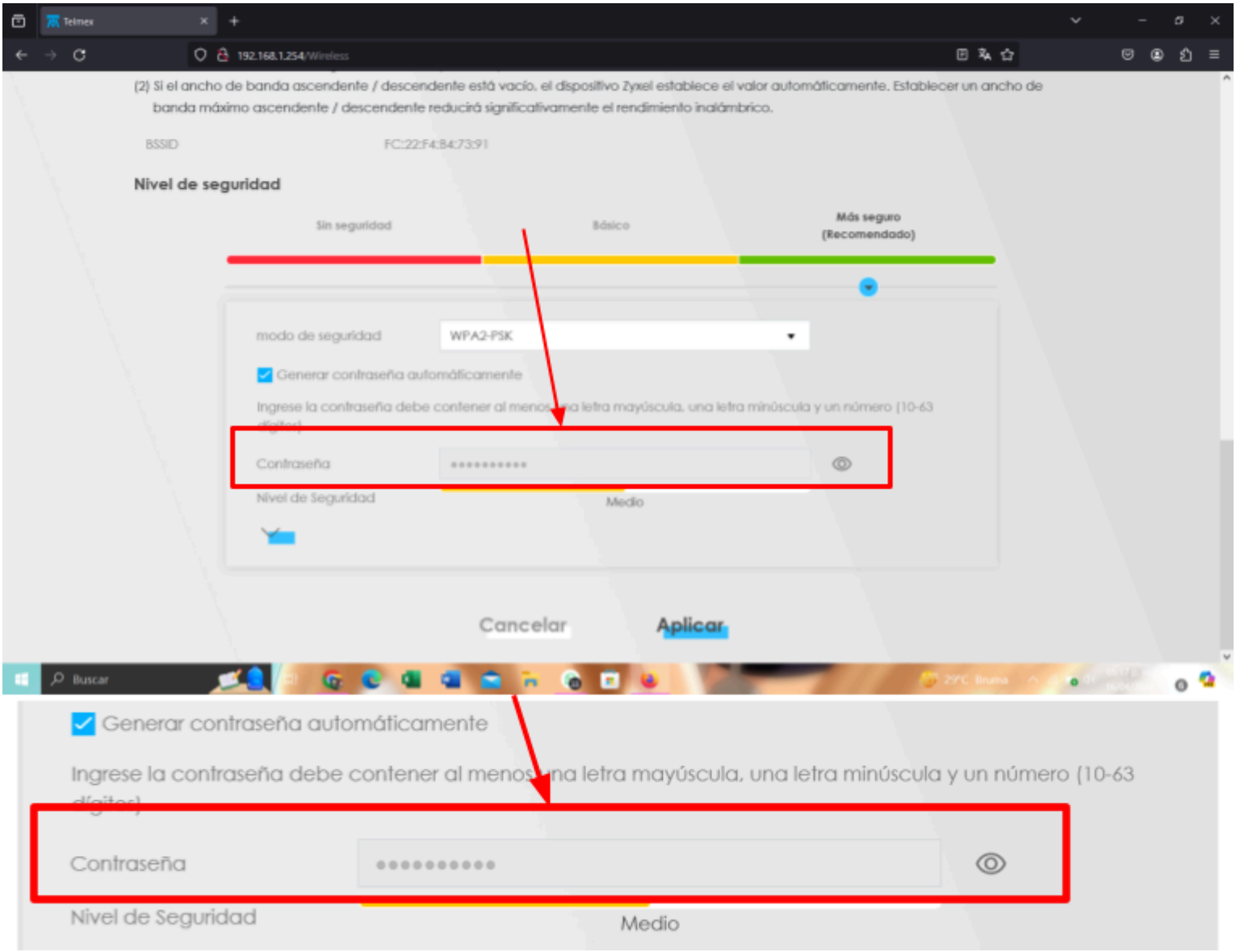
Cambiar contraseña modem telmex paso 5



- Dentro de esta sección, busca la opción para cambiar la contraseña de la red Wi-Fi. Puede estar etiquetada como "Contraseña", "Clave de seguridad", o similar.

Figura 6.30

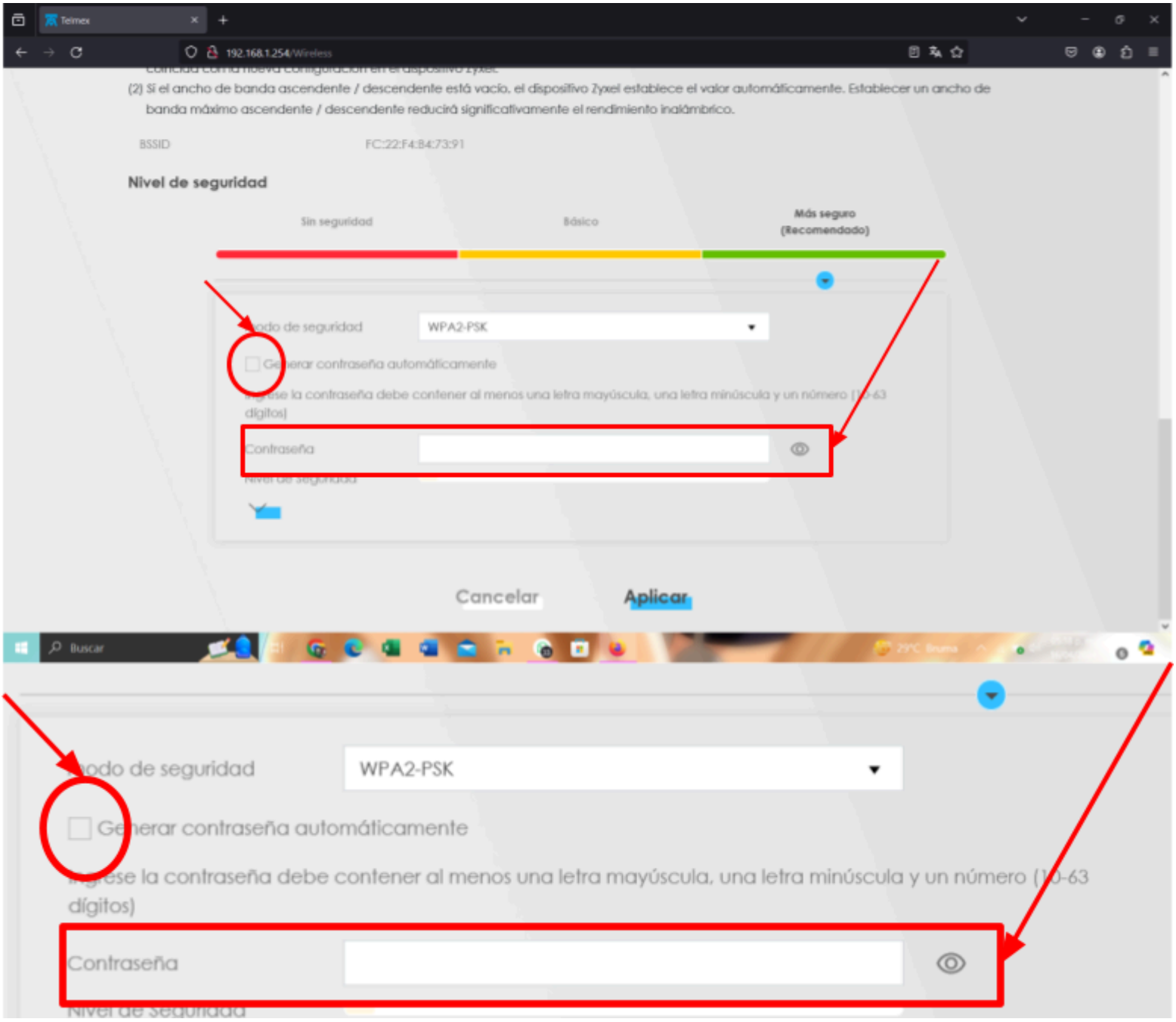
Cambiar contraseña modem telmex paso 6



- Desmarca la casilla de “generar contraseña automáticamente” e ingresa la nueva contraseña que deseas utilizar. Asegúrate de que sea una combinación segura de letras, números y caracteres especiales (Para más información puedes revisar el punto 2 “Creación de contraseñas seguras” de este manual).

Figura 6.31

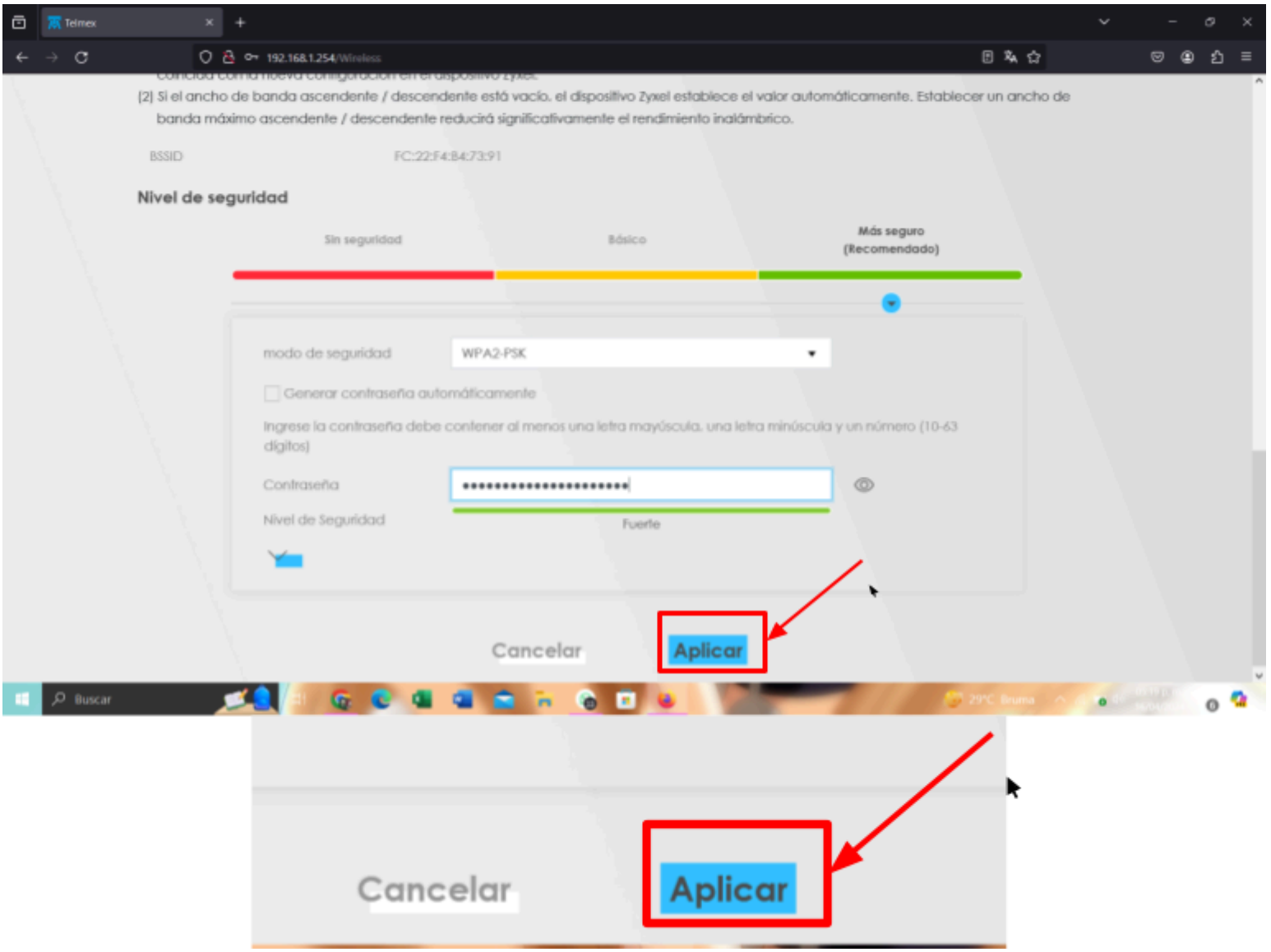
Cambiar contraseña modem Telmex paso 7



- Guarda los cambios y cierra la sesión del módem.

Figura 6.32

Cambiar contraseña modem Telmex paso 8

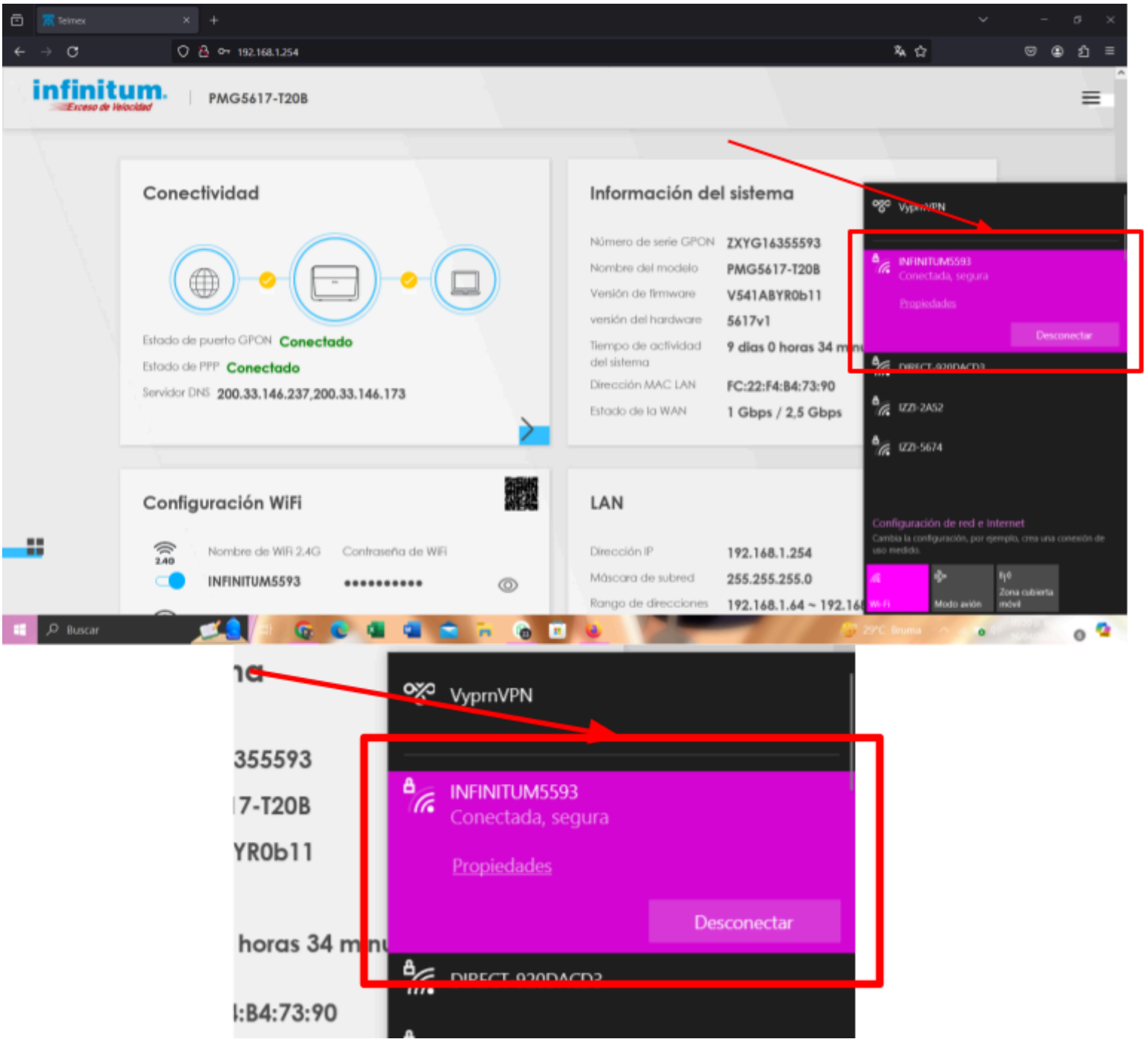


3. Verificar la Nueva Contraseña

- Para asegurarte de que la contraseña se ha cambiado correctamente, intenta conectarte a la red Wi-Fi utilizando la nueva contraseña.

Figura 6.33

Cambiar contraseña modem Telmex paso 9



Consideraciones Adicionales

- Contraseña Fuerte: Asegúrate de que la nueva contraseña sea fuerte y segura. Utiliza una combinación de letras mayúsculas, minúsculas, números y símbolos para aumentar la complejidad. Consulta el punto 2, "*Creación de contraseñas seguras*", de este manual para obtener instrucciones detalladas.
- Actualización Regular: Cambia la contraseña de tu módem periódicamente, por ejemplo, cada seis meses, para mantener la seguridad de tu red.
- No Compartir la Contraseña: Evita compartir la contraseña de tu Wi-Fi con personas no autorizadas. Si es necesario proporcionar acceso temporal, considera cambiar la contraseña después de que ya no sea necesario.
- Evita Usar Contraseñas Predeterminadas: Las contraseñas predeterminadas de los módems son conocidas y pueden ser vulnerables a ataques. Asegúrate de cambiar la contraseña predeterminada inmediatamente después de instalar el módem.
- Reinicio del Módem: Algunos módems requieren reiniciarse después de cambiar la contraseña. Asegúrate de seguir las instrucciones específicas de tu módem Telmex para completar el proceso de cambio de contraseña.
- Monitoreo de Dispositivos Conectados: Después de cambiar la contraseña, revisa qué dispositivos están conectados a tu red para asegurarte de que sólo los dispositivos autorizados tengan acceso. Puedes hacerlo desde la interfaz de administración del módem. Consulta el punto 11, "Verificar qué dispositivos están conectados a mi módem Telmex", de este manual para obtener instrucciones detalladas.

Nota:No olvides guardar tu contraseña en un lugar seguro para no olvidarla, para ello te puedes ayudar del punto 3 "Almacenamiento seguro de contraseñas" que se encuentra en este manual.

6.5 Cómo configurar IP Estática en tu Modem Telmex

6.5

Cómo Cambiar la Contraseña del módem Telmex

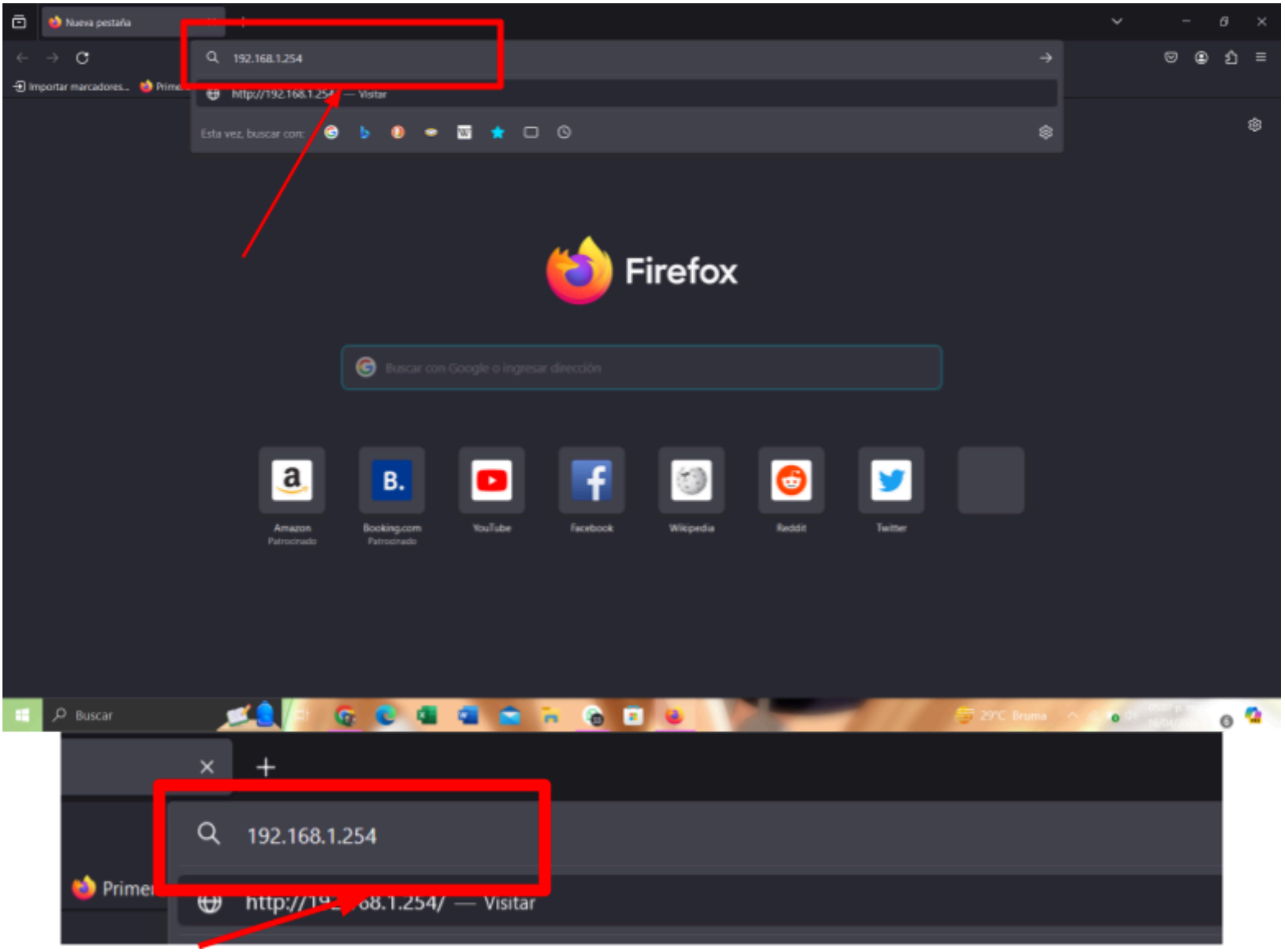
Asignar una IP estática a tu dispositivo desde el módem Telmex puede ser útil para asegurar una conexión estable en tu red doméstica, especialmente si tienes dispositivos que dependen de una dirección IP constante, como cámaras de seguridad o servidores. A continuación, se detallan los pasos para configurar una IP estática en tu módem Telmex.

Acceder a la Interfaz de Configuración del módem

1. Conecta tu computadora al módem Telmex mediante un cable Ethernet o una conexión Wi-Fi para acceder a la interfaz de configuración.
2. Abre un navegador web y escribe la dirección del módem en la barra de direcciones: http://192.168.1.254/. Luego, presiona Enter.
    - Nota: Si no puedes acceder a esta dirección, revisa el manual del módem para verificar la dirección de acceso.

Figura 6.34

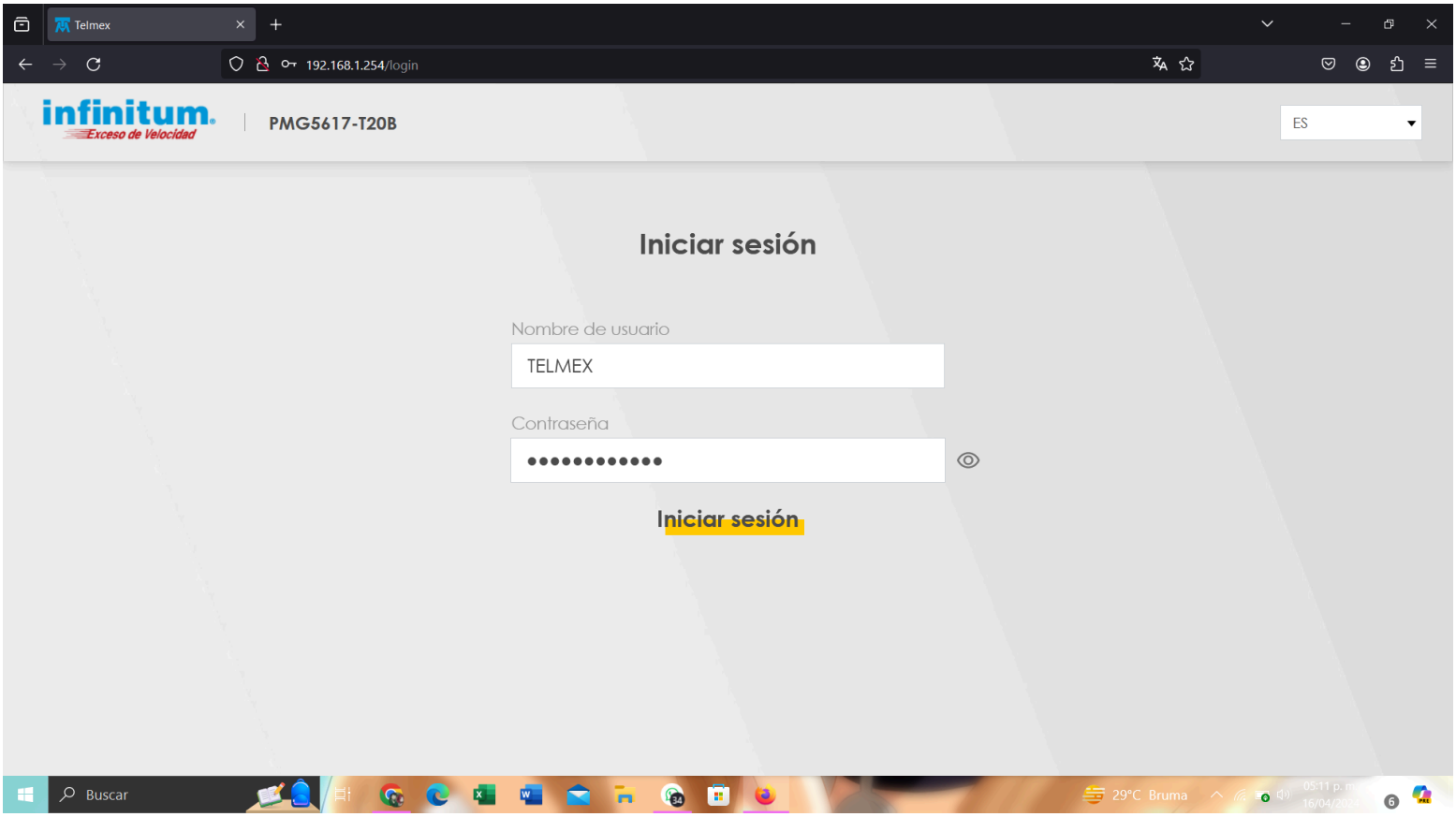
Cambiar contraseña modem Telmex paso 1



3. Inicia sesión en la interfaz. Ingresa el nombre de usuario y la contraseña de tu módem. Por lo general, ambos son "Telmex" o están impresos en una etiqueta en la parte trasera del módem.

Figura 6.35

Cambiar contraseña modem Telmex paso 2

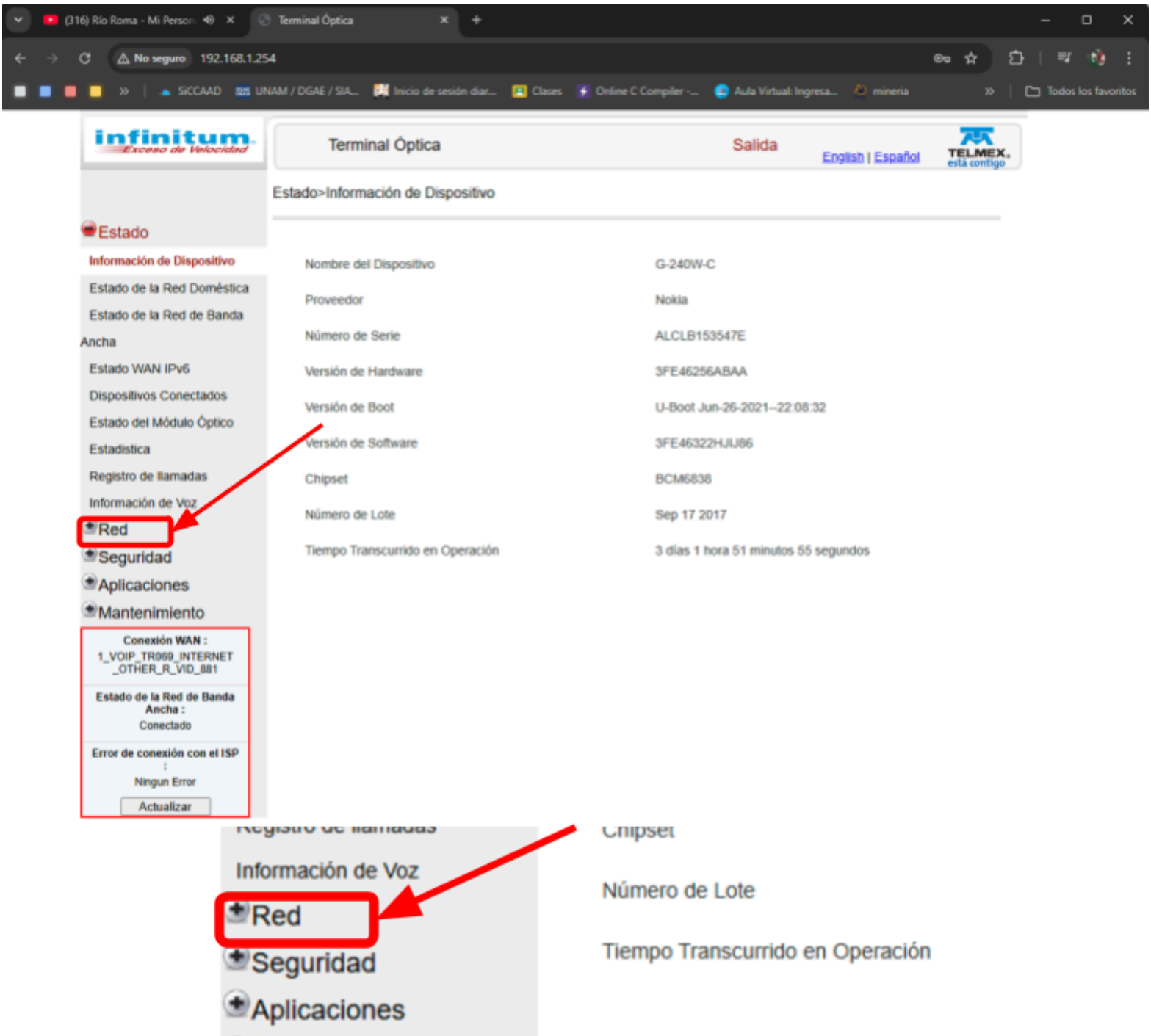


Configuración de IP Estática

1. Una vez que hayas iniciado sesión, dirígete a la sección de configuración de red o LAN. La ubicación exacta puede variar según el modelo del módem, pero suele estar en “Red” o “LAN Settings”.

Figura 6.36

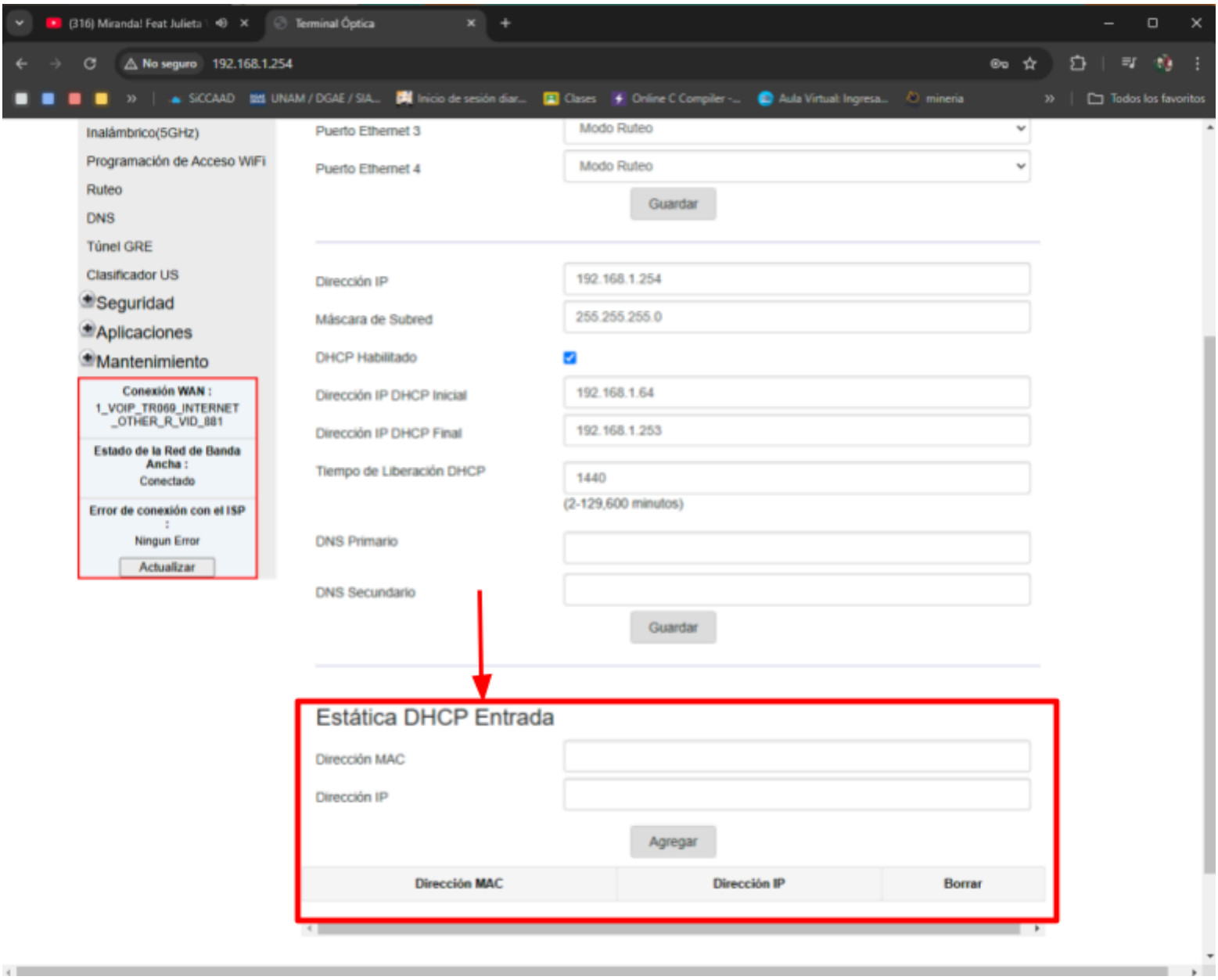
Cambiar contraseña modem Telmex paso 3



2. En esta sección, busca la opción para asignar IP estáticas o reservar direcciones IP. Esto puede aparecer como "Asignación de IP manual" o "Estática DHCP Entrada".

Figura 6.37

Cambiar contraseña modem Telmex paso 4



3. Localiza el dispositivo al que deseas asignar una IP estática. Deberías ver una lista de dispositivos conectados a la red, identificados por su nombre de dispositivo o dirección MAC, esto lo puedes ver desde el apartado “Estado -> Dispositivos conectados”. Para una explicación más detallada consulta el punto 11, “Verificar qué dispositivos están conectados a un módem Telmex”, de este manual para obtener instrucciones detalladas.

Figura 6.38

Cambiar contraseña modem Telmex paso 5

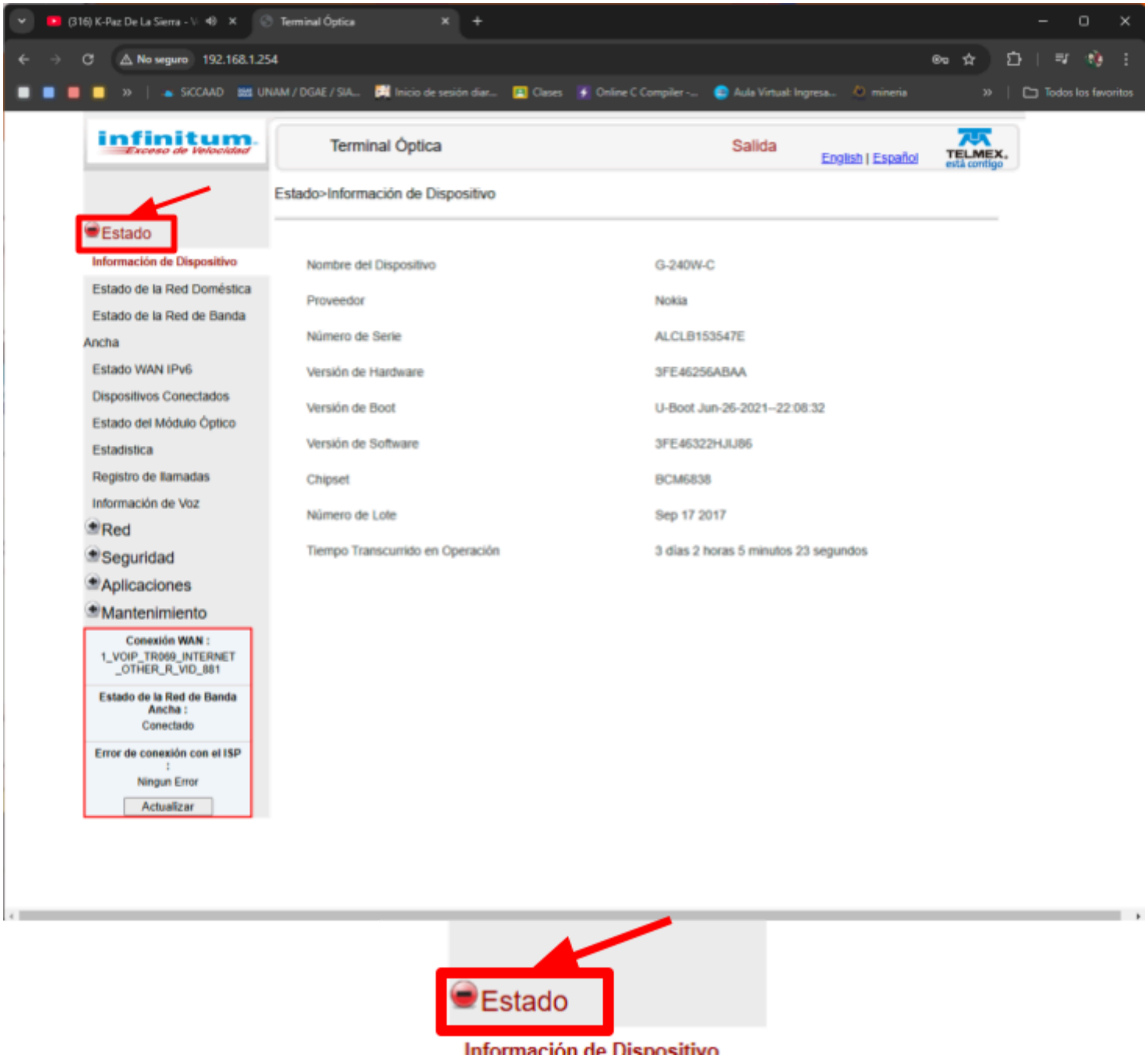
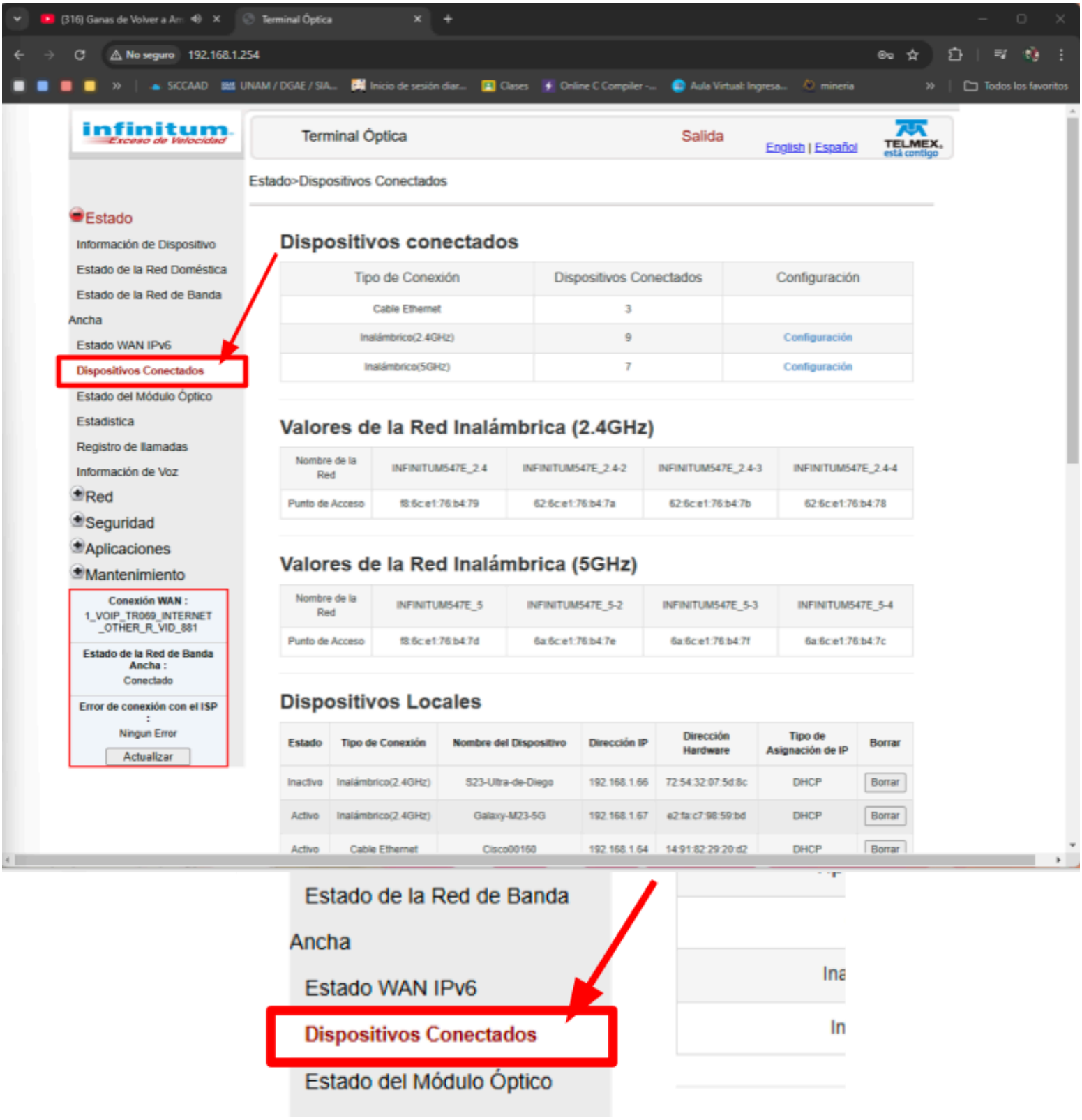


Figura 6.39

Cambiar contraseña modem Telmex paso 6



4. Aquí, deberás ubicar el dispositivo al que deseas asignar la dirección IP estática en la lista de dispositivos conectados, generalmente identificados por su nombre y dirección MAC (o dirección de hardware).

Figura 6.40

Cambiar contraseña modem Telmex paso 7

Dispositivos Locales

Estado	Tipo de Conexión	Nombre del Dispositivo	Dirección IP	Dirección Hardware	Tipo de Asignación de IP	Borrar
Inactivo	Inalámbrico(2.4GHz)	S23-Ultra-de-Diego	192.168.1.66	72:54:32:07:5d:8c	DHCP	Borrar
Activo	Inalámbrico(2.4GHz)	Galaxy-M23-5G	192.168.1.67	e2:fa:c7:98:59:bd	DHCP	Borrar
Activo	Cable Ethernet	Cisco00160	192.168.1.64	14:91:82:29:20:d2	DHCP	Borrar

5. Guarda la dirección IP que deseas asignar y anota la dirección MAC (o dirección de hardware) del dispositivo, ya que es necesaria para que el módem asocie la IP estática a ese dispositivo específico.
6. Volviendo al apartado de Red, agrega los datos del dispositivo deseado y asigna la dirección IP estática. Asegúrate de que la IP que elijas esté dentro del rango de la red (por ejemplo, 192.168.1.x) y que no se esté usando por otro dispositivo.
    - Ejemplo de IP estática: Si tu red usa la IP 192.168.1.0, puedes asignar al dispositivo la IP 192.168.1.100 para evitar conflictos.

Figura 6.41

Cambiar contraseña modem Telmex paso 8

Estática DHCP Entrada

Dirección MAC: 72:54:32:07:5d:8c

Dirección IP: 192.168.1.190

Agregar

Dirección MAC	Dirección IP	Borrar

7. Guarda los cambios y, si es necesario, reinicia el módem para aplicar la configuración.

Figura 6.42
Cambiar contraseña modem Telmex paso 9

Verificar la Configuración

1. Comprueba que el dispositivo esté usando la nueva IP estática. Puedes hacer esto desde la interfaz de configuración del módem o verificando la IP directamente en el dispositivo.
2. Realiza una prueba de conexión para asegurarte de que la conexión es estable y que el dispositivo se mantiene en la IP configurada.

Consideraciones Adicionales

- Evita conflictos de IP: Asegúrate de que la IP asignada no se encuentre en uso por otro dispositivo.
- Rango de IP adecuado: Si el módem permite un rango específico para las IP estáticas, asigna direcciones dentro de este rango.
- Mantenimiento de dispositivos críticos: Si algún dispositivo esencial en tu red pierde la conexión, verifica que su IP estática esté bien configurada.

Nota: Con esta configuración, tu dispositivo conservará la misma dirección IP en la red, lo que puede ser crucial para aplicaciones que requieren una conexión continua y predecible.

6.6

Cómo configurar una VPN en tu módem

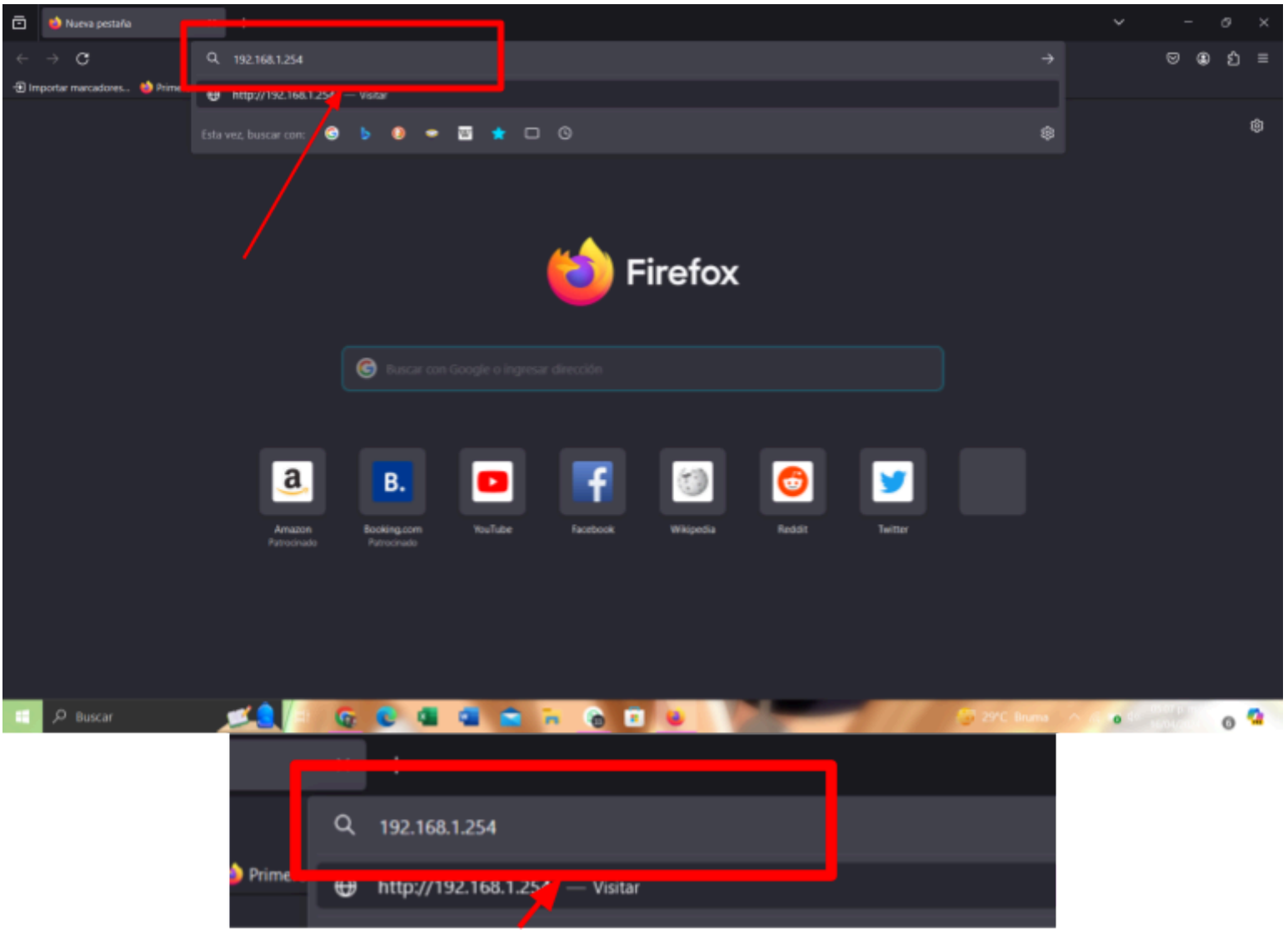
Configurar una VPN (Red Privada Virtual) en tu módem puede ayudarte a proteger tu privacidad y seguridad en internet. Una VPN en tu red doméstica permite que todos los dispositivos conectados se beneficien de una conexión más segura y privada, ocultando la dirección IP y cifrado el tráfico de internet. A continuación, se detallan los pasos para configurar una VPN en un módem .

Acceder a la interfaz de configuración del módem

1. Conecta tu computadora al módem mediante un cable Ethernet o a través de Wi-Fi para acceder a la interfaz de configuración.
2. Abre un navegador web e ingresa la dirección IP del módem en la barra de direcciones, generalmente http://192.168.1.254/. Luego, presiona Enter.

Figura 6.43

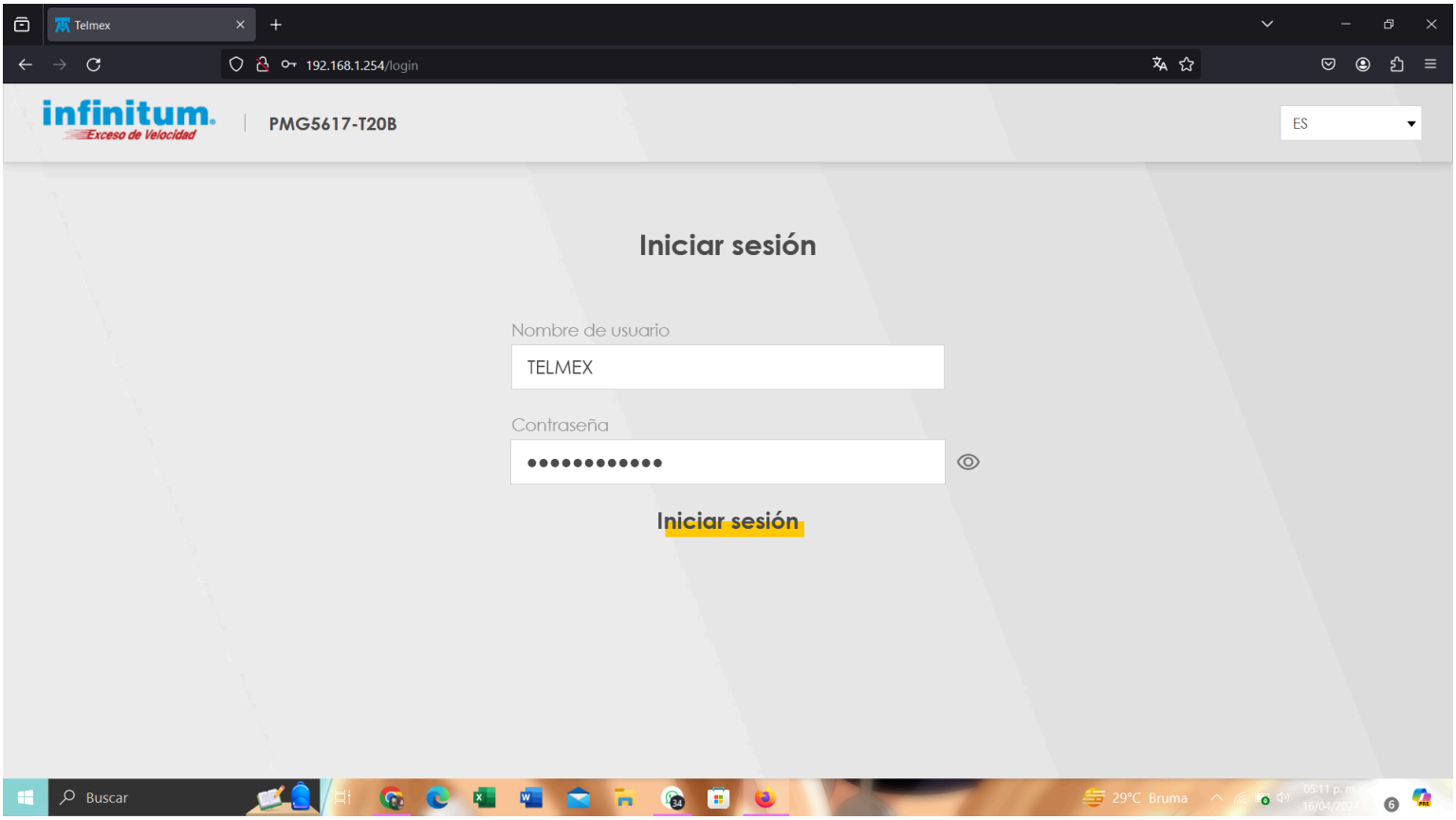
Configurar una VPN en tu módem paso 1



3. Inicia sesión en la interfaz del módem. Ingresa el nombre de usuario y la contraseña del módem. Por lo general, el nombre de usuario es "Telmex" y la contraseña suele estar en la etiqueta del módem.

Figura 6.44

Configurar una VPN en tu módem paso 2



Configurar la VPN en el módem

1. Una vez dentro de la interfaz, dirígete a la sección de configuración de red avanzada o busca una sección específica para VPN. Dependiendo del modelo del módem, esta opción puede aparecer como "VPN" o "Túneles VPN".

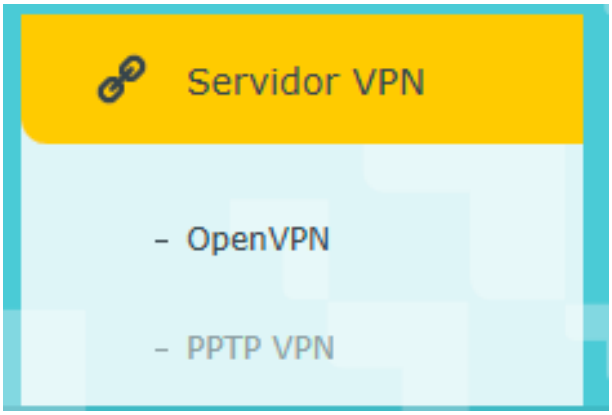
Figura 6.45

Configurar una VPN en tu módem paso 3

2. Selecciona el protocolo de VPN que deseas configurar. Algunos módems permiten configurar protocolos como PPTP, L2TP o OpenVPN. Asegúrate de elegir el protocolo adecuado según el tipo de conexión que necesitas y la compatibilidad de tus dispositivos.
    - Nota: OpenVPN suele ser el protocolo más seguro, mientras que PPTP es más fácil de configurar pero menos seguro.

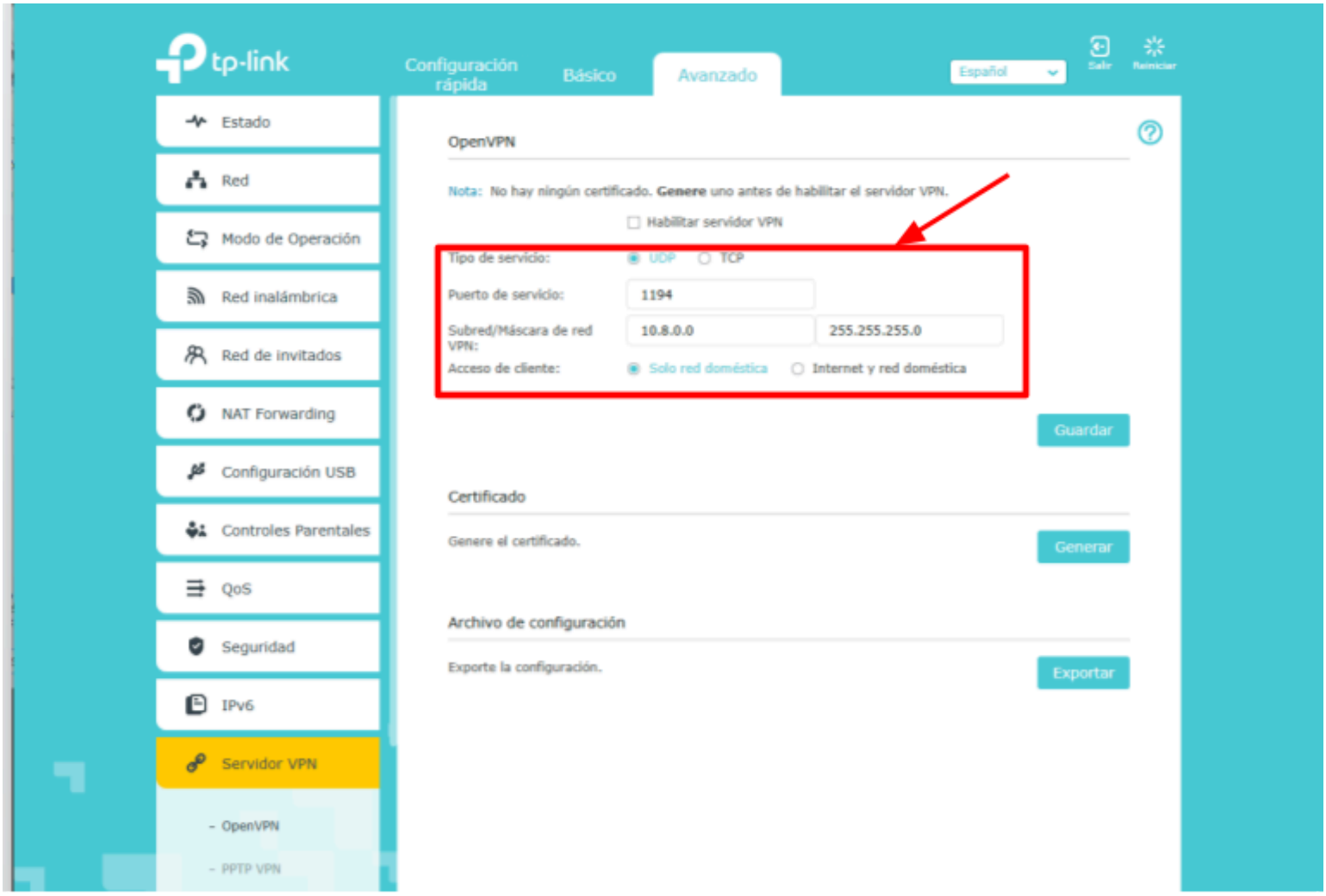
Figura 6.46

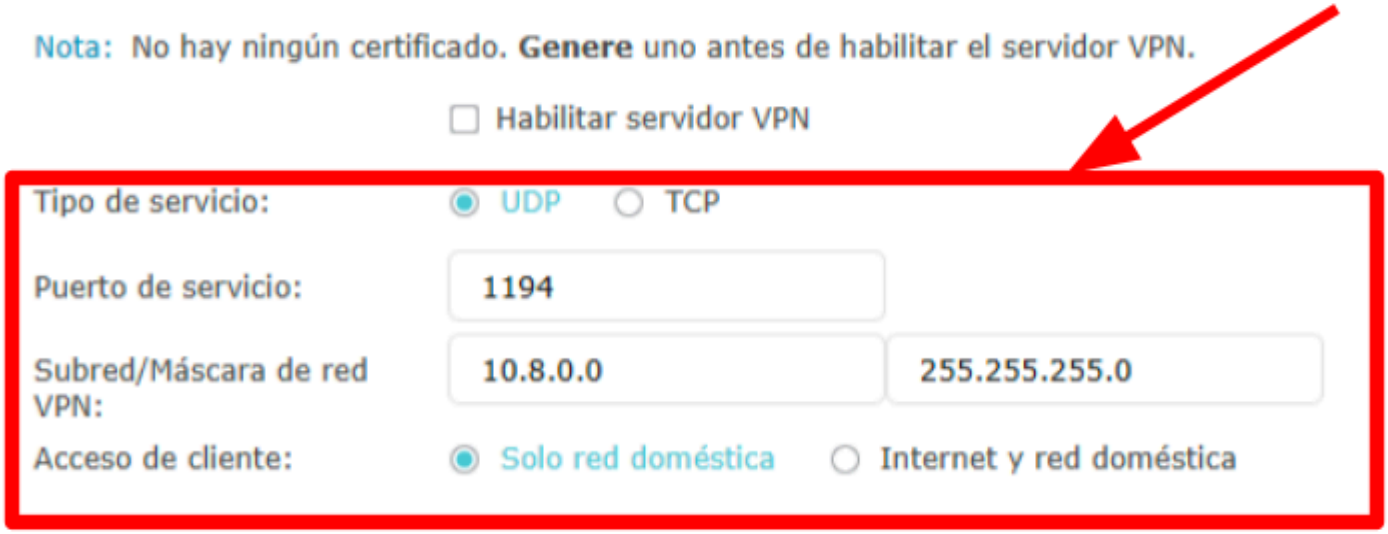
Configurar una VPN en tu módem paso 4



3. Introduce los detalles de la VPN:
    - Servidor VPN: Proporciona la dirección del servidor VPN que tienes. En este caso, verifica que sea la dirección correcta y que el puerto esté configurado según las recomendaciones, generalmente 1194 para OpenVPN.
    - Tipo de Servicio: Selecciona UDP o TCP según las recomendaciones de tu servicio de VPN o tus necesidades. UDP es generalmente más rápido, pero TCP puede ser más confiable en redes inestables.
    - VPN Subnet/Netmask: Ingresa la red y máscara de subred (en este caso, 10.8.0.0 / 255.255.255.0) para la red VPN. Esto define el rango de direcciones IP que se asignarán a los dispositivos conectados a la VPN.
    - Acceso del Cliente: Selecciona la opción que prefieras según el tipo de acceso que quieres dar a los dispositivos conectados a la VPN. Home Network Only permitirá solo el acceso a tu red local, mientras que Internet and Home Network permitirá acceso tanto a internet como a la red local.

Figura 6.47
Configurar una VPN en tu módem paso 5

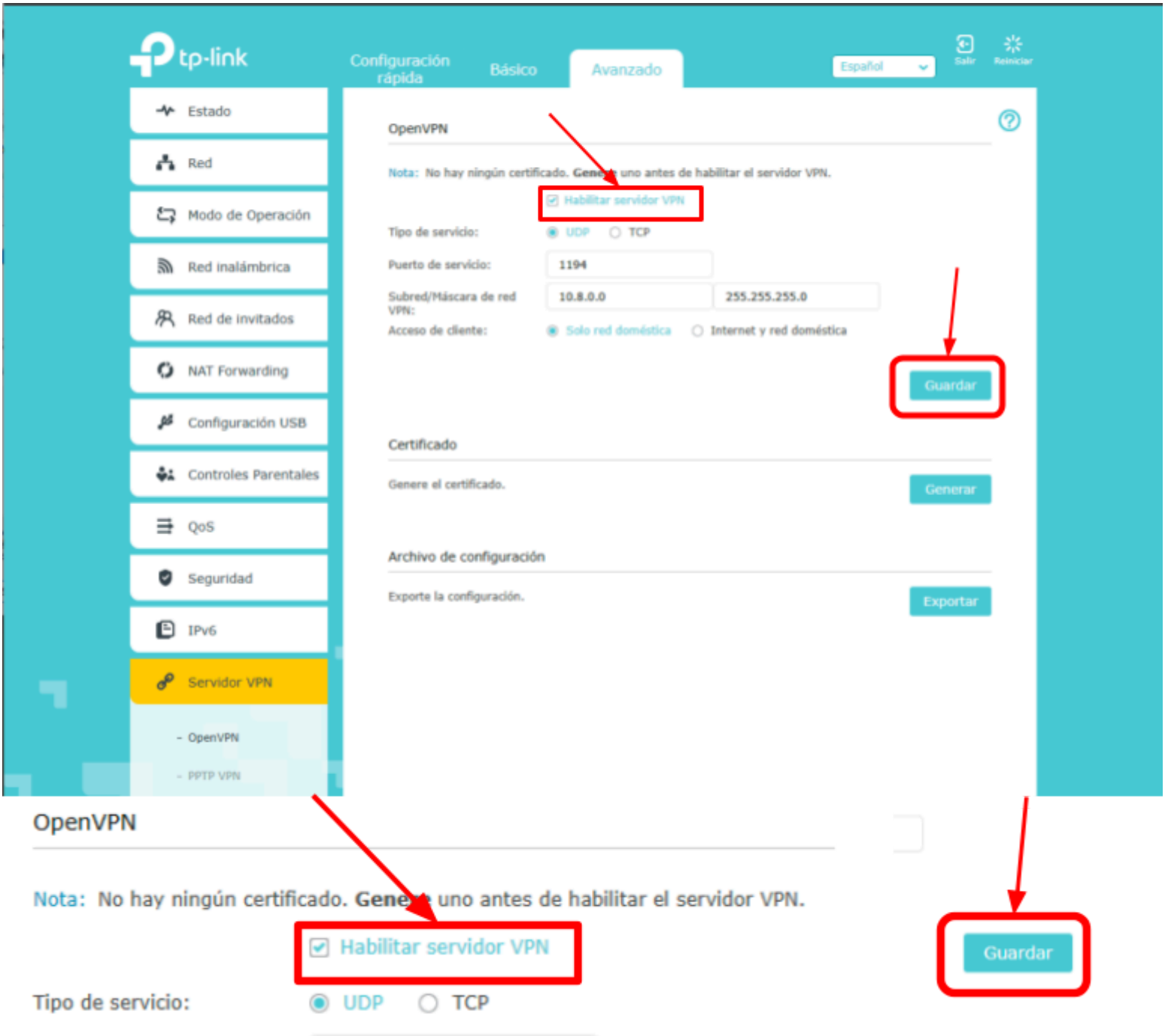




4. Habilita la VPN y guarda la configuración. Una vez que hayas ingresado toda la información, guarda los cambios y, si es necesario, reinicia el módem para que la configuración de la VPN se aplique correctamente.

Figura 6.48

Configurar una VPN en tu módem paso 6



Verificar la Conexión VPN

1. Una vez configurada, verifica que la VPN esté activa en la red. Todos los dispositivos conectados a través de este módem deberían ahora estar navegando bajo la IP y la protección del servidor VPN.
2. Puedes confirmar la conexión visitando un sitio como whatismyip.com para ver si la IP corresponde a la ubicación del servidor VPN en lugar de tu IP pública original.

Consideraciones Adicionales

- **Alternativa: Configuración de VPN en el Router o Dispositivos**: Si tu módem no permite la configuración de VPN, puedes configurar la VPN en un router secundario conectado al módem. Esto permite una capa extra de protección en los dispositivos clave sin necesidad de configurar la VPN en todo el módem.
- **Impacto en la Velocidad de Internet**: La VPN puede reducir ligeramente la velocidad de tu conexión, ya que añade cifrado y redirecciona el tráfico. Esto es normal y depende de la distancia al servidor VPN y el protocolo que uses.
- **Protocolo de Seguridad**: Si la seguridad es una prioridad, asegúrate de usar OpenVPN o protocolos más seguros en lugar de PPTP.
- **Desconectar la VPN cuando no sea necesaria**: Si no necesitas la VPN activada, puedes desactivarla desde la configuración del módem para liberar un poco de ancho de banda.
- **Mantenimiento de la VPN**: Revisa periódicamente la conexión de la VPN para asegurarte de que esté funcionando correctamente y que se mantenga segura. Algunos servicios de VPN requieren actualizaciones o reconexiones manuales, por lo que es importante monitorear la conexión para evitar desconexiones inesperadas.

Nota: Es importante recordar que no todos los módems y routers soportan la funcionalidad de servidor o cliente VPN de forma nativa. Antes de configurar una VPN, asegúrate de que tu dispositivo es compatible y que cuenta con esta función habilitada en la interfaz de configuración. Algunos routers permiten únicamente la configuración de VPN para acceso remoto de dispositivos específicos, mientras que otros pueden habilitar toda la red para enrutar a través de la VPN. Revisa la documentación del fabricante o consulta con el soporte técnico para confirmar que tu módem permite esta funcionalidad y que cumple con los requisitos para establecer una conexión VPN segura.

6.7

6.7. Cómo actualizar mi sistema operativo

Cómo actualizar mi sistema operativo

Actualizar el sistema operativo de tu dispositivo es fundamental para garantizar su seguridad y proteger tus datos debido a que presenta las siguientes mejoras:

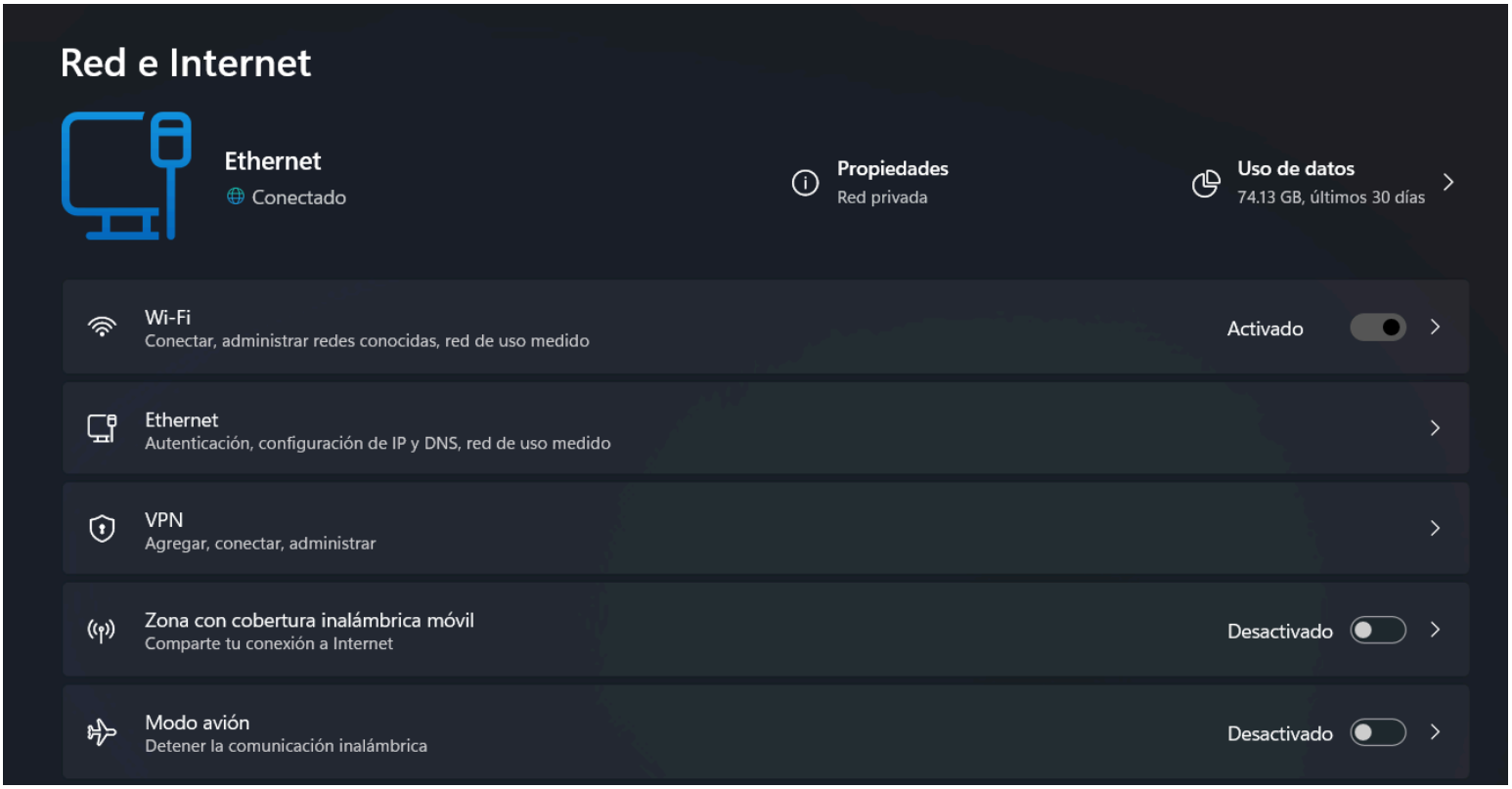
- Parches de seguridad: Las actualizaciones suelen incluir parches que corrigen vulnerabilidades conocidas en el sistema operativo. Estas vulnerabilidades podrían ser explotadas por ciberdelincuentes para infectar tu dispositivo con malware o acceder a tu información personal.
- Protección contra malware: Las actualizaciones también pueden incluir mejoras en la seguridad que ayudan a proteger tu dispositivo contra malware y otras amenazas. Estas mejoras pueden fortalecer la seguridad del sistema operativo y de las aplicaciones instaladas.
- Mejoras en la seguridad de datos: Al mantener tu sistema operativo actualizado, también te beneficias de mejoras en la seguridad de los datos. Esto incluye cifrado mejorado, controles de acceso más estrictos y medidas para proteger la privacidad de tus datos.
- Compatibilidad con aplicaciones y hardware: Las actualizaciones a menudo incluyen mejoras de compatibilidad que aseguran que tu dispositivo funcione correctamente con las más recientes aplicaciones y hardware. Esto también puede tener un impacto positivo en la seguridad al garantizar que todo esté actualizado y funcionando correctamente.

Pasos para actualizar el sistema operativo Windows:

1. Conexión a Internet: Asegúrate de tener una conexión a Internet estable antes de comenzar el proceso de actualización.

Figura 6.49

Actualización de sistema operativo Windows paso 1



2. Abrir Configuración: Haz clic en el botón de Inicio y selecciona "Configuración" (icono de engranaje) o presiona la tecla de Windows + I para abrir la Configuración.

Figura 6.50

Actualización de sistema operativo Windows paso 2

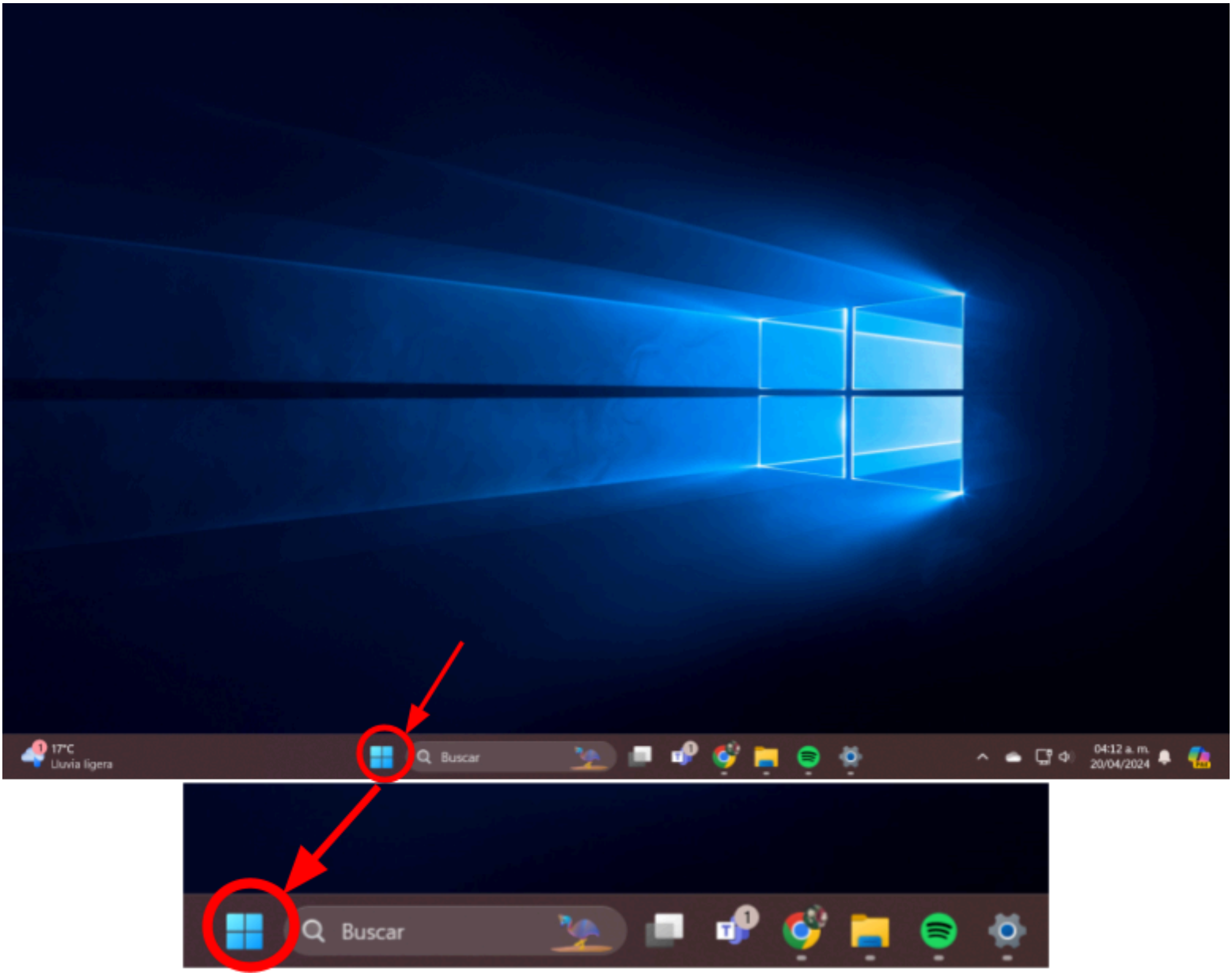
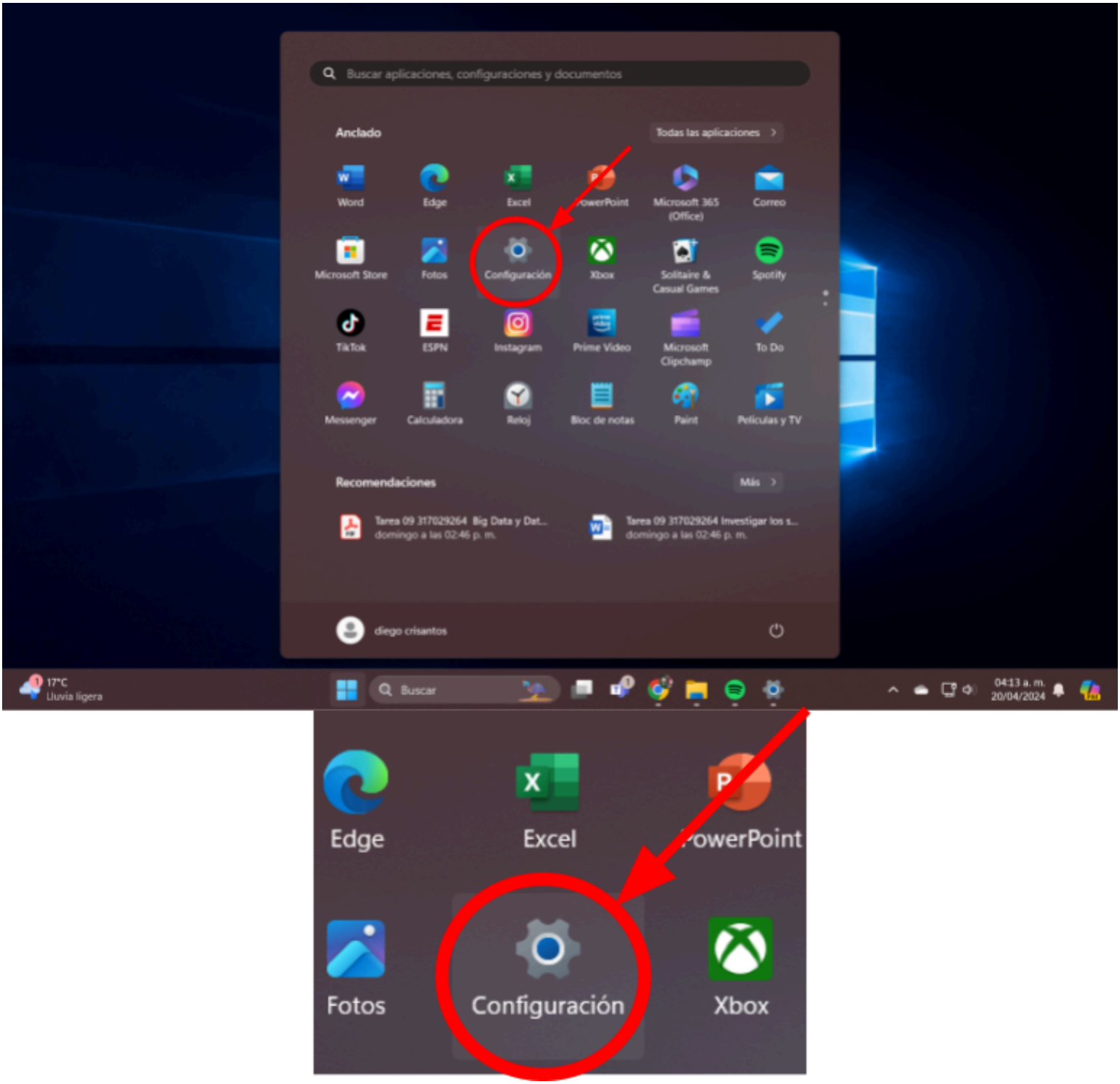


Figura 6.51

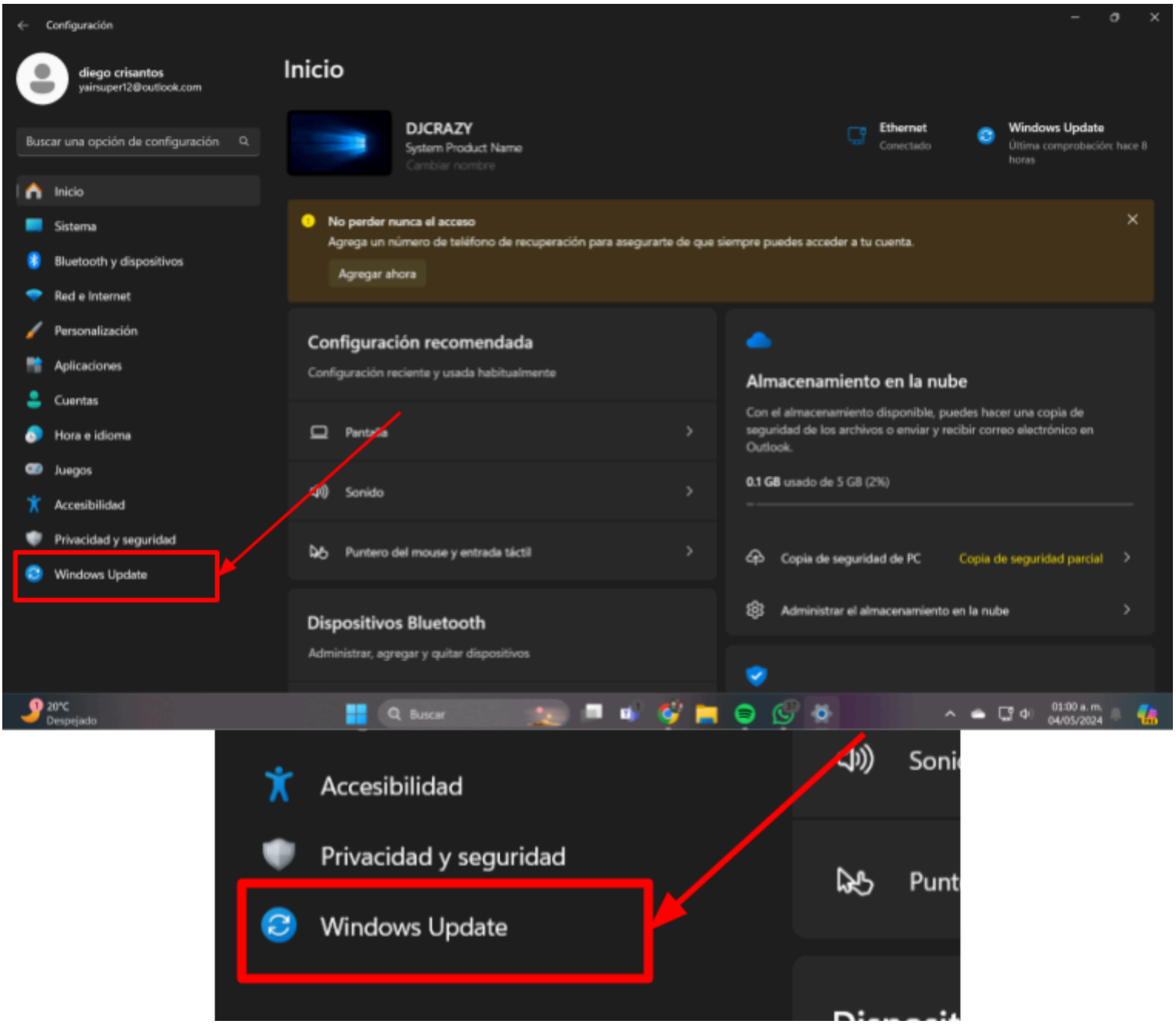
Actualización de sistema operativo Windows paso 3



3. Ir a Windows Update: Dentro de Configuración, haz clic en "Windows Update".

Figura 6.52

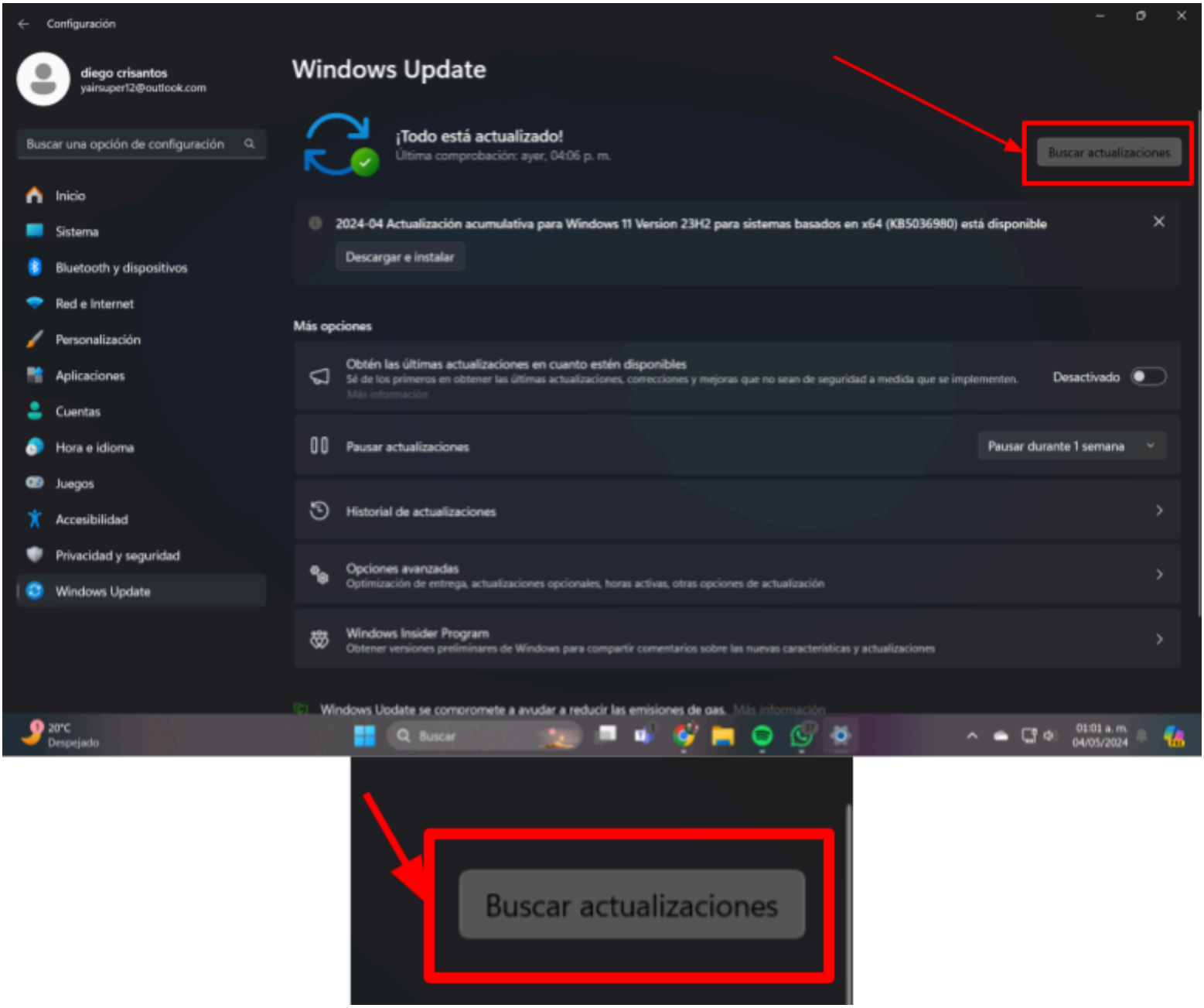
Actualización de sistema operativo Windows paso 4



4. Buscar actualizaciones: En la sección de Windows Update, haz clic en "Buscar actualizaciones". Windows buscará automáticamente actualizaciones disponibles para tu sistema.

Figura 6.53

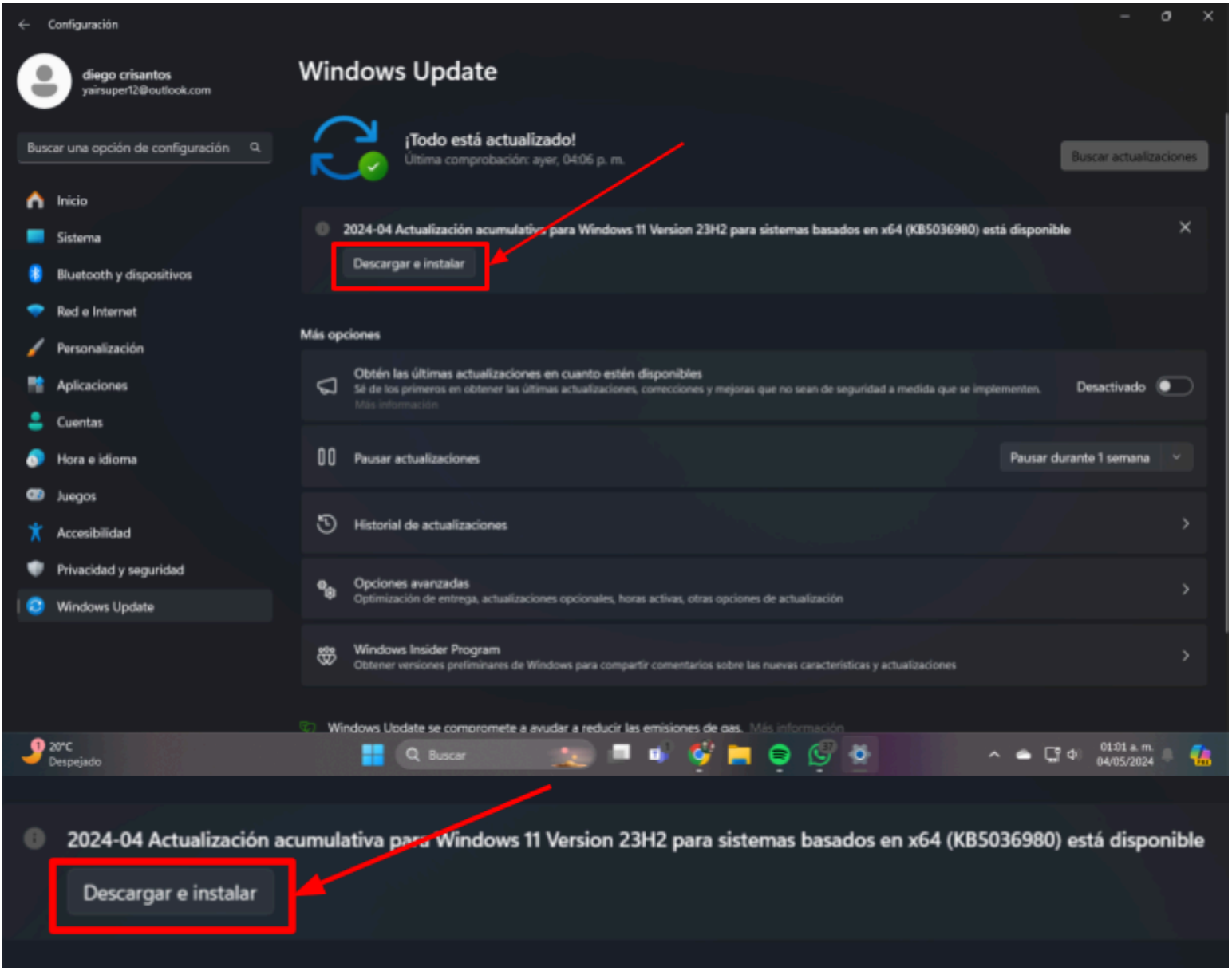
Actualización de sistema operativo Windows paso 5



5. Descargar e instalar actualizaciones: Si hay actualizaciones disponibles, haz clic en "Descargar" o "Descargar e instalar". Dependiendo del tamaño de las actualizaciones y la velocidad de tu conexión a Internet, esto puede tardar un tiempo.

Figura 6.54

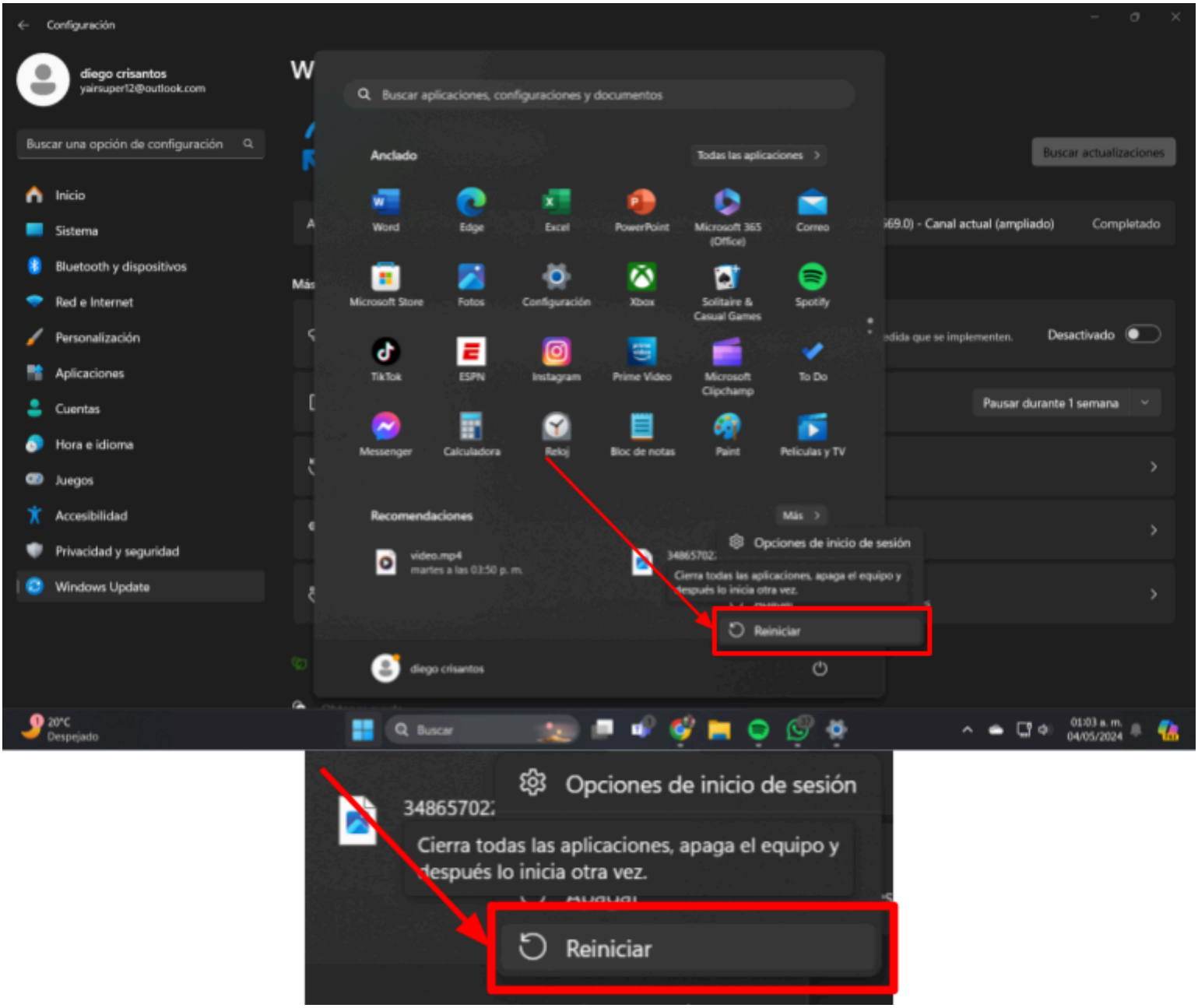
Actualización de sistema operativo Windows paso 6



6. Reiniciar: Después de descargar e instalar las actualizaciones, es posible que se te pida que reinicies tu computadora. Asegúrate de guardar cualquier trabajo antes de hacerlo.

Figura 6.55

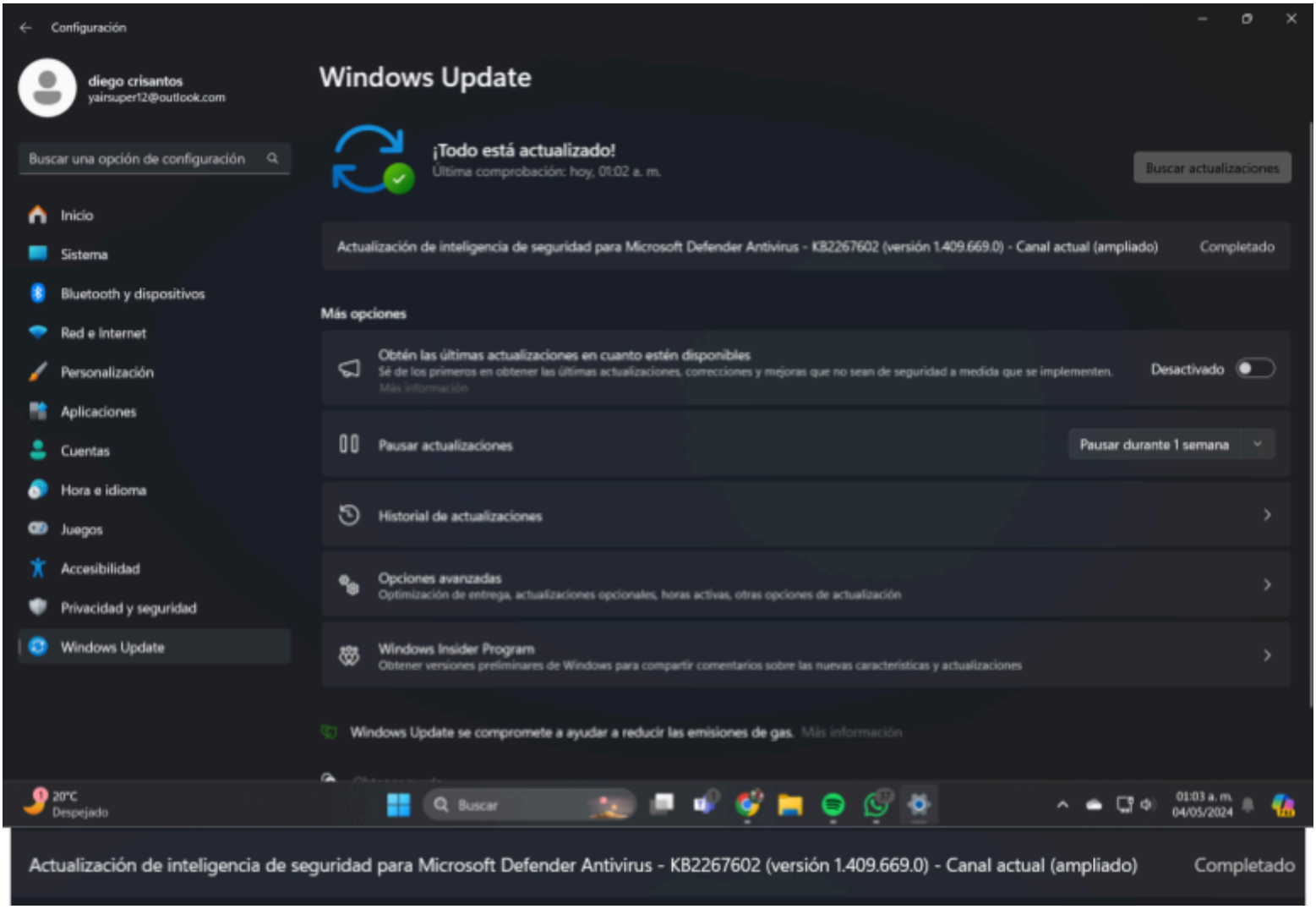
Actualización de sistema operativo Windows paso 7



7. Verificar la instalación: Una vez reiniciado, verifica en Configuración > Actualización y seguridad > Windows Update que no haya más actualizaciones pendientes.

Figura 6.56

Actualización de sistema operativo Windows paso 8



Pasos para actualizar el sistema operativo android:

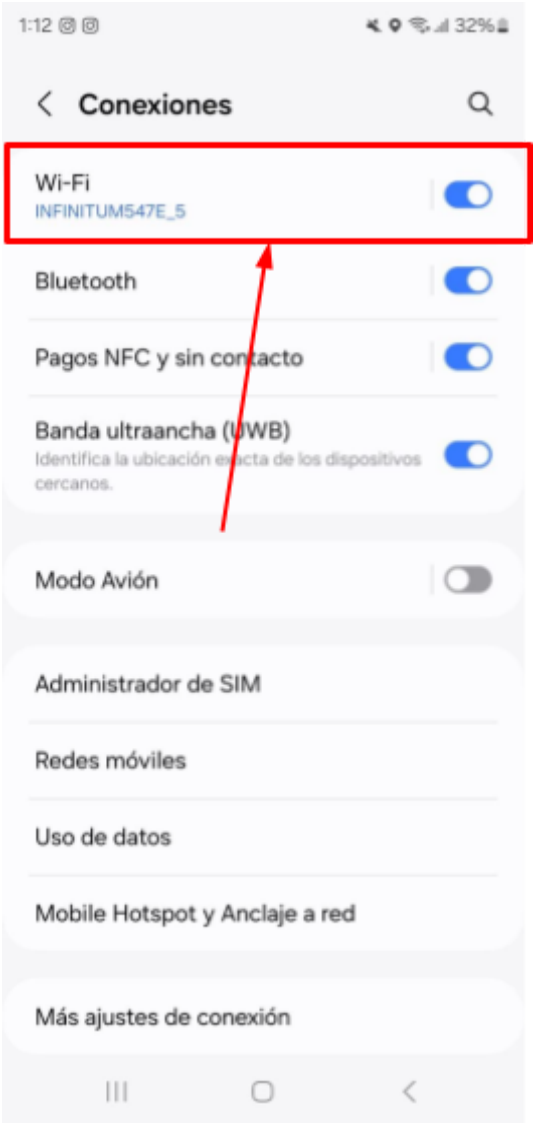
Samsung

A través de las siguientes 5 imagenes se puede observar el proceso para actualizar el sistema operativo en un dispositivo android de la marca samsung:

1. Conexión a Internet: Al igual que con Windows, asegúrate de tener una conexión a Internet activa y estable.

Figura 6.57

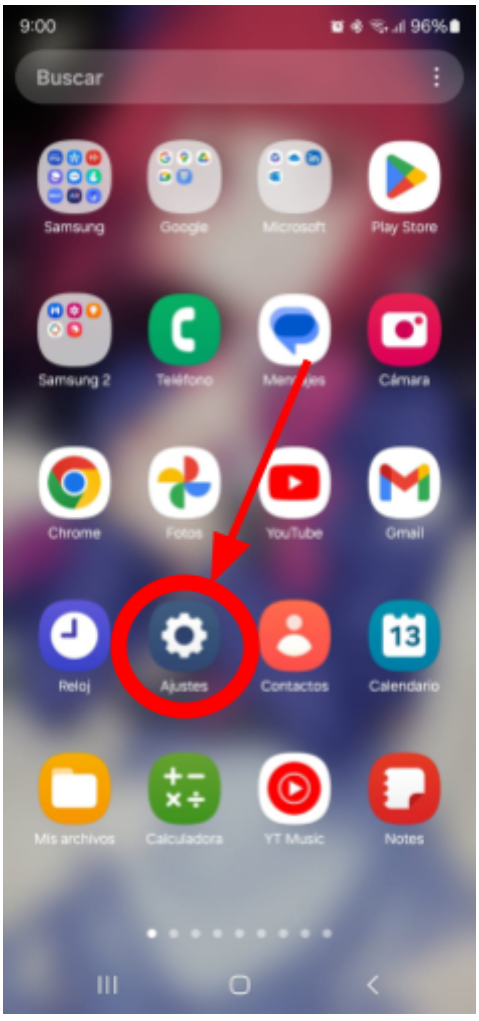
Actualización de sistema operativo samsung paso 1



2. Abrir Configuración: Abre la aplicación de Configuración en tu dispositivo Android. Puedes encontrarla en el cajón de aplicaciones o deslizando hacia abajo desde la parte superior de la pantalla y tocando el ícono de engranaje.

Figura 6.58

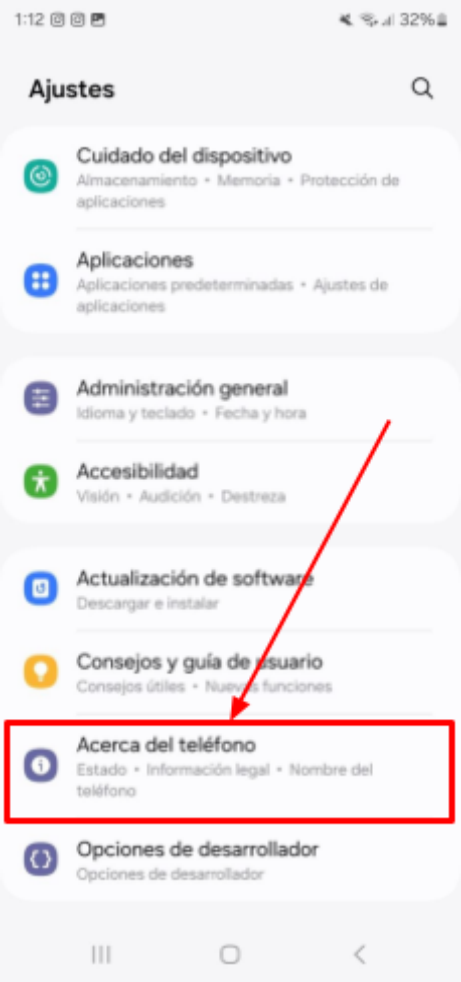
Actualización de sistema operativo samsung paso 2



3. Ir a la sección acerca del teléfono/dispositivo: Desplázate hacia abajo en la Configuración y busca la opción "Acerca del teléfono" o "Acerca del dispositivo". Esta opción puede variar ligeramente según la versión de Android y el fabricante del dispositivo ya que en algunos deberemos saltarnos este paso e ir directamente a la opción "Actualizar software".

Figura 6.59

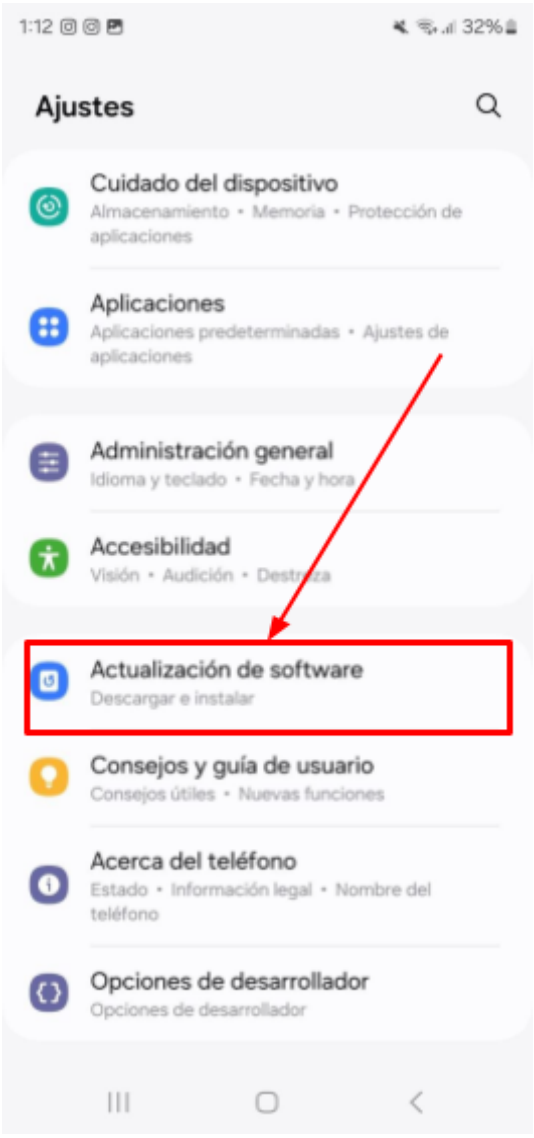
Actualización de sistema operativo samsung paso 3



4. Actualizar software/sistema: Dentro de "Acerca del teléfono/dispositivo", busca la opción "Actualizar software" o "Actualizar sistema". Tócala para comenzar a buscar actualizaciones disponibles para tu dispositivo.

Figura 6.60

Actualización de sistema operativo samsung paso 4



5. Descargar e instalar actualizaciones: Si hay una actualización disponible, tu dispositivo te mostrará la opción para descargar e instalar la actualización. Sigue las instrucciones en pantalla para proceder.

Figura 6.61

Actualización de sistema operativo samsung paso 5

6. Reiniciar: Una vez que se hayan descargado e instalado las actualizaciones, es posible que se te pida que reinicies tu dispositivo. Hazlo para completar el proceso de actualización.

Figura 6.62

Actualización de sistema operativo samsung paso 6

7. Verificar la instalación: Después de reiniciar, puedes verificar en "Acerca del teléfono/dispositivo" nuevamente para asegurarte de que tu dispositivo esté ejecutando la última versión del sistema operativo Android.

Figura 6.63

Actualización de sistema operativo samsung paso 7

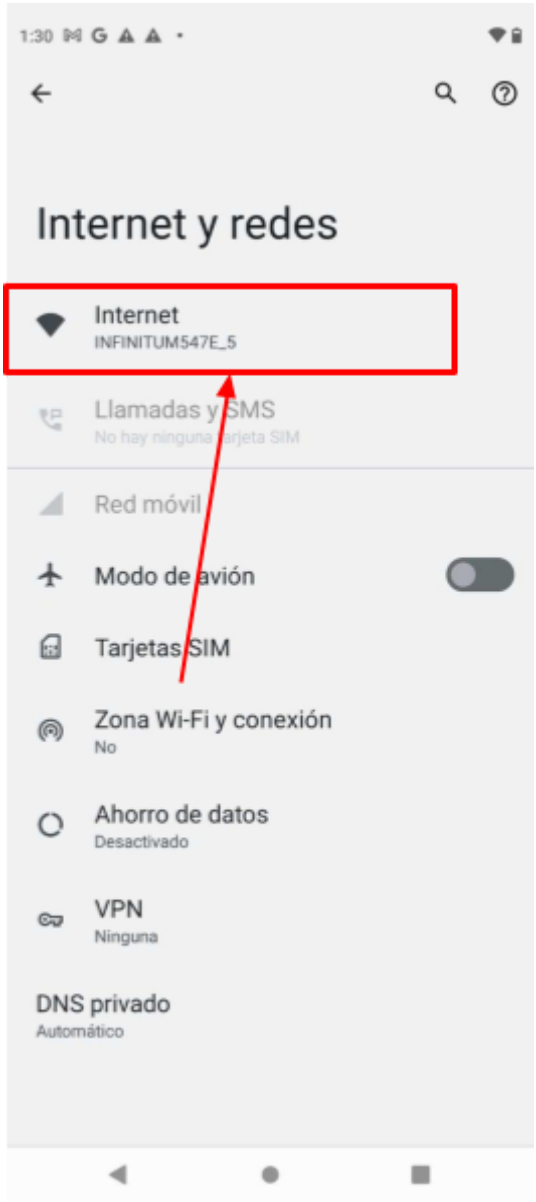
Motorola

A través de las siguientes 5 imagenes se puede observar el proceso para actualizar el sistema operativo en un dispositivo android de la marca Motorola:

1. Conexión a Internet: Al igual que con Windows, asegúrate de tener una conexión a Internet activa y estable.

Figura 6.64

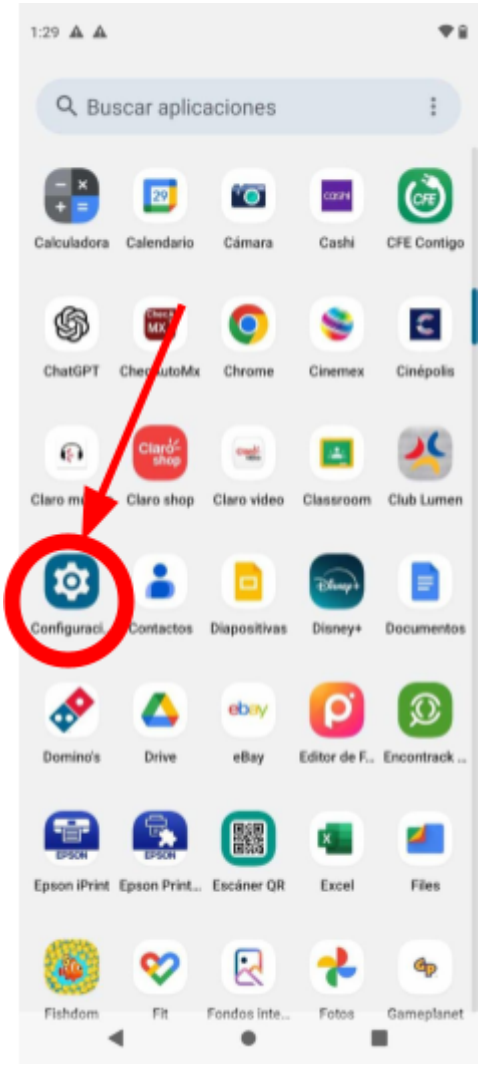
Actualización de sistema operativo motorola paso 1



2. Abrir Configuración: Abre la aplicación de Configuración en tu dispositivo Android. Puedes encontrarla en el cajón de aplicaciones o deslizando hacia abajo desde la parte superior de la pantalla y tocando el ícono de engranaje.

Figura 6.65

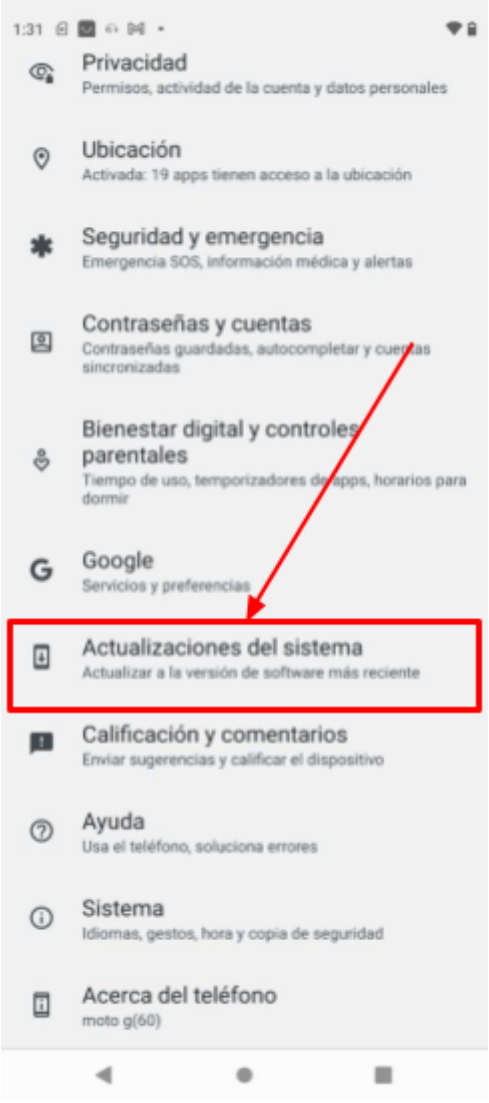
Actualización de sistema operativo motorola paso 2



3. Actualizar software/sistema: Dentro de "Configuración", busca la opción "Actualizaciones del sistema" o "Actualizar sistema". Tócala para comenzar a buscar actualizaciones disponibles para tu dispositivo.

Figura 6.66

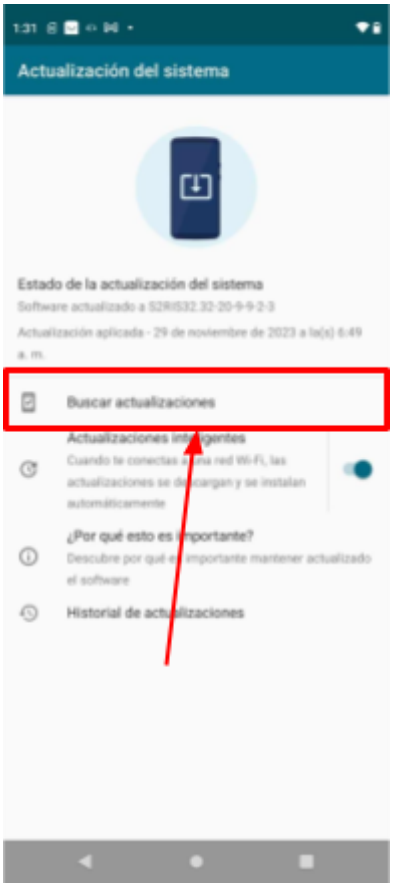
Actualización de sistema operativo motorola paso 4



4. Descargar e instalar actualizaciones: Dentro de actualización del sistema haz clic en Buscar actualizaciones. Esto iniciará una búsqueda automática de nuevas versiones del software. Si hay actualizaciones disponibles, sigue las instrucciones en pantalla para descargarlas e instalarlas, asegurándote de que tu dispositivo esté siempre al día con las mejoras de seguridad y rendimiento.

Figura 6.67

Actualización de sistema operativo motorola paso 5



5. Reiniciar: Una vez que se hayan descargado e instalado las actualizaciones, es posible que se te pida que reinicies tu dispositivo. Hazlo para completar el proceso de actualización.

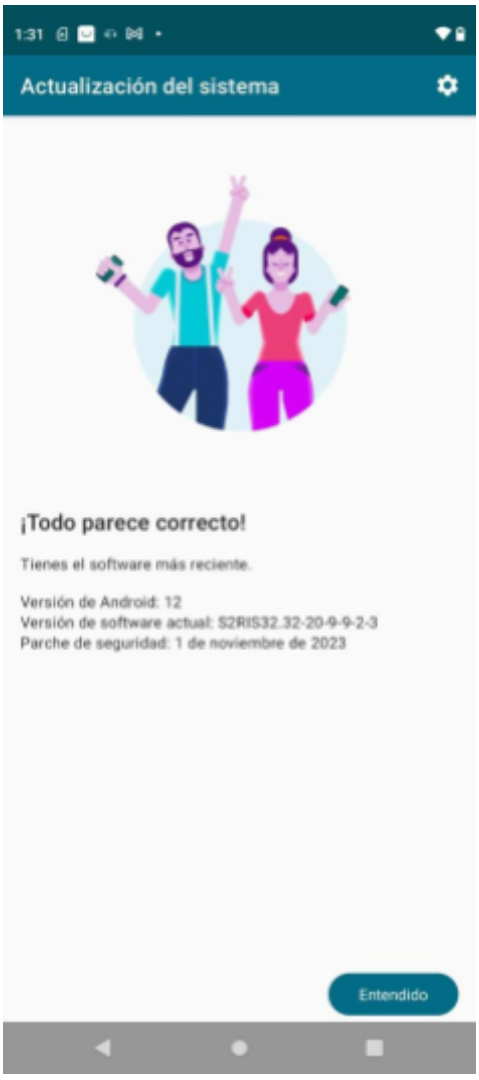
Figura 6.68

Actualización de sistema operativo motorola paso 6

6. Verificar la instalación: Después de reiniciar, puedes verificar en "Acerca del teléfono/dispositivo" nuevamente para asegurarte de que tu dispositivo esté ejecutando la última versión del sistema operativo Android.

Figura 6.69

Actualización de sistema operativo motorola paso 7



Consideraciones Adicionales:

- Copia de Seguridad: Realiza una copia de seguridad de tus datos antes de actualizar el sistema operativo para evitar la pérdida de información. Para realizar una copia de seguridad correcta puedes revisar el punto 9 "Cómo crear una copia de seguridad con Windows" de este mismo manual.
- Conexión Estable: Asegúrate de tener una conexión a internet estable para evitar interrupciones durante la actualización.
- Espacio Suficiente: Verifica que tienes suficiente espacio en el disco duro para completar la actualización.
- Desactivar Antivirus: Temporalmente desactiva tu antivirus si encuentras problemas al instalar la actualización.

Nota: Es importante realizar estas actualizaciones periódicamente para garantizar un funcionamiento óptimo y seguro de tus dispositivos.

6.8

Limpieza de Archivos en Windows

A medida que utilizamos nuestros equipos con Windows, acumulamos una gran cantidad de archivos temporales, programas innecesarios y otros datos que ocupan espacio en el disco duro. Además de ralentizar el rendimiento de la computadora, estos archivos pueden representar un riesgo para la seguridad de tus datos y de tu sistema. Por eso, es importante realizar regularmente una limpieza de archivos para mantener tu equipo en óptimas condiciones.

A continuación, te mostramos cómo limpiar tu equipo de manera segura y eficiente para mejorar su rendimiento y proteger tu información:

a) Eliminar Archivos Temporales

Antes de empezar, es importante comprender qué son los archivos temporales y por qué es necesario eliminarlos regularmente. Los archivos temporales son creados por el sistema operativo y las aplicaciones para almacenar datos temporales mientras se ejecutan. Estos archivos pueden acumularse con el tiempo y ocupar un espacio considerable en el disco duro. Además, algunos de estos archivos pueden contener información personal o sensible que podría ser comprometida si se accede de manera no autorizada. Para poder eliminar este tipo de archivos puedes hacer lo siguiente:

1. Abre el menú de inicio y busca "Ejecutar" o presiona Win + R.

Figura 6.70

Limpieza de archivos temporales paso 1

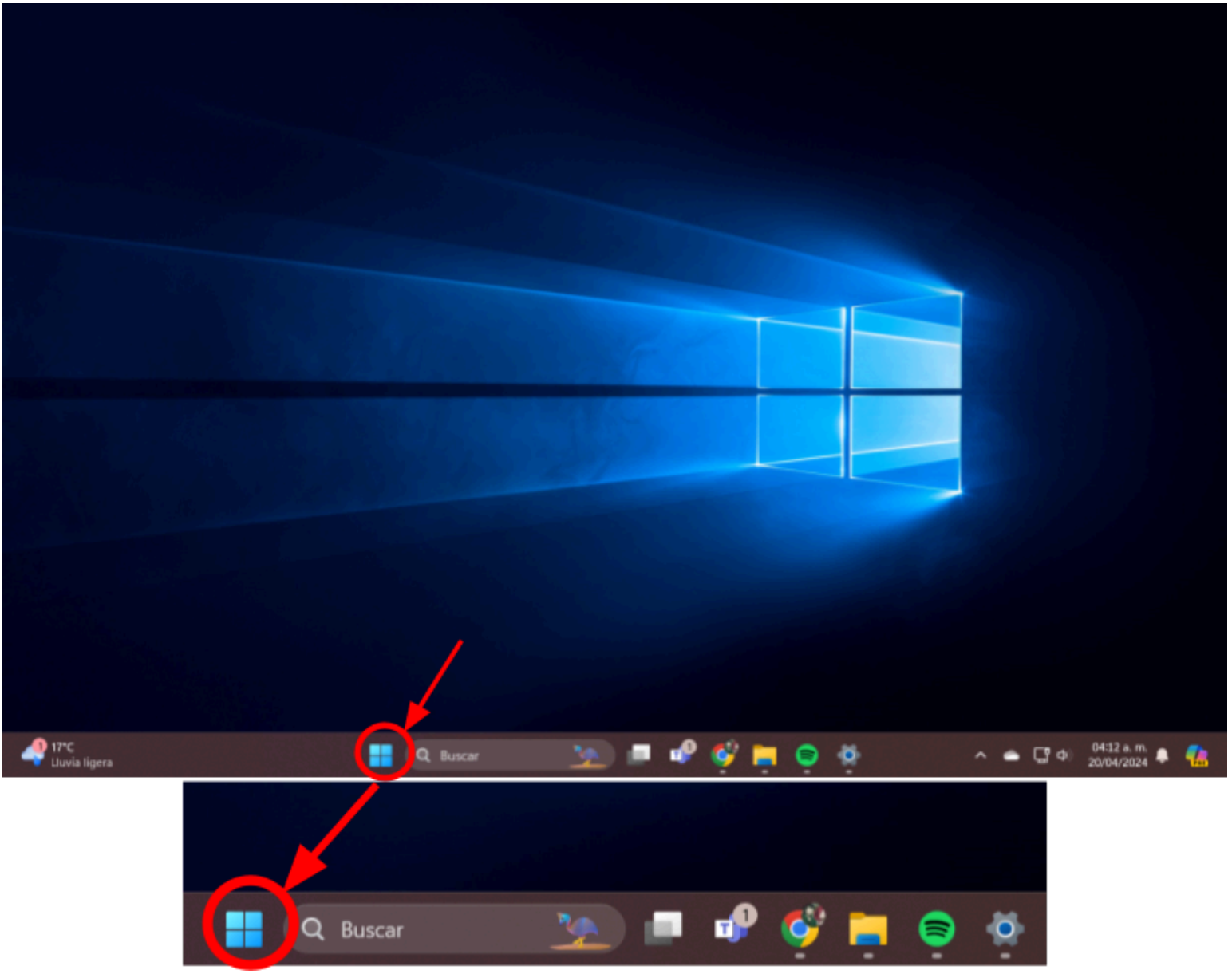
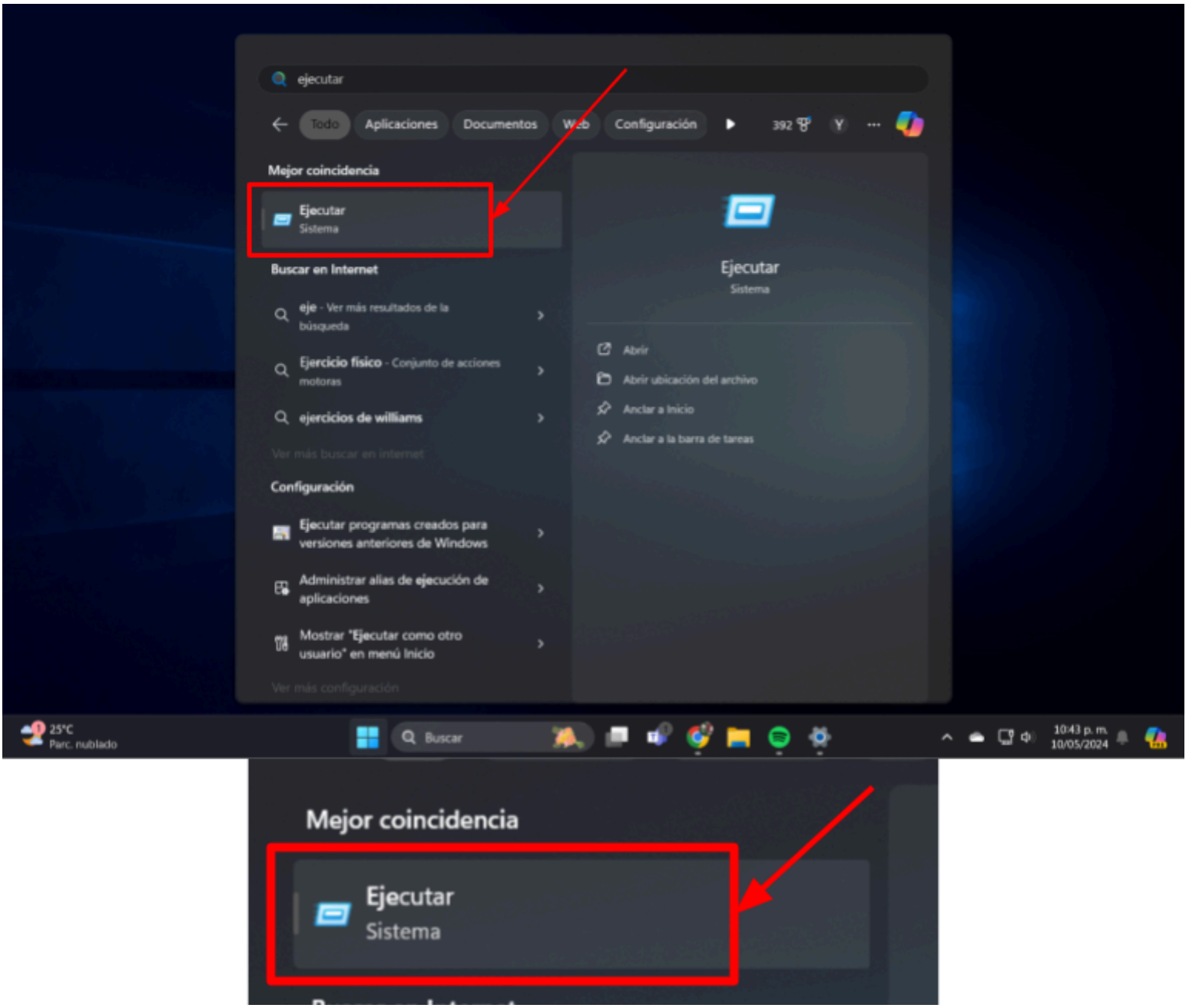


Figura 6.71

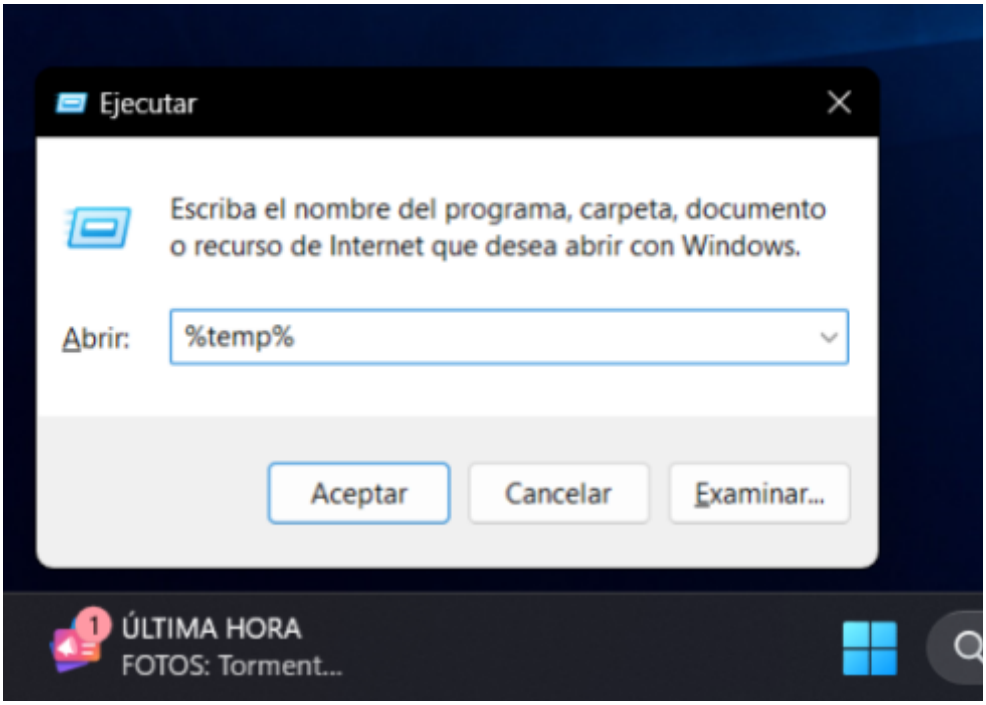
Limpieza de archivos temporales paso 2



2. En la ventana de "Ejecutar", escribe %temp% y presiona Enter. Se abrirá una carpeta con archivos temporales.

Figura 6.72

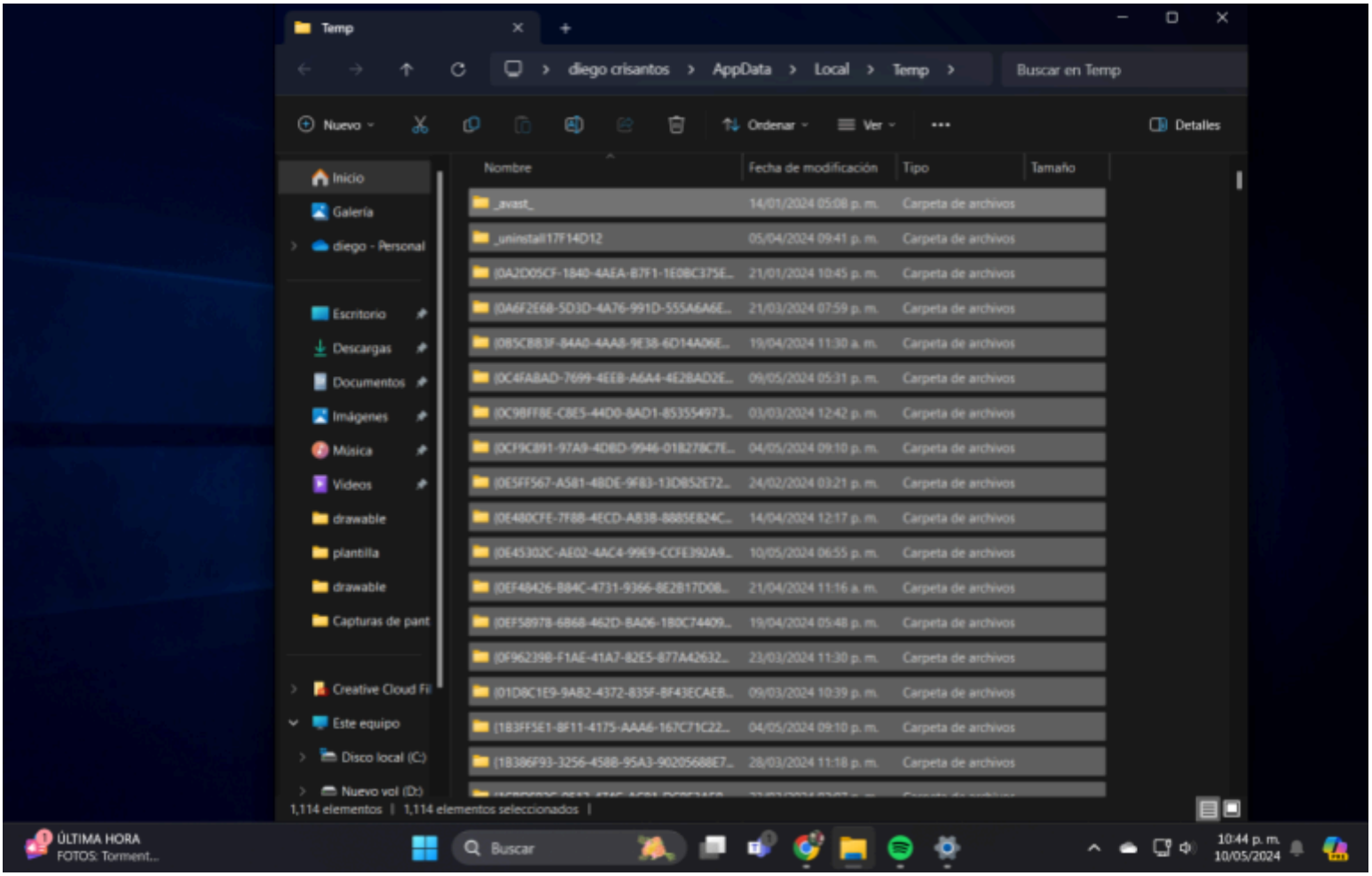
Limpieza de archivos temporales paso 3



3. Selecciona todos los archivos en esta carpeta (puedes presionar Ctrl + A) y presiona Supr en tu teclado.

Figura 6.73

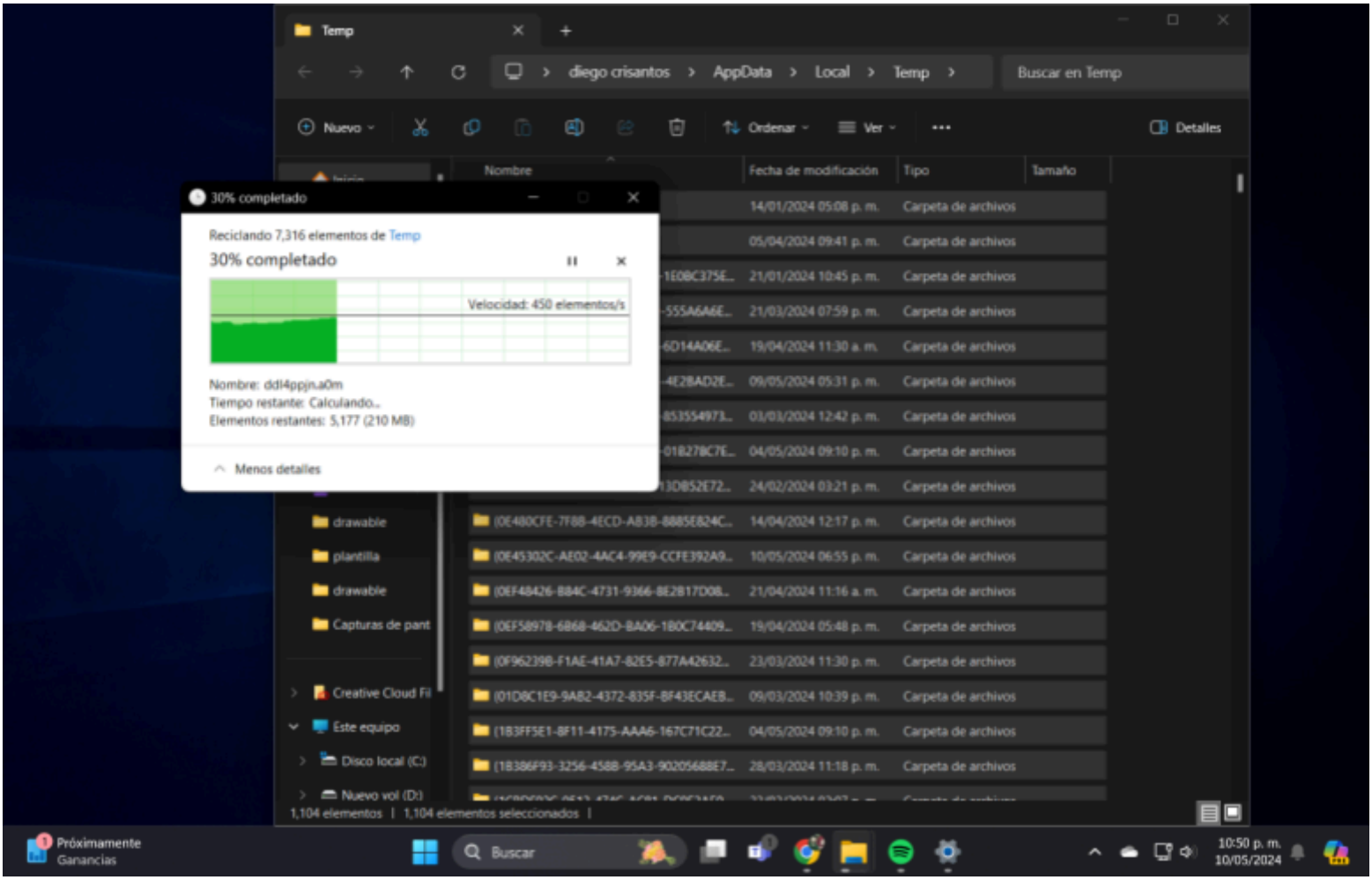
Limpieza de archivos temporales paso 4



4. Confirma la eliminación de los archivos.

Figura 6.74

Limpieza de archivos temporales paso 5



b) Liberar Espacio en Disco

A medida que utilizamos nuestra computadora, instalamos y desinstalamos programas, descargamos archivos de internet y creamos documentos, fotos y videos, el espacio en disco se va llenando. Esto puede llevar a que el sistema funcione más lento y reducir la capacidad de almacenamiento disponible. Liberar espacio en disco es una forma efectiva de mejorar el rendimiento de tu computadora y proteger tus datos y lo puedes hacer de la siguiente forma.

1. Abre el menú de inicio y busca"Explorador de archivos" y da clic en él .

Figura 6.75

Liberar espacio en disco paso 1

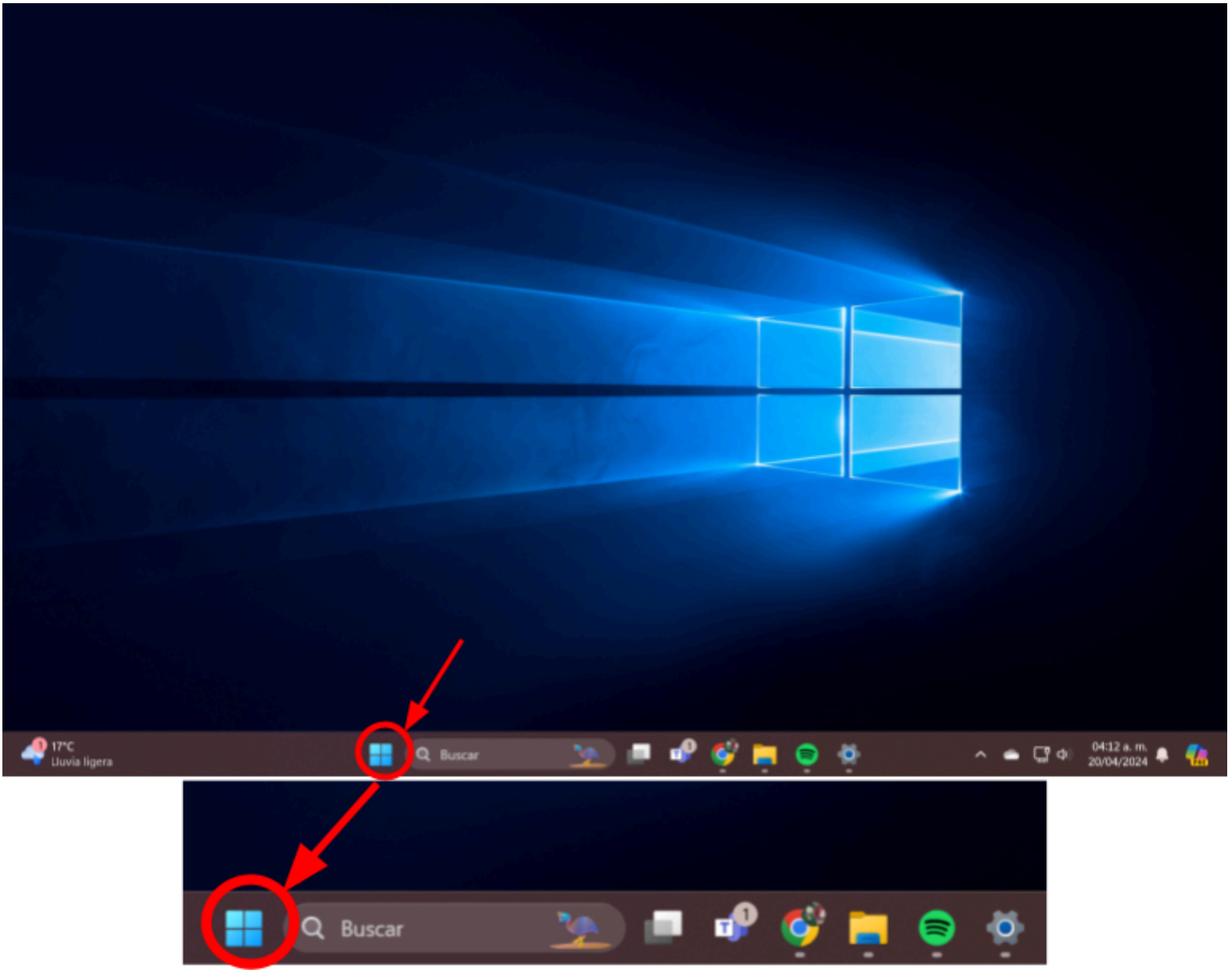
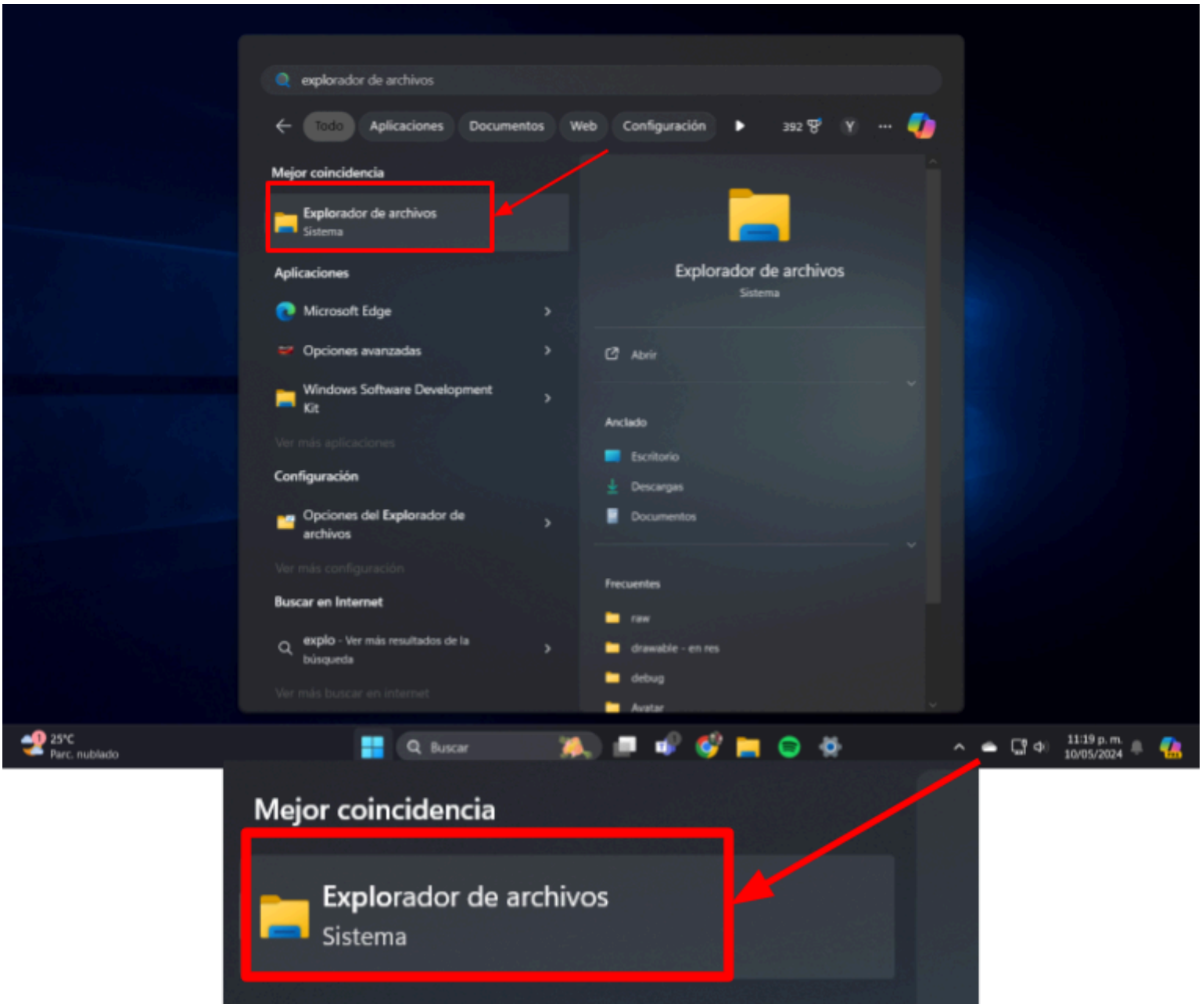


Figura 6.76

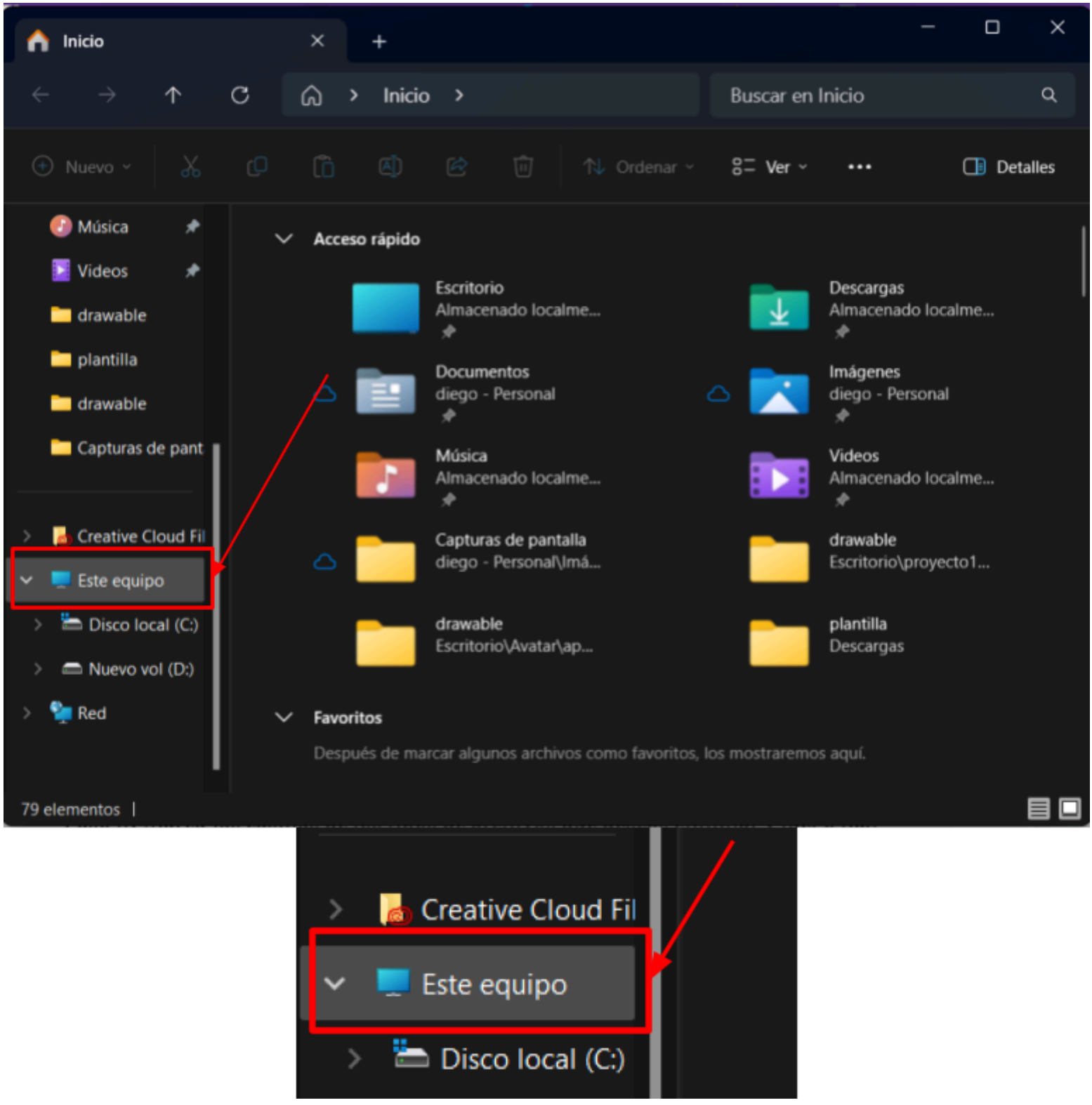
Liberar espacio en disco paso 2



2. En la parte izquierda busca y selecciona "Mi pc" o “Este equipo”.

Figura 6.77

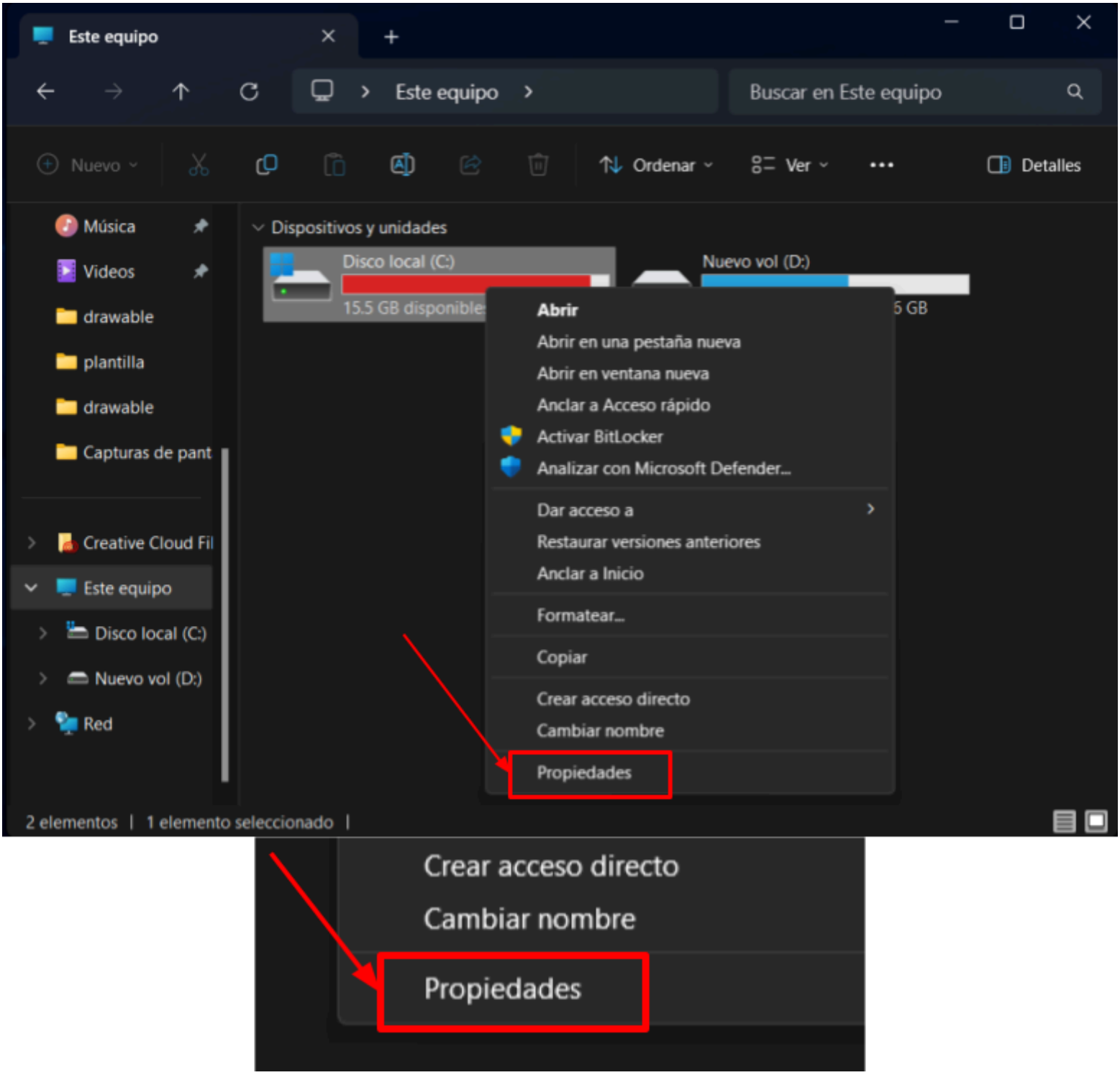
Liberar espacio en disco paso 3



3. Haz clic con el botón derecho en el disco duro principal (generalmente C:) y selecciona "Propiedades".

Figura 6.78

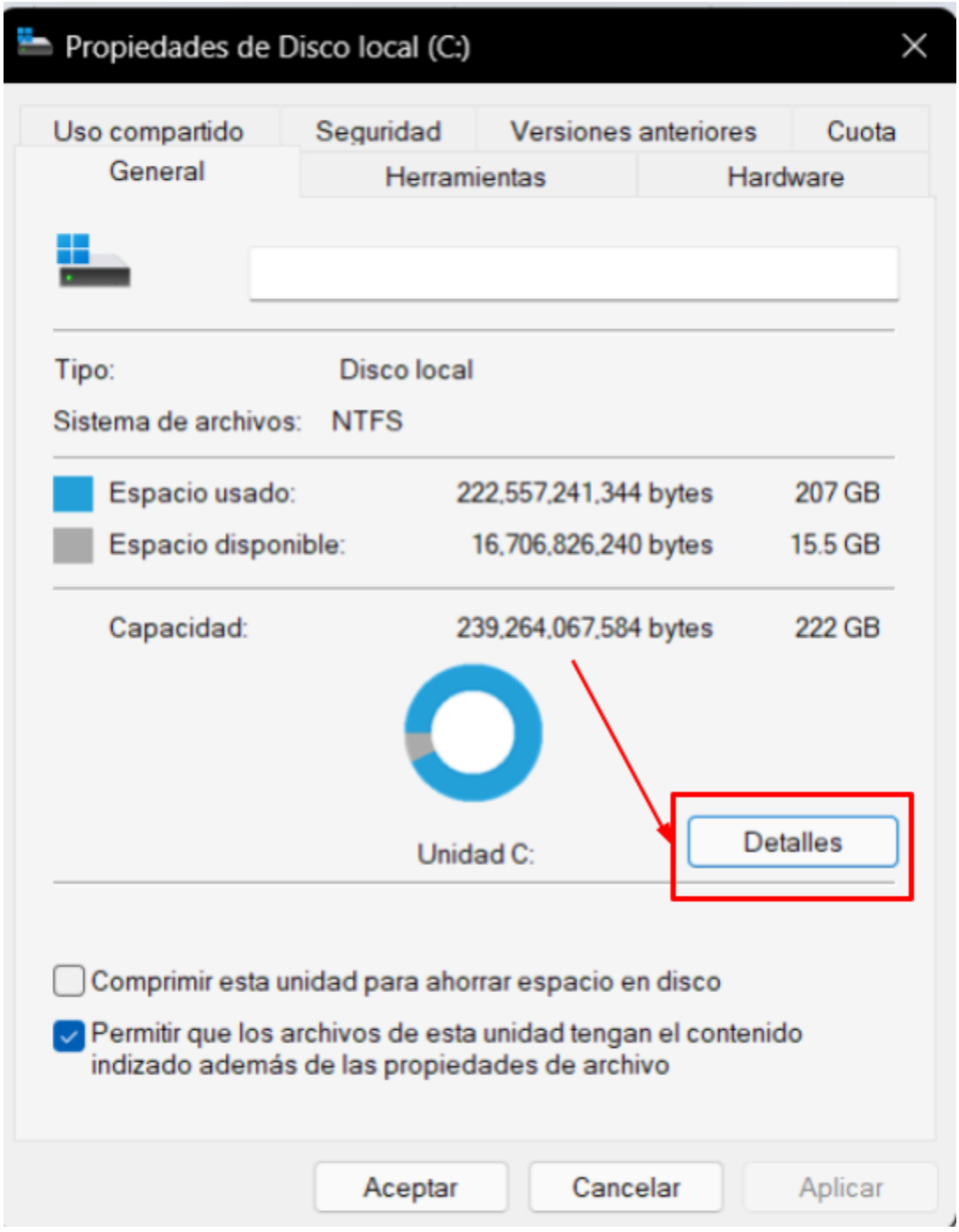
Liberar espacio en disco paso 4



4. En la pestaña "General", haz clic en "Detalles".

Figura 6.79

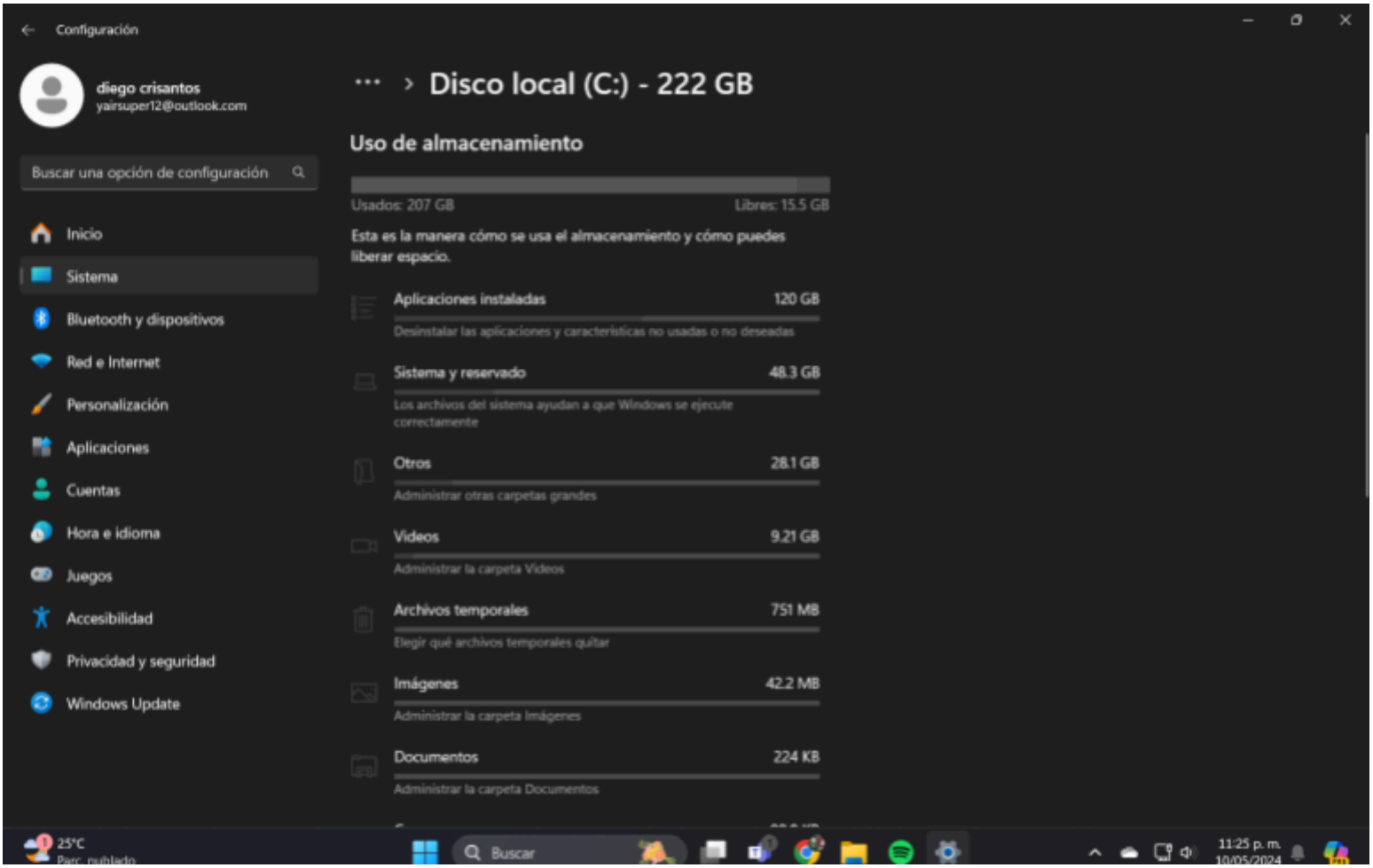
Liberar espacio en disco paso 5



5. En la ventana que se abre observaremos varios tipos de archivos y/o programas que windows nos sugiere revisar y si es el caso eliminar para liberar el disco.

Figura 6.80

Liberar espacio en disco paso 6



c) Desinstalar Programas Innecesarios

La desinstalación de programas innecesarios es importante no solo para liberar espacio en disco, sino también para mejorar la seguridad de tu sistema. Los programas que no utilizas pueden contener vulnerabilidades que podrían ser explotadas por malware. Desinstalar estos programas reduce el riesgo de exposición a amenazas y mantiene tu sistema más seguro. Para hacer esto puedes realizar lo siguiente:

1. Abre el menú de inicio y busca "Configuración".

Figura 6.81

Desinstalar programas innecesarios paso 1

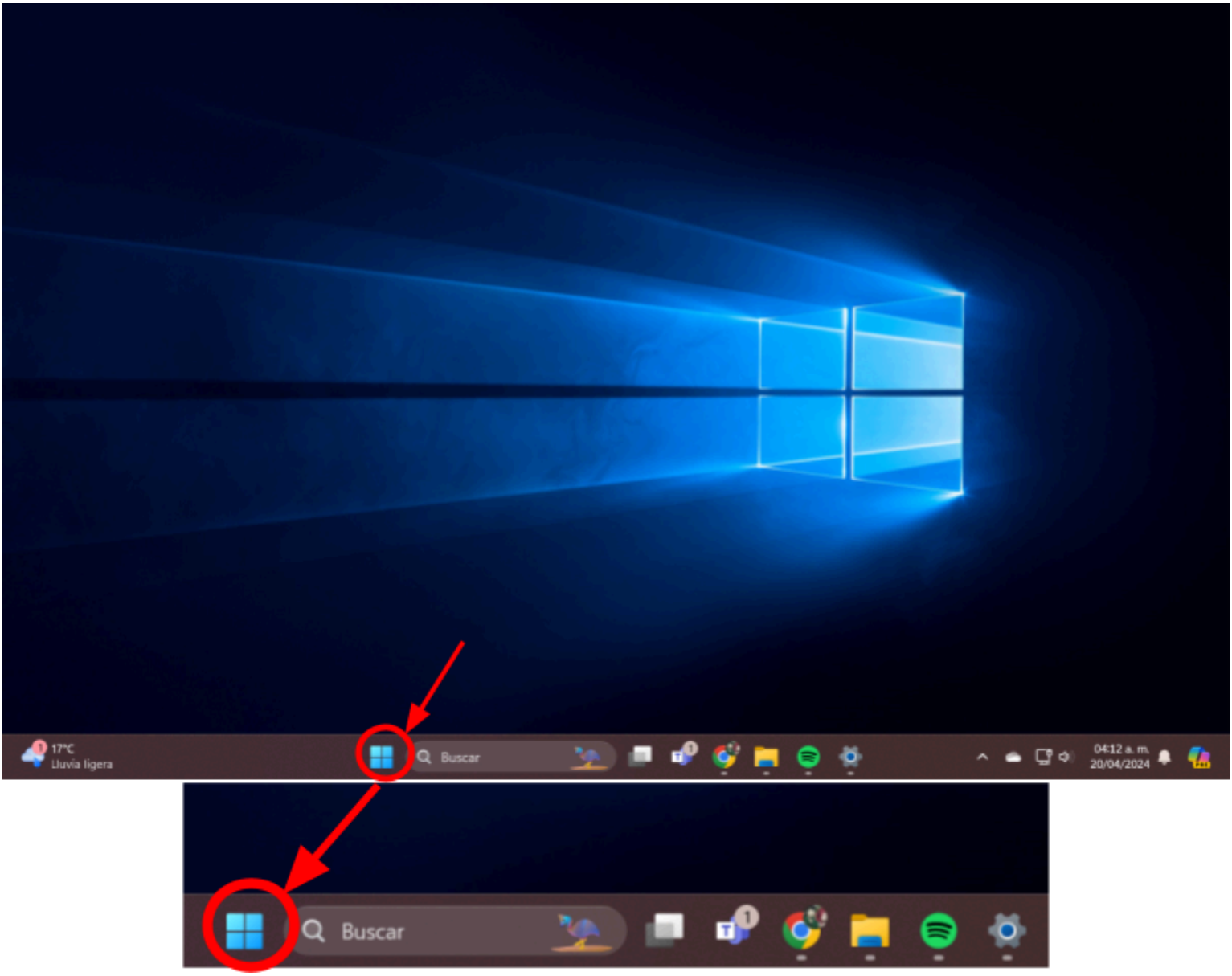
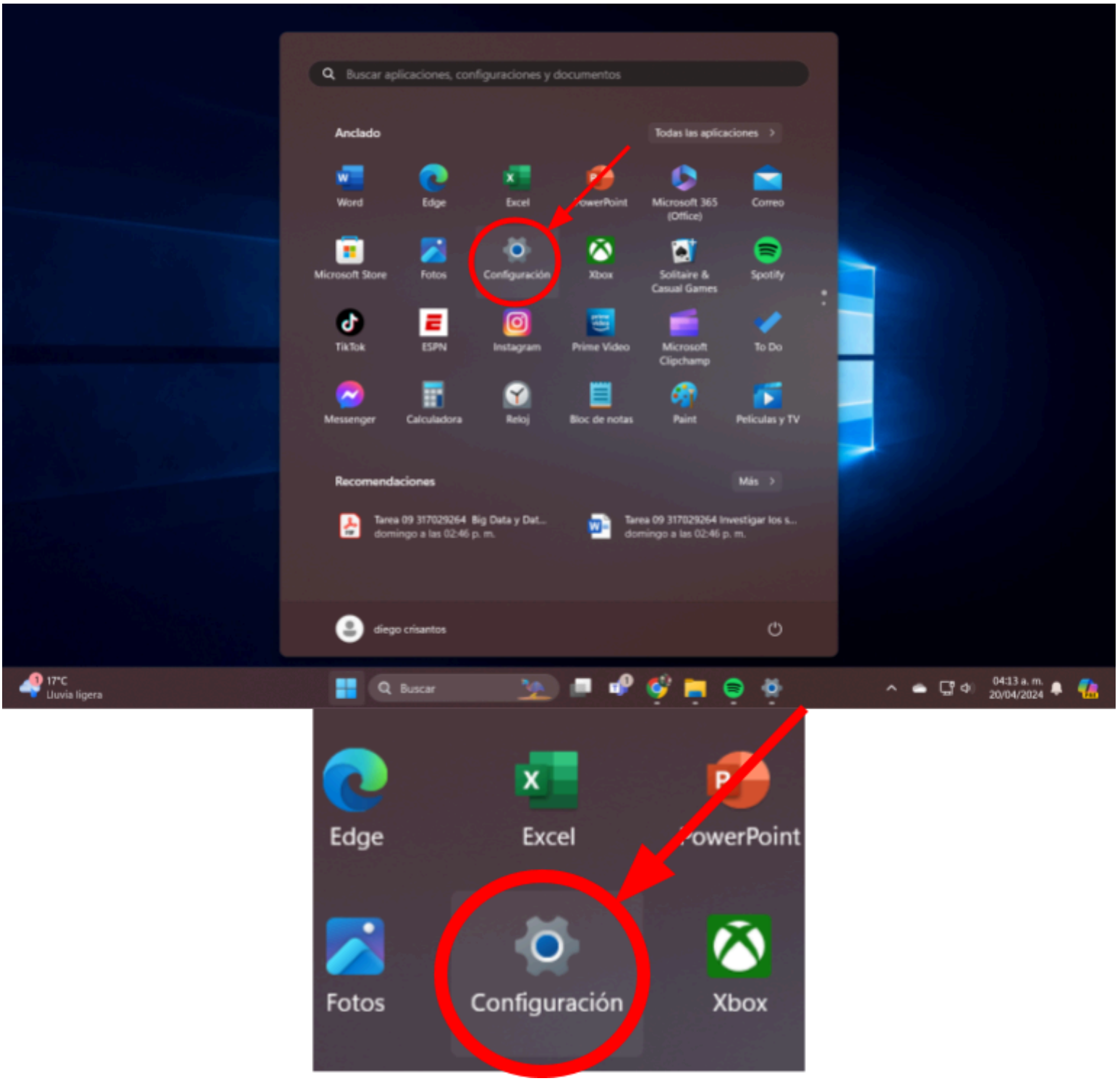


Figura 6.82

Desinstalar programas innecesarios paso 2



2. Ve a "Aplicaciones" y luego a "Aplicaciones instaladas".

Figura 6.83

Desinstalar programas innecesarios paso 3

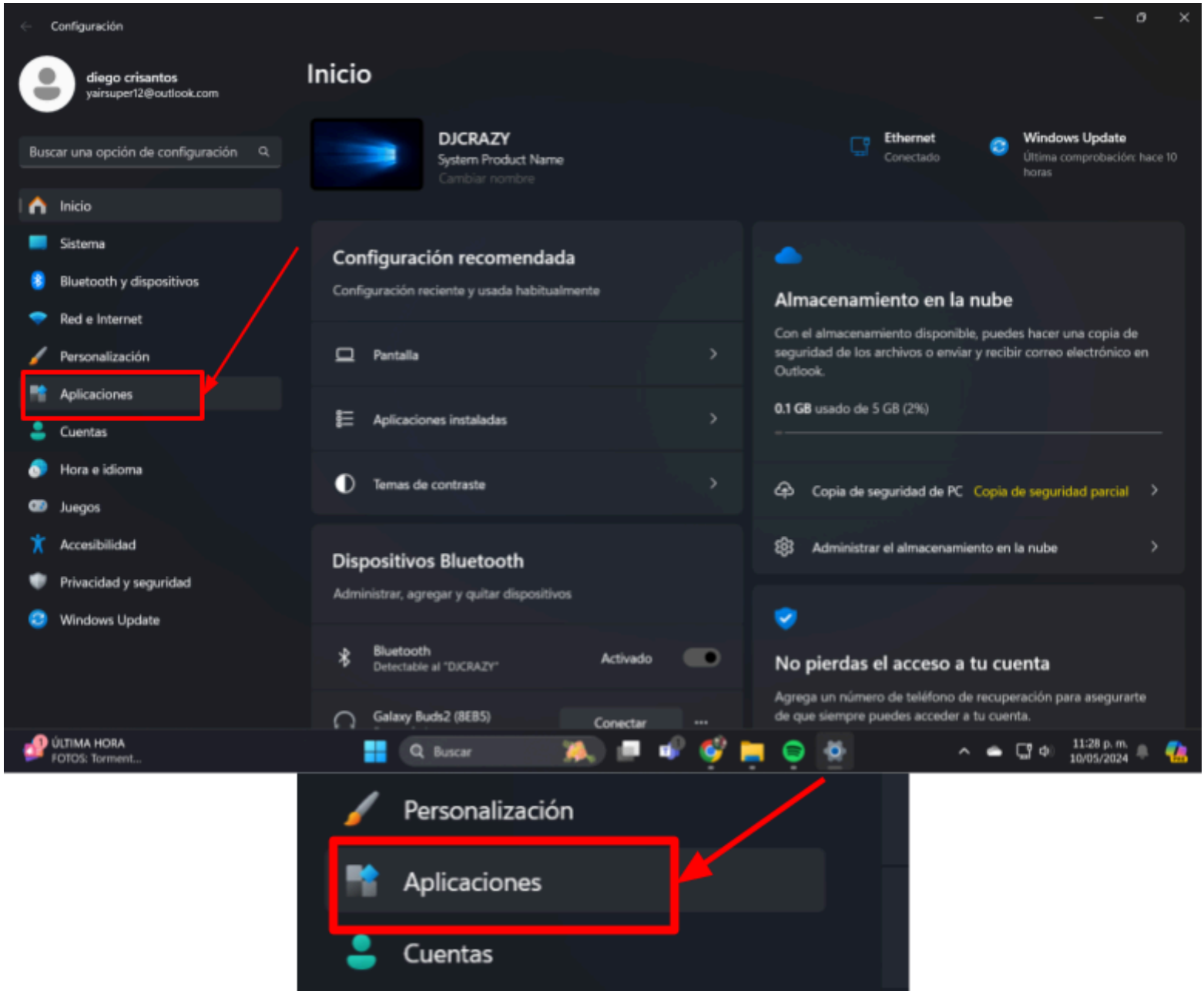
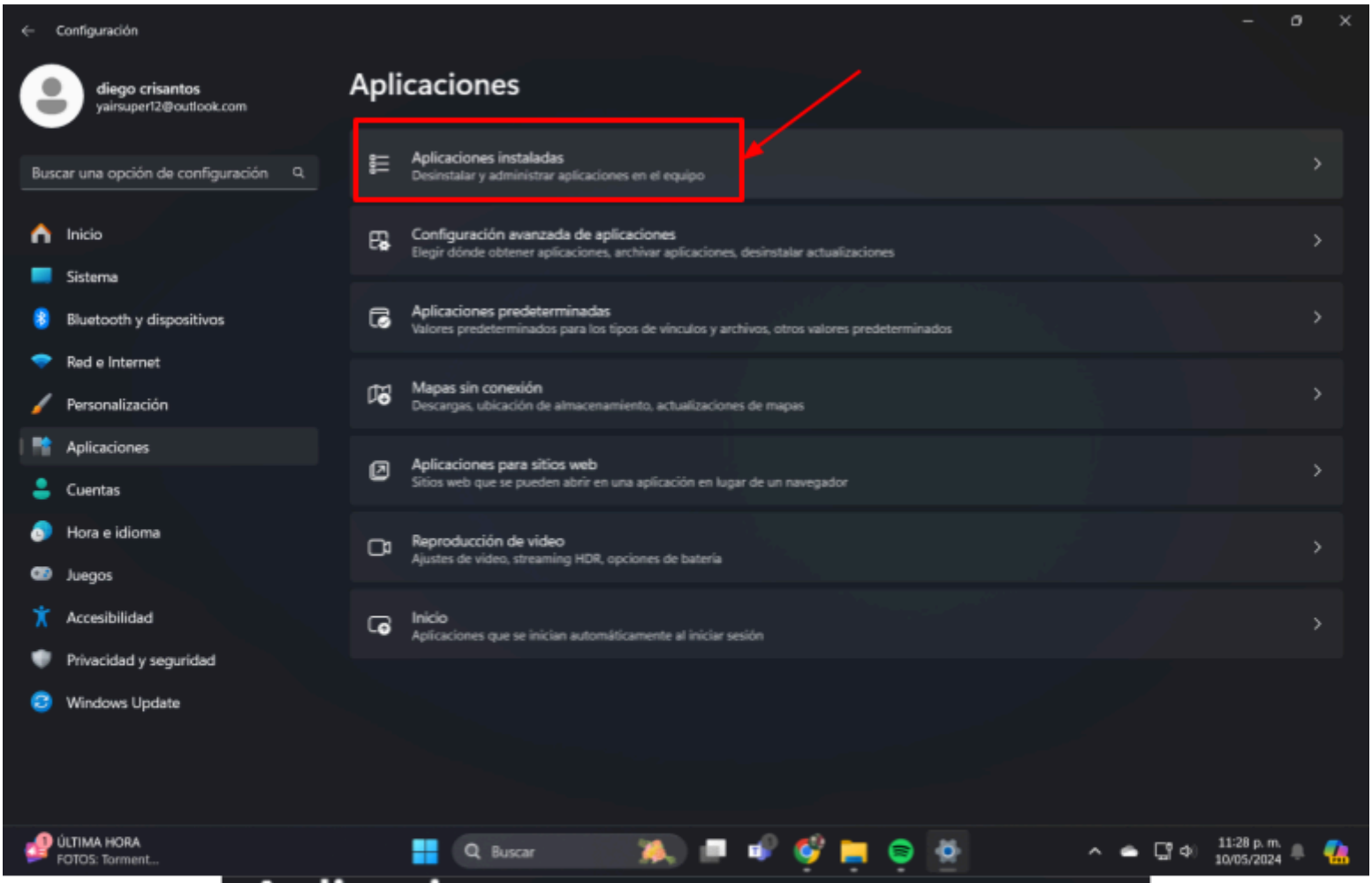
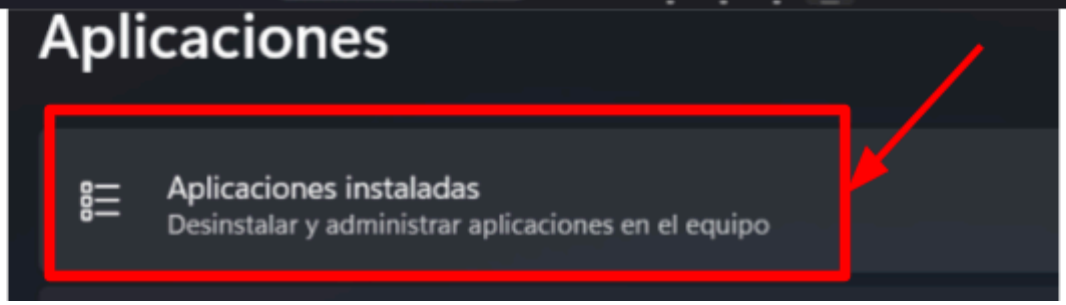


Figura 6.84

Desinstalar programas innecesarios paso 4

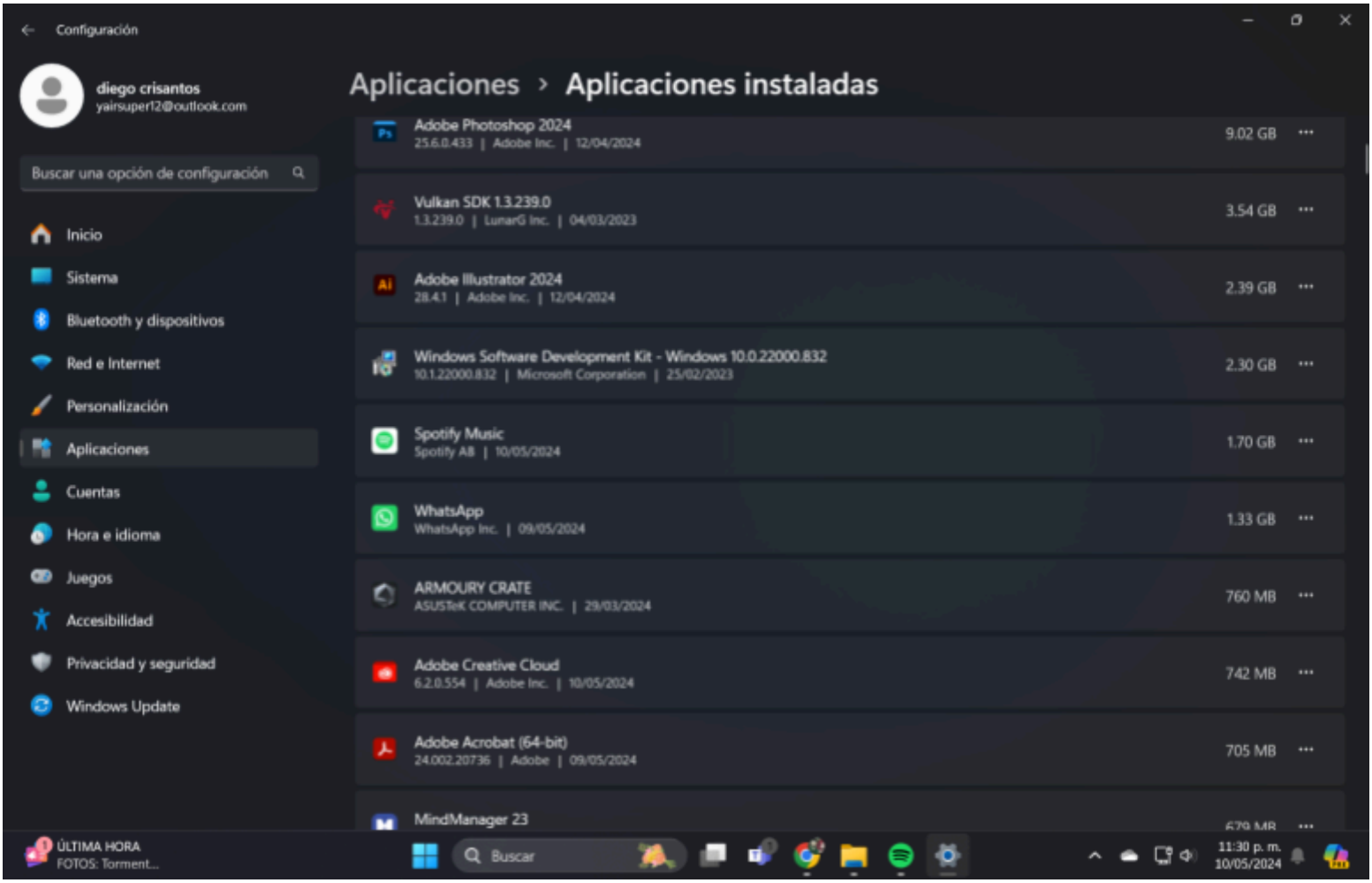




3. Desplázate por la lista de programas instalados y selecciona aquellos que deseas desinstalar.

Figura 6.85

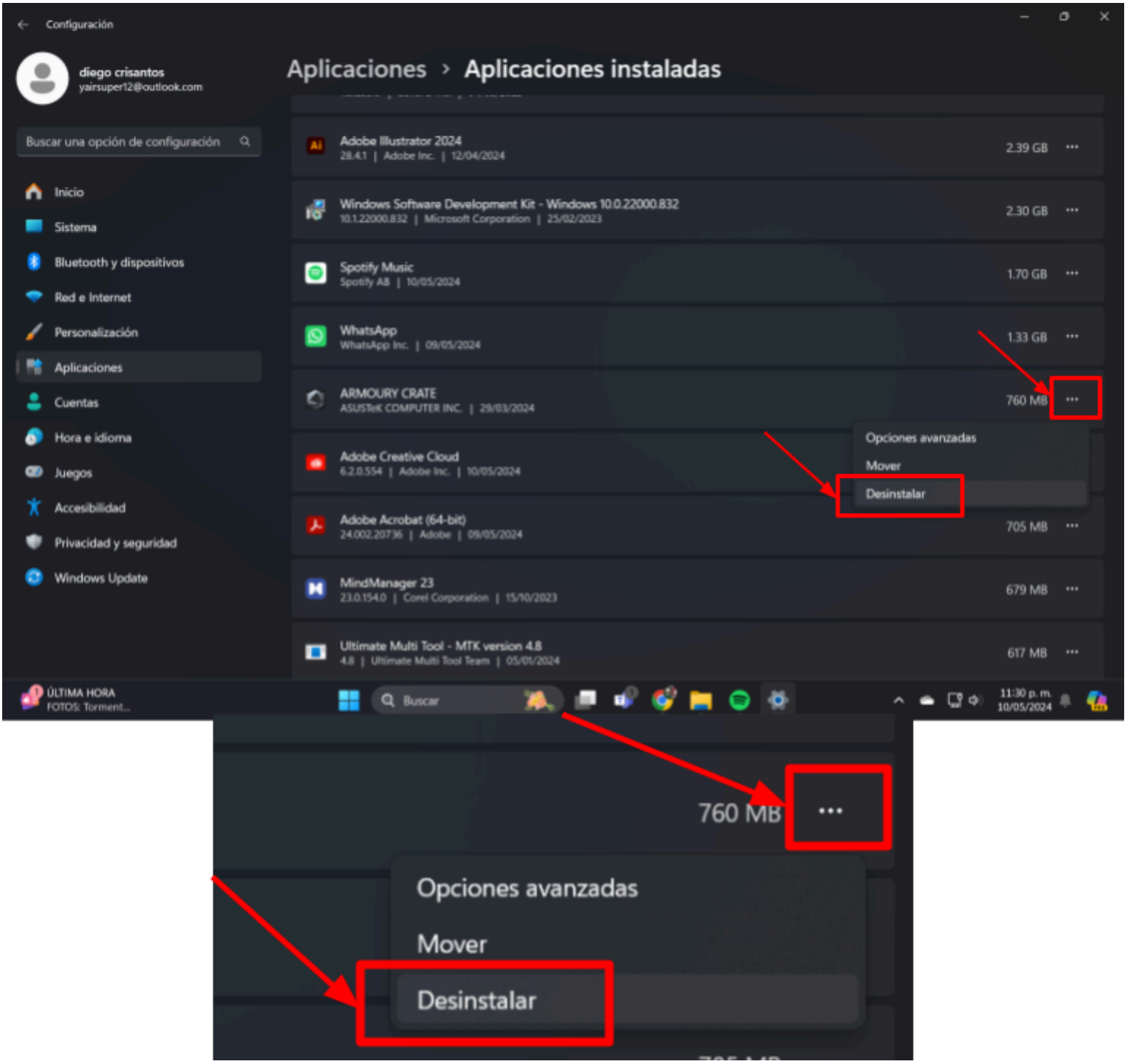
Desinstalar programas innecesarios paso 5



4. Haz clic en los tres puntos a la derecha del nombre y da clic en "Desinstalar" y sigue las instrucciones en pantalla.

Figura 6.86

Desinstalar programas innecesarios paso 6



d) Utilizar la Herramienta de Limpieza de Disco

La herramienta de limpieza de disco es una herramienta integrada en Windows que te permite eliminar archivos temporales, archivos de la papelera de reciclaje y otros archivos innecesarios para liberar espacio en disco y mejorar el rendimiento de tu computadora. Utilizar esta herramienta regularmente es una forma rápida y fácil de mantener tu sistema limpio y seguro, para realizar esto sigue los pasos que a continuación se presentan:

1. Abre el menú de inicio y busca "Limpieza de disco" o presiona Win + S y escribe "Liberador de espacio en disco".

Figura 6.87

Herramienta para limpieza de disco paso 1

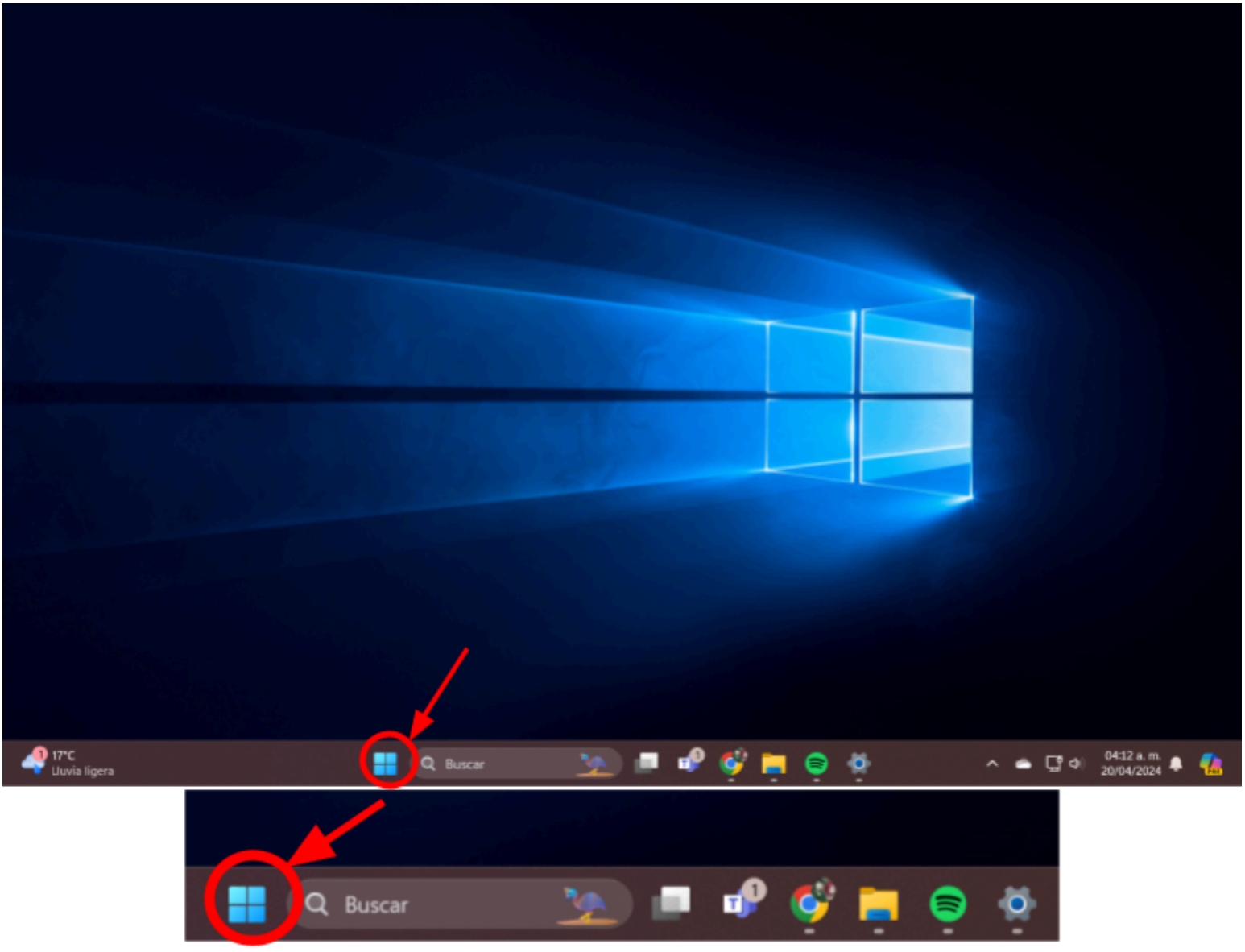
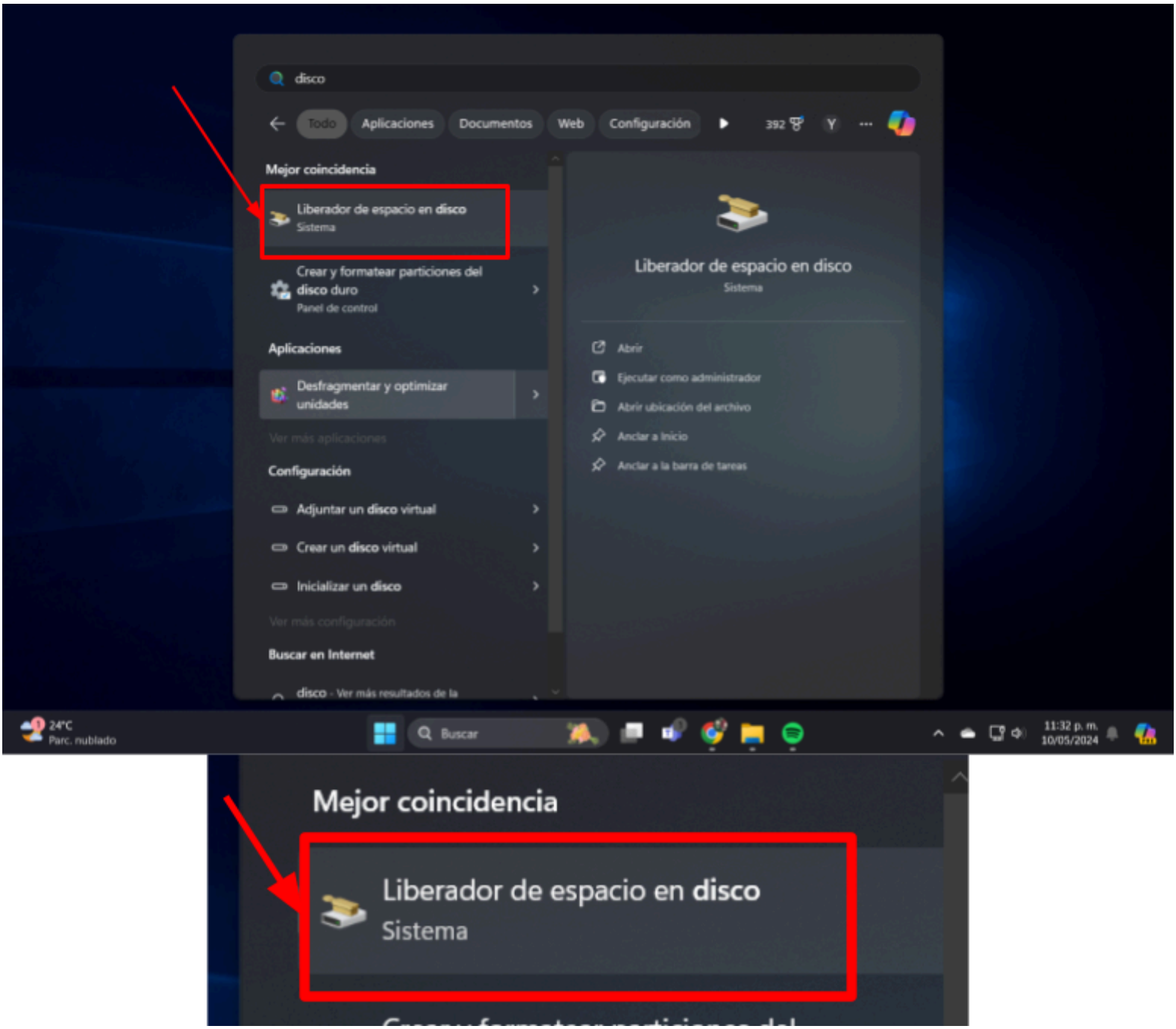


Figura 6.88

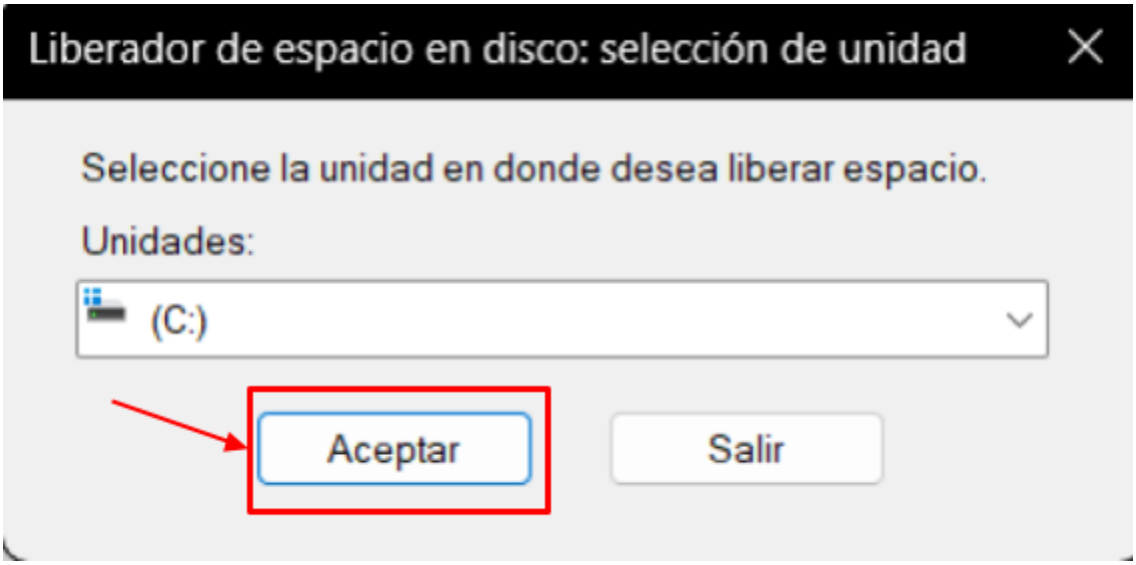
Herramienta para limpieza de disco paso 2



2. Selecciona el disco que deseas limpiar y haz clic en "Aceptar".

Figura 6.89

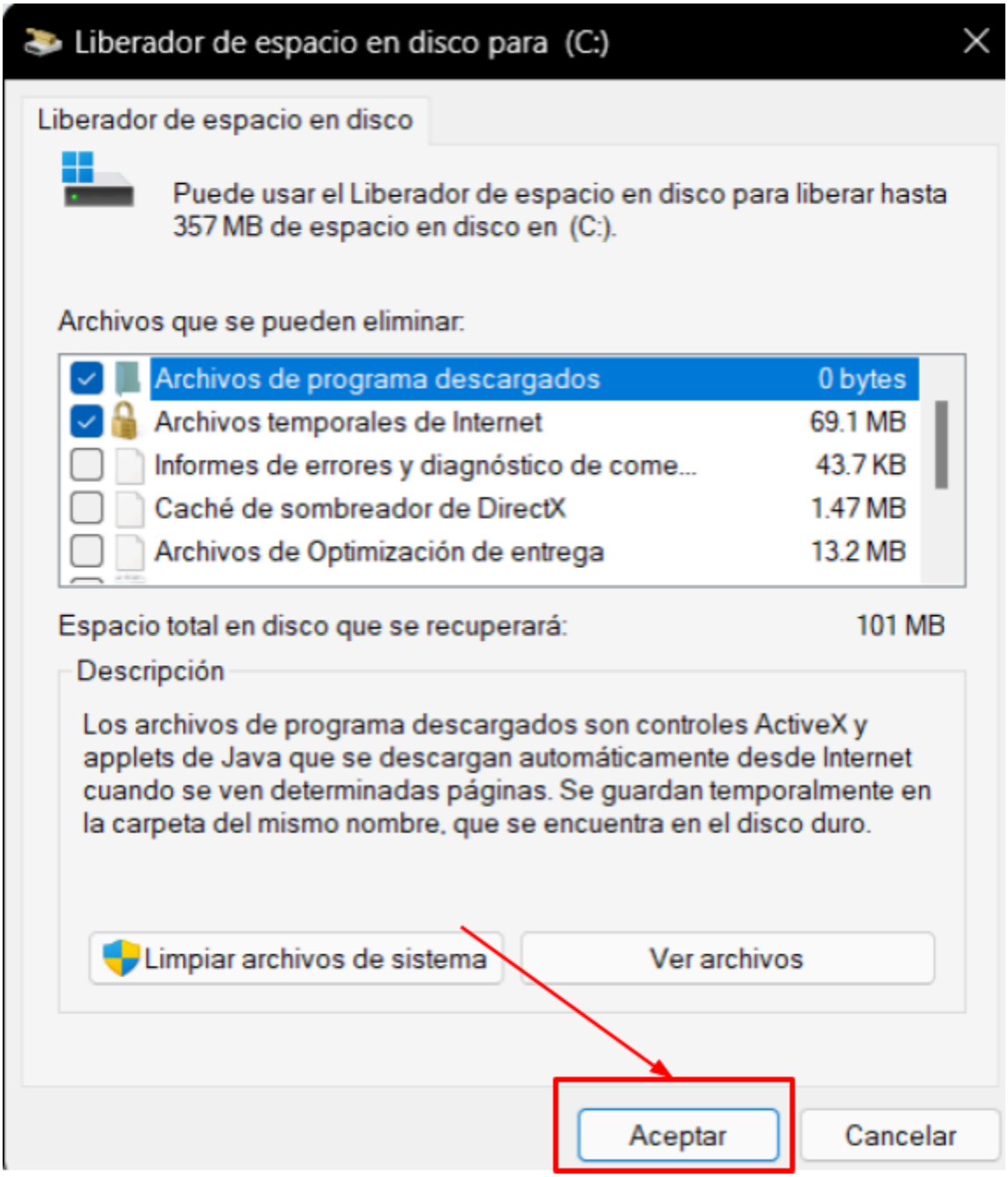
Herramienta para limpieza de disco paso 3



3. Marca las casillas de los archivos que deseas eliminar y luego haz clic en "Aceptar".

Figura 6.90

Herramienta para limpieza de disco paso 4

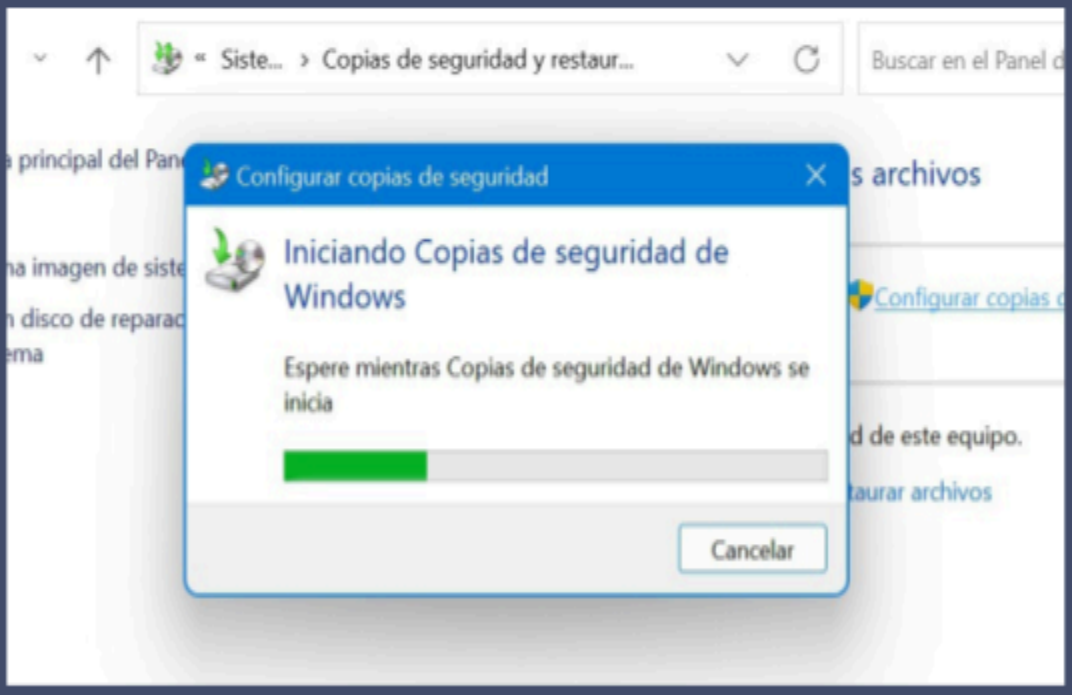


Nota: Recuerda siempre revisar los archivos antes de eliminarlos, ya que algunos podrían ser importantes.

6.9

6.9. Cómo crear una copia de seguridad con Windows

Cómo crear una copia de seguridad con Windows



Hacer copias de seguridad de tus datos es una de las prácticas más importantes en términos de seguridad informática. Una copia de seguridad garantiza que, en caso de fallos del sistema, ataques de malware, pérdida o robo de datos, puedas recuperar tu información sin mayores inconvenientes. Las copias de seguridad periódicas pueden salvarte de perder documentos importantes, archivos multimedia y configuraciones esenciales, proporcionando tranquilidad y protección contra imprevistos. Por esto a continuación puedes ver los pasos para crear una copia de seguridad de tus datos con Windows:

1. Abre el menú de inicio y busca "Panel de control" o presiona Win + S y escribe "Panel de control" y haz clic en la aplicación Panel de control que aparece en los resultados de búsqueda.

Figura 6.91

Copia de seguridad con Windows paso 1

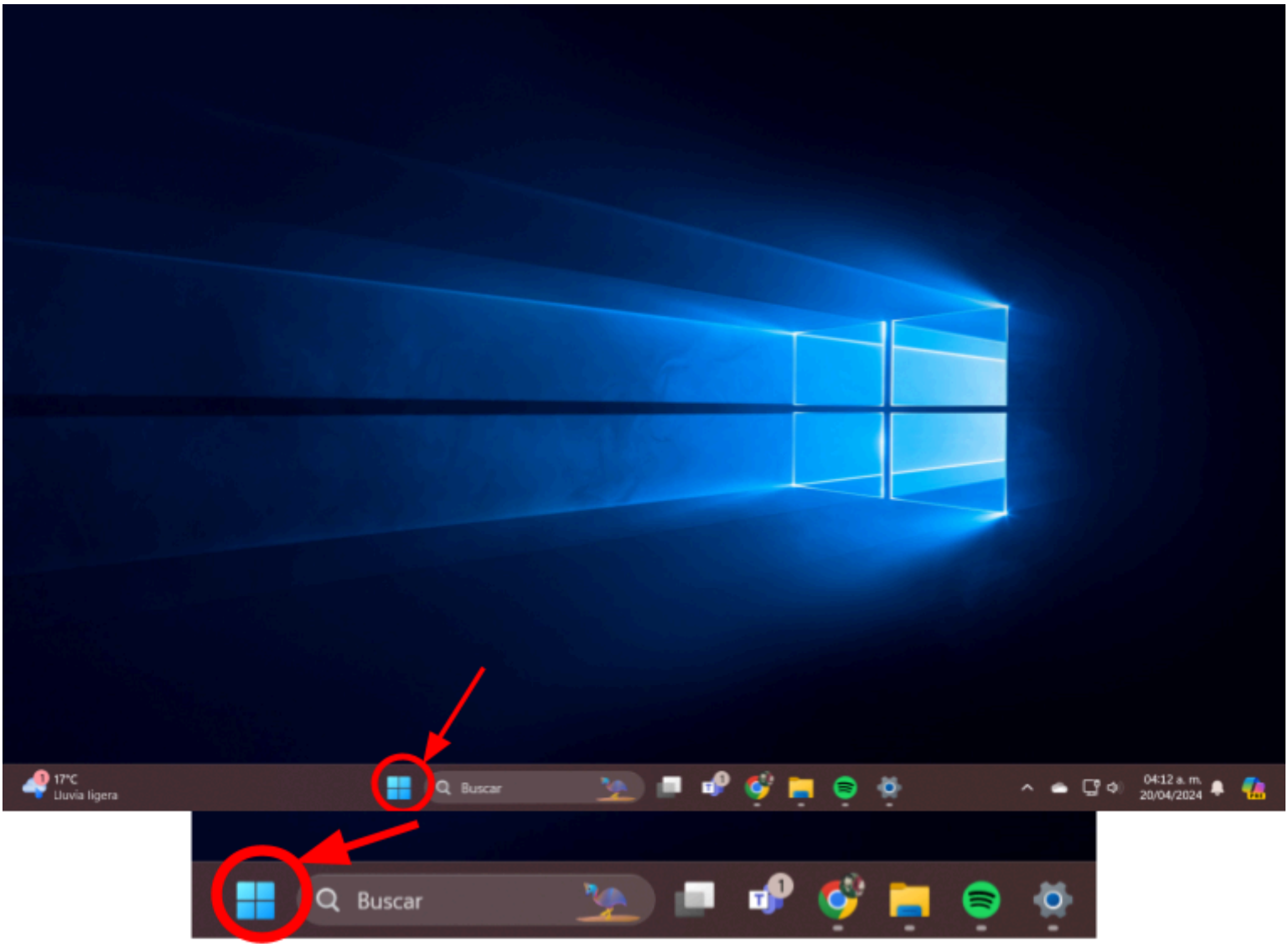
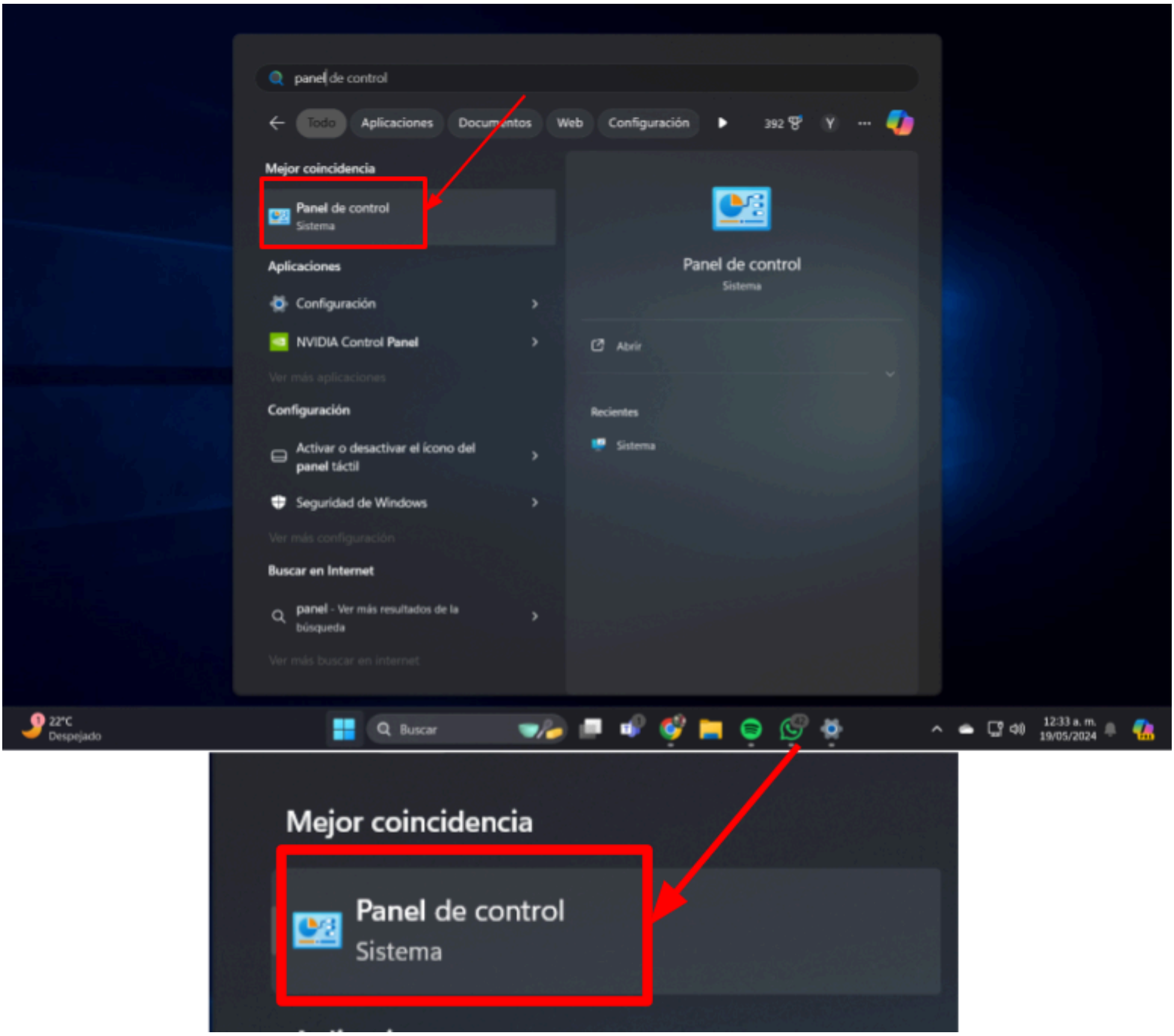


Figura 6.92

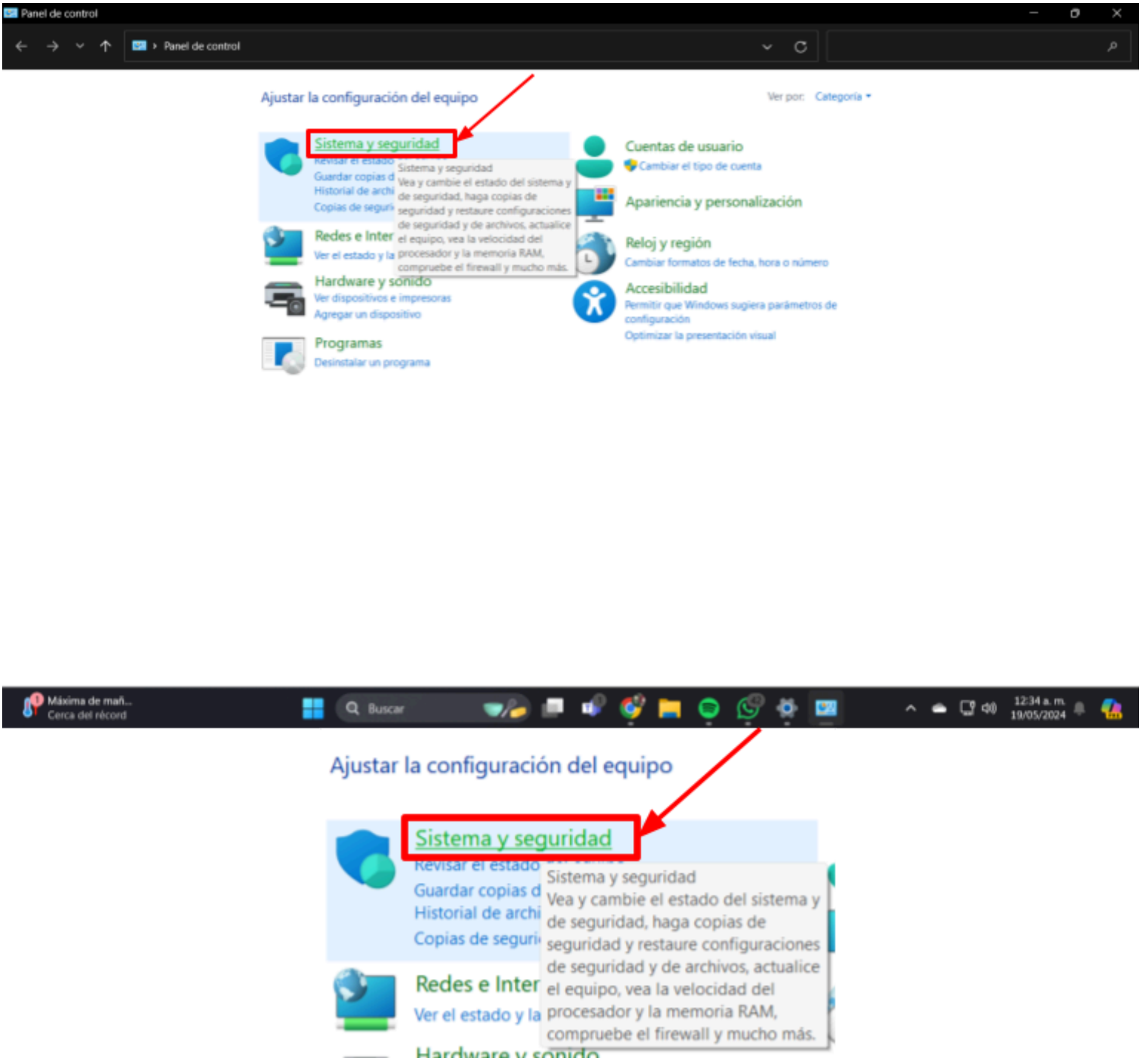
Copia de seguridad con Windows paso 2



2. Dentro del Panel de control, selecciona "Sistema y seguridad".

Figura 6.93

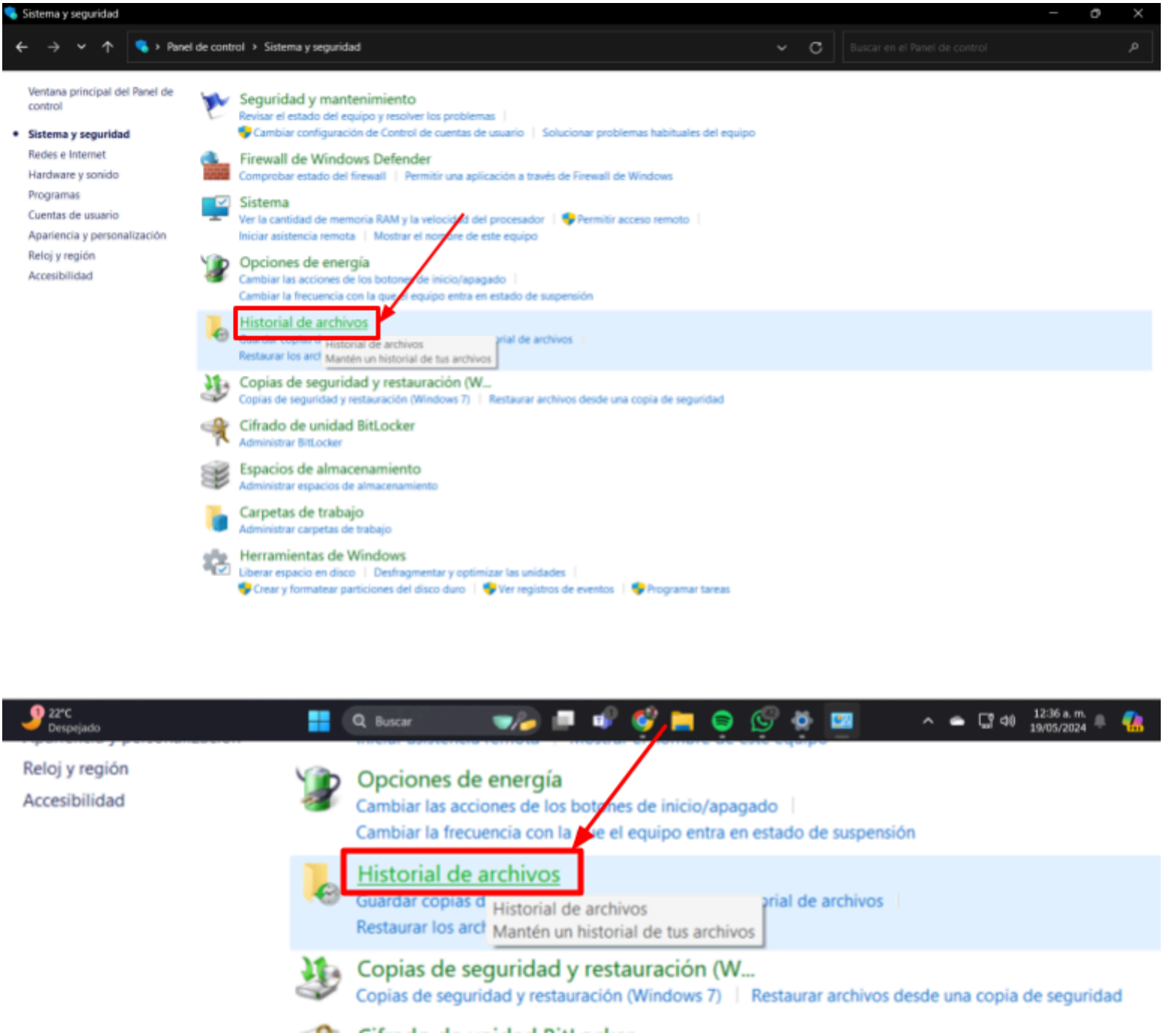
Copia de seguridad con Windows paso 3



3. Haz clic en "Historial de archivos".

Figura 6.94

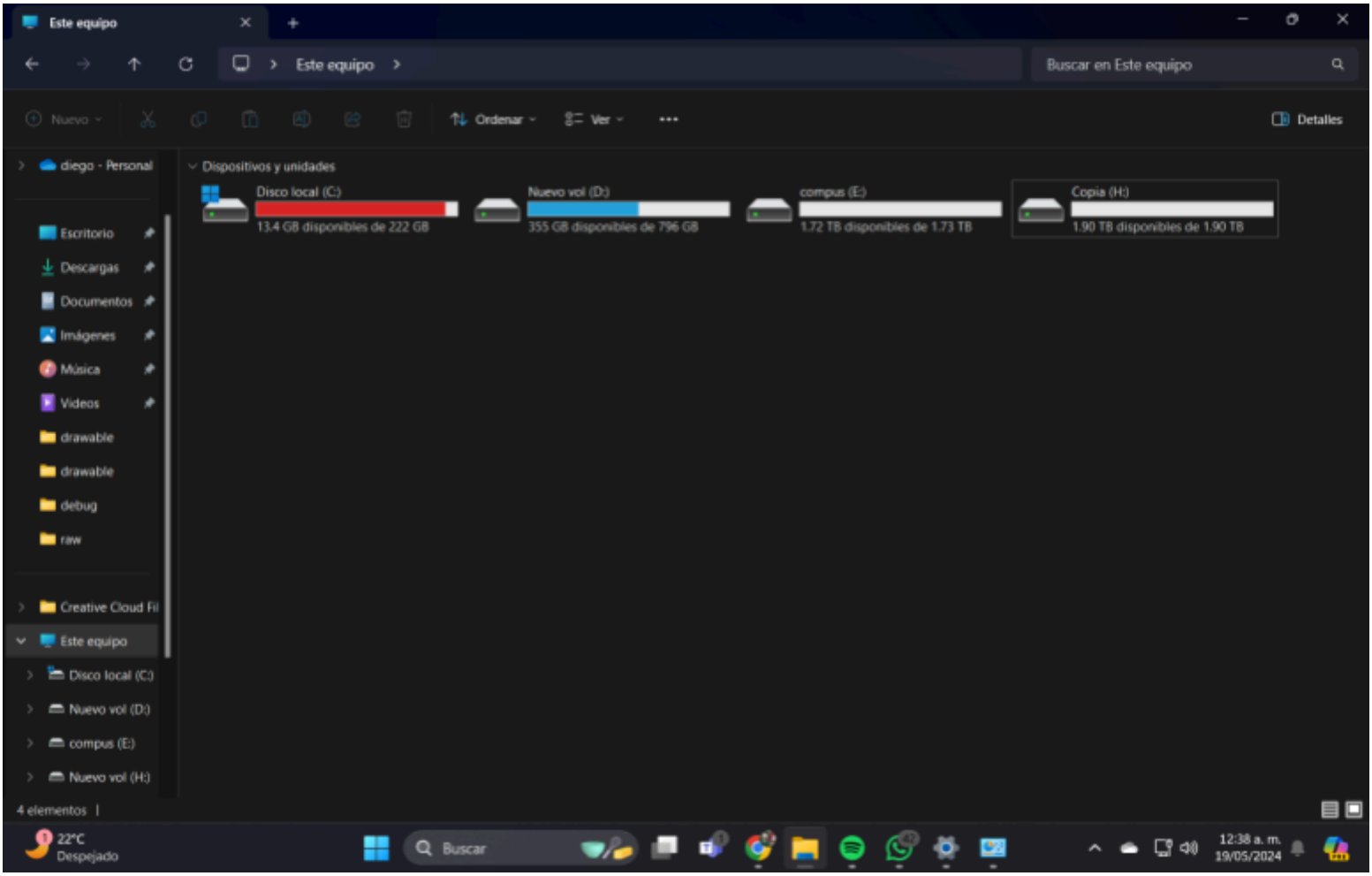
Copia de seguridad con Windows paso 4



4. Conecta una unidad externa (como un disco duro externo o una memoria USB) a tu computadora.

Figura 6.95

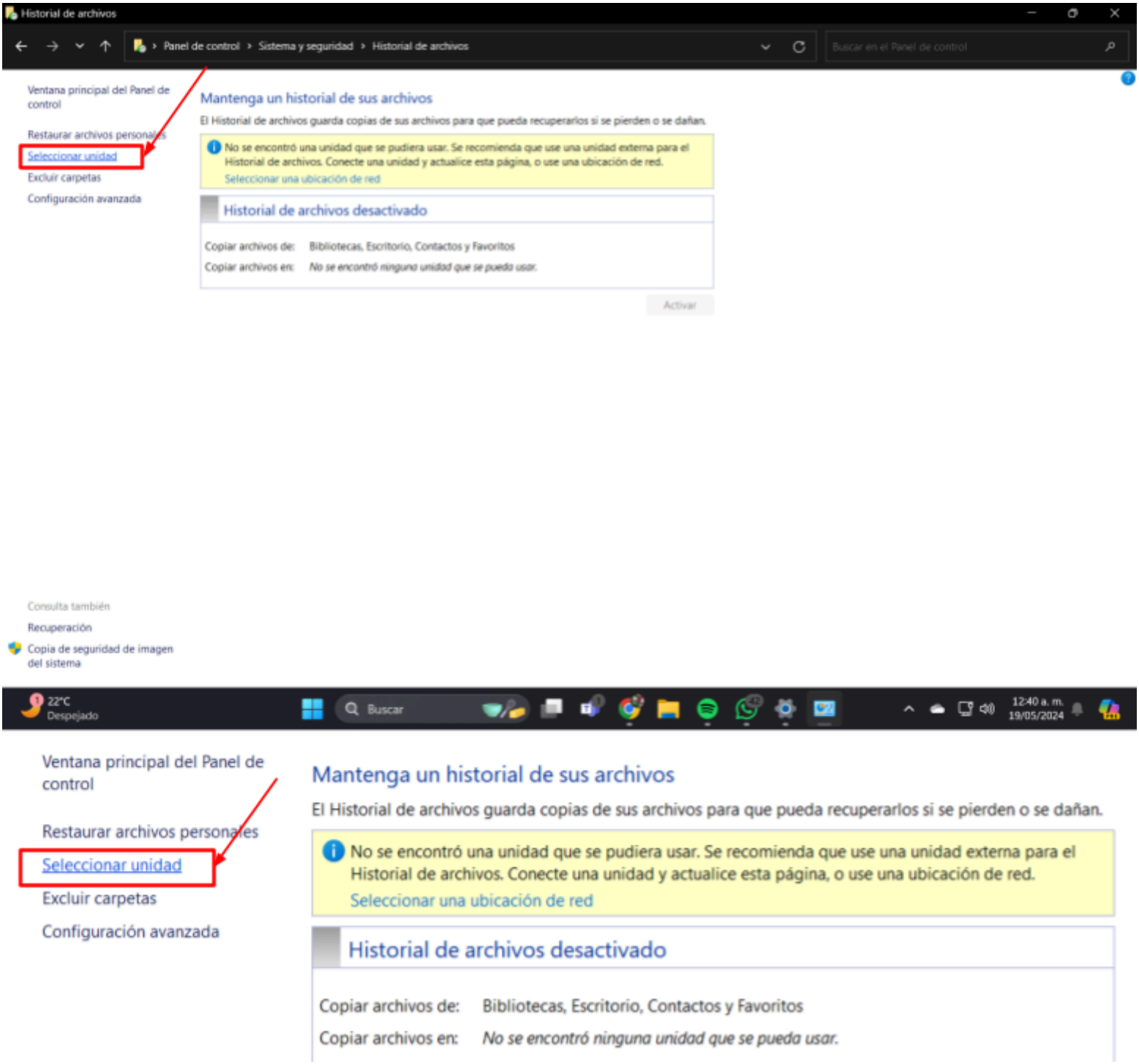
Copia de seguridad con Windows paso 5



5. En la ventana de "Historial de archivos", haz clic en "Seleccionar unidad" en el panel izquierdo.

Figura 6.96

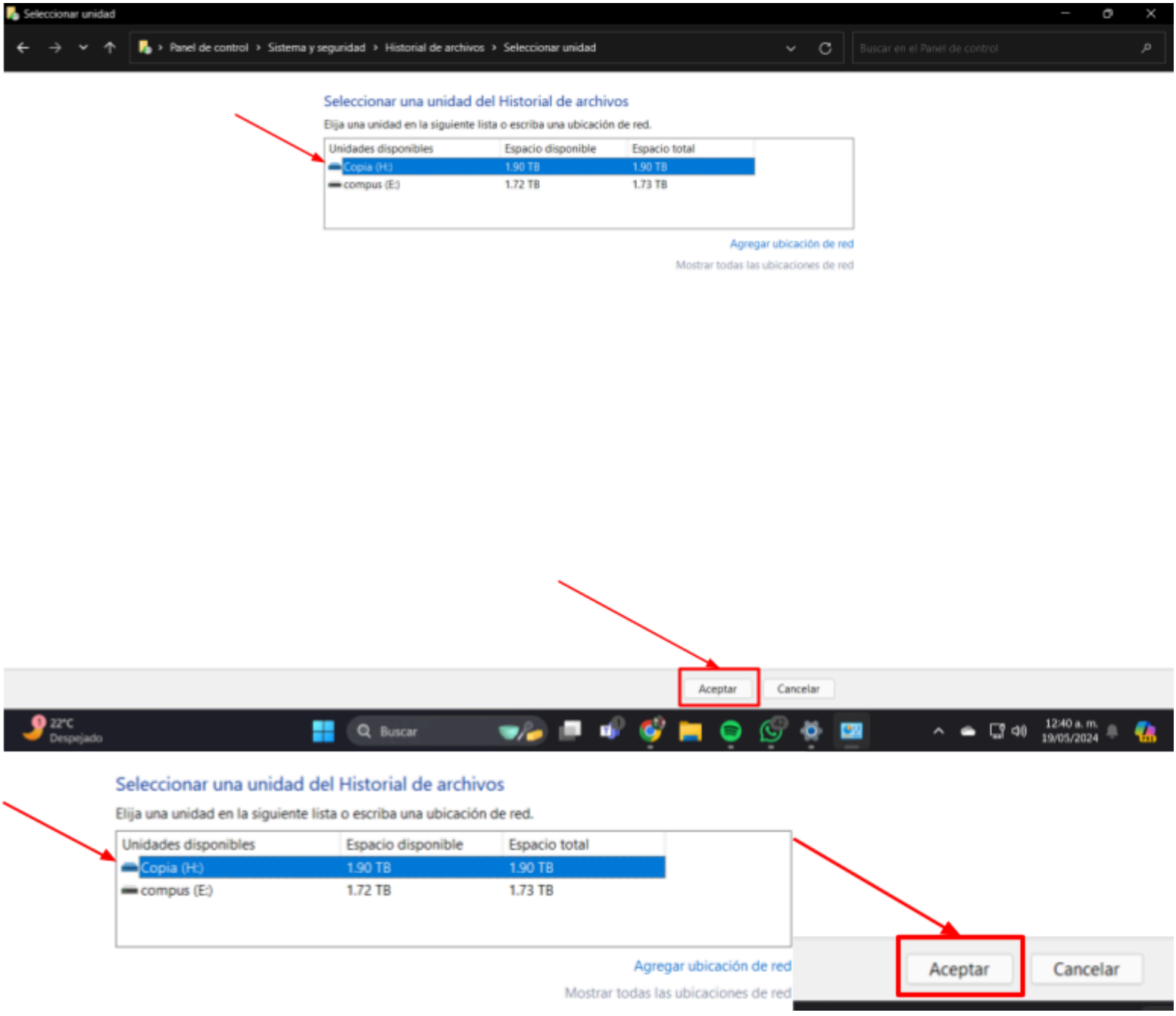
Copia de seguridad con Windows paso 6



6. Selecciona la unidad externa que conectaste y haz clic en Aceptar.

Figura 6.97

Copia de seguridad con Windows paso 7



7. Vuelve a la pantalla principal de "Historial de archivos" y haz clic en "Activar". Esto hará que Windows comience a guardar copias de seguridad de tus archivos automáticamente en la unidad seleccionada.

Figura 6.98

Copia de seguridad con Windows paso 8

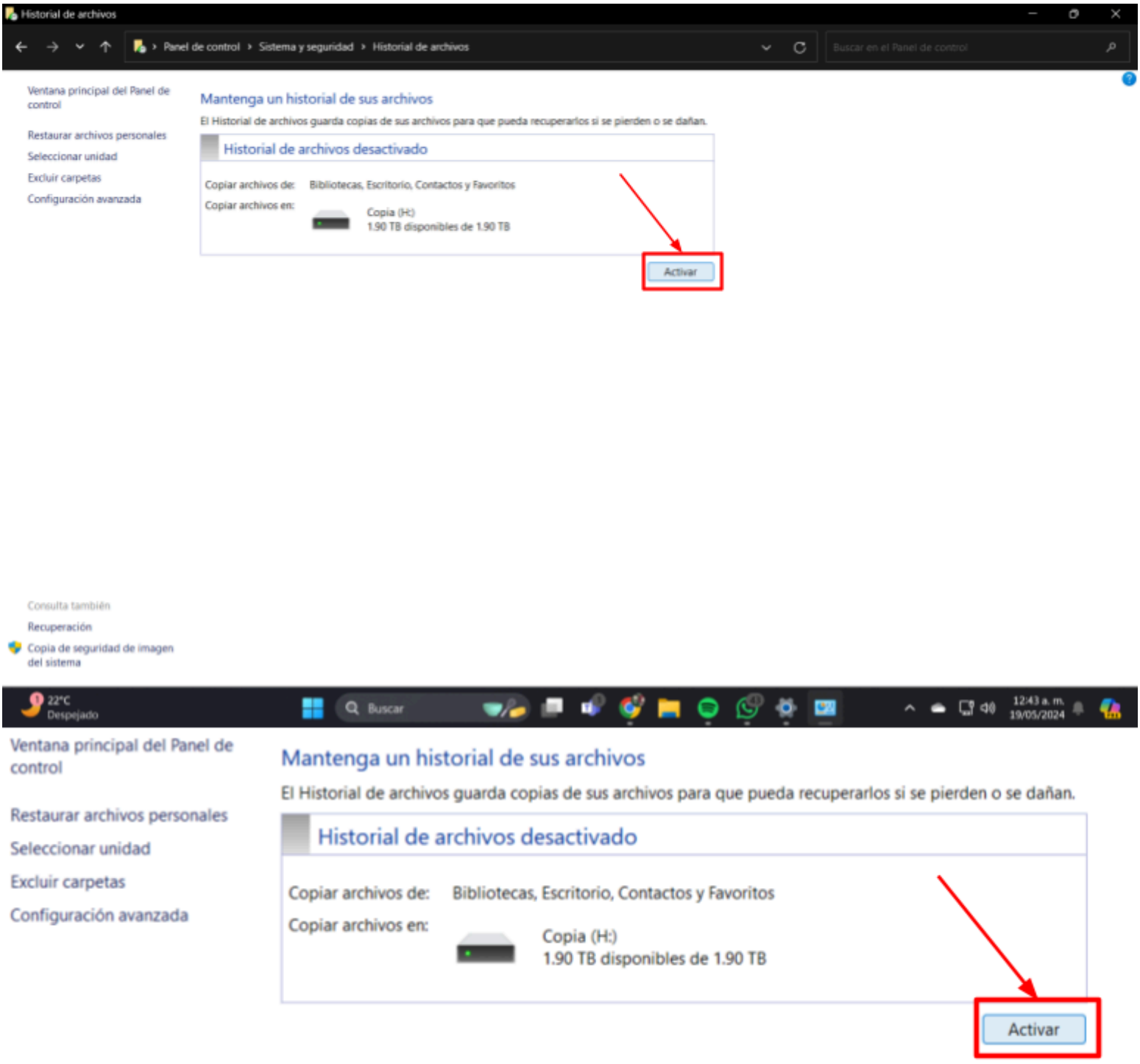
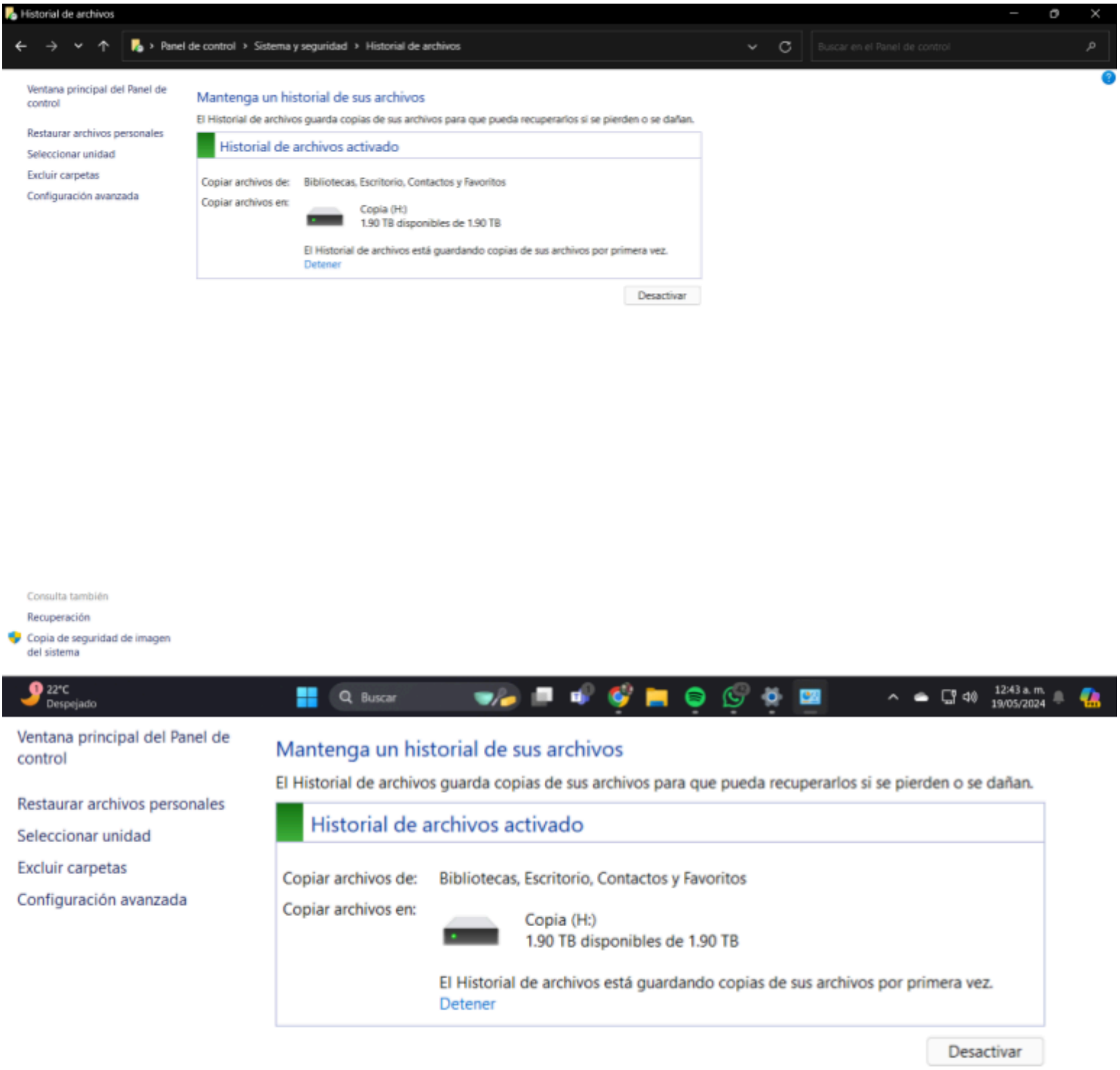


Figura 6.99

Copia de seguridad con Windows paso 9



Ventana principal del Panel de control

Restaurar archivos personales

Seleccionar unidad

Excluir carpetas

Configuración avanzada

Mantenga un historial de sus archivos

El Historial de archivos guarda copias de sus archivos para que pueda recuperarlos si se pierden o se dañan.

Historial de archivos activado

Copiar archivos de: Bibliotecas, Escritorio, Contactos y Favoritos

Copiar archivos en: Copia (H:)
1.90 TB disponibles de 1.90 TB

El Historial de archivos está guardando copias de sus archivos por primera vez.
Detener

Desactivar

8. Para ajustar la frecuencia de las copias de seguridad y cuánto tiempo se conservarán, haz clic en "Configuración avanzada" en el panel izquierdo. Aquí puedes elegir cada cuánto tiempo se realizarán las copias de seguridad y cuánto tiempo se conservarán las versiones de los archivos.

Figura 6.100

Copia de seguridad con Windows paso 10

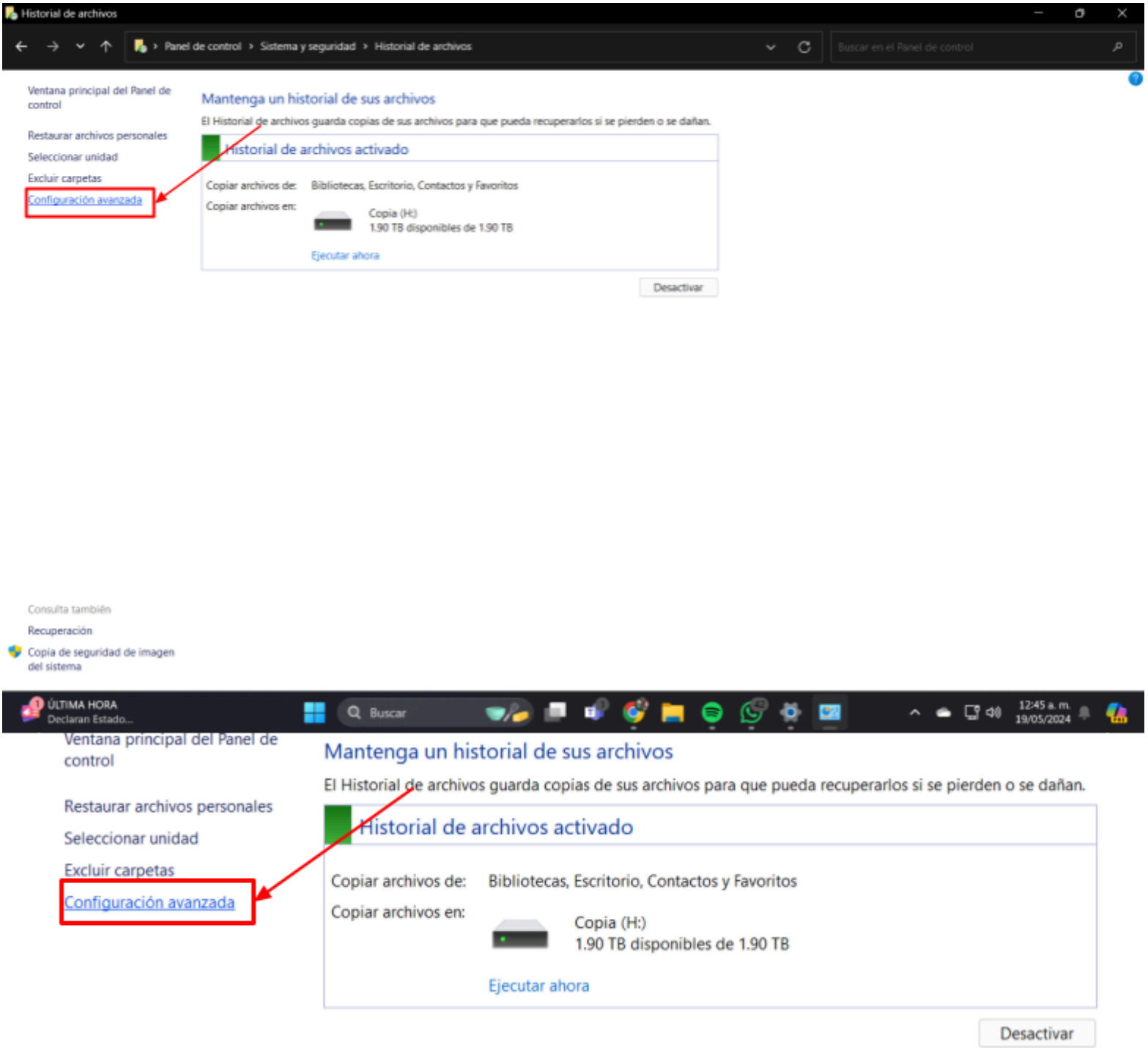
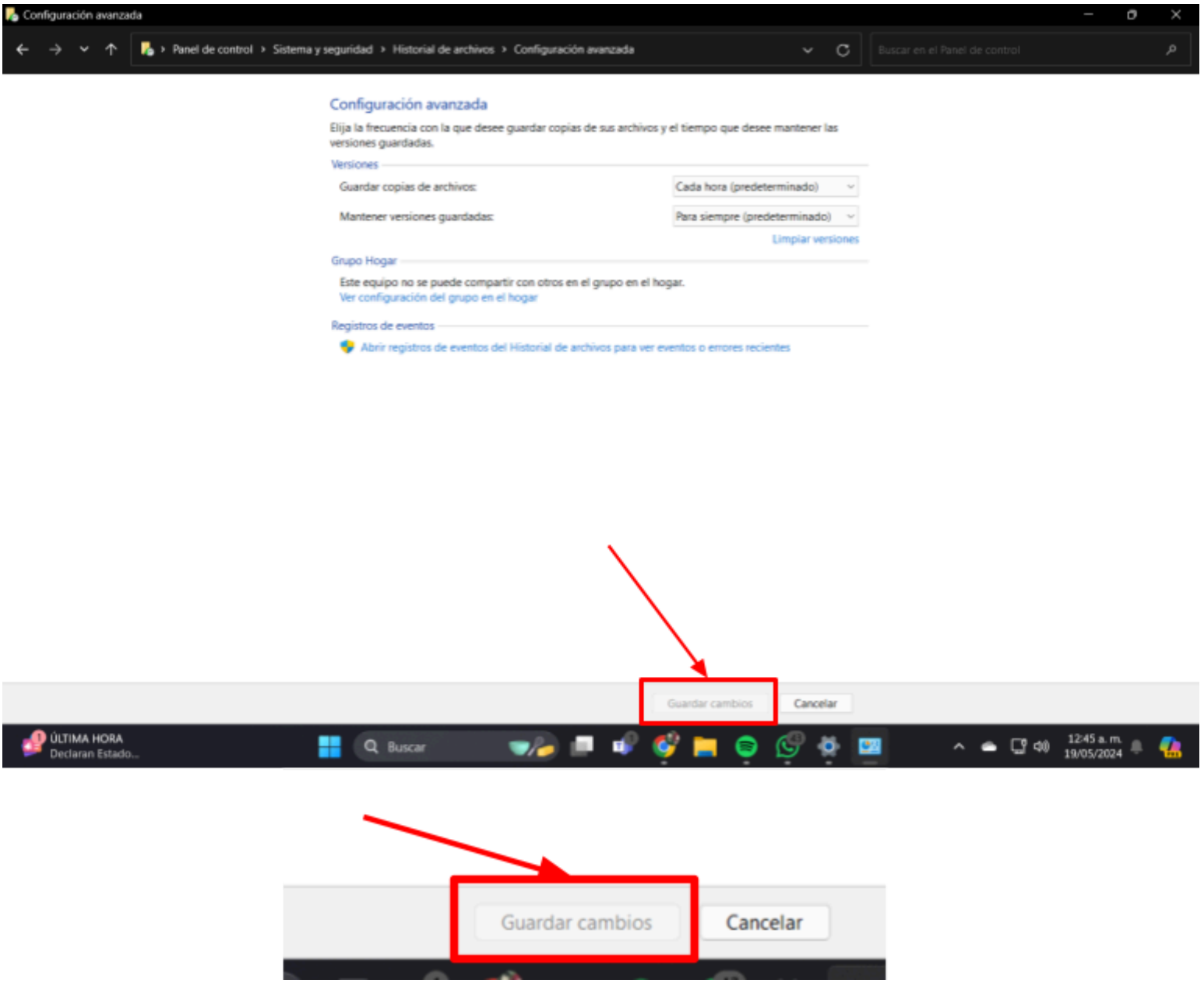


Figura 6.101

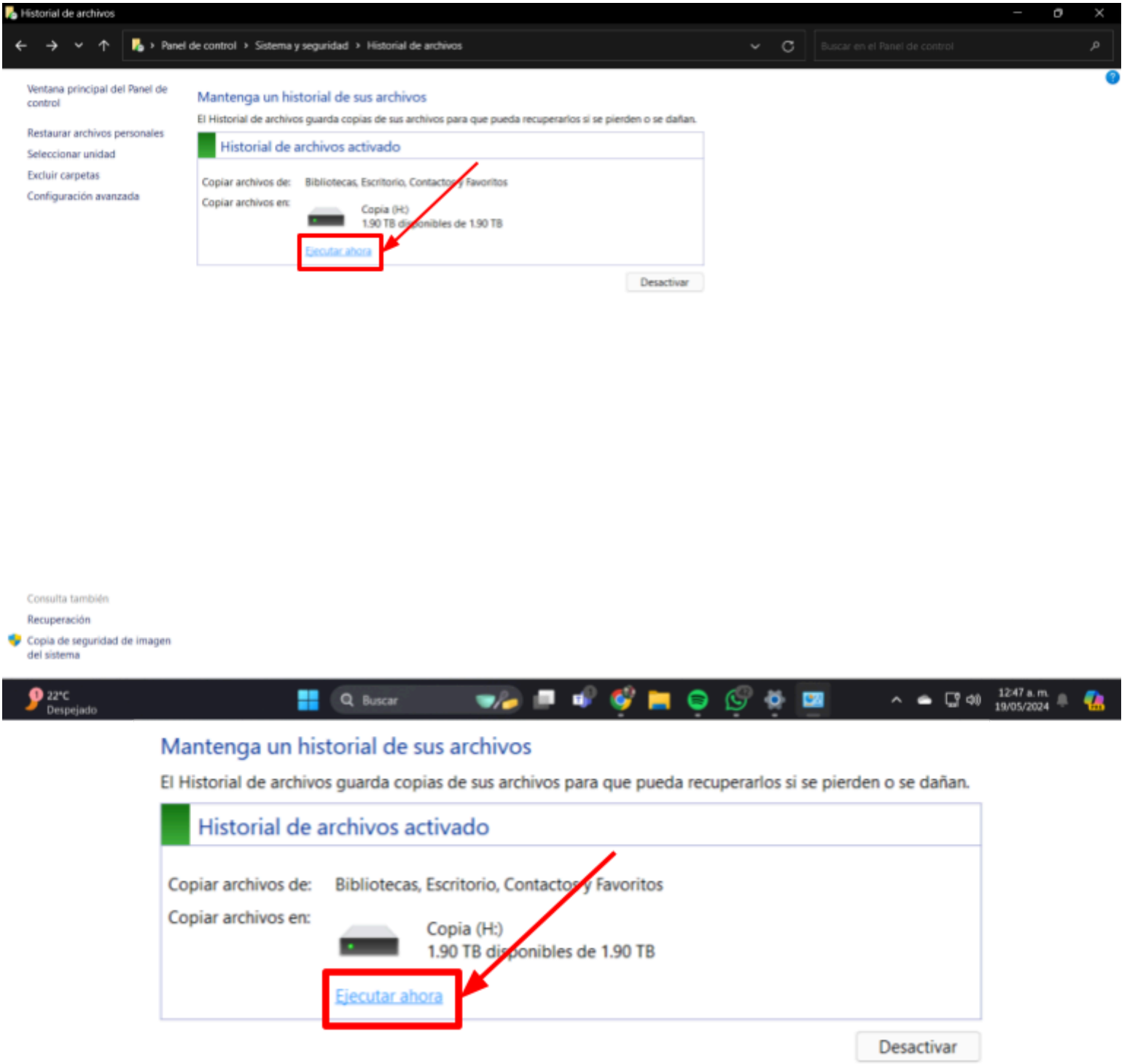
Copia de seguridad con Windows paso 11



9. Si deseas hacer una copia de seguridad manual de inmediato, haz clic en "Ejecutar ahora" en la pantalla principal de "Historial de archivos".

Figura 6.102

Copia de seguridad con Windows paso 12



10. Para recuperar archivos, haz clic en "Restaurar archivos personales" en el panel izquierdo de la pantalla principal de "Historial de archivos". Navega hasta los archivos o carpetas que deseas recuperar.

Figura 6.103

Copia de seguridad con Windows paso 13

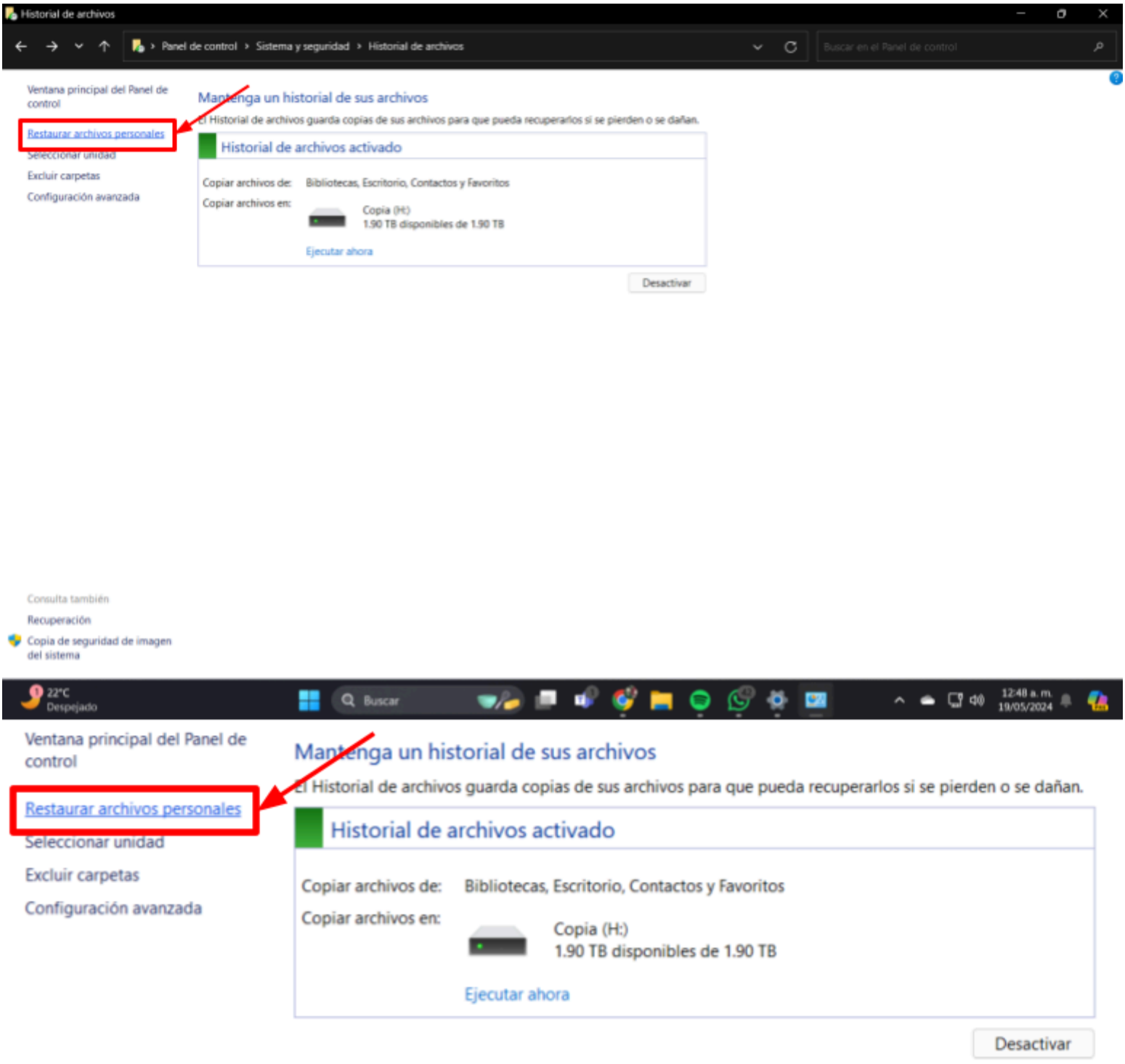
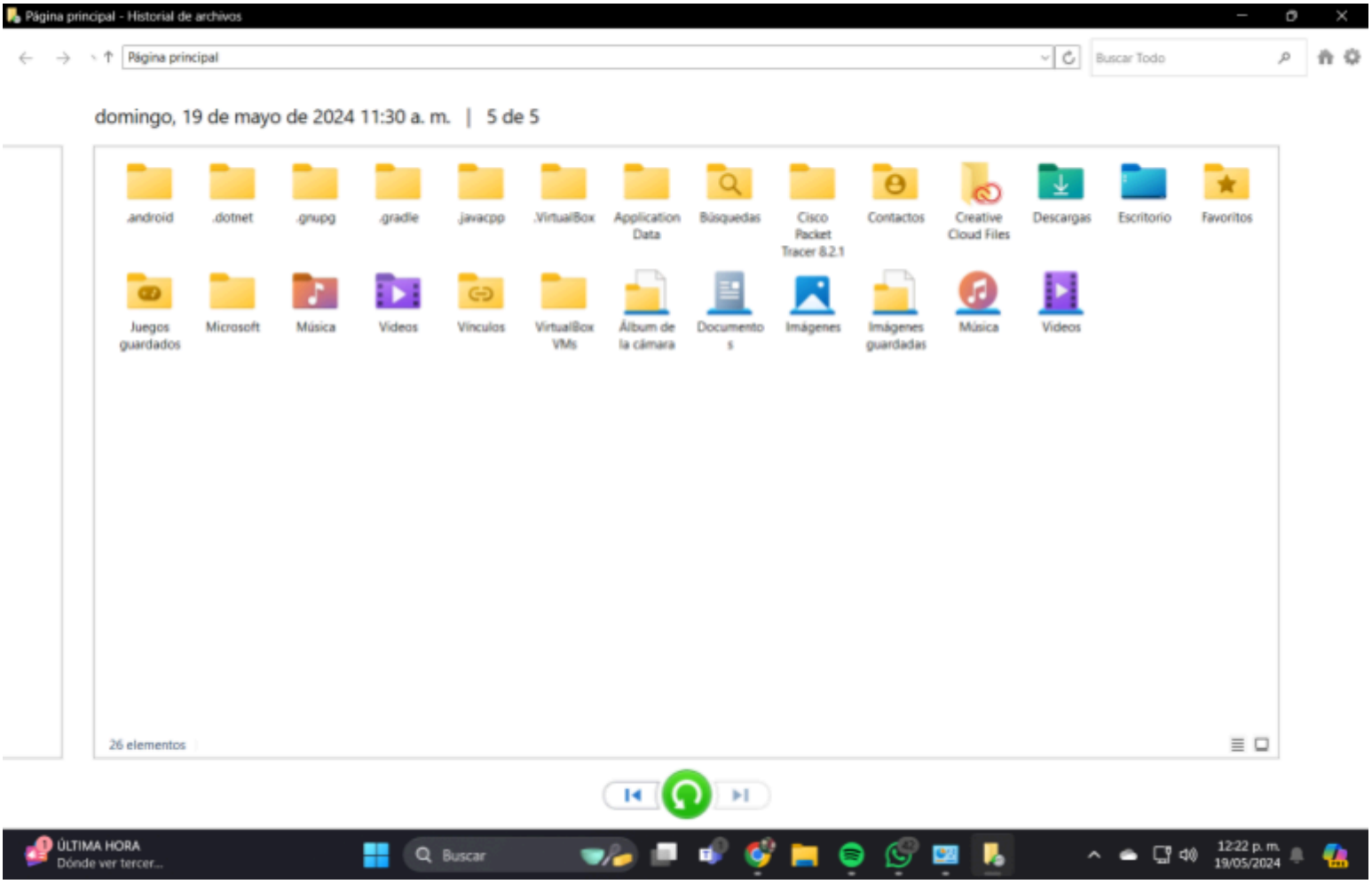


Figura 6.104

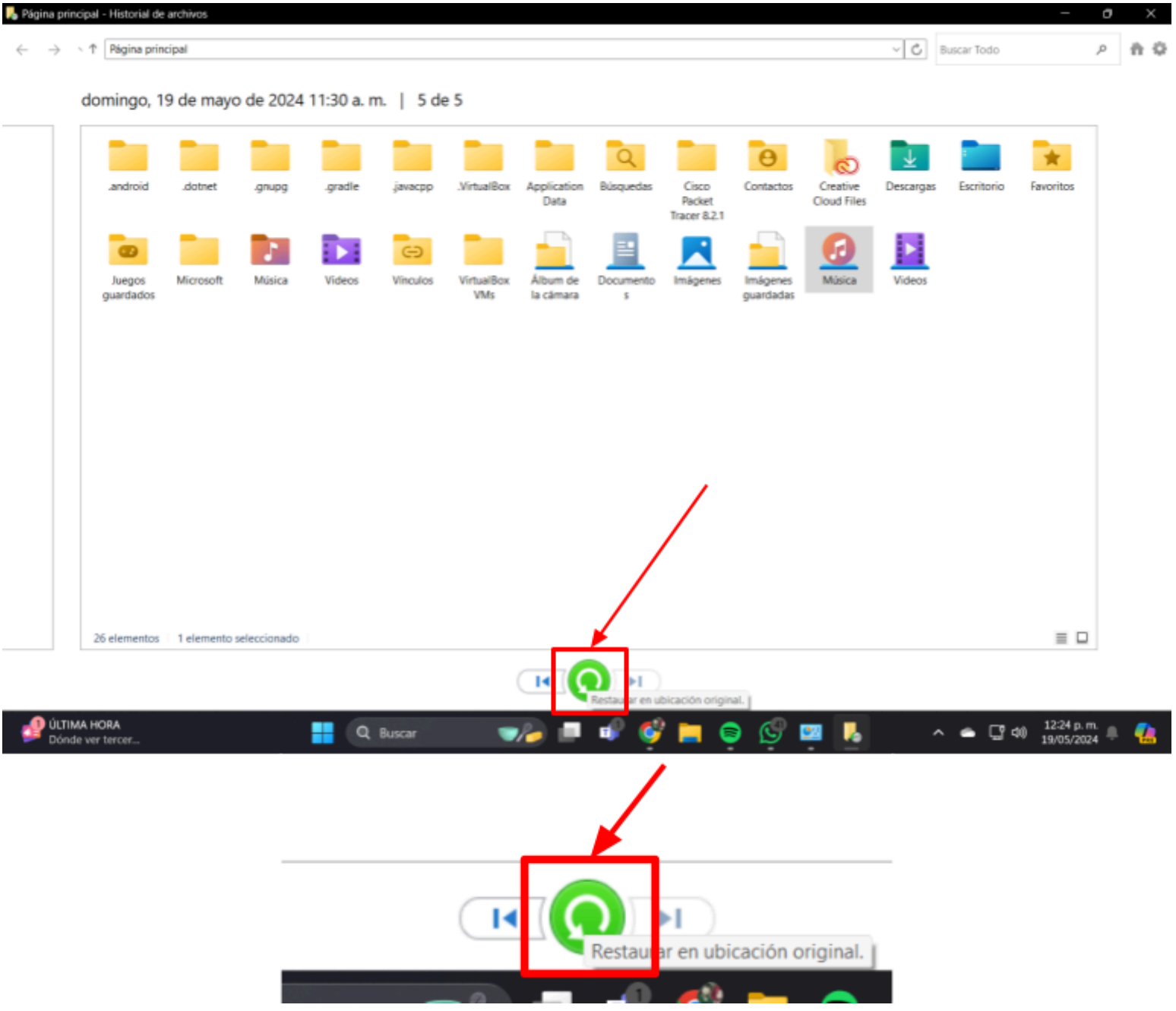
Copia de seguridad con Windows paso 14



11. Selecciona los archivos o carpetas y haz clic en el botón verde que dice Restaurar en la parte inferior de la ventana. También puedes hacer clic derecho en los archivos y seleccionar “Restaurar en” para elegir una ubicación diferente.

Figura 6.105

Copia de seguridad con Windows paso 15



Consideraciones Adicionales

- Frecuencia de las copias de seguridad: Es recomendable hacer copias de seguridad regularmente, por ejemplo, semanal o mensualmente, dependiendo de la cantidad de datos nuevos o modificados que manejes.
- Almacenamiento en la Nube: Considera también utilizar servicios de almacenamiento en la nube como OneDrive, Google Drive o Dropbox para copias de seguridad adicionales y acceso remoto.
- Verificación de Copias de Seguridad: Revisa periódicamente que las copias de seguridad se estén realizando correctamente y que los datos sean recuperables.
- Revisión de Configuración de Respaldo Automático en Teléfonos para Cada Aplicación: En los teléfonos, muchas aplicaciones realizan automáticamente sus respaldos en la nube en horarios de baja actividad del dispositivo sin necesidad de intervención del usuario. Es recomendable verificar que estos respaldos se están realizando correctamente y que cada aplicación, como mensajería, fotos y documentos, esté gestionando sus datos de acuerdo con su propio método de respaldo. Esto asegura que los datos de cada aplicación sean recuperables sin afectar el rendimiento del dispositivo en horarios de uso.

Nota: Realizar estas copias de seguridad de manera rutinaria te ayudará a mantener tus datos seguros y minimizará el impacto de posibles problemas futuros.

6.10

Cómo Identificar Correos Electrónicos con malware

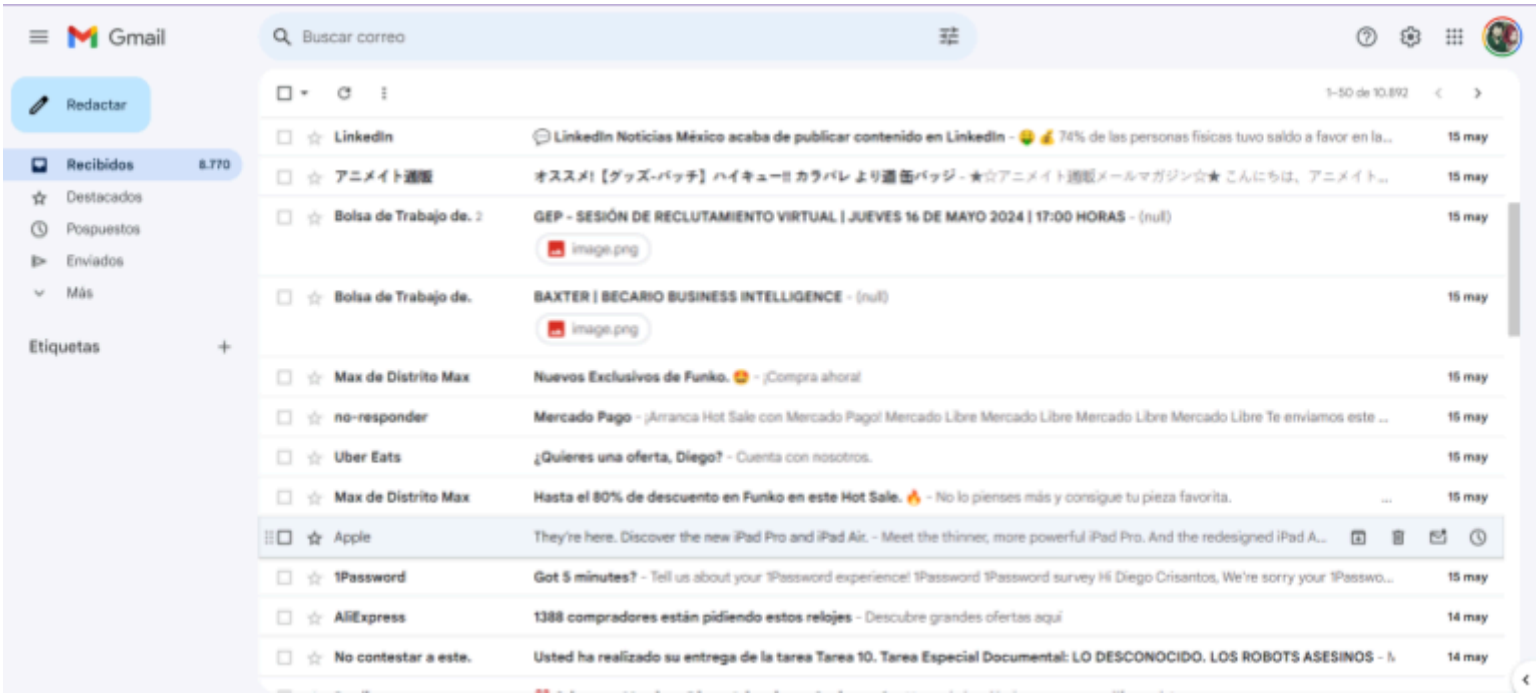
El malware es un término general que se refiere a cualquier software malicioso diseñado para dañar, explotar o acceder sin autorización a sistemas informáticos. Los correos electrónicos con malware pueden parecer legítimos, pero hay varios indicios que pueden ayudarte a identificarlos y evitar caer en la trampa. A continuación, puedes ver los pasos para identificar correos electrónicos con malware y algunos tipos comunes de malware.

1. Verifica el remitente:

- Abre el correo electrónico y observa la dirección de correo del remitente.

Figura 6.106

verificar remitente



- Los correos con malware a menudo utilizan direcciones que parecen legítimas pero tienen ligeras variaciones (por ejemplo: en lugar de bank@example.com, pueden usar b@nk@example.com).

Figura 6.107

Correo con remitente correcto

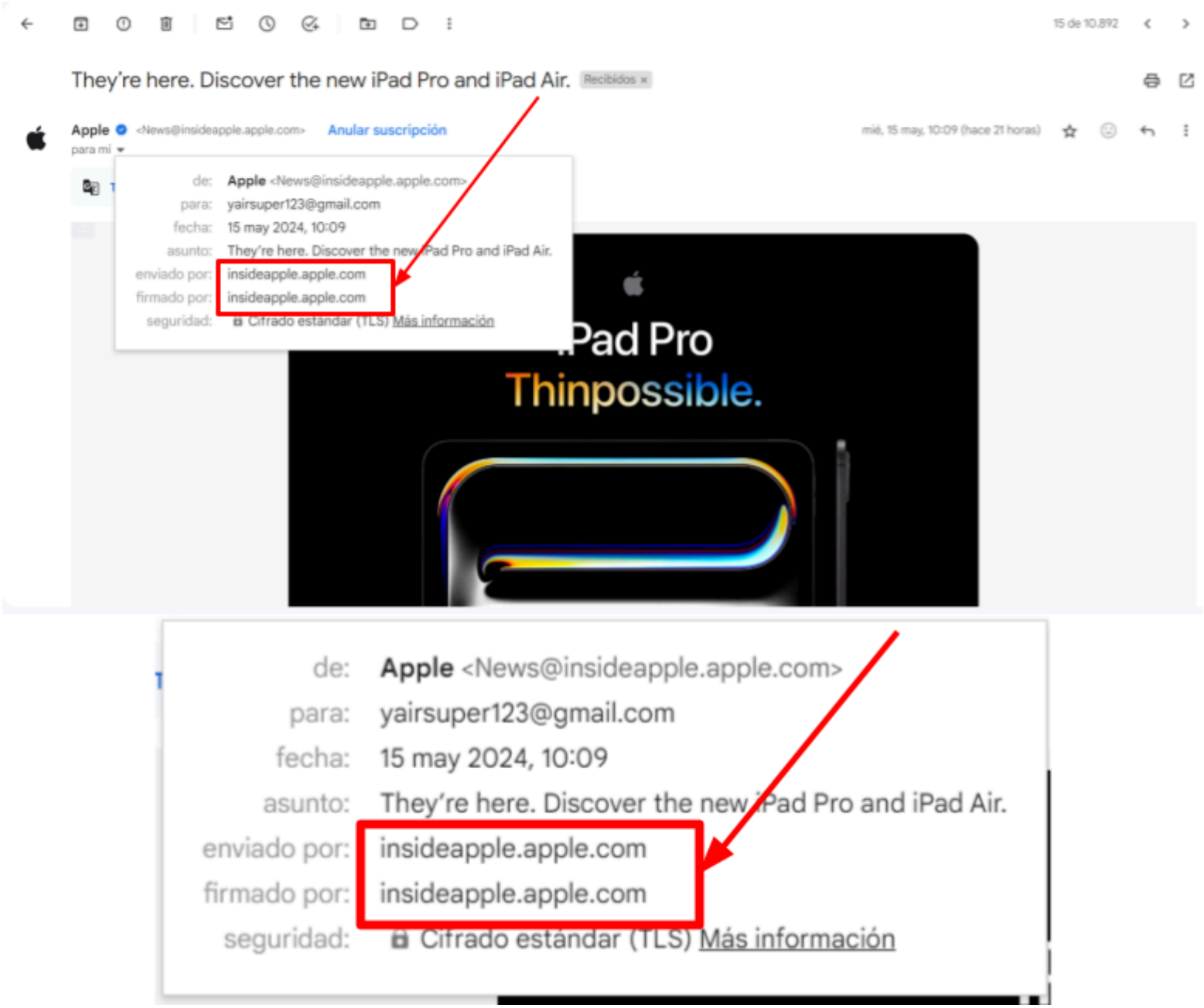
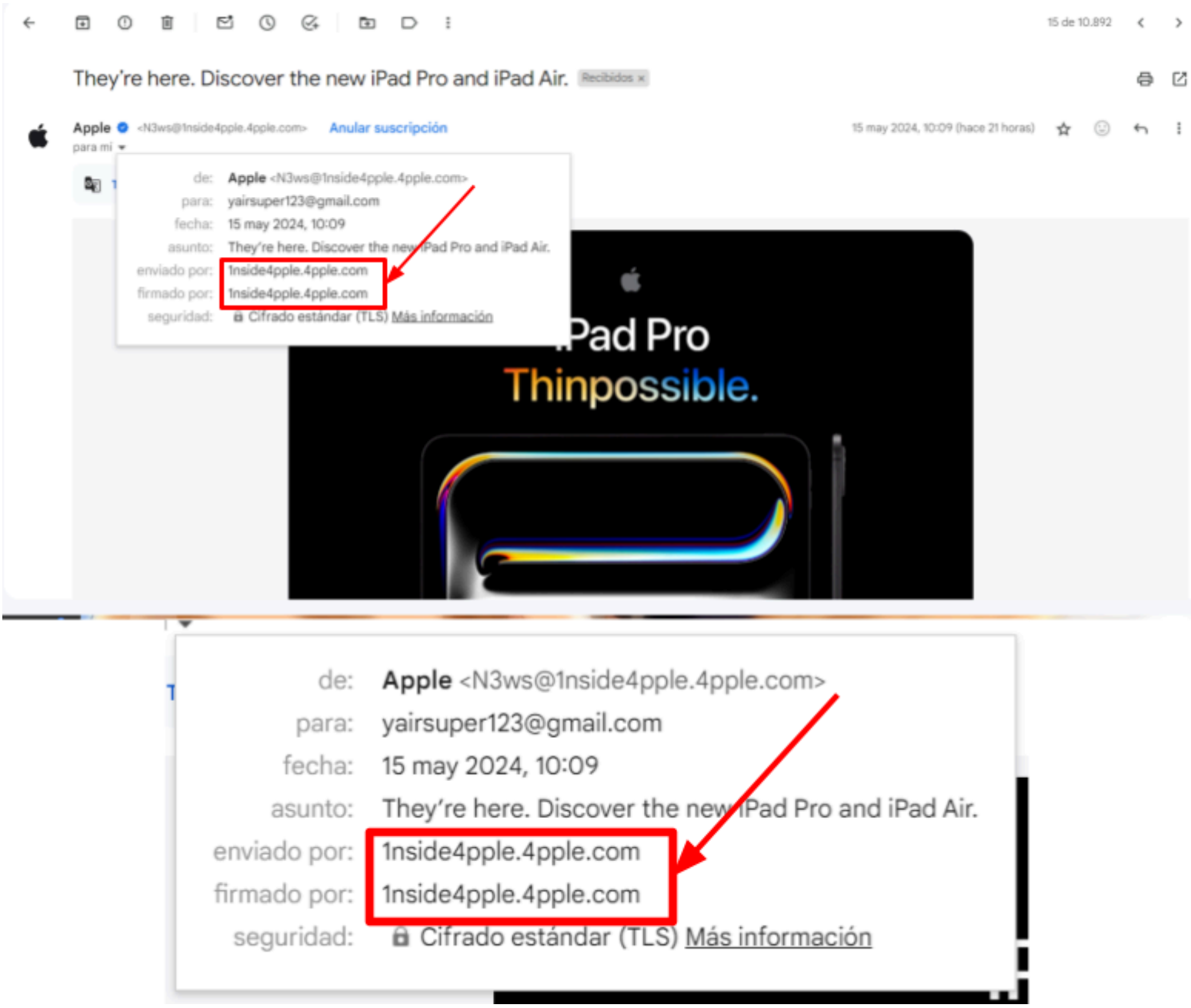


Figura 6.108

Correo con remitente incorrecto

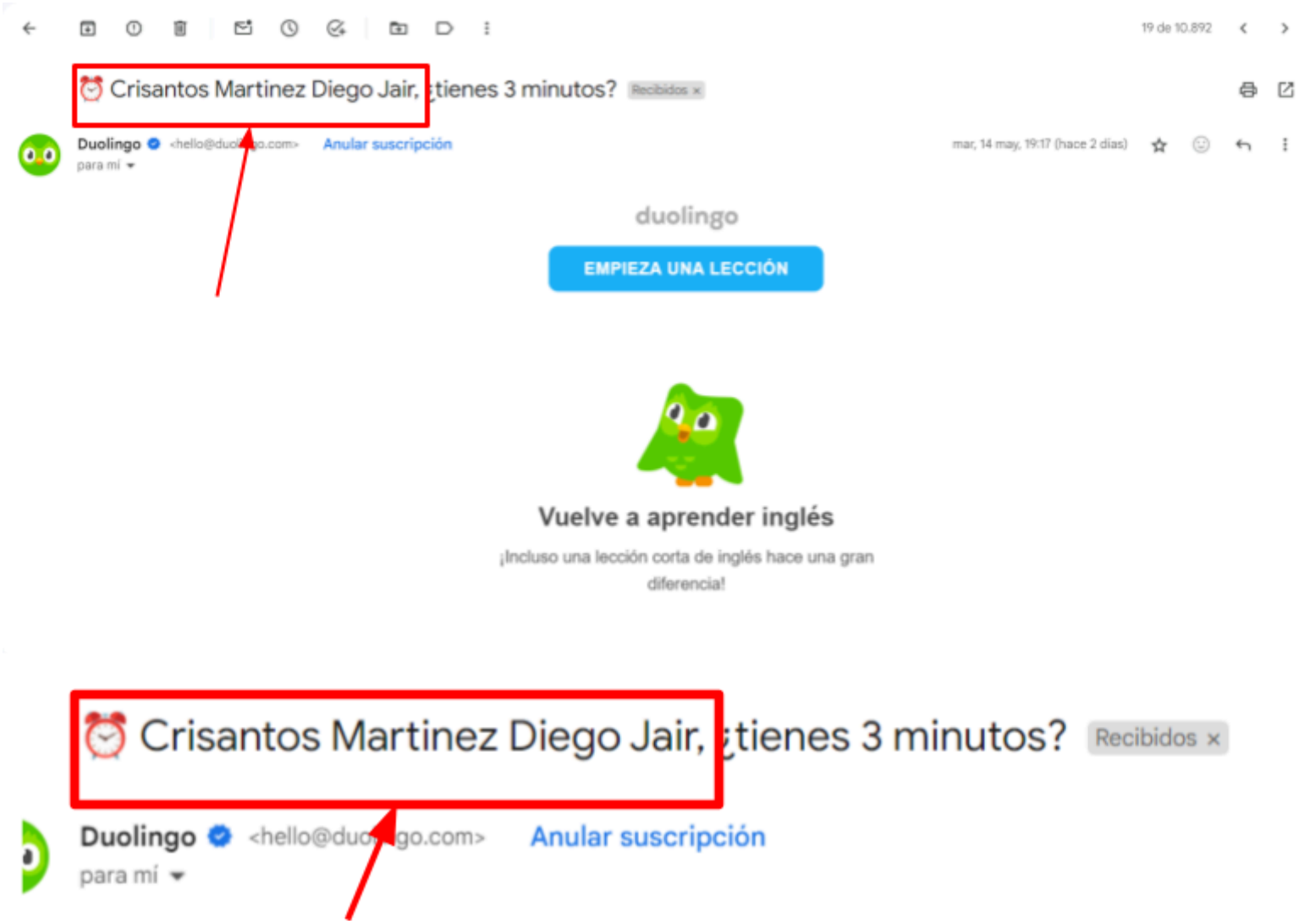


2. Presta atención al saludo:

- Los correos legítimos generalmente usan tu nombre real.

Figura 6.109

Correo con nombre real



- Los correos con malware suelen comenzar con un saludo genérico como "Estimado usuario" o "Querido cliente" y en algunos casos usan el nombre de tu correo electrónico.

Figura 6.110
Correo sin nombre

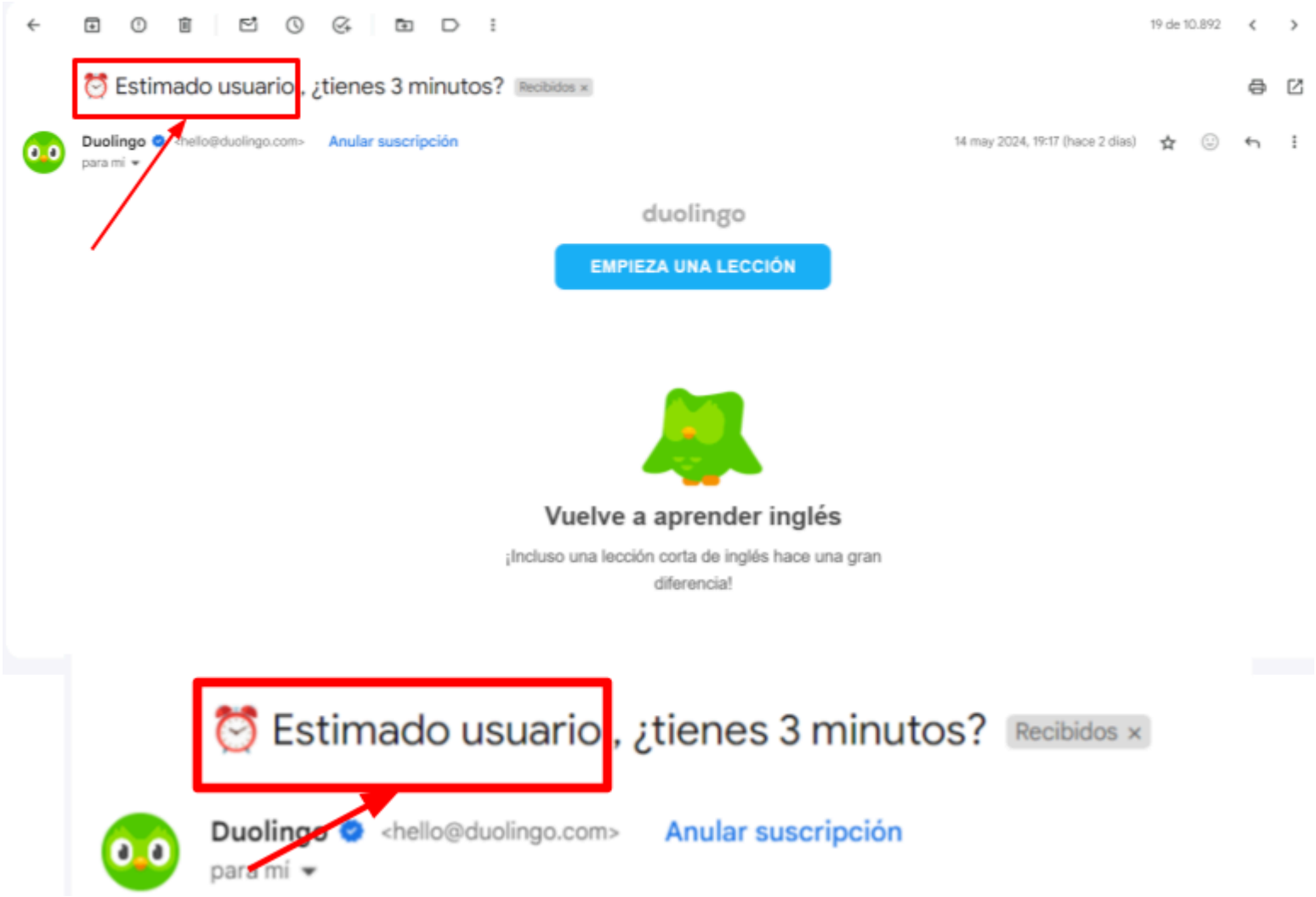
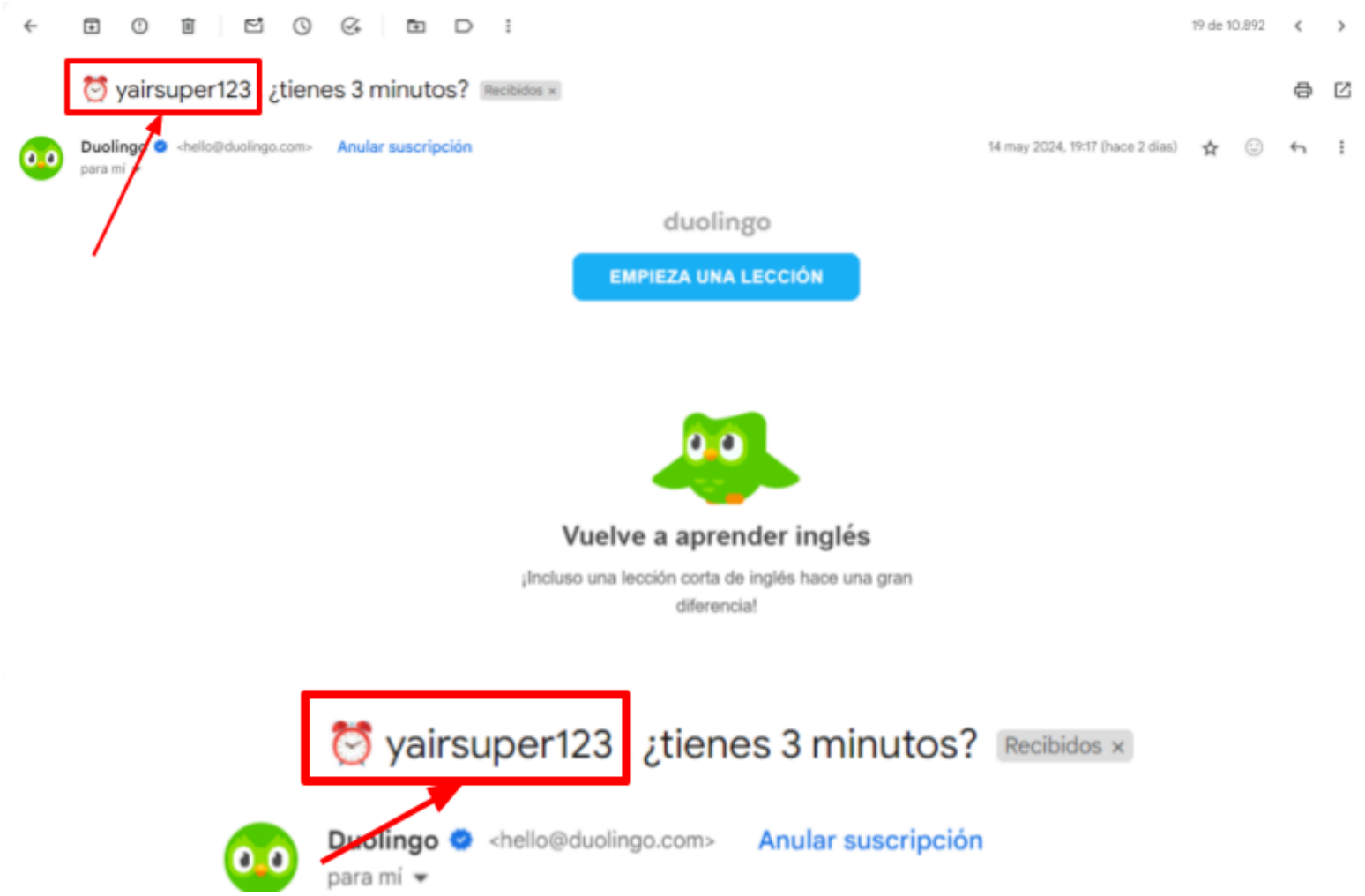


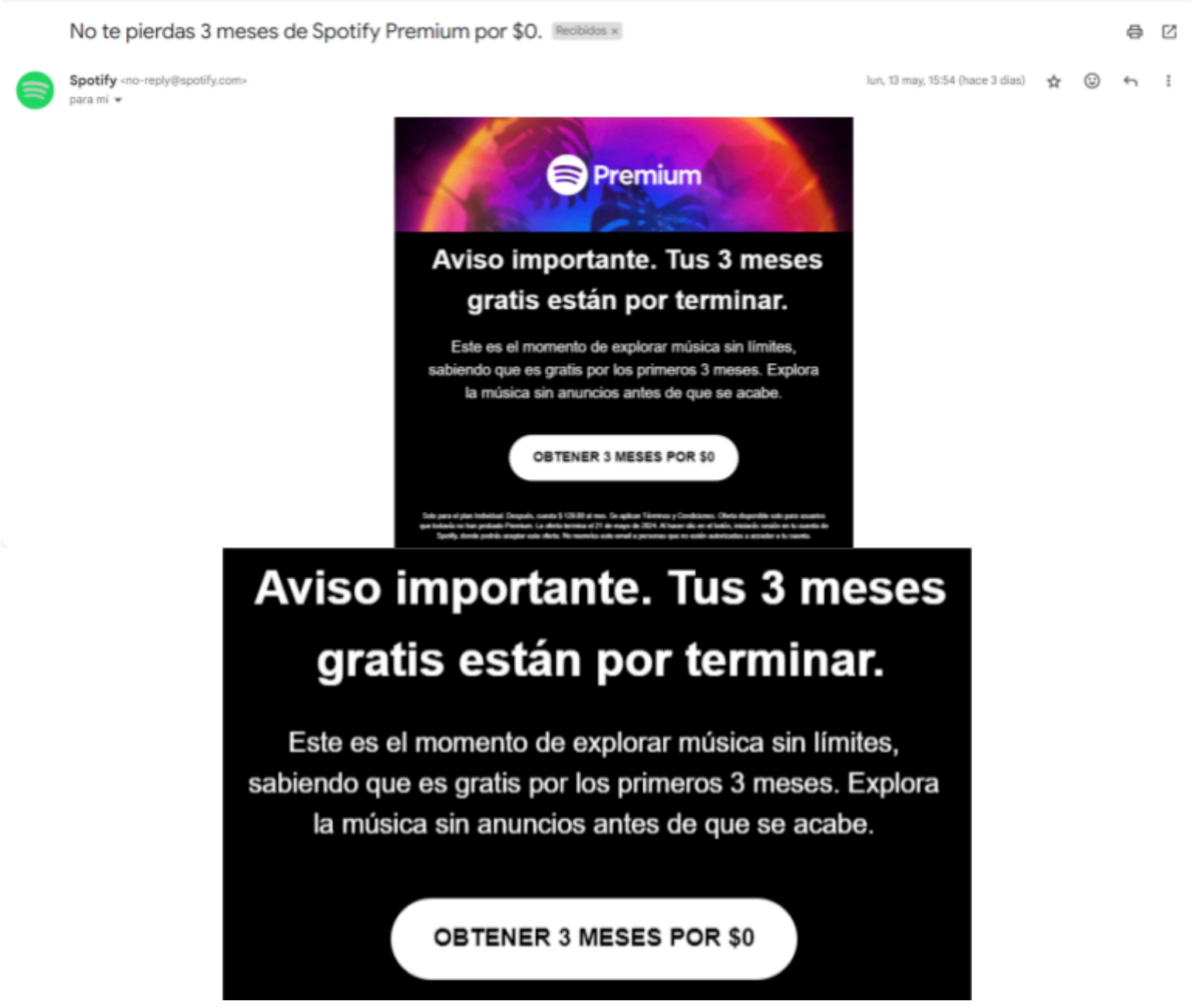
Figura 6.111

Correo con nombre del e-mail



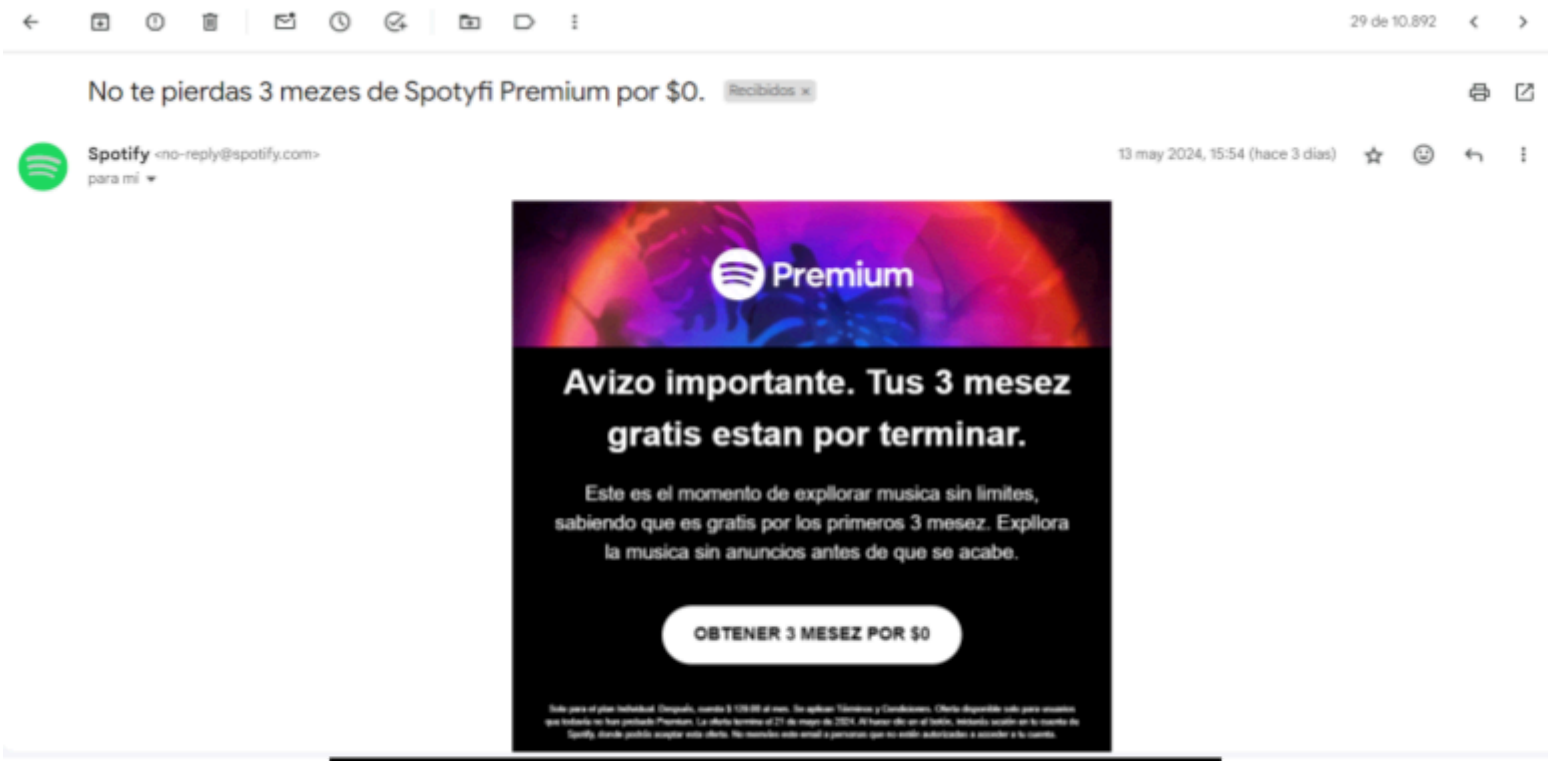
3. Examina el contenido del mensaje:
- Los correos legítimos de empresas suelen estar bien redactados y sin errores.

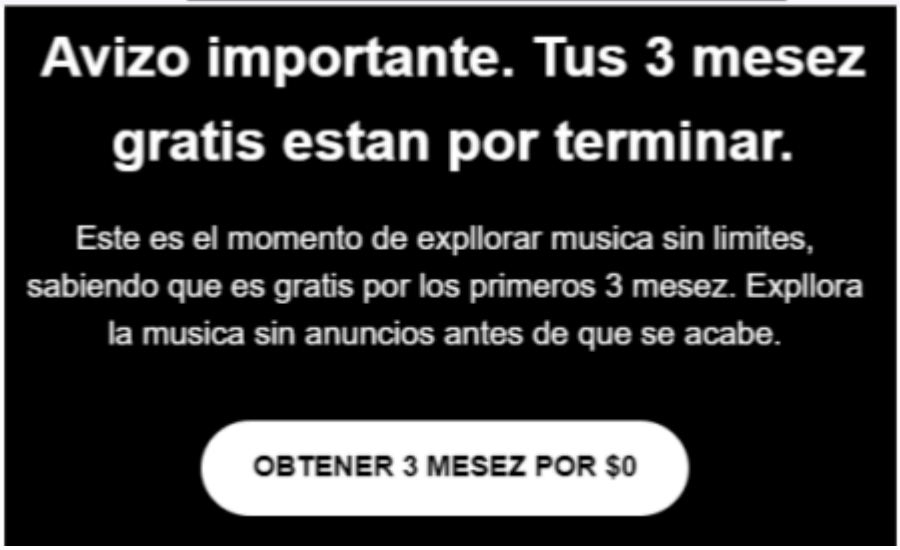
Figura 6.112
Correo sin errores



- Busca errores gramaticales y ortográficos. Los correos con malware a menudo contienen muchos errores.

Figura 6.113
Correo con errores gramaticales



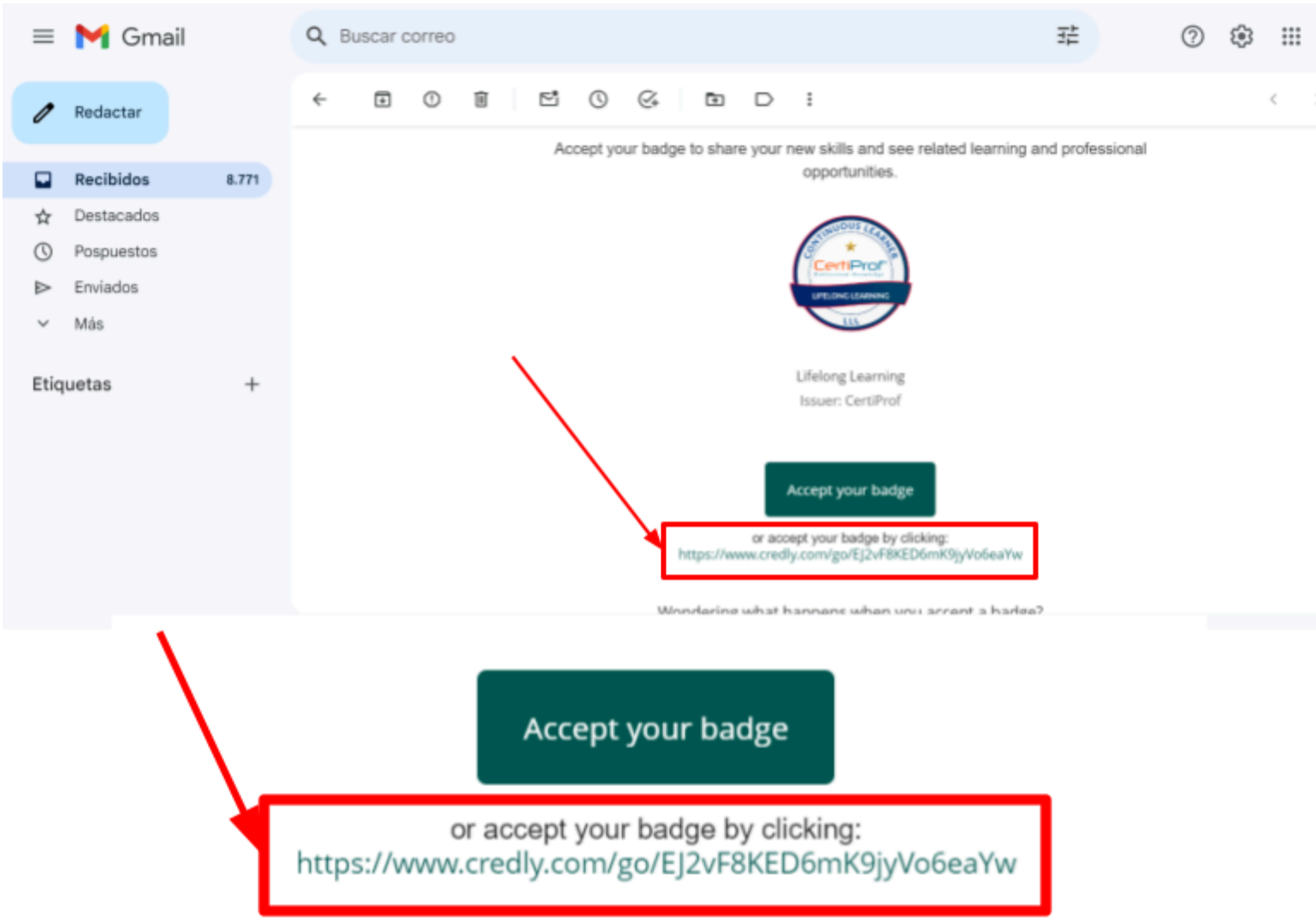


4. Analiza los enlaces:

- Observa la URL que aparece. Si la URL parece sospechosa o no coincide con la dirección oficial del sitio web, es probable que contenga malware.

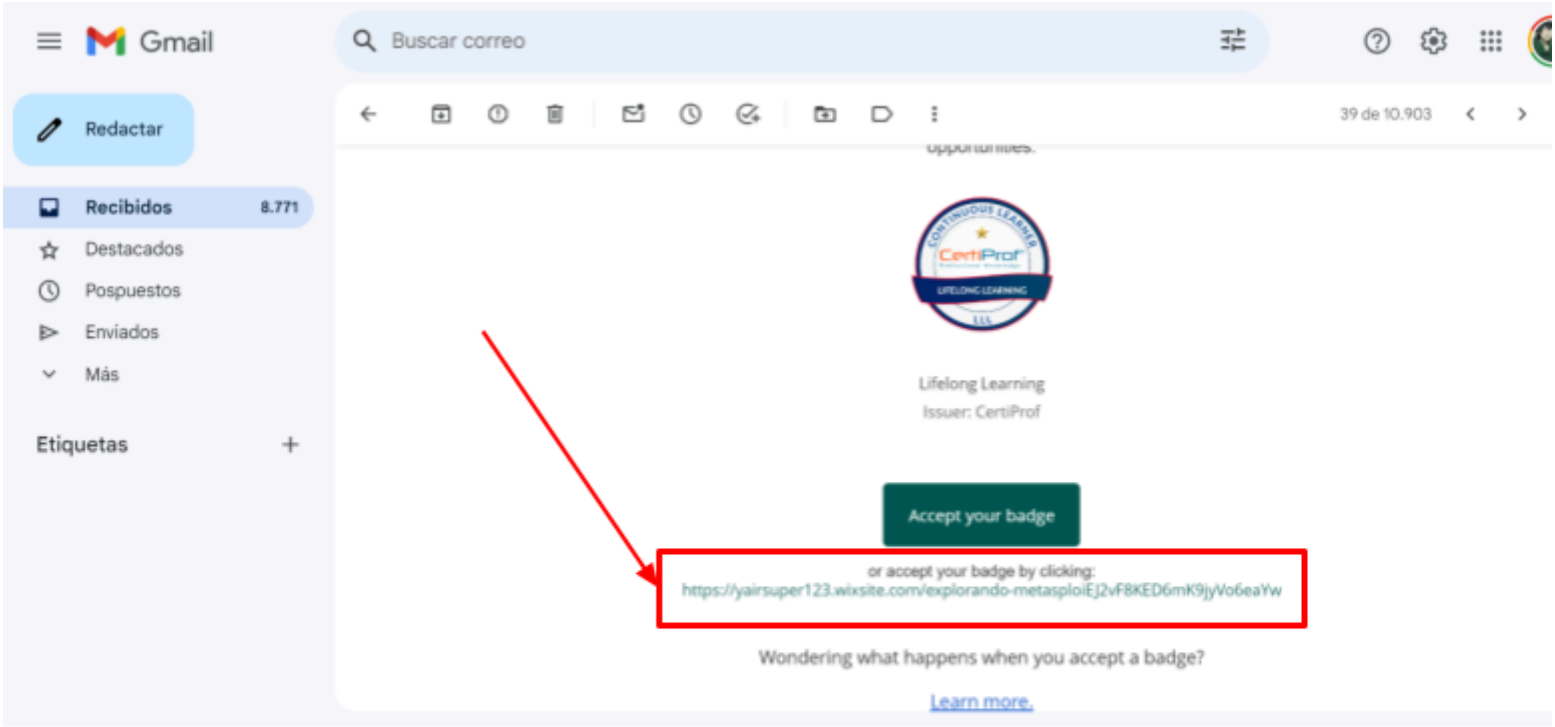
Figura 6.114

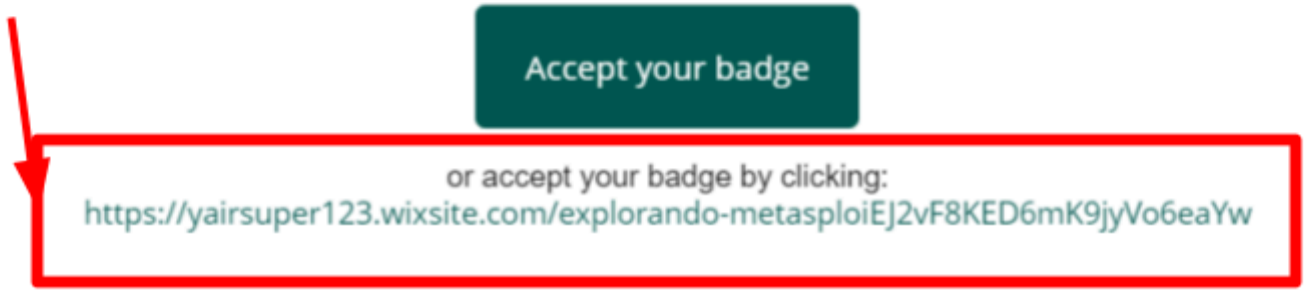
Correo con URL correcta



- Los enlaces maliciosos pueden contener nombres de dominio extraños o caracteres inusuales.

Figura 6.115
Correo con URL falsa



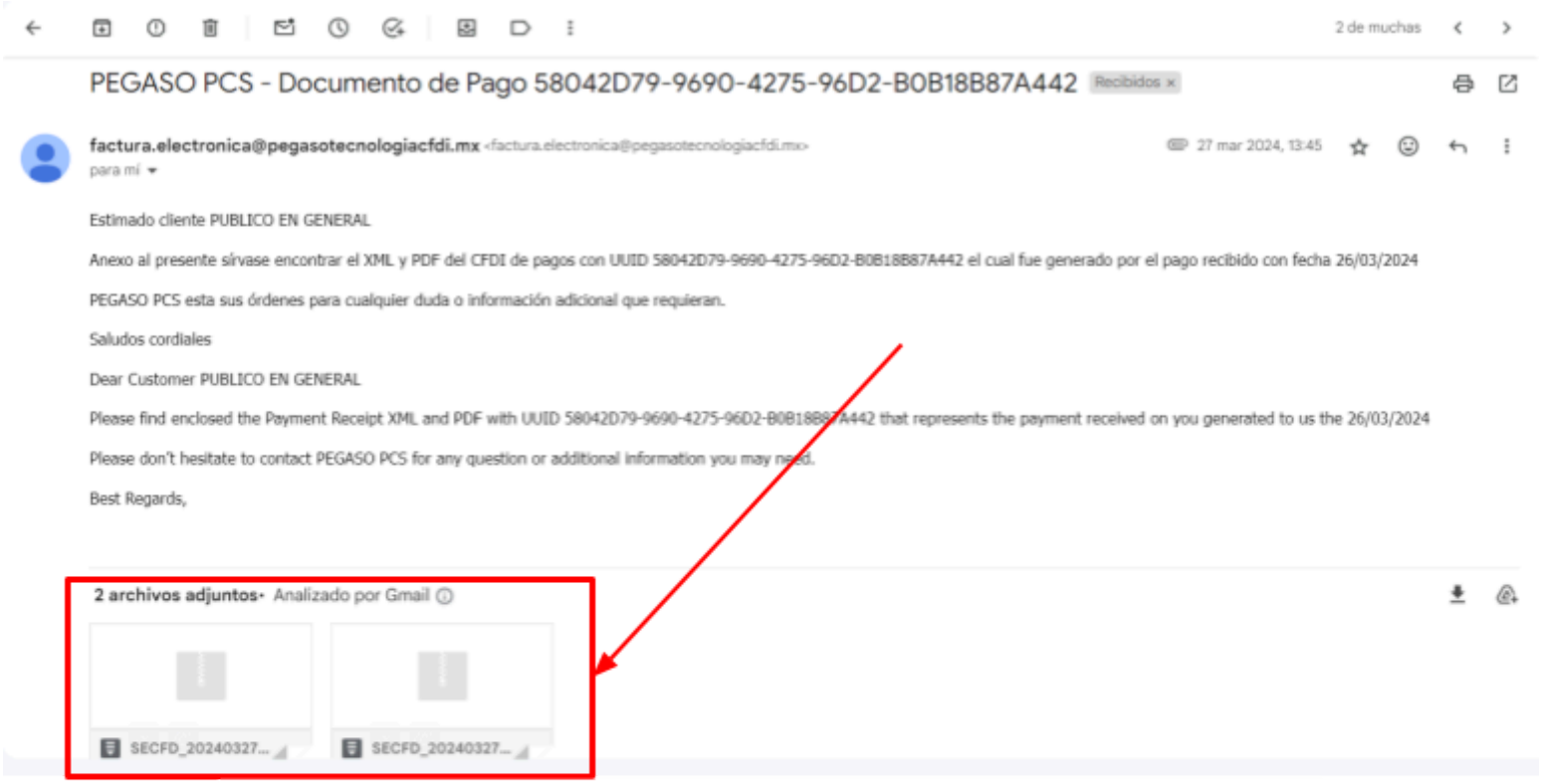


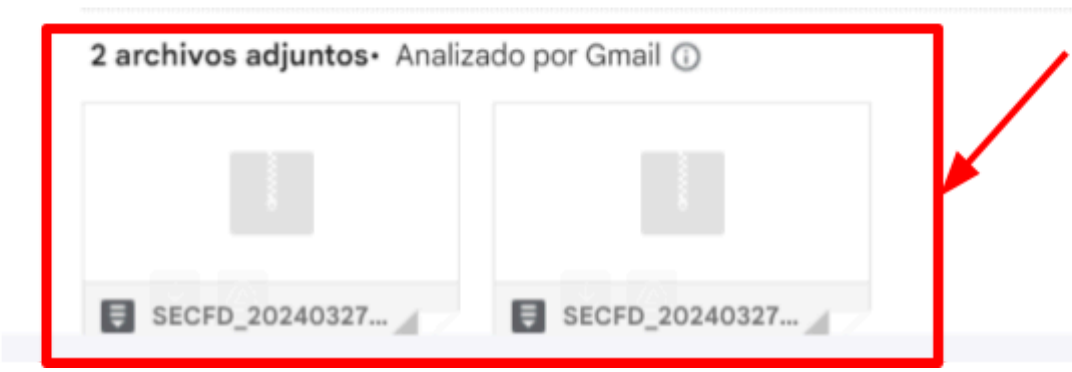
5. Desconfía de los archivos adjuntos:

- Los correos con malware pueden contener archivos maliciosos adjuntos.

Figura 6.116

Correo con archivos maliciosos





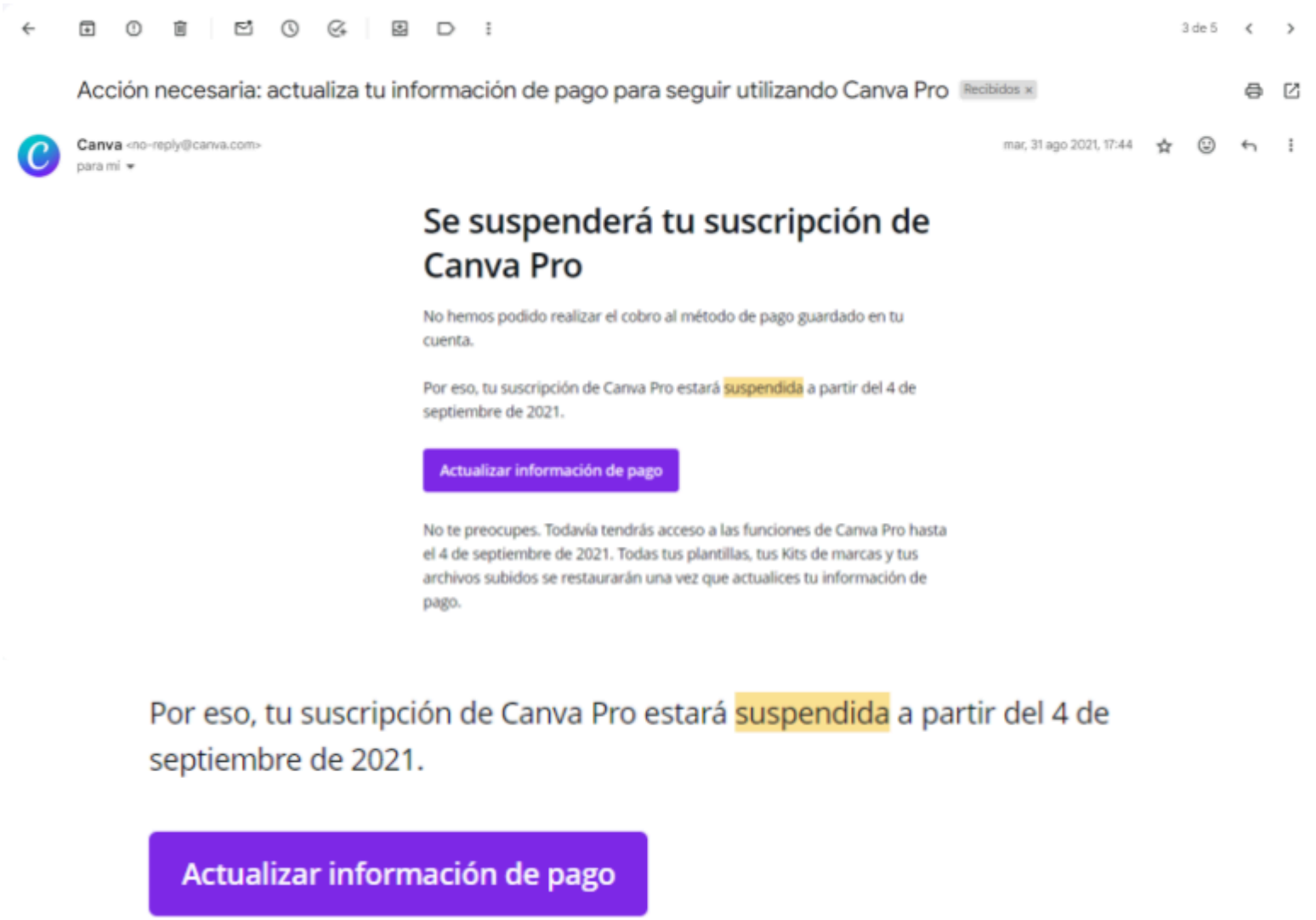
Nota: No abras archivos adjuntos de remitentes desconocidos o si no esperabas recibir un archivo.

6. Observa el sentido de urgencia:

- Los correos con malware suelen intentar crear una sensación de urgencia para que actúes rápidamente. Frases como "¡Actúa ahora!" o "Tu cuenta será suspendida" son comunes en estos correos.

Figura 6.117

Correo de urgencia



7. Comprueba la personalización:

- Los correos legítimos de empresas con las que tienes una relación suelen incluir información personal o detalles sobre tu cuenta.

Figura 6.118

Correo con datos reales

- Los correos con malware a menudo carecen de personalización y utilizan información genérica.

Figura 6.119
Correo con información genérica

8. Verifica con la empresa:

- Si tienes dudas sobre la legitimidad de un correo, contacta directamente con la empresa a través de su sitio web oficial o su número de atención al cliente.

Tipos Comunes de Malware:

- Virus:
  - Programas maliciosos que se adjuntan a otros programas y se propagan cuando se ejecutan. Pueden dañar archivos y sistemas.
- Troyanos:
  - Parecen software legítimo pero contienen código malicioso. Una vez instalados, pueden permitir el acceso remoto no autorizado.
- Ransomware:
  - Cifra los archivos del usuario y exige un rescate para liberar los datos. Es altamente destructivo y difícil de eliminar.
- Spyware:
  - Recopila información sobre el usuario sin su conocimiento. Puede capturar datos sensibles como contraseñas y detalles financieros.

- Adware:
    - Muestra anuncios no deseados en el dispositivo. Puede ralentizar el sistema y ser molesto, pero generalmente no es tan peligroso como otros tipos de malware.

Consideraciones Adicionales:

- Actualización de Software: Mantén tu software de seguridad y navegadores web actualizados para protegerte contra las últimas amenazas de malware. Consulta el punto 7, "*Cómo actualizar mi sistema operativo*", de este manual para obtener instrucciones detalladas.
- Doble Verificación: Utiliza la autenticación de dos factores (2FA) en tus cuentas importantes para añadir una capa extra de seguridad.
- Reportar: Reporta cualquier correo sospechoso a tu proveedor de correo electrónico y a la entidad supuestamente involucrada.
- Cuidado con el Phishing: Muchos correos con malware también intentan phishing. Mantente alerta y sigue las mejores prácticas para identificar ambos tipos de amenazas.

Nota: Identificar correos con malware puede prevenir que tu información personal y financiera caiga en manos equivocadas, protegiéndote a ti y a tu entorno de posibles fraudes y daños cibernéticos.

6.11

6.11 Verificar qué dispositivos están conectados a un módem Telmex

Verificar qué dispositivos están conectados a un módem Telmex

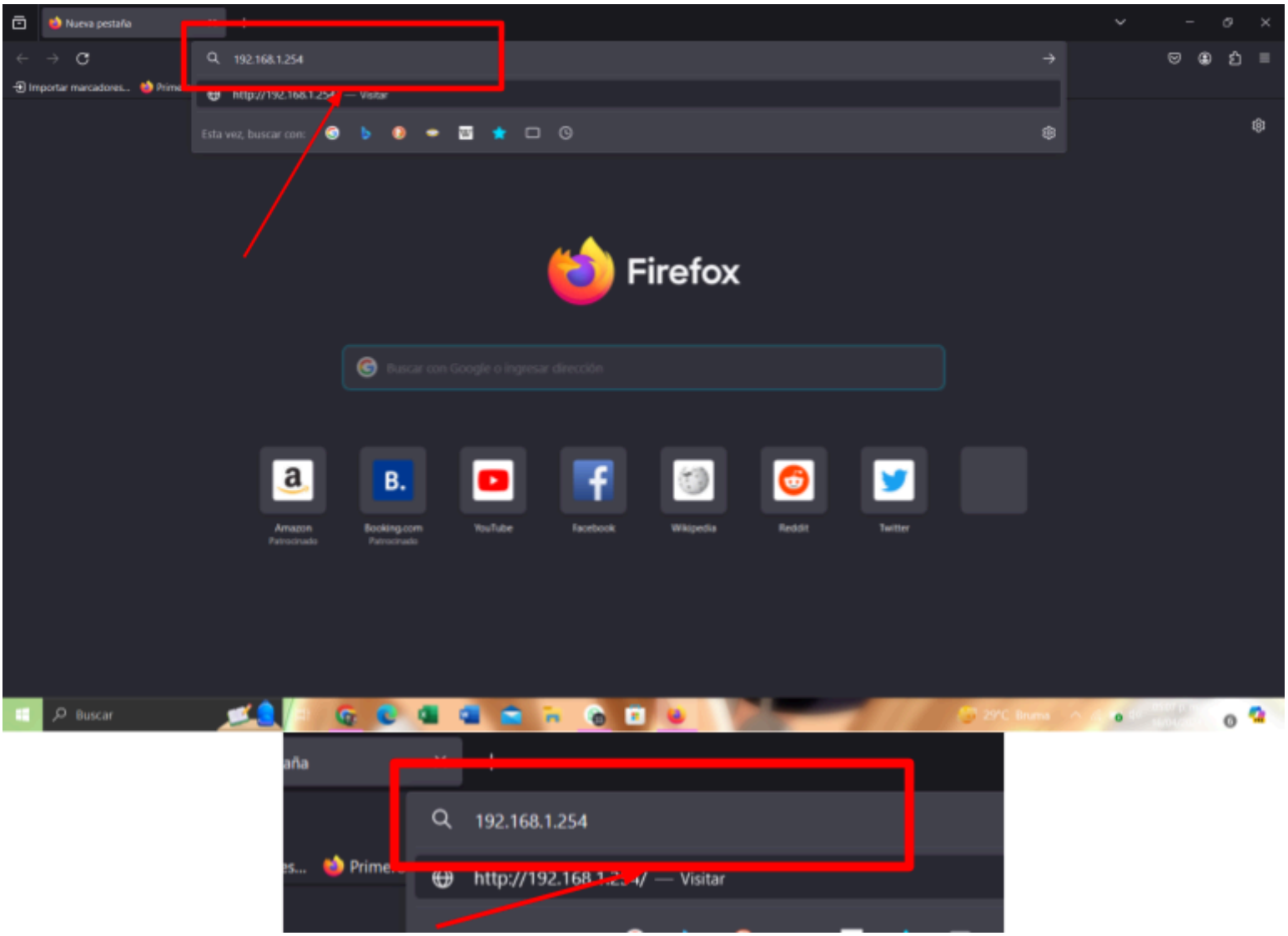
Saber qué dispositivos están conectados a tu módem es crucial para mantener la seguridad de tu red. Esto te permite identificar dispositivos no autorizados y asegurar que sólo los dispositivos confiables tengan acceso. A continuación, se presentan los pasos detallados para verificar qué dispositivos están conectados a un módem Telmex:

1. Acceder a la Interfaz de Configuración del Módem.

- Conecta tu computadora al módem Telmex mediante un cable Ethernet o a través de una conexión Wi-Fi.
- Abre un navegador web e ingresa la siguiente dirección en la barra de direcciones: http://192.168.1.254/. Presiona Enter.

Figura 6.120

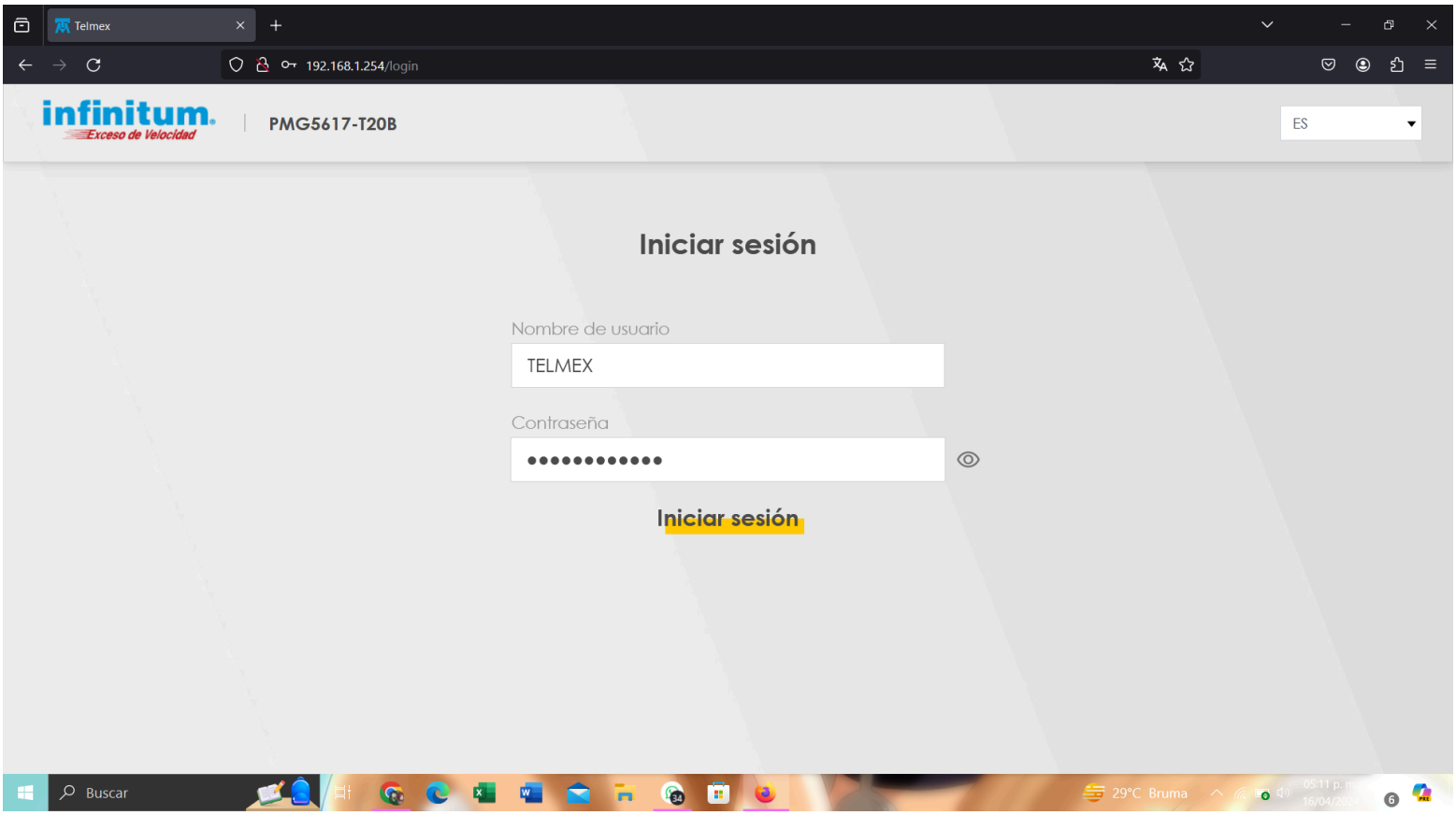
Dispositivos conectados a mi red paso 1



2. Se abrirá la página de inicio de sesión del módem. Ingresa el nombre de usuario y la contraseña y da click en “iniciar sesión”. Por lo general, el nombre de usuario es Telmex y la contraseña es Telmex o está en la etiqueta del módem.

Figura 6.121

Dispositivos conectados a mi red paso 2

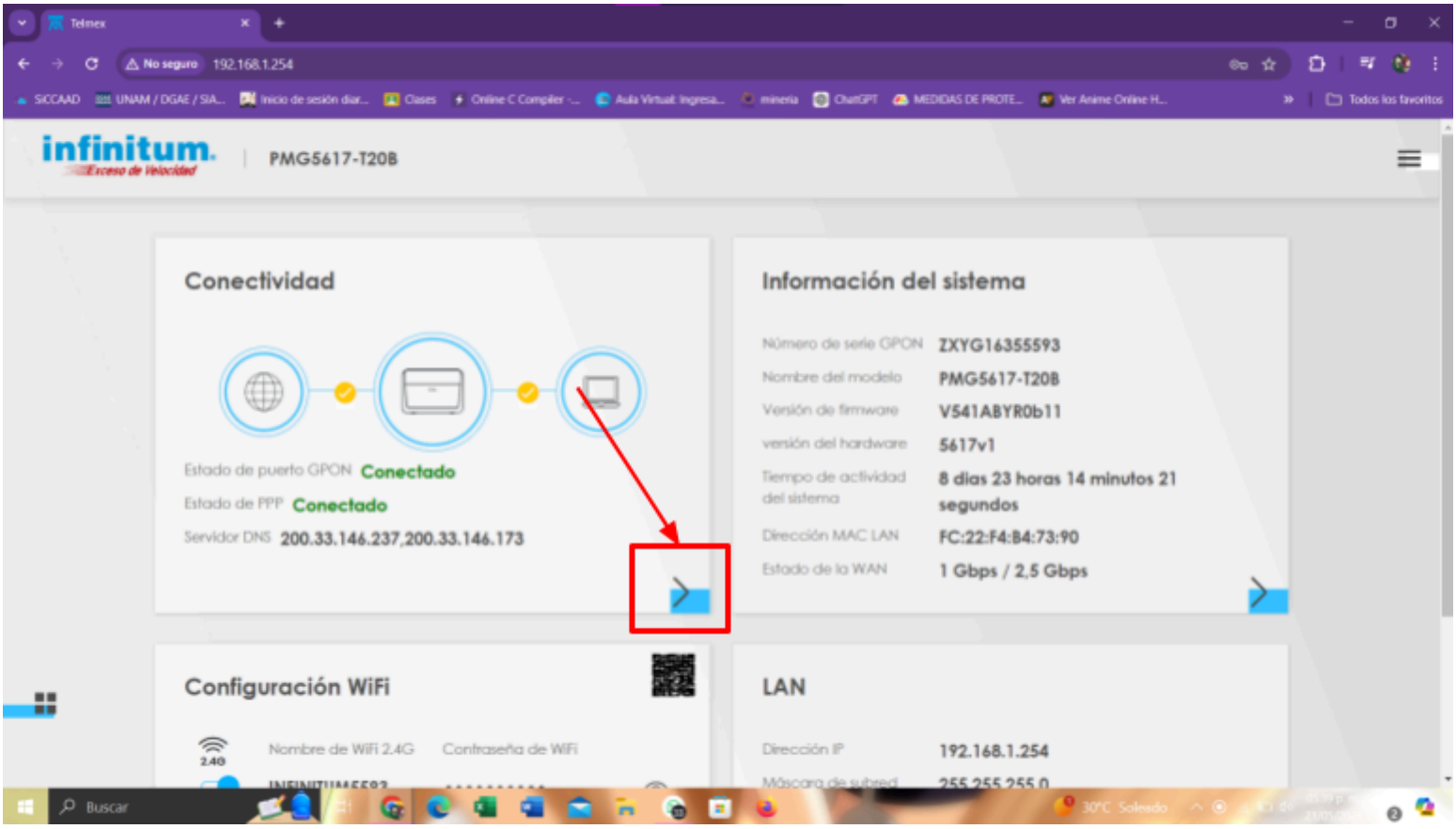


3. Navega a la sección de dispositivos conectados:

- Una vez dentro de la página de configuración, busca y haz clic en la parte superior derecha “mas”.

Figura 6.122

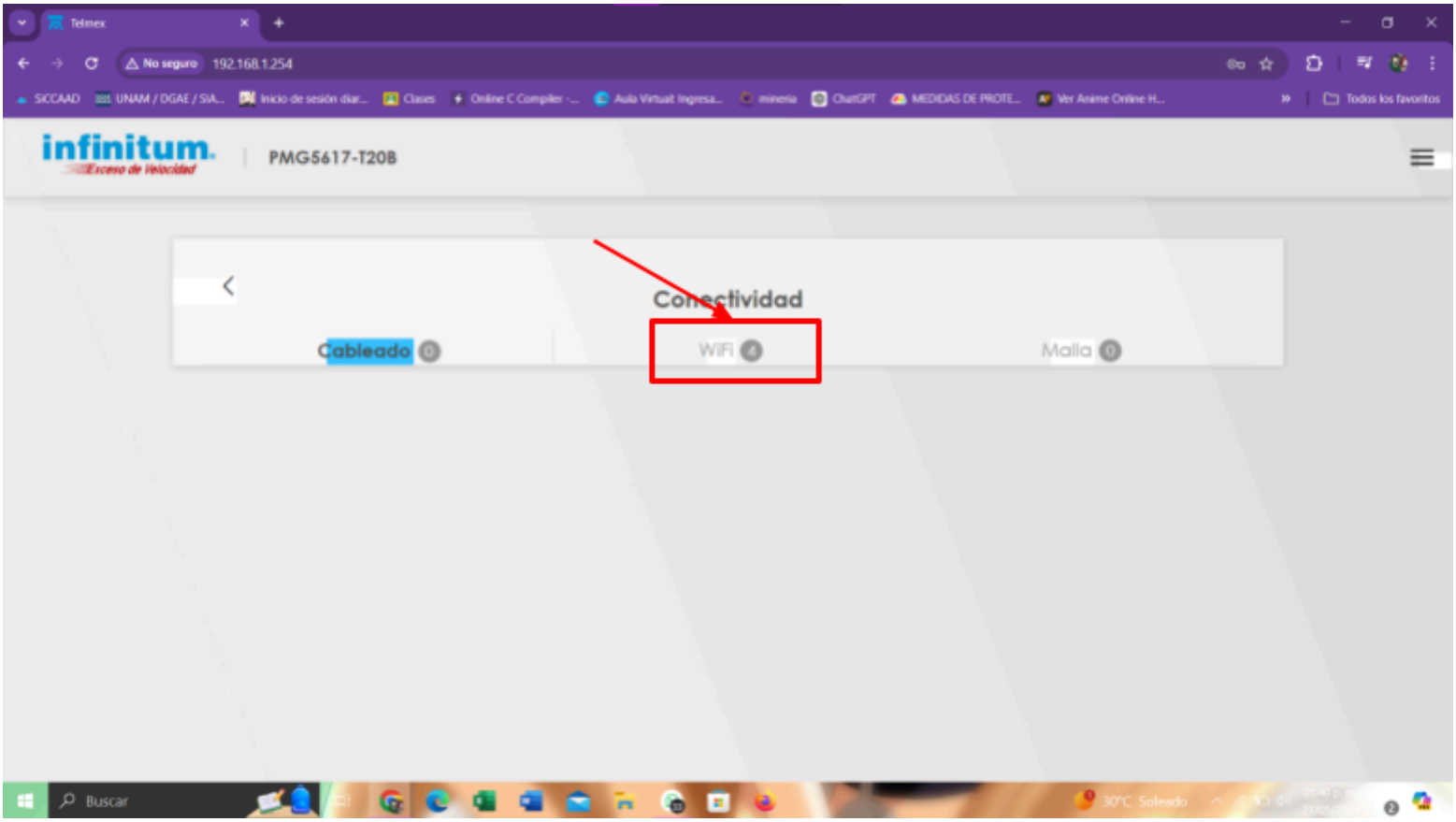
Dispositivos conectados a mi red paso 3



- Ahora da clic sobre la opción de Wi-Fi

Figura 6.123

Dispositivos conectados a mi red paso 4

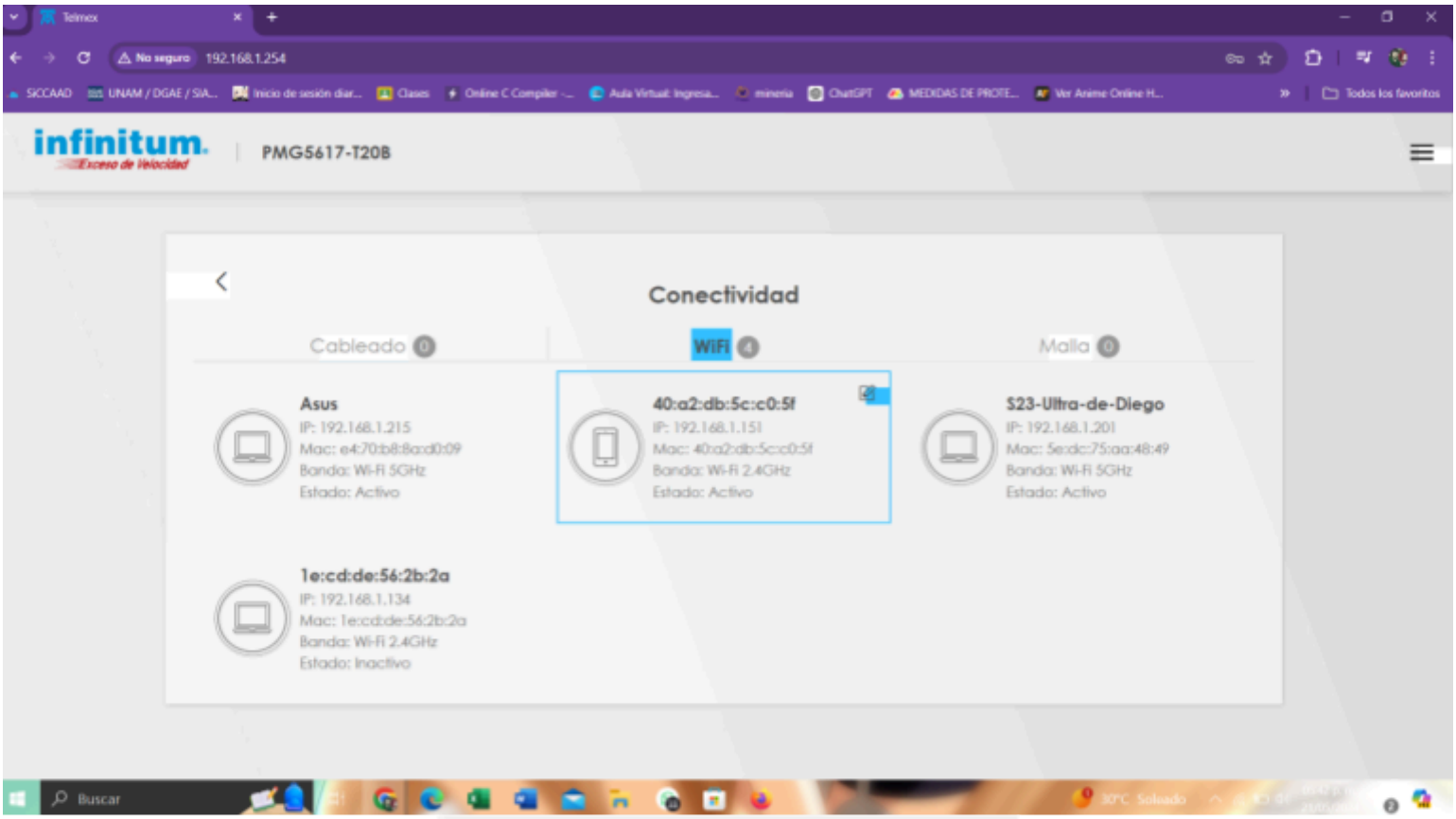


4. Revisa la lista de dispositivos conectados:

- Verás una lista de todos los dispositivos actualmente conectados a tu red.

Figura 6.124

Dispositivos conectados a mi red paso 5



- La lista generalmente incluye el nombre del dispositivo, la dirección IP y la dirección MAC.

5. Identifica dispositivos desconocidos:

- Revisa la lista para identificar todos los dispositivos conectados. Algunos de estos dispositivos tendrán el nombre “unknown” o tendrán su dirección mac , lo que significa que el dispositivo oculta su nombre, pero no necesariamente es un intruso. Para verificar si el dispositivo es nuestro, podemos hacerlo comprobando la IP del mismo. Si no sabemos cómo buscar la IP de nuestros dispositivos, podemos encontrar esta información en el punto 1, “Cómo encontrar la dirección IP de tu dispositivo”, de este mismo manual.

Figura 6.125

Dispositivos conectados a mi red paso 6

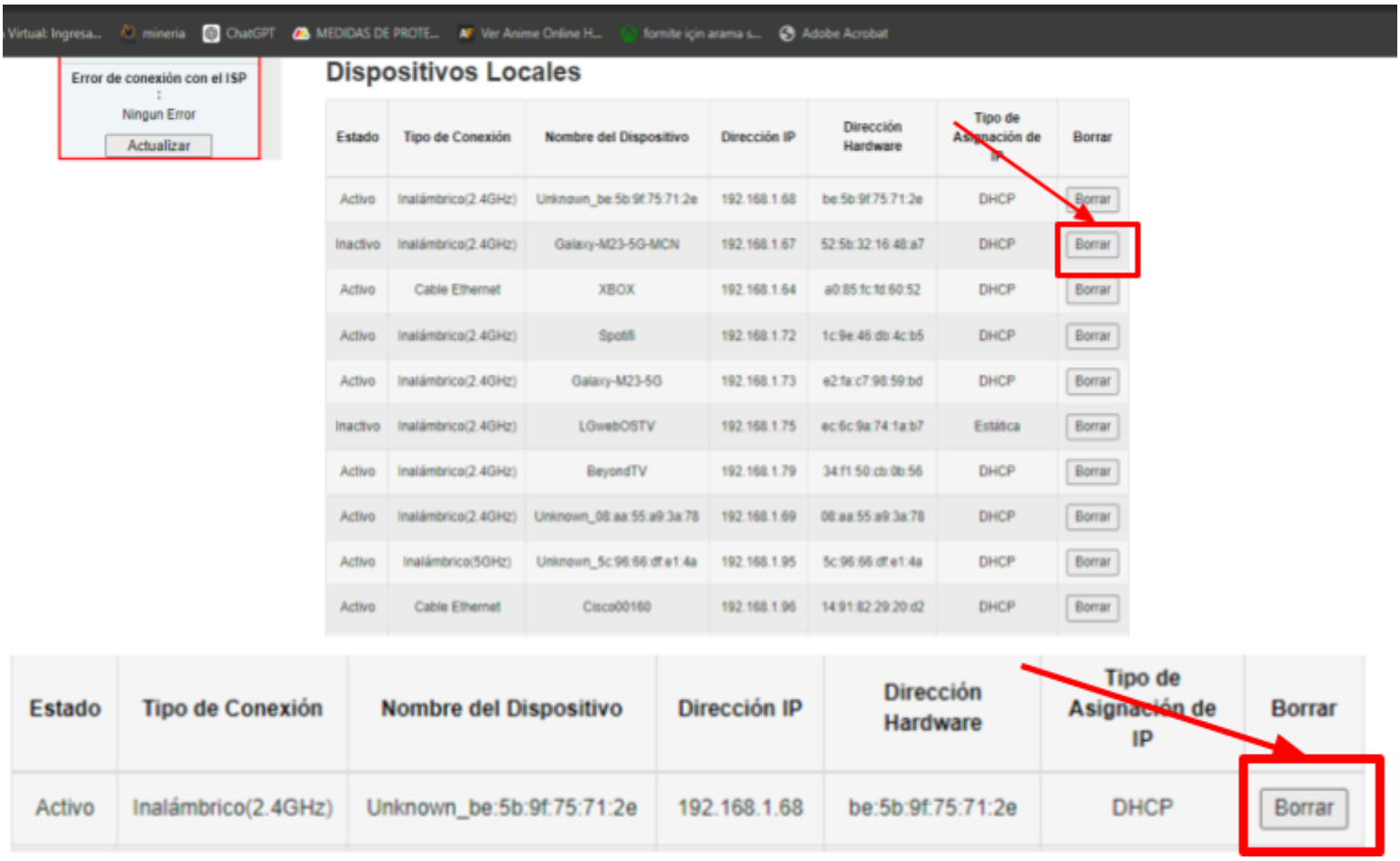
- Si encuentras dispositivos que no reconoces, podrían ser intrusos en tu red.

6. Desconectar dispositivos no autorizados (opcional):

- Algunos módems Telmex permiten desconectar o bloquear dispositivos directamente desde la página de configuración.

Figura 6.126

Dispositivos conectados a mi red paso 7



- Busca la opción para bloquear el dispositivo o eliminarlo de la red.

7. Cambiar la contraseña del Wi-Fi (opcional):

- Si encuentras dispositivos no autorizados, considera cambiar la contraseña de tu red Wi-Fi para evitar futuros accesos no deseados, los pasos para llevarlo a cabo lo encuentras en el punto 4 “Cómo cambiar la contraseña del módem Telmex” de este mismo manual.

8. Guardar los cambios:

Asegúrate de guardar cualquier cambio realizado en la configuración del módem.

Consideraciones Adicionales

- Actualizar el Sistema del Módem: Mantener el firmware de tu módem actualizado es crucial para la seguridad y el rendimiento de tu red. Los fabricantes de módems lanzan actualizaciones periódicas que corrigen vulnerabilidades, mejoran la estabilidad y añaden nuevas funciones de seguridad. Si no actualizas el sistema de tu módem, podrías estar expuesto a

amenazas conocidas que los ciberdelincuentes podrían aprovechar para atacar tu red. Revisa regularmente la página de configuración de tu módem para verificar si hay actualizaciones disponibles. Si es posible, habilita la opción de actualizaciones automáticas para asegurarte de que siempre estés protegido contra las últimas amenazas.

- Monitoreo Regular: Revisa periódicamente los dispositivos conectados para asegurar que no haya accesos no autorizados.

- Uso de Filtrado MAC: El filtrado de direcciones MAC es una medida de seguridad adicional que te permite controlar qué dispositivos pueden conectarse a tu red. Cada dispositivo tiene una dirección MAC única, y al habilitar el filtrado, puedes crear una lista blanca que solo permite la conexión de dispositivos específicos, como tu computadora, smartphone o impresora. Para configurarlo, accede a la configuración de tu router, localiza la opción de filtrado de MAC, y agrega las direcciones MAC de los dispositivos que deseas autorizar. Esto puede ayudar a reducir las conexiones no deseadas en tu red. Sin embargo, debes tener en cuenta que el filtrado de MAC no es infalible, ya que un atacante avanzado podría falsificar una dirección MAC permitida. Por lo tanto, es recomendable usar esta función junto con otras medidas de seguridad, como WPA3 y contraseñas robustas, para una protección más completa.

- Cambiar el Nombre del Router (SSID): Es recomendable cambiar el nombre predeterminado de tu red Wi-Fi (SSID), ya que a menudo este incluye el modelo del router o información que podría facilitar que los atacantes identifiquen vulnerabilidades específicas asociadas a ese equipo. Además, evita usar nombres que contengan datos personales como tu nombre, dirección o cualquier información que pueda identificarte fácilmente. Opta por un nombre único pero genérico, que no revele ninguna información sobre el hardware o los usuarios de la red. Este simple paso puede dificultar que alguien intente atacar tu red utilizando información sobre el modelo de tu router o la ubicación del dispositivo, mejorando así la seguridad de tu conexión Wi-Fi.

- Implementar un Sistema de Detección de Intrusos (IDS): Es altamente recomendable implementar un IDS en tu red, ya que este sistema monitorea constantemente el tráfico en busca de actividades sospechosas o maliciosas. Un IDS puede identificar patrones de comportamiento anómalos y alertarte sobre posibles intrusiones, lo que te permite tomar medidas inmediatas para proteger tu red. Existen dos tipos principales de IDS: basado en red (NIDS), que analiza todo el tráfico que fluye a través de tu red, y basado en host (HIDS), que se enfoca en actividades dentro de un dispositivo específico. Es crucial elegir el tipo adecuado según tus necesidades.

Nota: Mantener un control regular de los dispositivos conectados a tu red te ayudará a asegurar que solo usuarios autorizados tengan acceso, mejorando así la seguridad de tu red.

6.12

Manejo Seguro de Información Personal en Redes Sociales

Hoy en día las redes sociales se han convertido en una herramienta poderosa para conectar con los demás y compartir momentos importantes de nuestras vidas. Sin embargo, es fundamental aprender a utilizar estas plataformas de manera segura y responsable, especialmente en lo que respecta a la información que compartimos.Por ello es indispensable tomar en cuenta las siguientes recomendaciones para publicar contenido de forma consciente, protegiendo tu privacidad y evitando riesgos de seguridad al compartir detalles de tu vida en línea.

1. Sé Cauteloso con la Información Personal Sensible

- Evita publicar datos personales como tu dirección, número de teléfono, y número de identificación personal. Compartir esta información puede poner en riesgo de robo de identidad o de ser localizado por personas no deseadas.
- Considera no publicar detalles sobre tu ubicación exacta en tiempo real (como el lugar donde estás comiendo o tu dirección) para evitar comprometer tu seguridad.

2. Pública con Moderación sobre tu Trabajo y Actividades Diarias

- Si trabajas en una empresa o tienes un rol profesional público, evita compartir información confidencial sobre tu lugar de trabajo, proyectos específicos o problemas internos.
- Publicar detalles excesivos sobre tu rutina diaria puede hacerte predecible y más vulnerable a riesgos de seguridad.

3. Piensa en la Privacidad de Terceros

- Respeta la privacidad de amigos y familiares antes de compartir fotos o información sobre ellos. Pregunta si están cómodos con que publiques contenido en el que aparecen, especialmente si se trata de menores de edad.
- No etiquetes a personas en ubicaciones sensibles (como su hogar o lugar de trabajo) sin su consentimiento.

4. Reflexiona Antes de Compartir Opiniones Personales o Temas Controversiales

- Publicar sobre temas sensibles o controvertidos, como política o religión, puede generar conflictos. Piensa si estás preparado para lidiar con posibles debates o reacciones negativas antes de compartir tus opiniones en redes sociales.
- Mantén un tono respetuoso y evita comentarios que puedan malinterpretarse o parecer ofensivos.

5. Comparte Contenido Positivo y Útil

- Compartir logros, momentos felices o consejos que puedan ayudar a otros es una excelente manera de generar interacciones positivas. Elige contenido que refleje lo que deseas proyectar sobre ti y que contribuya de forma constructiva a la red.

- Evita compartir quejas constantes o contenido negativo, ya que esto puede afectar cómo te perciben los demás.

6. Evita Publicar Información Sobre tus Finanzas

- Nunca compartas detalles financieros, como el saldo de tus cuentas, tarjetas de crédito o planes de inversión. Esto puede poner en riesgo tu seguridad financiera.
- Desconfía de publicar fotos de bienes valiosos, como joyas o dispositivos costosos, ya que esto podría atraer la atención de personas con malas intenciones.

7. Revisa y Reflexiona Antes de Publicar

- Antes de publicar, pregúntate si la información podría ser utilizada en tu contra o si podrías arrepentirte en el futuro. Las redes sociales guardan un registro, y algo que compartas hoy podría tener consecuencias más adelante.
- Utiliza la opción de "revisión de publicaciones" que muchas redes ofrecen para revisar etiquetas y publicaciones en las que apareces antes de que se hagan públicas en tu perfil.

Consideraciones Adicionales:

- Privacidad de tus Publicaciones: Ajusta la configuración de privacidad para que solo las personas en quienes confías puedan ver tus publicaciones más personales.
- Evita Publicar en Vivo (en Tiempo Real): Considera publicar fotos y detalles de eventos una vez que hayan terminado para reducir riesgos de seguridad.
- Mantén la coherencia: Recuerda que la imagen que proyectas en redes sociales puede influir en tus oportunidades profesionales y personales. Sé coherente con los valores y principios que quieres mostrar.

6.13

6.13 Manejo Seguro de Información Personal en Línea

Manejo Seguro de Información Personal en Línea

El manejo seguro de la información personal en línea es crucial en la era digital hoy en día. Con el incremento de amenazas cibernéticas y la creciente cantidad de datos personales que compartimos en internet, es vital adoptar prácticas seguras para proteger nuestra privacidad y evitar el robo de identidad. Para ello a continuación puedes ver algunos pasos a seguir para tener tu información correctamente protegida:

1. Usa contraseñas seguras y únicas para cada cuenta:
- Evita utilizar la misma contraseña para múltiples cuentas.
- Crea contraseñas largas y complejas que incluyan una combinación de letras mayúsculas, minúsculas, números y símbolos.
- Utiliza un gestor de contraseñas para generar y almacenar contraseñas seguras.
- Evita que tus contraseñas contengan información personal.

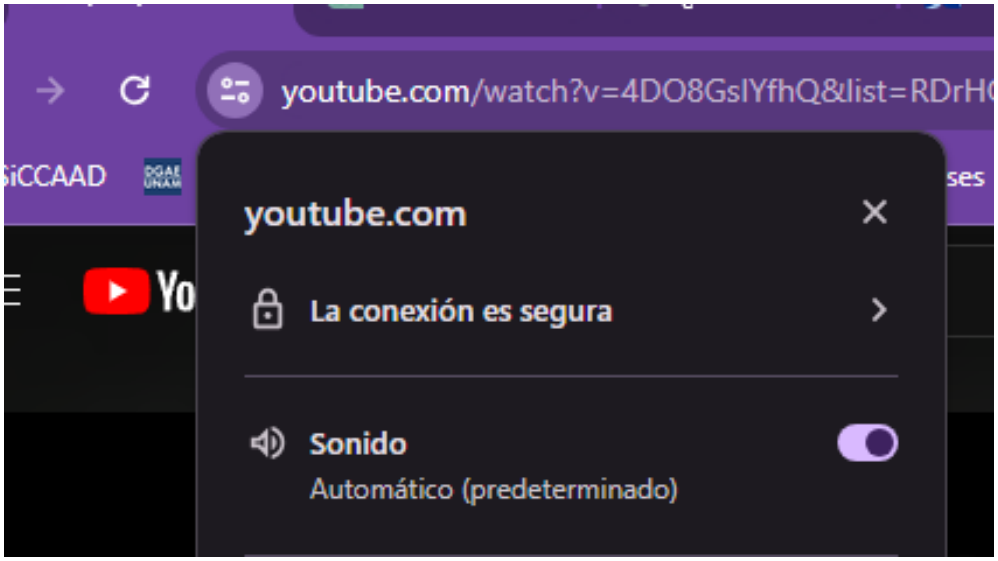
(Consulta el punto 2 del manual: Creación de contraseñas seguras)

2. Habilita la autenticación de dos factores (2FA):
- Activa 2FA en todas las cuentas que lo permitan. Esto añade una capa extra de seguridad al requerir un segundo paso de verificación además de la contraseña.
- Puedes usar aplicaciones de autenticación como Google Authenticator o Authy.
3. Configura la privacidad en redes sociales:
- Revisa y ajusta las configuraciones de privacidad en tus cuentas de redes sociales.
- Limita quién puede ver tus publicaciones, fotos y la información de tu perfil.
- Evita compartir información personal sensible como tu dirección, número de teléfono o detalles financieros.
4. Sé consciente de los correos electrónicos y mensajes sospechosos:
- No compartas información personal a través de correos electrónicos o mensajes de texto no solicitados.
- Si recibes un mensaje de una entidad conocida pidiendo información personal, verifica su legitimidad contactando directamente a la entidad a través de sus canales oficiales.

(Consulta el punto 10 del manual: Identificar Correos Electrónicos con malware)

5. Utiliza conexiones seguras:
- Asegúrate de que la URL del sitio web comience con "https://" antes de ingresar información personal o financiera. La "s" indica que la conexión es segura.

Figura 6.127
Conexión segura



- Evita realizar transacciones financieras o ingresar datos personales en redes Wi-Fi públicas o no seguras.

6. Revisa regularmente tus configuraciones de privacidad:

- Realiza revisiones periódicas de las configuraciones de privacidad en todas tus cuentas en línea.
- Asegúrate de estar al tanto de cualquier cambio en las políticas de privacidad de los servicios que utilizas.

7. Monitorea tu información personal:

- Usa servicios de monitoreo de crédito y alertas de identidad para estar informado sobre cualquier actividad sospechosa relacionada con tu información personal.
- Revisa regularmente tus estados de cuenta bancarios y de tarjetas de crédito para detectar transacciones no autorizadas.

(Consulta el punto 11 del manual: Verificar qué dispositivos están conectados a un módem Telmex)

8. Desactiva las cuentas no utilizadas:

- Elimina o desactiva las cuentas en línea que ya no utilizas para reducir el riesgo de que sean comprometidas.
- Asegúrate de eliminar cualquier información personal almacenada en estas cuentas antes de desactivarlas.
- Para eliminar tu cuenta, puedes solicitarlo en el área de atención al cliente del servicio correspondiente.

9. Desactiva Wi-Fi y Bluetooth cuando no los utilices:

- Mantener estas conexiones activadas sin usar aumenta el riesgo de accesos no autorizados o intentos de intrusión por parte de terceros.
- Desactivar estas funciones reduce la posibilidad de que tus dispositivos se conecten automáticamente a redes o dispositivos no seguros.
- Apagar Wi-Fi y Bluetooth evita que otros dispositivos cercanos detecten tu equipo, lo que disminuye el riesgo de que intenten acceder a tu red o enviar archivos maliciosos.
- Cuando los utilices, asegúrate de que las conexiones sean solo con redes y dispositivos conocidos para mantener tu seguridad.

Consideraciones Adicionales:

- Educación Continua: busca informarte continuamente sobre las mejores prácticas de seguridad en línea y las últimas amenazas cibernéticas.
- Actualización de Software: Mantén tus dispositivos y aplicaciones actualizados con las últimas versiones y parches de seguridad.
- Utilización de Herramientas de Seguridad: Instala y utiliza software antivirus y antimalware para proteger tus dispositivos contra amenazas.

Nota: Adoptar estos hábitos de seguridad te ayudará a proteger tu información personal en línea y a mantener tu privacidad en la era digital.

6.14

Recomendaciones

A continuación, te presentamos una serie de recomendaciones clave para proteger tu red y dispositivos. Siguiendo estas sugerencias, podrás minimizar riesgos de seguridad, mejorar el rendimiento de tus equipos y garantizar la protección de tus datos. Implementarlas es fundamental para mantener una red segura y eficiente:

- Cambia las contraseñas predeterminadas de tu router y otros dispositivos conectados.
- Usa cifrado WPA3 o WPA2 en la red Wi-Fi para asegurar las conexiones.
- Actualiza el firmware del router y los sistemas operativos de los dispositivos regularmente.
- Habilita un firewall en el router y en cada dispositivo conectado a la red.
- Desactiva el acceso remoto al router si no lo necesitas.
- Crea una red de invitados separada para que tus dispositivos principales estén más seguros.
- Configura una VPN para cifrar la conexión cuando accedas a redes públicas.
- Desconecta dispositivos que no utilices regularmente para minimizar el riesgo.
- Monitorea los dispositivos conectados a tu red con frecuencia para detectar actividades sospechosas.
- Realiza copias de seguridad de tus datos de forma regular y guárdalas en lugares seguros.
- Usa autenticación de dos factores (2FA) en cuentas sensibles, como las de correo electrónico y banca.
- Instala software antivirus y mantenlo actualizado para detectar y bloquear malware en todos los dispositivos de TI incluyendo teléfonos celulares,iPads,etc.
- Configura una política de contraseñas fuertes en todos los dispositivos y servicios.
- Cambia las contraseñas de tu red regularmente para prevenir accesos no autorizados la sugerencia es hacerlo cada 6 meses procura que no pasen más de 2 años.
- Desactiva el WPS (Wi-Fi Protected Setup), ya que puede ser un punto débil en la seguridad del router.
- Desactiva la opción de administración remota del router para evitar accesos externos no deseados.
- Habilita el filtrado por direcciones MAC para limitar qué dispositivos pueden conectarse a tu red.
- Desactiva el servicio UPnP (Universal Plug and Play) si no lo usas, ya que puede abrir vulnerabilidades.
- Crea nombres de red (SSID) que no revelen información personal o el modelo

del router.

- Revisa constantemente los dispositivos conectados en tu router para detectar accesos o intentos de acceso no autorizados.
- Usa un router con actualizaciones automáticas para que siempre esté protegido con los últimos parches de seguridad.
- Desactiva el Bluetooth y Wi-Fi en dispositivos móviles cuando no los estés usando.
- No uses redes Wi-Fi públicas sin protección, a menos que sea estrictamente necesario y estés usando una VPN.
- Instala un sistema de detección de intrusos (IDS) para monitorear tu red en busca de amenazas.
- Evita acceder a sitios web no seguros (aquellos sin el protocolo HTTPS) desde cualquier dispositivo conectado.
- Cifra tus discos duros para proteger los datos en caso de que se pierdan o te roben el equipo.
- Revisa los permisos de las aplicaciones instaladas en tu equipo y dispositivos móviles para evitar accesos indebidos a tus datos.
- Usa dispositivos de seguridad avanzados como un router con firewall integrado o un dispositivo especializado en seguridad de redes.
- Limpia con regularidad los dispositivos de archivos basura para optimizar su rendimiento.
- Desinstala o desactiva aplicaciones que no se utilicen.
- Conecta los dispositivos sensibles a cambios de corriente a No-breaks con regulador para prevenir daños por descargas eléctricas.
- Mantén los dispositivos ventilados para evitar que se dañen por sobrecalentamiento.
- Limpia internamente los dispositivos para evitar el sobrecaliento y cortocircuitos.
- Trata con cuidado los dispositivos al trasladarlos para evitar torsiones que puedan dañar sus componentes.
- Realiza conexiones alámbricas con un margen de holgura considerable para no forzar el cableado.
- Protege el cableado con canaletas para evitar impactos y cortaduras.
- Evita colocar dispositivos de red cerca de motores eléctricos y fuentes electromagnéticas.
- Identifica los cables de telefonía y cableado para evitar confundirlos. Haz clic aquí para más detalles, o consulta la página [].
- Evita compartir contraseñas.
- Identifica y elimina los correos spam como por ejemplo publicidad, ofertas y tratos de fuentes poco confiables.

- Minimiza el tiempo de sesión en páginas y aplicaciones bancarias.
- Cierra las sesiones iniciadas en aplicaciones y dispositivos que no se utilicen.

7. Resultado, impacto y conclusiones

El Manual de protección digital propone varias configuraciones en equipos de cómputo para que los usuarios puedan mejorar la seguridad de las redes de datos que utilizan con diversos propósitos, y con ello disminuir los riesgos asociados al uso de sus datos personales y confidenciales, siendo un material de referencia importante para todo el que utiliza un equipo de cómputo sin importar su conocimiento previo y su impacto se describe en esta sección.

7.1. Resultado

El proyecto de creación del manual de Medidas de protección digital busca atender la necesidad de difundir la información pertinente a los sistemas computacionales y los equipos de cómputo, a fin de que los usuarios con poco conocimiento sobre el funcionamiento de los equipos eviten confundir conceptos básicos en temas como el internet, las aplicaciones, la conexión web, las conexiones de redes, el WiFi, entre otros.

Además, se espera que el manual ayude a que los casos de configuración errónea de estas medidas no afecten a las redes domésticas y a los equipos de cómputo, a fin de evitar requerir una intervención fuera del alcance del manual realizado, por lo que se espera una inclusión en los materiales de enseñanza dentro de las áreas de Tecnologías de la Información y Comunicación.

7.2. Impacto

El impacto del manual de Medidas de Protección Digital en Redes de Datos busca lograr una mejora en los conocimientos sobre seguridad de redes para cumplir su propósito educativo, dando herramientas de aprendizaje a los usuarios sobre las medidas de protección digital, y con ello aumentar su capacidad para gestionar la seguridad de sus redes domésticas.

Se desea que el manual contribuya a aumentar la conciencia sobre la importancia de la seguridad en redes de datos en un entorno donde las amenazas cibernéticas son cada vez más prevalentes, y donde tener conocimientos sólidos sobre cómo proteger las redes personales es crucial para la protección de datos, siendo esto un cambio de mentalidad fundamental para la creación de un entorno digital más seguro.

Además, se espera que el manual fomente la adopción de buenas prácticas en la seguridad digital al proporcionar instrucciones claras y prácticas en temas como la creación de contraseñas seguras, el almacenamiento seguro de contraseñas y la actualización de sistemas operativos como medidas para protegerse contra una amplia gama de amenazas, para reducir la vulnerabilidad de los usuarios a ataques cibernéticos.

Se considera que la difusión de este manual en los ambientes de aprendizaje como lo son el Laboratorio de Redes de Datos y Seguridad beneficiará a las generaciones de estudiantes que cursen carreras afines a las Tecnologías de la Información y Comunicaciones, teniendo un impacto en la sociedad una vez que el material proporcionado sea aplicado fuera de las aulas.

De manera personal, ha brindado un mayor entendimiento a efecto y situaciones que ocurren en los ambientes físicos y que son poco explorados en la enseñanza de las redes de datos, así como una gran experiencia en el uso de estas y de los equipos de computo en que se aplican las medidas de seguridad del manual.

7.3. Conclusiones

El proyecto de desarrollo del manual de Medidas de Protección Digital en Redes de Datos ha cumplido con éxito sus objetivos centrales y secundarios; a través de una estructura clara y bien organizada, el manual busca educar a los usuarios sobre la importancia de la seguridad en redes de datos y cómo implementar medidas prácticas para protegerse contra diversas amenazas.

- Cumplimiento de Objetivos:

El objetivo central del proyecto, que era desarrollar un manual que mejore el rendimiento y la seguridad en redes domésticas, se ha alcanzado plenamente y se espera que tras su difusión, haya mejoría en los conocimientos sobre seguridad entre los usuarios. De igual manera se han cumplido los objetivos secundarios, abarcando temas como los componentes de las redes domésticas, las vulnerabilidades del internet, los hábitos de los usuarios en la red, y la solución de fallas comunes en redes domésticas.

- Utilidad y Aplicabilidad:

Las secciones prácticas del manual, como la creación de contraseñas seguras, el almacenamiento seguro de contraseñas, y la actualización de sistemas operativos, son especialmente valiosas para los usuarios, y por ellos se han proporcionado herramientas concretas y fácilmente implementables para aumentar la seguridad de las redes domésticas de los usuarios. La claridad y accesibilidad del manual garantiza que incluso los usuarios con poca experiencia en tecnología puedan beneficiarse de la información proporcionada.

- Contribución a la Comunidad Digital:

En resumen, el manual de Medidas de Protección Digital en Redes de Datos proporciona un análisis exhaustivo y técnico de las redes de datos y su seguridad, y ofrece recursos prácticos accesibles y relevantes para los usuarios finales con el objetivo de aumentar la conciencia sobre importancia de la seguridad digital y proporciona herramientas educativas para ello, contribuyendo significativamente a la creación de un entorno digital más seguro y confiable cuya digitalización avanza constantemente.

Glosario de Términos

A

- **Accesibilidad**: Capacidad de acceder y utilizar los recursos y servicios de una red de manera fácil y efectiva.
- **Ancho de banda**: Cantidad de datos que se pueden transmitir en un período determinado.

B

- **Banda ancha**: Tipo de conexión de red de alta velocidad que permite la transmisión simultánea de varios tipos de datos.
- **Broadcast**: Transmisión de datos desde un solo remitente a todos los dispositivos en una red.
- **Bus** (Topología en bus): Topología de red donde todos los dispositivos están conectados a una línea de comunicación central.

C

- **Cobertura**: Extensión territorial que abarca la disponibilidad de servicios, especialmente en el caso de las telecomunicaciones.
- **Conexión**: Enlace establecido entre dispositivos para permitir la comunicación y el intercambio de datos.
- **Conexión de Red**: Enlace establecido entre un dispositivo y una red para permitir la comunicación del dispositivo en la red.

D

- **DHCP (Dynamic Host Configuration Protocol)**: Protocolo que asigna dinámicamente direcciones IP a dispositivos en una red.
- **Dispositivos**: Equipos electrónicos utilizados para conectarse y comunicarse en una red.
- **Dispositivos de red**: Equipos específicamente diseñados para facilitar la comunicación y el intercambio de datos en una red, como routers y switches.
- **DNS (Domain Name System)**: Sistema que traduce nombres de dominio legibles por humanos en direcciones IP numéricas.

E

- **Ethernet**: Tecnología utilizada para la transmisión de datos en redes locales mediante cable.

F

- **Firewall**: Dispositivo o software de seguridad que supervisa y controla el tráfico de red entrante y saliente, basado en reglas predeterminadas.
- **FTP (File Transfer Protocol)**: Protocolo usado para la transferencia de archivos entre dispositivos en una red.

G

- **Gateway**: Dispositivo que actúa como un "puente" entre diferentes redes.

H

- **HTTP (Hypertext Transfer Protocol)**: Protocolo utilizado para la transferencia de datos a través de la web.
- **HTTPS (Hypertext Transfer Protocol Secure)**: Versión segura del protocolo HTTP, con cifrado de datos.

I

- **ICMP (Internet Control Message Protocol)**: Protocolo utilizado para enviar mensajes de error y control en redes IP.
- **IPv4**: Sistema de direcciones que permite identificar dispositivos en una red.
- **IPv6**: Versión más reciente del protocolo de Internet, que permite un número más grande de direcciones IP.
- **IPsec (Internet Protocol Security)**: Conjunto de protocolos para asegurar las comunicaciones en una red IP.

L

- **LAN (Local Area Network)**: Red de área local que conecta dispositivos en un área geográfica limitada, como una oficina o hogar.
- **Latencia**: Tiempo que tarda un dato en viajar desde su origen hasta su destino en una red.

M

- **MAC Address (Media Access Control Address)**: Dirección única asignada a un dispositivo de red.

- **Medios de transmisión**: Tecnologías como cables o señales inalámbricas que permiten la transmisión de datos.
- **Multicast**: Método de transmisión de datos a varios receptores en una red.

N

- **NAT (Network Address Translation)**: Método que permite a varios dispositivos en una red privada compartir una sola dirección IP pública.
- **Normatividad**: Conjunto de normas y reglamentos que regulan el uso y la operación de las redes y los servicios de comunicación.

P

- **Ping**: Comando usado para probar la conexión de red entre dos dispositivos.
- **Protocolo**: Conjunto de reglas que gobiernan la comunicación entre dispositivos en una red.
- **Proxy**: Servidor que actúa como intermediario para las solicitudes de los clientes que buscan recursos de otros servidores.

Q

- **QoS (Quality of Service)**: Tecnología que gestiona el tráfico de red para asegurar el rendimiento de aplicaciones específicas.

R

- **Red de Datos**: Infraestructuras diseñadas para transmitir información a través del intercambio de datos entre dispositivos.
- **Repetidor/Access Point**: Dispositivo que amplifica o extiende la señal de la red, especialmente en redes inalámbricas.
- **Ring** (Topología en anillo): Topología de red en la que cada dispositivo está conectado a otros dos dispositivos, formando un anillo.
- **Router**: Dispositivo que dirige el tráfico de internet, seleccionando las rutas más eficientes para la transmisión de datos.

S

- **Seguridad**: Medidas y procedimientos utilizados para proteger los datos y la información en una red.

- **Seguridad de la información**: Protección de la información contra accesos no autorizados, uso indebido, divulgación, interrupción o destrucción.
- **Seguridad informática**: Protección de los sistemas de computadoras y datos contra el acceso, uso, divulgación, interrupción o destrucción no autorizados.
- **SMTP (Simple Mail Transfer Protocol)**: Protocolo utilizado para el envío de correos electrónicos.
- **SFTP (SSH File Transfer Protocol)**: Versión segura de FTP que utiliza Secure Shell (SSH) para transferir archivos.
- **SSID (Service Set Identifier)**: Nombre que identifica de manera única una red inalámbrica.
- **Star** (Topología en estrella): Topología de red donde todos los dispositivos están conectados a un punto central.
- **Switch**: Dispositivo que conecta varios equipos dentro de una red para gestionar y distribuir el tráfico de datos.
- **Switching**: Proceso de conmutación que permite la transferencia de datos dentro de una red.

T

- **TCP/IP (Transmission Control Protocol/Internet Protocol)**: Conjunto de protocolos que permiten la conexión de dispositivos en redes.
- **Telecomunicaciones**: Transmisión de señales de audio, video y datos a largas distancias utilizando tecnologías como cables, radio, microondas y satélites.
- **Topología de red**: Forma en que se organizan y conectan los elementos de una red.

U

- **Unicast**: Transmisión de datos de un solo remitente a un solo receptor en una red.
- **Usuario**: Persona u entidad que utiliza una red para acceder a recursos y servicios.

V

- **VLAN**: Red de área local virtual que permite segmentar lógicamente una red física.

- **VoIP (Voice over IP)**: Tecnología que permite la transmisión de voz a través de redes IP.
- **VPN**: Red privada virtual que crea una conexión segura a través de una red pública.

W

- **WAN (Wide Area Network)**: Red de área amplia que cubre grandes distancias, conectando múltiples redes locales.
- **WiFi**: Tecnología que permite la conexión inalámbrica a internet.

Bibliografía

Coronado, G. (2019). Seguridad Informática: Guía Práctica para el Usuario. Alfaomega.

Forouzan, B. A. (2013). Comunicación de Datos y Redes de Computadoras (4ª ed.). McGraw-Hill.

Huerta, J. (2016). Administración de Redes y Seguridad. Marcombo.

Jiménez, F. (2012). Guía Práctica de Redes y Seguridad. Paraninfo.

Liberatori, M. C. (2018). Redes de Datos y sus Protocolos. EUDEM. http://www2.mdp.edu.ar/images/eudem/pdf/redes%20de%20datos.pdf

Liberatori, M. C. (2018). Redes de Datos y sus Protocolos. EUDEM. http://www2.mdp.edu.ar/images/eudem/pdf/redes%20de%20datos.pdf

Moreno, E. (2015). Protocolos y Servicios en Redes de Datos. RA-MA.

Rodríguez, R. (2014). Fundamentos de Seguridad en Redes. Alfaomega.

Rueda, M. (2017). Redes y Seguridad de Computadoras. Ediciones UPC.

Stallings, W. (2017). Seguridad de Redes: Principios y Prácticas (6ª ed.). Pearson Educación.

Tanenbaum, A. S., & Wetherall, D. J. (2014). Redes de Computadoras (5ª ed.). Pearson Educación.

Mesografía

- “Configuración dinámica de las opciones del servidor DHCP”. Cisco. Accedido el 4 de octubre de 2023. https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

- “Introducción a Plug and Play - Windows drivers”. Microsoft Learn: Build skills that open doors in your career. Accedido el 4 de octubre de 2023. Disponible: https://learn.microsoft.com/es-es/windows-hardware/drivers/kernel/introduction-to-plug-and-play

- Alonso, C. (2015, agosto 3). ISO 27000 y el conjunto de estándares de Seguridad de la Información. GlobalSuite Solutions. Recuperado el 20 de marzo de 2024, de https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

- Andino, C., & Aguilar, F. (s/f). Detector de Caídas en IoT. Edu.ar. Recuperado el 22 de Enero de 2024, de https://uai.edu.ar/ciiti/2023/buenos-aires/certamen-de-trabajos-estudiantiles-del-CIITI/trabajos/Andino%20Proyecto%20IoT.pdf

- AQUACOMMS. (s/f). Submarine cable map. Submarinecablemap.com. Recuperado el 12 de febrero de 2024, de https://www.submarinecablemap.com/

- Bottini, C. (2022, primavera 7). PERFILES DE RED EN WINDOWS. RedUSERS. Recuperado el 6 de febrero de 2024, de https://www.redusers.com/noticias/publicaciones/perfiles-de-red-en-windows/

- Centro mexico digital. (2022, agosto 8). Reporte brecha de genero. Centromexico.digital. Accedido el 13 de octubre de 2023. https://centromexico.digital/wp-content/uploads/2022/11/reporte-brecha-de-genero.pdf

- Centurylink. (s/f). ¿Qué Velocidad de Internet Necesito? Centurylink.com. Recuperado el 2 de marzo de 2024, de https://www.centurylink.com/home/help/internet/what-internet-speed-do-i-need.html

- CompuSoluciones. (2020, abril 29). Soluciones de Ciberseguridad. CompuSoluciones. Recuperado el 4 de marzo de 2024, de https://www.compusoluciones.com/soluciones/ciberseguridad/

- Dansimp. (s/f). Cómo Microsoft identifica el malware y las aplicaciones potencialmente no deseadas. Microsoft.com. Recuperado el 8 de abril de 2024, de https://learn.microsoft.com/es-es/microsoft-365/security/defender/criteria?view=o365-worldwide.

- De Luz, S. (2021, agosto 12). VLANs: Qué son, tipos y para qué sirven. RedesZone. Recuperado el 27 de marzo de 2024, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

- De Luz, S. (2021, agosto 12). VLANs: Qué son, tipos y para qué sirven. RedesZone. Recuperado el 6 de abril de 2024, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

- Dell, M. X. (s/f). Cómo identificar y reducir la interferencia de señal inalámbrica. Dell.com. Recuperado el 3 de febrero de 2024, de https://www.dell.com/support/kbdoc/es-mx/000150359/c%C3%B3mo-identificar-y-reducir-la-interferencia-de-se%C3%B1al-inal%C3%A1mbrica

- Díaz, L. F. (2020, julio). GUÍA DE IMPLEMENTACIÓN E INTERPRETACIÓN DE REQUISITOS DEL ESTÁNDAR ISO 50001:2018. Gob.mx. Recuperado el 3 de abril de 2024, de https://www.conuee.gob.mx/transparencia/boletines/SGEn/manuales/Guia_ISO_50001_2018_paginas_web1.pdf

- Discusión:Espectro electromagnético. (s/f). Ingeniería Topográfica y Fotogramétrica Wiki; Fandom, Inc. Recuperado el 2 de febrero de 2024, de https://ingenieriatopografica.fandom.com/es/wiki/Discusi%C3%B3n:Espectro_electromagn%C3%A9tico

- Farrier, E. (2021, abril 22). Direcciones IP públicas frente a privadas: ¿en qué se diferencian? Direcciones IP públicas frente a privadas: ¿en qué se diferencian?Recuperado el 6 de febrero de 2024, de Avast. https://www.avast.com/es-es/c-ip-address-public-vs-private

- Felt. (s/f). Mapa interactivo de cobertura 4G - IFT –Felt . Recuperado el 19 de febrero de 2024, de https://felt.com/map/Mapa-interactivo-de-cobertura-4G-IFT-nkwEcoI4S9BSa7vgFt6uctD?loc=24.627,-101.917,5.52z

- HUAWEI. (2021, otoño 4). Fundamentos sobre ONT: Cómo configurar el filtrado de direcciones MAC en ONT. Huawei.com. Recuperado el 15 de marzo de 2024, de

https://forum.huawei.com/enterprise/es/fundamentos-sobre-ont-botones-de-la-ont-de-la-parte-frontal/thread/667223987203227648-667212890693840896

- Iana. (s/f). Number Resources. Iana.org. Recuperado el 17 de febrero de 2024, de https://www.iana.org/numbers

- IBM. (2023, noviembre 22). ¿Qué es un ataque cibernético? Ibm.com. Recuperado el 6 de abril de 2024, de https://www.ibm.com/mx-es/topics/cyber-attack

- IDET. (2017, diciembre 8). Aprobarán NOM para antenas de telefonía. IDET. Recuperado el 18 de febrero de 2024, de https://www.idet.org.mx/noticias/aprobaran-nom-antenas-telefonia/

- IFT. (2022, septiembre 11). El 46.6% de personas usuarias de internet fijo están informadas sobre riesgos cibernéticos: Encuesta IFT (Comunicado 101/2022) 9 de noviembre. Ift.org.MX. Recuperado el 22 de octubre de 2023, de https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-466-de-personas-usuarias-de-internet-fijo-estan-informadas-sobre-riesgos-ciberneticos-encuesta

- INEGI. (2022, mayo 16). ESTADÍSTICAS A PROPÓSITO DEL DÍA MUNDIAL DEL INTERNET (17 DE MAYO): DATOS NACIONALES. Org.mx. Accedido el 13 de octubre de 2023. https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2022/EAP_Internet22.pdf

- J. Ramírez Sánchez y J. V. Díaz Martínez. “Las redes inalámbricas, más ventajas que desventajas.” Universidad Veracruzana. Accedido el 4 de octubre de 2023. Disponible: https://www.uv.mx/iiesca/files/2012/12/redes2008-2.pdf

- Kochhar, K. (2018, noviembre 20). Las mujeres, la tecnología y el futuro del trabajo. Imf.org.Accedido el 13 de octubre de 2023. https://www.imf.org/es/Blogs/Articles/2018/11/16/blog-Women-Technology-the-Future-of-Work

- Lukor (2008). Redes WiFi. Recuperado el 04 de octubre de 2023 del sitio web http://www.lukor.com

- Martín, C. (2021, septiembre 3). Estándares y normas ISO para mejorar la ciberseguridad. GlobalSuite Solutions. Recuperado el 23 de marzo de 2024,

de https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/#La_ciberseguridad_y_las_normas_ISO

- Martínez, J. L. (2018, agosto 8). La absorción en las ondas y radioenlaces. PRORED. Recuperado el 27 de Enero de 2024, de https://www.prored.es/la-absorcion-en-las-ondas-y-radioenlaces/

- Martínez, J. L. (2018a, julio 13). Zonas de Fresnel en un radioenlace. Recuperado el 27 de Enero de 2024, de PRORED. https://www.prored.es/zonas-de-fresnel-en-un-radioenlace/

- Networks, H. A. (s/f). ¿Qué es control de acceso a la red (NAC)? Arubanetworks.com. Recuperado el 8 de marzo de 2024, de https://www.arubanetworks.com/latam/faq/que-es-control-de-acceso-a-la-red-nac/

- Nkongolo, M. N. W. (s/f). Zero-day vulnerability prevention with recursive feature elimination and ensemble learning. Iacr.org. Recuperado el 16 de octubre de 2023, de https://eprint.iacr.org/2023/1843.pdf

- Restauración de ecosistemas (s/f). Portada. Restauración de Ecosistemas; Restauraciondeecosistemas.com. Recuperado el 10 de abril de 2024, de https://www.restauraciondeecosistemas.com

- Ríos, M. E. M. (2009, Octubre). Apuntes de la Asignaturas de Redes de Datos I Y Redes de Datos II. Unam.Mx. Recuperado el 25 de octubre de 2023, de http://profesores.fi-b.unam.mx/victor/CCNA/Productos/Notas%20de%20Curso/Manual%20de%20la%20Asignatura%20de%20Redes%20de%20Datos%20I%20y%20II%20%20%28avance%2050%25%29.pdf

- Techradar. (s/f). Mejor antivirus. Techradar.com. Recuperado el 5 de abril de 2024, de https://www.techradar.com/best/best-antivirus.

- Ticnologia. (s/f). Firewall. Ticnologia; Fandom, Inc. Recuperado el 12 de marzo de 2024, de https://ticnologia.fandom.com/es/wiki/Firewall--

- Valois, A. (2023, agosto 21). Qué es un dominio en internet, para qué sirve y cómo funciona. Hostgator.mx. Recuperado el 15 de febrero de 2024, de https://www.hostgator.mx/blog/que-es-un-dominio-en-internet/

- Velazquez, N. (2021, febrero 17). IPv4 e IPv6. Trustnet. Recuperado el 6 de febrero de 2024, de https://trustnet.com.mx/ipv4-e-ipv6/