UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI



FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información"

Trabajo de titulación previa la obtención del
título de Ingeniería en Informática

AUTORES: Chamorro Pantoja Anderson Daniel.
Pupiales Chacón Silvia Verónica.

TUTOR: Hidalgo Guijarro Jairo Vladimir, MSc.

Tulcán, 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Chamorro Pantoja Anderson Daniel con el número de cédula 0402042030 ha elaborado el trabajo de titulación: “Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información”.

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

f.....

Hidalgo Guijarro Jairo Vladimir, MSc.

TUTOR

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.09.23 10:33:58 -05'00'

f.....

Del Hierro Mosquera Milton Gabriel, MSc.

LECTOR

Tulcán, septiembre de 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que la estudiante Pupiales Chacón Silvia Verónica con el número de cédula 1003991062 ha elaborado el trabajo de titulación: “Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información”.

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

f.....

Hidalgo Guijarro Jairo Vladimir, MSc.

TUTOR

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.09.23 10:34:46 -05'00'

f.....

Del Hierro Mosquera Milton Gabriel, MSc.

LECTOR

Tulcán, septiembre de 2021

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de Ingeniero en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales.

Yo, Chamorro Pantoja Anderson Daniel con cédula de identidad número 0402042030 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.



f.....

Chamorro Pantoja Anderson Daniel

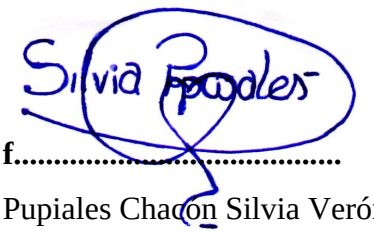
AUTOR

Tulcán, septiembre de 2021

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de Ingeniera en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales.

Yo, Pupiales Chacón Silvia Verónica con cédula de identidad número 1003991062 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.



f.....

Pupiales Chacón Silvia Verónica

AUTORA

Tulcán, septiembre de 2021

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Chamorro Pantoja Anderson Daniel declaro ser autor de los criterios emitidos en el trabajo de investigación: “Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....

Chamorro Pantoja Anderson Daniel

AUTOR

Tulcán, septiembre de 2021

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Pupiales Chacón Silvia Verónica declaro ser autora de los criterios emitidos en el trabajo de investigación: “Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.



f.....

Pupiales Chacón Silvia Verónica

AUTORA

Tulcán, septiembre de 2021

AGRADECIMIENTO

A Dios, por guiar mi camino, cuidarme y permitirme concluir con mi carrera universitaria.

A la Universidad Politécnica Estatal del Carchi, por abrirme sus puertas para cumplir una etapa más en mi vida.

A los docentes de la carrera de Computación / Ingeniería en Informática por guiarme con rectitud, paciencia y valores a lo largo de mi trayectoria académica.

A mis padres, por brindarme su amor y apoyo incondicional en cada etapa de mi vida.

Anderson Chamorro

DEDICATORIA

A mis queridos padres Aníbal Chamorro y Rosa Pantoja.

Por brindarme su apoyo y amor incondicional, estar en las buenas, malas y peores, de lo que me siento orgulloso por su esfuerzo y dedicación para formarme con valores y ser una persona de bien.

Por apoyarme en esta etapa tan importante de mi vida, les dedico este trabajo por ser uno de los logros que he alcanzado gracias a ellos.

Anderson Chamorro

AGRADECIMIENTO

A la Universidad Politécnica Estatal del Carchi, por permitirme adquirir nuevos conocimientos con docentes preparados, por darme la oportunidad de hacer amistades y facilitarme los recursos necesarios para desarrollar mi proyecto de investigación.

A mis padres, por aportar significativamente en mi crecimiento académico y personal, enseñarme el valor de las cosas y conseguirlas con esfuerzo y constancia.

A mis abuelitos, por cuidarme durante mi infancia y apoyarme en mis estudios, llenarme de amor y sabios consejos, y enseñarme a valorar cada momento de la vida y no rendirme ante las dificultades.

Y a Dios, por cuidar de los que más quiero y darme la fuerza para seguir adelante.

Verónica Pupiales

DEDICATORIA

A mi hermana Kimberly Pupiales.

Crecimos juntas y logramos superar cada obstáculo con el fin de superarnos y ser cada día mejores, y a pesar de nuestras discusiones y diferencias, nunca dejamos de querernos y apoyarnos mutuamente.

Juntas aprendimos que un tropezón no es una caída, con voluntad y esfuerzo todo se puede, y que lo más valioso en el mundo es la familia y los amigos sinceros.

Gracias por ser mi confidente y un pilar muy importante en mi vida.

Verónica Pupiales

ÍNDICE GENERAL

I. PROBLEMA 34
1.1. PLANTEAMIENTO DEL PROBLEMA 34
1.2. FORMULACIÓN DEL PROBLEMA 36
1.3. JUSTIFICACIÓN 36
1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN 37
1.4.1. Objetivo general 37
1.4.2. Objetivos específicos 37
1.4.3. Preguntas de Investigación 37
II. FUNDAMENTACIÓN TEÓRICA 39
2.1. ANTECEDENTES INVESTIGATIVOS 39
2.2. MARCO TEÓRICO 41
2.2.1. Equipo de respuesta ante incidentes informáticos (CSIRT) 41
2.2.2. Servicios de un CSIRT 42
2.2.2.1. Servicios proactivos 43
2.2.2.2. Servicios reactivos 44
2.2.2.3. Servicios en mejoras de la calidad 45
2.2.3. Tipos de CSIRT 46
2.2.3.1. CSIRT académico 46
2.2.3.2. CSIRT comercial 50
2.2.3.3. CSIRT de sector público 51
2.2.3.4. CSIRT de sector militar 51
2.2.3.5. CSIRT nacionales 51
2.2.3.6. CSIRT de pequeñas y medianas empresas 52
2.2.3.7. CSIRT de proveedores 52
2.2.3.8. CSIRT gubernamental 52

2.2.3.9. CSIRT de infraestructuras críticas 53
2.2.4. Beneficios de un CSIRT 53
2.2.5. Modelos organizacionales de un CSIRT 55
2.2.5.1. Modelo de negocio independiente 55
2.2.5.2. Modelo incrustado 55
2.2.5.3. Modelo campus 56
2.2.5.4. Modelo matricial 56
2.2.5.5. Modelo voluntario 56
2.2.5.6. Modelo hibrido 56
2.2.6. Estructura organizacional de un CSIRT 57
2.2.6.1. Dirección 57
2.2.6.2. Operaciones 57
2.2.6.3. TI. 57
2.2.6.4. I&D. 57
2.2.6.5. Servicios de apoyo 58
2.2.7. Tamaño y cantidad de recursos humanos 58
2.2.8. Recursos tecnológicos de un CSIRT 59
2.2.8.1. Sitio web público 59
2.2.8.2. Correo electrónico 59
2.2.8.3. Teléfono 60
2.2.8.4. Herramientas de manejo de incidentes 60
2.2.8.5. Sistemas operativos 60
2.2.8.6. Respaldo de datos 60
2.2.8.7. Herramientas forenses 60
2.2.8.8. Servidor DNS 61
2.2.8.9. Tecnologías de acceso remoto 61
2.2.8.10. Caja fuerte 61

2.2.8.11. Firmas electrónicas 61
2.2.8.12. Conexión a internet 61
2.2.8.13. Sistemas SIEM 61
2.2.9. Estructura de las políticas de seguridad de un CSIRT 62
2.2.10. Acuerdo de nivel de servicio (SLA) 63
2.2.10.1. Tipos de SLA 63
2.2.10.2. Composición de un SLA 64
2.2.10.3. Métricas que miden un SLA 64
2.2.10.4. Componentes de un informe SLA 64
2.2.11. Seguridad de la información 65
2.2.12. ISO/IEC serie 27000 66
2.2.13. Normativa de directrices y principios para gestionar el riesgo de las organizaciones ISO 31000 67
2.2.14. "Biblioteca de infraestructura de tecnologías de información" ITIL 68
2.2.15. "Ley orgánica de educación intercultural" LOEI 68
2.2.16. "Consorcio de gobiernos autónomos provinciales del Ecuador" CONGOPE 69
2.2.17. Transparencia de un CSIRT bajo los estándares de referencia RFC2350 69
2.2.17.1. Definición 69
2.2.17.2. Relaciones entre diferentes CSIRTs 70
2.2.17.3. Establecimiento de comunicaciones seguras 70
2.2.17.4. Publicación de políticas y procedimientos de un CSIRT 70
2.2.17.5. Información, políticas y procesos 70
2.2.17.6. Obtención del documento 70
2.2.17.7. Información de contacto 71
2.2.17.8. Carta 71
2.2.17.9. Políticas 71
2.2.17.10. Servicios 72

2.2.17.11. Formulario de notificación de incidentes 72
2.2.17.12. Renuncias 72
III. METODOLOGÍA 73
3.1. ENFOQUE METODOLÓGICO 73
3.1.1. Enfoque 73
3.1.1.1. Cualitativo 73
3.1.2. Tipo de investigación 73
3.1.2.1. Documental 73
3.1.2.2. De campo 74
3.1.3. Técnicas 74
3.1.3.1. Revisión de literatura 74
3.1.3.2. Entrevistas 74
3.1.3.3. Validación de instrumentos 74
3.2. IDEA A DEFENDER 78
3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES 79
3.4. MÉTODOS UTILIZADOS 81
3.4.1. Inductivo - deductivo 81
3.4.2. Analítico 81
3.4.3. Sintético 81
3.5. POBLACIÓN Y MUESTRA 81
3.5.1. Muestreo por conveniencia 81
3.6. RECURSOS 82
3.6.1. Humanos 82
3.6.2. Institucionales 82
3.6.3. Materiales de trabajo 83
IV. RESULTADOS Y DISCUCIÓN 84
4.1. RESULTADOS DE LA ENTREVISTA 84

4.1.1. Unidad educativa 84
4.1.2. Gobierno seccional. 88
4.2. DESARROLLO DE LA PROPUESTA 92
4.2.1. Planificación 92
4.2.1.1. Documentos de constitución 92
4.2.1.2. Comunidad objetivo 93
4.2.1.3. Servicios 93
4.2.1.4. Organización y RRHH 95
4.2.2. Ejecución 96
4.2.2.1. Instalaciones e infraestructura TI 96
4.2.2.2. Políticas y procedimientos operacionales 135
4.2.2.3. Acuerdo de nivel de servicios (SLA) 170
4.2.3. Cierre 178
4.2.3.1. Presupuesto referencia para la implementación de CSIRT UPEC 178
V. CONCLUSIONES Y RECOMENDACIONES 181
5.1. CONCLUSIONES 181
5.2. RECOMENDACIONES 182
VI. REFERENCIAS BIBLIOGRÁFICAS 183
VII. ANEXOS 187

ÍNDICE DE FIGURAS

Figura 1. Estructura organizacional de CSIRT UPEC 95
Figura 2. Servidor web con sistema operativo CentOS7 97
Figura 3. Gestor de contenido WordPress para el sitio web público del CSIRT 97
Figura 4. Cabecera página de inicio del sitio web público 98
Figura 5. Cuerpo página de inicio del sitio web público 99
Figura 6. Página nosotros del sitio web público 99
Figura 7. Página norma RFC 2350 del sitio web público 100
Figura 8. Página manuales del sitio web público 101
Figura 9. Página de servicios del sitio web público 101
Figura 10. Página del servicio alertas y avisos del sitio web público 102
Figura 11. Página del servicio manejo de incidentes del sitio web público 103
Figura 12. Página del servicio anuncios del sitio web público 104
Figura 13. Página del servicio concientización tecnológica del sitio web público 104
Figura 14. Parte uno de la página reportar incidente del sitio web público 105
Figura 15. Parte dos de la página reportar incidente del sitio web público 106
Figura 16. Página contacto del sitio web público 106
Figura 17. Página principal del sistema de tickets “Centro de Respuesta y Soporte a Incidentes de Seguridad” 107
Figura 18. Vista cliente - Página abrir un nuevo ticket con la sección información de contacto y temas de ayuda 108
Figura 19. Vista cliente - Formulario del servicio para crear un ticket con el tema de ayuda CSIRT- Reportar incidente 109
Figura 20. Vista cliente - Formulario del servicio para crear un ticket con el tema de ayuda CSIRT- Concienciación tecnológica 110
Figura 21. Vista cliente - Mensaje de ticket creado con éxito junto con instrucciones para ver su estado e información de contacto en el sistema de tickets 111
Figura 22. Vista cliente - Formulario de registro de cuenta en el sistema de tickets 112
Figura 23. Vista cliente - Página de confirmación de registro del sistema de tickets 112
Figura 24. Vista cliente - Página de administración de tickets 113
Figura 25. Vista cliente – Detalles del ticket y área de interacción con el agente a cargo del caso 114
Figura 26. Vista agente – Inicio de sesión en el sistema de tickets 114

Figura 27. Vista agente – Reporte estadístico de actividad de los tickets en el menú panel de control 115
Figura 28. Vista agente – Directorio de usuarios registrados al sistema de tickets en el menú usuarios 116
Figura 29. Vista agente – Administrador de organizaciones del sistema de tickets en el menú usuarios 117
Figura 30. Vista agente – Administrador de tickets 118
Figura 31. Vista agente – Seguimiento de tickets asignados 118
Figura 32. Sistema operativo Kali Linux para el servidor de monitoreo 119
Figura 33. Herramienta de código abierto nmap 120
Figura 34. Analizador de protocolos de red Wireshark 121
Figura 35. Herramienta WhatWeb 122
Figura 36. Aplicación de comandos DMitry 123
Figura 37. Herramienta dnsenum 124
Figura 38. Herramienta dnstracer 125
Figura 39. Herramienta dnswalk 126
Figura 40. Herramienta dotdotpwn 127
Figura 41. Herramienta de escaneo de vulnerabilidades Nessus 128
Figura 42. Herramienta Domain Dossier 129
Figura 43. Herramienta Google Apps Messageheader 130
Figura 44. Herramienta de diagnóstico de problemas MXToolBox 131
Figura 45. Herramienta online Virus Total 132
Figura 46. Herramienta Hybrid Analysis 133
Figura 47. Herramienta Sandbox 134
Figura 48. Herramienta GPG 135
Figura 49. Proceso de gestión de incidentes CSIRT UPEC 148
Figura 50. Proceso de alertas y avisos CSIRT UPEC 155
Figura 51. Proceso de Publicación de Anuncios CSIRT UPEC 158
Figura 52. Formato distribución de anuncios CSIRT UPEC 160
Figura 53. Proceso de concientización tecnológica CSIRT UPEC 161
Figura 54. Proceso para la gestión de riesgo 165
Figura 55. Matriz de calor para el análisis de riesgo 169

Figura 56. Acta de pre defensa del proyecto de titulación denominado equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información – Anderson Chamorro 187
Figura 57. Acta de pre defensa del proyecto de titulación denominado equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información – Silvia Pupiales 188
Figura 58. Informe de turnitin del documento de investigación..... 189
Figura 59. Validación del abstract por parte del CIDEN parte 1 190
Figura 60. Validación del abstract por parte del CIDEN parte 2 191
Figura 61. Oficio para el acceso al laboratorio de Ciberseguridad dirigido al Msc. Jairo Hidalgo – "Docente Investigador de la Carrera de Computación/ Ingeniería en Informática de la UPEC" 192
Figura 62. Oficio dirigido al Lic. Oscar Villarreal – "Director Distrital 04D01" 193
Figura 63. Oficio dirigido a la Msc. Lourdes Del Hierro – "Directora Distrital 04D03" 194
Figura 64. Oficio dirigido al Lic. Washington Mafla – "Director Distrital 04D02" 195
Figura 65. Formato entrevista para unidades educativas de la provincia del Carchi 197
Figura 66. Formato entrevista para gobiernos seccionales de la provincia del Carchi 199
Figura 67. Entrevista a la Lic. Mariela Narváez – "Docente de la Unidad Educativa San Antonio de Padua"..... 200
Figura 68. Entrevista a la Lic. Carolina De La Vega - "Docente de la Unidad Educativa José Julián Andrade"..... 200
Figura 69. Entrevista al Ing. Diego Rosales - "Docente de la Unidad Educativa Tulcán" 201
Figura 70. Entrevista al Ing. Diego Erazo - "Encargado del Área de Tecnología del GAD Municipal San Pedro de Huaca"..... 201
Figura 71. Entrevista al Ing. Fred Carrera - "Encargado de la Jefatura de Sistemas del GAD Municipal de Tulcán" 202
Figura 72. Entrevista a la Ing. Doris Arcos - "Encargada del Área de Tecnología del Gobierno Provincial del Carchi" 202
Figura 73. Entrevista al Msc. Jhony Enríquez - "Director del Centro de TIC de la Universidad Politécnica Estatal del Carchi" 203
Figura 74. Oficio de habilitación de correo electrónico dirigido al Sr. Msc. Wilson Zabala - "Director de Tecnologías de Información y Comunicación". 204
Figura 75. Oficio de habilitación de dominio dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi" 205

Figura 76. Oficio de habilitación de CSIRT UPEC dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi" (parte 1)..... 206
Figura 77. Oficio de habilitación de CSIRT UPEC dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi"(parte 2)..... 207
Figura 78. Informe de conformidad en cumplimiento de los resultados de la propuesta CSIRT UPEC..... 208
Figura 79. Actualización de paquetes Apache..... 209
Figura 80. Instalación del servidor web Apache..... 210
Figura 81. Detalles de la instalación del servidor web Apache..... 211
Figura 82. Habilitado de puertos 80 y 443 en el firewall del servidor..... 211
Figura 83. Arranque del servidor web Apache..... 212
Figura 84. Verificación de la página predeterminada del servidor web Apache..... 212
Figura 85. Obtención del certificado SSL utilizando el cliente Certbot..... 213
Figura 86. Instalación de certificados SSL para el sitio web..... 214
Figura 87. Descarga del repositorio MySQL al servidor..... 215
Figura 88. Preparación del repositorio MySQL..... 215
Figura 89. Instalación de MySQL Server..... 216
Figura 90. Detalles de la instalación de MySQL..... 217
Figura 91. Inicio del servicio MySQL Server..... 217
Figura 92. Consulta de contraseña temporal de MySQL..... 218
Figura 93. Modificación de contraseña de acceso root en MySQL..... 219
Figura 94. Acceso root a la base de datos MySQL..... 219
Figura 95. Descarga de los repositorios REMI y EPEL..... 220
Figura 96. Preparación de los repositorios REMI y EPEL..... 221
Figura 97. Habilitado del repositorio REMI..... 221
Figura 98. Instalación de PHP y sus dependencias..... 222
Figura 99. Detalles de instalación de PHP..... 223
Figura 100. Creación de la base de datos en MySQL Server..... 224
Figura 101. Creación de usuario y contraseña en la base de datos MySQL..... 224
Figura 102. Asignación de privilegios de acceso a la base de datos al usuario..... 225
Figura 103. Descarga del gestor de contenido WordPress..... 226

Figura 104. Extracción del directorio WordPress 226
Figura 105. Reubicación del archivo WordPress 227
Figura 106. Agregar carpeta para archivos generados en WordPress 227
Figura 107. Asignar propiedad y permisos al directorio WordPress 228
Figura 108. Actualización del archivo wp-config de WordPress 228
Figura 109. Conexión con la base de datos en el archivo de configuración WordPress 229
Figura 110. Configuración de idioma para la instalación de WordPress 230
Figura 111. Instalación de WordPress en su interfaz web 230
Figura 112. Fin del proceso de instalación WordPress 231
Figura 113. Formulario de inicio de sesión WordPress 231
Figura 114. Área de trabajo de WordPress 232
Figura 115 Ajustes generales para el gestor de contenido WordPress 233
Figura 116. Ajustes de escritura para el gestor de contenido WordPress 233
Figura 117. Ajuste de lectura para el gestor de contenido WordPress 234
Figura 118. Ajuste de comentarios para el gestor de contenido WordPress 235
Figura 119. Ajuste multimedia para el gestor de contenido WordPress 235
Figura 120. Ajuste de enlaces permanentes para el gestor de contenido WordPress 236
Figura 121. Ajustes de privacidad 236
Figura 122. Búsqueda e instalación de plugins requeridos para distintas funcionalidades en el gestor de contenido WordPress 237
Figura 123.Visualización de plugins instalados 238
Figura 124. Configuración del plugin ARForm Builder 239
Figura 125. Configuración del plugin Easy WP SMTP 239
Figura 126. Configuración del plugin Real-Time Find and Replace 240
Figura 127. Configuración del plugin Sassy Social Share 241
Figura 128. Configuración del plugin Smart Slider 3 241
Figura 129. Creación de usuario para la administración del sitio web 242
Figura 130. Administrador de usuarios del gestor de contenido WordPress 243
Figura 131. Añadir tema al gestor de contenido WordPress 243
Figura 132. Selección e instalación del tema para el gestor de contenido WordPress 244
Figura 133. Activación del tema Kahuna en WordPress 245
Figura 134. Opción personalizar el menú de navegación WordPress 245
Figura 135. Personalizar identidad del sitio en WordPress 246

Figura 136. Opción identidad del sitio para agregar título, descripción y favicon al sitio web 247
Figura 137. Inserción de imagen como cabecera para las páginas del sitio web 247
Figura 138. Personalizar diseño en WordPress 248
Figura 139. Establecer diseño principal, alineación y dimensiones en la estructura del sitio web 249
Figura 140. Definir diseño de las entradas y pie de página del sitio web 249
Figura 141. Personalizar cabecera en WordPress 250
Figura 142. Definir altura, posición y alineación del menú para la cabecera del sitio web 251
Figura 143. Establecer descripción, altura, comportamiento, ancho y alineación de la imagen de cabecera para el sitio web 251
Figura 144. Personalización general en WordPress 252
Figura 145. Activación de navegación, títulos de páginas y categorías y diseño del pie de página del sitio web 253
Figura 146. Marcar los títulos de cabecera para su visibilidad en la cabecera del sitio web 253
Figura 147. Establecer el diseño de las imágenes destacadas en las entradas del sitio web 254
Figura 148. Activación de la caja de búsqueda en el sitio web 254
Figura 149. Personalizar colores para el sitio web en WordPress 255
Figura 150. Establecer colores del contenido del sitio web 256
Figura 151. Establecer colores para la cabecera del sitio web 256
Figura 152. Establecer colores para el pie de página del sitio web 257
Figura 153. Establecer colores para la página de destino del sitio web 257
Figura 154. Personalizar tipografía en WordPress 258
Figura 155. Definir la tipografía para la fuente general del sitio web 258
Figura 156. Definir la tipografía para las fuentes de cabecera del sitio web 259
Figura 157. Definir la tipografía para las fuentes del contenido del sitio web 260
Figura 158. Definir la tipografía para las fuentes de los widgets del sitio web 260
Figura 159. Definir los formatos en dimensiones para el sitio web 261
Figura 160. Personalizar la información de la entrada en WordPress 261
Figura 161. Definir el comportamiento de la imagen destacada para el sitio web 262
Figura 162. Definir la información meta para las entradas del sitio web 262
Figura 163. Activación de extracto para las entradas y establecer sus propiedades para el sitio web 263

Figura 164. Definir las propiedades de los comentarios para las publicaciones del sitio web 264
Figura 165. Crear la página de inicio para el sitio web 264
Figura 166. Establecer una página estática para la página de inicio del sitio web 265
Figura 167. Personalizar página de destino en WordPress 265
Figura 168. Activación de la página de destino personalizada para el sitio web 266
Figura 169. Activación del carrusel con el uso de shortcode para el sitio web 267
Figura 170. Agregar contenido multimedia para el carrusel ubicado en la página de inicio . 267
Figura 171. Activar entradas como contenido destacado para el cuerpo de la página de inicio del sitio web 268
Figura 172. Vista previa de la página de inicio 269
Figura 173. Selección de bloques para la estructura de la página servicios del sitio web 270
Figura 174. Configuración de la página servicios para su publicación en el sitio web 270
Figura 175. Vista previa de la página de servicios 271
Figura 176. Selección de bloques para la estructura de la página alertas y avisos del sitio web 272
Figura 177. Configuración de la página alertas y avisos para su publicación en el sitio web 272
Figura 178. Vista previa de la página de alertas y avisos 273
Figura 179. Selección de bloques para la estructura de la página manejo de incidentes del sitio web 274
Figura 180. Configuración de la página manejo de incidentes para su publicación en el sitio web 274
Figura 181. Vista previa de la página de manejo de incidentes 275
Figura 182. Selección de bloques para la estructura de la página anuncios del sitio web 276
Figura 183. Configuración de la página anuncios para su publicación en el sitio web 276
Figura 184. Vista previa de la página de anuncios 277
Figura 185. Selección de bloques para la estructura de la página concientización tecnológica del sitio web 278
Figura 186. Configuración de la página concientización tecnológica para su publicación en el sitio web 278
Figura 187. Vista previa de la página de concientización tecnológica 279
Figura 188. Incluir shortcode del formulario reportar incidente de seguridad informática en la página reportar incidente 279

Figura 189. Configuración de la página reportar incidente para su publicación en el sitio web 280
Figura 190. Vista previa de la página de reportar incidente 280
Figura 191. Selección de bloques para la estructura de la página política de privacidad 281
Figura 192. Configuración de la página política de privacidad - CSIRT UPEC para su publicación en el sitio web 282
Figura 193. Vista previa de la página política de privacidad 282
Figura 194. Selección de bloques para la estructura de la página nosotros del sitio web 283
Figura 195. Configuración de la página nosotros para su publicación en el sitio web 284
Figura 196. Vista previa de la página nosotros 284
Figura 197. Selección de bloques para la estructura de la página contacto del sitio web 285
Figura 198. Configuración de la página contacto para su publicación en el sitio web 286
Figura 199. Vista previa de la página de contacto 286
Figura 200. Selección de bloques para la estructura de la página norma RFC 2350 del sitio web 287
Figura 201. Configuración de la página norma RFC 2350 para su publicación en el sitio web 288
Figura 202. Vista previa de la página norma RFC 2350 288
Figura 203. Selección de bloques para la estructura de la página manuales del sitio web 289
Figura 204. Configuración de la página manuales para su publicación en el sitio web 290
Figura 205. Vista previa de la página manuales 290
Figura 206. Lista de páginas creadas para el sitio web en el administrador de páginas 291
Figura 207. Crear entradas para el sitio web 292
Figura 208. Configuración de las entradas para su publicación en el sitio web 292
Figura 209. Vista Previa de las entradas publicadas en el sitio web 293
Figura 210. Lista de entradas y sus opciones de personalización 294
Figura 211. Administración de comentarios emitidos en las entradas 295
Figura 212. Crear nuevo formulario con ARForms Lite en WordPress 295
Figura 213. Configuración de identidad del formulario en WordPress 296
Figura 214. Selección de campos de entrada para la estructura del formulario 296
Figura 215. Configuración de la etiqueta para la sección información de contacto para el formulario de reporte a incidentes de seguridad informática 297

Figura 216. Configuración del campo quien reporta en el formulario de reporte a incidentes de seguridad informática 298
Figura 217. Configuración del campo correo electrónico para el formulario de reporte a incidentes de seguridad informática 299
Figura 218. Configuración del campo teléfono para el formulario de reporte a incidentes de seguridad informática 300
Figura 219. Configuración del campo tipo de organización para el formulario de reporte a incidentes de seguridad informática 301
Figura 220. Configuración del campo nombre de la organización para el formulario de reporte a incidentes de seguridad informática 302
Figura 221. Configuración del campo estado actual del incidente para el formulario de reporte a incidentes de seguridad informática 303
Figura 222. Configuración del campo cuando se detectó, fecha del incidente para el formulario de reporte a incidentes de seguridad informática 303
Figura 223. Configuración del campo cuando se detectó, hora del incidente para el formulario de reporte a incidentes de seguridad informática 304
Figura 224. Configuración de la etiqueta para la sección detalles del incidente para el formulario de reporte a incidentes de seguridad informática 305
Figura 225. Configuración del campo descripción del incidente en el formulario de reporte a incidentes de seguridad informática 306
Figura 226. Configuración del campo de comprensión de políticas de seguridad para el formulario de reporte a incidentes de seguridad informática 307
Figura 227. Personalizar las opciones de estilo para el formulario de reporte a incidentes de seguridad informática 307
Figura 228. Configuración del estilo básico para el formulario de reporte a incidentes de seguridad informática 308
Figura 229. Configuración avanzada para el formulario de reporte a incidentes de seguridad informática 309
Figura 230. Configuración de los campos de entrada para el formulario de reporte a incidentes de seguridad informática 309
Figura 231. Configuración del botón enviar para el formulario de reporte a incidentes de seguridad informática 310

Figura 232. Configuración de notificación por correo automática después del envió del formulario de reporte a incidentes de seguridad informática 311
Figura 233. configuración de la acción de envío del formulario de reporte a incidentes de seguridad informática 311
Figura 234. Administrador de formularios de ARForms Lite en WordPress 312
Figura 235. Entradas del formulario de ARForms Lite en WordPress 313
Figura 236. Configuración de los tickets en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 314
Figura 237. Configuración de avisos de tickets en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 315
Figura 238. Configuración del tema de ayuda CSIRT – Reportar Incidente en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 316
Figura 239. Configuración del tema de ayuda CSIRT – Concienciación Tecnológica en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 317
Figura 240. Página de los temas de ayuda registrados en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 318
Figura 241. Crear la página ventana principal en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 319
Figura 242. Crear la página CSIRT UPEC - Página de agradecimiento en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 320
Figura 243. Crear la página fuera de servicio en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 321
Figura 244. Administración de páginas creadas en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 322
Figura 245. Configuración del formulario CSIRT UPEC - Concienciación tecnológica en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 323
Figura 246. Configuración del formulario CSIRT UPEC - Reportar incidente informático en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 324
Figura 247. Página de administración de formularios personalizados en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 325
Figura 248. Configuración de correo electrónico de CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 326

Figura 249. Página de administración de correos electrónicos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....327
Figura 250. Configuración de plantillas de correo electrónico automáticas en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....328
Figura 251. Página de administración de plantillas automáticas de correo electrónico CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....329
Figura 252. Configuración de agentes CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....329
Figura 253. Página de administración de agentes CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 330
Figura 254. Configuración de departamentos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....331
Figura 255. Página de administración de departamentos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 332
Figura 256. Configuración de un nuevo usuario CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 333
Figura 257. Página de administración de usuarios CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 334
Figura 258. Configuración de la organización Gobiernos Seccionales Provincia Carchi en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....335
Figura 259. Configuración de la organización Unidades Educativas Provincia Carchi en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad.....336
Figura 260. Página de administración de organizaciones CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad 337
Figura 261. Descarga del paquete Nessus de la página oficial.....338
Figura 262. Verificar y descomprimir el paquete de instalación Nessus con la terminal de Kali Linux.....339
Figura 263. Activar el arranque automático y verificar el estado de la herramienta Nessus. 339
Figura 264. Selección de la versión de la herramienta Nessus a instalar 340
Figura 265. Registro para obtener el código de verificación de la herramienta Nessus.....341
Figura 266. Correo electrónico con el código de activación para la herramienta Nessus 342
Figura 267. Ingreso del código de verificación de la herramienta Nessus 343
Figura 268. Registro de cuenta de usuario para la administración de la herramienta Nessus 344

Figura 269. Instalación de complementos de la herramienta Nessus 345
Figura 270. Área de trabajo de la herramienta Nessus 346
Figura 271. Formato solicitud de destrucción de información 347
Figura 272. Formato informe final de destrucción de información 348
Figura 273. Formato compromiso de confidencialidad 349
Figura 274. Formato reporte de incidentes informáticos 350
Figura 275. Formato de valoración de incidentes 352
Figura 276. Formato de notificación por correo sobre la confirmación del formulario para reportar incidentes 353
Figura 277. Formato de informe de resultados en la gestión del incidente 354
Figura 278. Formato para la identificación de confiabilidad de la fuente 356
Figura 279. Formato para la distribución de alertas y avisos 357
Figura 280. Formato de solicitud para concientización tecnológica 358

ÍNDICE DE TABLAS

Tabla 1. Abreviaturas de CSIRTs 42
Tabla 2. CSIRTs del sector académico en Ecuador 47
Tabla 3. Lista de unidades educativas del distrito de educación 04D01 Tulcán - San Pedro de Huaca 47
Tabla 4. Lista de unidades educativas del Distrito 04D02 Montúfar – Bolívar 48
Tabla 5. Lista de unidades educativas Distrito 04D03 Mira – Espejo 49
Tabla 6. CSIRTs del sector comercial en Ecuador 50
Tabla 7. CSIRT del sector militar en Ecuador 51
Tabla 8. CSIRTS nacionales de Sudamérica 51
Tabla 9. Lista de los gobiernos seccionales de la provincia del Carchi 53
Tabla 10. CSIRTs del sector de infraestructuras críticas en Ecuador 53
Tabla 11. Tamaño y cantidad de recursos humanos en fase inicial y madurez del CSIRT 58
Tabla 12. Validación de instrumentos primera aplicación 75
Tabla 13. Validación de instrumentos segunda aplicación 77
Tabla 14. Operacionalización de variables 79
Tabla 15. Recursos humanos 82
Tabla 16. Recursos institucionales 82

Tabla 17. Materiales de trabajo 83
Tabla 18. Funciones y responsabilidades en el CSIRT 95
Tabla 19. Política de clasificación de información 135
Tabla 20. Política de protección de datos 137
Tabla 21. Política de destrucción de información 138
Tabla 22. Política de divulgación de información 140
Tabla 23. Política de acceso a la información 141
Tabla 24. Política de uso apropiado de los sistemas de CSIRT UPEC 142
Tabla 25. Política de cooperación 144
Tabla 26. Política de privacidad 145
Tabla 27. Ficha de proceso gestión de incidentes 149
Tabla 28. Priorizar incidente 152
Tabla 29. Estado de incidente 153
Tabla 30. Ficha de proceso alertas y visos 156
Tabla 31. Ficha de proceso publicación de anuncios 158
Tabla 32. Ficha de proceso concientización tecnológica 162
Tabla 33. Ficha de proceso gestión de riesgos 165
Tabla 34. Identificación de riesgos 167
Tabla 35. Fórmula calculo riesgo 169
Tabla 36. Valores de los ejes de probabilidad y de impacto 169
Tabla 37. Prioridad tiempo de respuesta 170
Tabla 38. Horario de los servicios que brinda CSIRT UPEC 172
Tabla 39. Horario para interrupción programada 173
Tabla 40. Métrica gestión de solicitudes del servicio manejo de incidentes 174
Tabla 41. Métrica gestión de solicitudes del servicio concientización tecnológica 175
Tabla 42. Métrica gestión de niveles de los servicios 176
Tabla 43. Horario para solicitar soporte a CSIRT UPEC 177
Tabla 44. Costo referencial de tecnología hardware y software de CSIRT UPEC 178
Tabla 45. Costo referencial gastos operativos de CSIRT UPEC 179
Tabla 46. Costo referencia equipos de oficina de CSIRT UPEC 179
Tabla 47. Costo referencial servicios básicos de CSIRT UPEC 180
Tabla 48. Costo referencial total para la implementación de CSIRT UPEC 180
Tabla 49. Métrica gestión de solicitudes del servicio alertas y avisos 359

Tabla 50. Métrica gestión de solicitudes del servicio anuncios 359
Tabla 51. Métrica nivel de gestión de riesgo 360

ÍNDICE DE ANEXOS

Anexo 1 Acta de pre defensa 187
Anexo 2 Informe de turnitin 189
Anexo 3 Validación del abstract 190
Anexo 4 Autorización para el desarrollo del proyecto de investigación en el laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi. 192
Anexo 5 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D01 San Pedro de Huaca – Tulcán". 193
Anexo 6 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D03 Mira - Espejo" 194
Anexo 7 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D02 Montufar - Bolívar". 195
Anexo 8 Formato de entrevista 196
Anexo 9 Evidencia de aplicación de entrevistas a unidades educativas y gobiernos seccionales de la provincia del Carchi. 200
Anexo 10 Oficio de habilitación de correo electrónico institucional para CSIRT UPEC. 204
Anexo 11 Oficio de petición de dominio csirt.upec.edu.ec. 205
Anexo 12 Oficio de autorización para el funcionamiento de CSIRT UPEC en el Laboratorio de Ciberseguridad de la Carrera de Computación. 206
Anexo 13 Informe de conformidad 208
Anexo 14 Adecuación y configuración del servidor CentOS 7 para la implementación del servidor web 209
Anexo 15 Instalación y configuración de WordPress 223
Anexo 16 Configuración diseño sitio web 243
Anexo 17 Creación y configuración vistas del sitio web 264
Anexo 18 Creación y configuración formularios del sitio web 295
Anexo 19 Configuración servidor de registro y seguimiento de incidentes. 313
Anexo 20 Instalación y configuración de Nessus Essentials en Kali Linux. 337
Anexo 21 Formato solicitud de destrucción de información. 346

Anexo 22 Formato informe final de destrucción de información. 347
Anexo 23 Formato compromiso de confidencialidad..... 349
Anexo 24 Formato reporte de incidentes informáticos. 350
Anexo 25 Formato de valoración de incidentes. 351
Anexo 26 Formato de notificación por correo sobre la confirmación del formulario para reportar incidentes. 352
Anexo 27 Formato de informe de resultados en la gestión del incidente. 353
Anexo 28 Formato para la identificación de confiabilidad de la fuente..... 355
Anexo 29 Formato para la distribución de alertas y avisos. 356
Anexo 30 Formato de solicitud para concientización tecnológica. 358
Anexo 31 Métricas e indicadores para medir los procesos alertas - avisos, publicación de anuncios y gestión de riesgos 358

RESUMEN

La presente investigación tiene como objetivo, diagnosticar el adecuado proceso de solución a incidentes informáticos en unidades educativas y gobiernos seccionales de la provincia del Carchi, para la seguridad de la información.

Se empleó el enfoque cualitativo y su tipo de investigación es documental para el análisis e interpretación de varias fuentes de consulta, y de campo para recolectar información directamente de la unidades educativas y gobiernos seccionales de la provincia del Carchi.

Las técnicas utilizadas son: la revisión de literatura para aumentar el nivel de conocimiento en el área de estudio, la validación de la entrevista semiestructurada con dos docentes de la carrera de Computación/Ingeniería en Informática, para su posterior aplicación al personal a cargo del área técnica de la comunidad objetivo.

Se conformó un Equipo de Respuesta ante Incidentes Informáticos CSIRT con misión, visión y valores y se desarrolló un catálogo de servicios con políticas y procesos operacionales requeridos por las unidades educativas y gobiernos seccionales en la gestión de incidentes. La estructura organizacional se conformó por departamentos, funciones y responsabilidades, y se establecieron matrices e indicadores para evaluar la calidad de los servicios.

La implementación de CSIRT UPEC, se llevó a cabo en el Laboratorio de Ciberseguridad de la Carrera de Computación, se realizó la instalación y configuración de un sitio web https://csirt.upec.edu.ec/ bajo en el sistema operativo CentOS 7.0. Además, se estableció herramientas de monitoreo en el sistema operativo Kali Linux para obtener más información sobre incidentes o vulnerabilidades, obtener resultados más precisos y emitir recomendaciones apropiadas a la comunidad objetivo.

Palabras clave: Seguridad informática, servicios, procesos, políticas.

ABSTRACT

The objective of this research is to diagnose the appropriate process to solve computer incidents in educational units and sectional governments of the province of Carchi regarding information security.

The qualitative approach was used and the type of research applied is documentary for the analysis and interpretation of various sources, and the field type to collect information directly from the educational units and sectional governments of the Carchi province.

The techniques used are: the literature review to increase the level of knowledge in the study area, and the validation of the semi-structured interview made by two professors of the Computer Science / Computer Engineering career for its subsequent application to the staff in charge of the target community technical area.

A Computer Incident Response Team (CSIRT) was conformed with mission, vision and values. Also, a catalog of services was developed with policies and operational processes required by educational units and sectional governments in incident management. The organizational structure was made up of departments, functions and responsibilities. Additionally, matrices and indicators were established to evaluate the quality of services.

The CSIRT UPEC implementation was conducted in the Cybersecurity Laboratory of the Computing Career. The installation and configuration of a website https://csirt.upec.edu.ec/ was done under the CentOS 7.0 operating system. Finally, monitoring tools were established in the Kali Linux operating system to obtain more information about incidents or vulnerabilities. They helped to get more accurate results and provide recommendations to the target community.

Keywords: IT security, services, processes, policies.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Desde el punto de vista de Guzmán (2019), en el mundo existen muchas entidades al día que son víctimas de ciberataques realizados por terceras personas, con el objetivo de obtener beneficios de las mismas; esto trae consigo provocar daños económicos, manipular gestiones políticas o ambientales, generar pérdida económica y de información, difundir datos falsos en redes sociales u otros medios de comunicación y el dejar a los empresarios en un nivel bajo y de poca reputación.

Además, se dan muchos ataques de forma jerárquica, primero en empresas de tecnología y comunicaciones, después están las de comercialización de productos y servicios en grandes cantidades, le siguen las de manufactura y producción y por último las compañías financieras. Los atacantes se adaptan al uso de las nuevas tecnologías remodelando sus modos de actuación para filtrarse en los sistemas de las empresas sin importar su tamaño, país en el que se encuentren o a lo que se dediquen, si tienen lo que ellos quieren buscarán los medios para conseguirlo, pasar desapercibidos y así cumplir su objetivo, ya sea manipular la información o robarla, dañar los procesos que ahí se ejecutan, sustraer contraseñas o efectuar la manipulación completa de los sistemas, provocando el desprecio de una organización o país entero debido a su desequilibrio en su seguridad.

Reyes (2018) menciona que los países de donde se lanzan gran cantidad de ciberataques son: Reino Unido, Turquía, Francia, Alemania, Ucrania, Brasil, China, Rusia y Estados Unidos; México se posiciona como el país que más ciberataques recibe en el mundo, las empresas más atacadas son las que superan los 400 empleados, y los ataques más comunes se realizan mediante el internet a través de links maliciosos, correos electrónicos y SPAM como los principales.

De acuerdo con la Agencia AFP (2020), debido al covid-19 que se originó en China, los hackers han aprovechado el miedo de las personas para difundir virus informático de manera sofisticada por correo electrónico, generando el phishing para luego producir una estafa, todos los países que han sido infectados por el coronavirus están atravesando por esto y el trabajo en línea es una situación perfecta para que los hackers puedan sustraer información, por otro lado crean publicidad engañosa o links en donde ofrecen vacunas o medicamentos falsos que supuestamente curan el coronavirus, con el fin de obtener datos personales y así poder robar su dinero; esto se ha convertido en una amenaza mundial.

Como lo hace notar la BBC News Mundo (2019), el Ecuador sufrió el peor ciberataque en el año 2019 por la filtración de datos de millones de personas. Integrantes informáticos de vpnMentor descubrieron este hecho tras indagar y llegar a descubrir que los datos de los ecuatorianos se encontraban en un servidor muy inseguro de Novaestrat en Miami- Florida; allí estaba información de niños, jóvenes, adultos, mayores y hasta de personas ya fallecidas. En el servidor se encontraba información que se sustrajo de los Registros Civiles del gobierno ecuatoriano, Asociación de Empresas Automotrices del Ecuador (AEDE) e información del BIESS.

Como expresa el diario El Comercio (2019) los datos se encuentran a la vista de todos y muy pronto en manos equivocadas, esta filtración trae consigo varias consecuencias como es la estafa, fraudes monetarios a los ciudadanos, el despojo de bienes y la más impactante que es el robo o suplantación de identidad entre los más comunes.

AETecno (2019) manifiesta que, Ecuador es el noveno país con ciberataques en Latinoamérica y el Caribe, y recibió más de 40 millones de ataques tras el retiro del asilo político de Julián Assange, por otra parte, El Comercio (2021) afirma que el incremento de la tecnología en la época de pandemia, ha convertido al cibercrimen en un negocio multimillonario, a esto le favorece la escasez de personal capacitado, el exceso de programadores y muy pocos profesionales en el área de seguridades, excluir la asignación de presupuesto para el tema seguridades y no contar con requerimientos tecnológicos necesarios para la protección de los sistemas.

La provincia del Carchi tiene un incremento en el uso de las “Tecnologías de la Información y Comunicación -TIC” por parte de sus habitantes, mismas que les permite administrar su información, lo digital está más presente en la vida de los Carchenses al igual que los ataques cibernéticos que cada vez buscan contraer información delicada de personas y entidades, para lograr fines que perjudican o ponen en peligro el prestigio de las mismas.

En la provincia se está incrementando el uso de las redes como un medio útil y fundamental para las labores en unidades educativas, gobiernos seccionales, entidades financieras y empresas dedicadas a la comercialización de un producto o servicio; mismas que son propensas a ser vulneradas por personas maliciosas con el fin de infiltrarse en sus sistemas y perjudicarles.

1.2. FORMULACIÓN DEL PROBLEMA

El débil reporte y seguimiento a incidentes informáticos produce inseguridad de la información en unidades educativas y gobiernos seccionales de la provincia del Carchi, lo que genera vulnerabilidad de la información en el año 2020.

1.3. JUSTIFICACIÓN

Un "Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT" aumentará la capacidad de mitigación y eliminación de eventos indeseados o inesperados que atentan contra las actividades de las organizaciones, seguridad de la información digital y sus equipos. Además, brindará servicios proactivos tales como el manejo de alertas y advertencias, mejoras de la calidad en concientización y educación sobre las mejores prácticas de políticas y normas permitiendo anticiparse ante ciertas amenazas; y reactivos mediante reporte, análisis y manejo de incidentes proporcionando una actuación inmediata y así evitar que terceras personas logren su objetivo.

El CSIRT estará orientado al sector académico como son las unidades educativas y al sector gubernamental en municipios y gobierno provincial de la provincia del Carchi que cuenten con una red establecida para ayudar en la protección de su información, infraestructura y generando una mayor disponibilidad de sus sistemas.

Se constituirá en el laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi, mismo que se encargará de recomendar soluciones temporales o definitivas en caso de presentar daños en los sistemas del sector académico y gubernamental , se tendrá un sitio web para brindar información sobre : los servicios, tendencias y mejores prácticas tecnológicas, información de medios de contacto con el equipo, además contará con un formulario para el reporte de incidentes informáticos para solicitar asistencia.

Estará conformado por personal que se encargará de llevar planificaciones estratégicas, monitoreo, análisis y gestión de incidentes, operaciones de alertas y advertencias, gestionar el sitio web, manejo de comunicados, configuración y mantenimiento de la seguridad, desarrollo de herramientas y capacitación a los miembros del CSIRT.

La presente investigación ayudará a contrarrestar o mitigar incidentes informáticos del sector académico y gubernamental de la provincia del Carchi, para que docentes, personal administrativo y estudiantes puedan realizar sus actividades diarias de forma segura y eficiente en el manejo de su información; además en el sector gubernamental permitirá mejorar la calidad en sus servicios de manera confiable y segura para sus habitantes.

Quiñonez (2019) informa que el uso de la tecnología va creciendo y volviéndose muy útil en la vida cotidiana de las personas, por otra parte, las amenazas y vulnerabilidades van aumentando, creándose y adaptándose a las circunstancias en las que se encuentre una provincia, país, continente o mundo entero. Ecuador ha aumentado un 70 % en delitos y estafas durante el confinamiento debido al COVID-19, los principales delitos se basan en la compra de medicina o material sanitario por redes sociales o sitios web, por ello, se han dado numerosos reportes sobre fraudes de compras que han realizado pero que nunca llegaron.

Durante el confinamiento de marzo hasta mayo de 2020 existen 209 investigaciones por estafa, según el Código Integral Penal sancionan a los estafadores con prisión de 3 a 5 años de cárcel por delito informático. El fin de crear un equipo de respuesta a incidentes contribuirá con la reducción de problemas informáticos como el anterior, brindando educación acerca de la seguridad en las redes y como aplicar las respectivas políticas de seguridad para proteger su información.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo general

Diagnosticar el adecuado proceso de solución a incidentes informáticos por parte de la Universidad Politécnica Estatal del Carchi para la seguridad de la información.

1.4.2. Objetivos específicos

- Fundamentar bibliográficamente el reporte y seguimiento a incidentes informáticos, seguridad de la información para la sustentación del proyecto.
- Identificar el correcto reporte y seguimiento a incidentes informáticos en la Universidad Politécnica Estatal del Carchi para el desempeño de un Equipo de Respuesta ante Incidencias de Seguridad Informática CSIRT.
- Determinar la seguridad de la información requerida por las organizaciones para la integridad de los datos.
- Implementar un Equipo de Respuesta ante Incidentes Informáticos CSIRT en la Universidad Politécnica Estatal del Carchi.

1.4.3. Preguntas de investigación

- ¿Por qué es necesario un “Equipo de Respuesta ante Incidentes de Seguridad Informática - CSIRT”?

- ¿Qué es el reporte y seguimiento a incidentes informáticos?
- ¿Cómo se efectúa el reporte y seguimiento a incidentes informáticos para asegurar la información en unidades educativas y gobiernos seccionales?
- ¿Cómo se manejan los incidentes informáticos y la protección de la información en la Universidad Politécnica Estatal del Carchi?
- ¿Cómo actúa un "Equipo de Respuesta ante Incidentes de Seguridad Informática - CSIRT"?
- ¿Qué políticas o normativas permiten la protección e integridad de los datos?
- ¿Cuáles son los servicios de un CSIRT que requieren las unidades educativas y gobiernos seccionales de la provincia del Carchi?
- ¿Cómo implementar un" Equipo de Respuesta ante Incidentes de Seguridad Informática - CSIRT"?
- ¿Qué recursos se necesitan para la implementación de un CSIRT en la Universidad Politécnica Estatal del Carchi?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

En la "Universidad Nacional Abierta y a Distancia de Bogotá DC – Cundinamarca" llevaron a cabo el desarrollo de la "Propuesta de los documentos para la creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA ". Investigación que permitió a la empresa socializar con otros equipos de Colombia para el desarrollo de habilidades en delitos informáticos y generar habilidades de investigación y análisis para ganar más experiencia.

Dentro de la documentación para la creación de un CSIRT se menciona su orientación hacia las entidades del sector empresarial y accionista para generarles beneficios como dar respuestas eficientes con la protección requerida, elevar el proceso de conocimientos para realizar un trabajo optimo, ser portavoces de la seguridad informática y demostrar responsabilidad con los miembros del CSIRT generando confianza.

Se menciona la evolución de equipos de respuesta ante incidentes informáticos, donde su origen fue en la Universidad de Carnegie Mellon de Pensilvania el 2 de noviembre de 1988 con la finalidad de combatir el Morris o gusano de internet; el primer equipo CSIRT que conformó Latinoamérica fue en los años 90 y estaba enfocado al sector empresarial. Se considera el impacto de un equipo CSIRT como elemental para enfrentarse a ciberdelincuentes con procedimientos reactivos y proactivos de la información digital y equipos para las organizaciones logrando disminuir considerablemente los ataques.

Un CSIRT siempre cuenta con apoyo normativo como parte del funcionamiento y que genera confianza para sus miembros; estas normativas son las ISO 27037 orientada a la administración de incidentes , ISO 27001 orientada a la seguridad informática con prevención y mitigación de riesgos, ISO 27002 enfocada en la incrementación de seguridad de los gastos y equipos gracias a una serie de controles y la normativa Magerit V3 como metodología para el reconocimiento de vulnerabilidades, mitigar o evitar riesgos y generar procedimientos para asegurar la información (Cano, 2020).

La presente investigación plantea la propuesta de un "Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT en la Universidad de las Fuerzas Armadas ESPE en Sangolquí" para recibir alertas y dar el respectivo procedimiento al solucionar o frenar ataques que se puedan dar u ocasionar. Surge el compromiso educativo de mantener los servidores activos y

disponibles para dar una atención de calidad y confianza a las entidades para las que se crea dicho equipo.

La institución brinda servicios a sus miembros y personas externas a ella que visitan sus sistemas y sitios web, por ello, la universidad también está expuesta a posibles ataques a su sistema por el uso incorrecto de políticas de seguridad o escaso mantenimiento de sus sistemas, además, la institución no dispone de un área establecida para la colaboración con la creación de nuevas políticas de seguridad y ayuda con los reportes, mitigación y seguimiento a incidentes informáticos.

Es de gran importancia consolidar un CSIRT, mismo que asuma el desarrollo y cumplimiento de actividades proactivas y reactivas, además de formar relaciones con otros equipos de respuesta y así contribuir en la mejora de la protección de los datos de la universidad. La implementación de un equipo resulta muy compleja por su alojamiento y ubicación, pero que a la final termina siendo de gran beneficio para todas las entidades del sector académico no importa si esta es pública o privada (De La Torre & Parra, 2018).

La investigación denominada "Implementación de un equipo de respuesta ante incidentes de seguridad informática CSIRT para la Universidad Regional Autónoma de los Andes UNIANDES" en Ambato, permite la actuación inmediata ante amenazas al sistema. La institución requiere de un área especializada que brinde un constante monitoreo para evitar o mitigar ataques y ejecutar el correcto procedimiento para dar soluciones.

La modalidad utilizada es cualitativa, cuantitativa y mixta para el desarrollo de los procesos y las normas de seguridad que adoptó la universidad; además su tipo de investigación es bibliográfica documental ya que se requiere de bases fundamentales y esenciales de autores que se han enfocado al mismo tema y así sustentar la investigación con hechos para el problema.

Se basa en el método inductivo- deductivo porque primero se obtuvo fuentes e investigaciones generales con respecto al tema y que al final se llegará al tipo de conocimientos en procesos a seguir y reglas a cumplir para la implementación de un CSIRT; por otra parte, la tesis concluye en que la implementación de un CSIRT aporta en el beneficio de la seguridad de los datos de la "UNIANDES", también trae un gran beneficio el prototipo de aplicación web para reforzar la seguridad del sistema universitario que se encuentra en constante movimiento a través de la red.

Se da a conocer la propuesta en el diseño y funcionamiento para el área CSIRT y conformación del personal en donde, se designa espacios para la gestión de los servicios proactivos y reactivos, área de documentación y evidencias, servicios compartidos (impresiones y

archivadores de evidencia), sala de reuniones y el manejo de un sistema de detección de incendios. En cuanto al personal se menciona al director general quien debe demostrar liderazgo, motivación y ser capaz de adentrarse en cada una de las labores de los integrantes de trabajo para apoyarlos en su rendimiento; además mencionan a los asesores quienes son los colaboradores en la investigación y solución ante ciertas vulnerabilidades (Palacios, 2018).

El proyecto "Análisis y gestión de la seguridad en la red del GAD Municipal de Rioverde mediante el diseño de un equipo de respuesta a incidentes de seguridad informática CSIRT", aporta al sector gubernamental, generan informes del estado en el que se encontraba la red y las normas y estándares aplicados en su sistema. Para empezar con el desarrollo de un CSIRT, lo principal es el análisis de su infraestructura como: el estado de los servidores, cableado y su distribución y sistemas integrados; aquello es fundamental para la identificación de anomalías detectadas y que pueden o estarían provocando ciertas vulnerabilidades.

Lo siguiente es investigar sobre los CSIRT, para determinar su tipo y en qué aspectos contribuirá con la integridad de los datos, en este caso del municipio es recomendable adelantarse en el diseño, conformación del personal y los servicios que se prestará. Los municipios siempre cuentan con información delicada y si su red se la está usando de manera inadecuada, en cualquier instante esta podría sufrir un ataque.

La creación del equipo es con el fin de ayudar o contribuir con la protección de la información comercial y administrativa, de esta manera se procederá a dar un plan de contingencia para mitigar e indicar al personal institucional ciertas recomendaciones y que hacer en caso de presentar algún ataque. La presente tesis concluye que cierto personal a cargo del área de sistemas no está capacitado para gestionar la información y protegerla como es debido; por otro lado, el personal se involucra en todas las áreas de mantenimiento de la red y los datos que ahí procesan, por lo que las tareas no tienen lógica de resultado, carecen de coherencia y no son efectuadas de la manera correcta en caso de realizar mantenimiento, mitigación o detener un ataque (Quiroz, 2017).

2.2. MARCO TEÓRICO

2.2.1. Equipo de respuesta ante incidentes informáticos (CSIRT)

La "Organización de los Estados Americanos OEA (2016)" menciona que un equipo de respuesta a incidentes informáticos, es una organización o grupo de personas que brindan servicios en el área de gestión de incidentes en seguridad informática a entidades o comunidades objetivo en general (p.3).

Se acoge la mención de la "Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia CEDIA (2020)", donde menciona que se trata de un equipo orientado a recibir reportes de incidentes que ponen en peligro los sistemas e información de una entidad. Se encarga del análisis de vulnerabilidades encontradas para posteriormente ayudar con el problema o dar una recomendación, permitiendo mejorar la seguridad de la información al igual que sus redes. En la tabla 1 se menciona los acrónimos con los que se identifica un CSIRT.

Tabla 1. Abreviaturas de CSIRTs

Abreviaturas	**Nombre**
CIRT	"Equipo de Respuesta a Incidentes Informáticos o Equipos Cibernéticos"
CERT	"Equipo de Respuesta ante Emergencias Informáticas o Equipos Cibernéticos"
CIRC	"Capacidad de Respuesta a Incidentes Informáticos o Equipo Cibernético"
CERC	"Capacidad de Respuesta de Emergencia Cibernética o Informática"
SIRT	"Equipo de Respuesta a Incidentes de Seguridad"
SERT	"Equipo de Respuesta a Emergencias de Seguridad"
SIRC	"Capacidad de Respuesta a Incidentes de Seguridad"
SERC	"Capacidad de Respuesta a Emergencias de Seguridad"
IRT	"Equipo de Respuesta a Incidentes"
ERT	"Equipo de Respuesta de Emergencia"
IRC	"Capacidad de Respuesta a Incidentes"
ERC	"Capacidad de Respuesta a Emergencias"
CSIRT	"Equipo de Respuesta ante Incidentes de Seguridad Informática"

La tabla 1 muestra los acrónimos que usan los CSIRTs. Adaptado del proyecto de investigación "Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad De Las Fuerzas Armadas ESPE", De La Torre & Parra, 2018.

Con las investigaciones sobre la definición de la primera variable, se establece el uso del acrónimo "CSIRT" para mencionar el equipo de respuesta desarrollado en la Universidad Politécnica Estatal del Carchi.

2.2.2. Servicios de un CSIRT

Como parte del establecimiento de un CSIRT, Van Der Heide (2020**)** menciona que existen muchos servicios que se puede brindar a una organización, pero se puede empezar con dos o

tres servicios para el inicio de sus actividades y es obvio que los servicios que no deben faltar son el manejo de incidentes y anuncios.

Hurtado & Chuquiguanca (2020) mencionan que la determinación de los servicios se los brinda de acuerdo a los requerimientos de las instituciones, propósito y misión como equipo, esto incluye su ámbito de seguridad física y lógica, por lo que, para el inicio de sus operaciones, los autores determinan los servicios de monitoreo y detección, análisis y gestión de incidentes, análisis de vulnerabilidades y concientización tecnológica para iniciar con sus operaciones.

2.2.2.1. Servicios proactivos

Los servicios proactivos se orientan a la implementación de mejoras a los procesos que se realizan, así como también a la infraestructura que permite el manejo de la información de los miembros del CSIRT, dichas actividades se las realiza antes de que se presenten incidentes informáticos que atenten con la organización (Van Der Heide, 2020).

Los principales servicios son:

- Anuncios

  El CSIRT mediante su sistema web provee información actual y verificada sobre tendencias informáticas, herramientas, procedimientos y otros sobre seguridad informática, nuevas vulnerabilidades encontradas en los sistemas, soluciones para mitigar los problemas de una forma comprensiva y de fácil acceso para sus miembros. Dicha información puede ser compartida mediante manuales, afiches, archivos y anuncios. Permitiendo a los miembros corregir y proteger sus sistemas con antelación y estar preparados antes de que puedan ser atacados.

- Vigilancia tecnológica

  El CSIRT está a la vanguardia sobre los nuevos desarrollos tecnológicos, tendencias y actividades que se relacionen con la tecnología, seguridad informática, ataques cibernéticos, entre otros, dichas actividades las realiza con el fin de identificar posibles vulnerabilidades y amenazas que atenten contra los sistemas informáticos pertenecientes a los miembros del CSIRT.

- Evaluaciones de seguridad

  Ofrece la revisión y análisis detallada de la infraestructura y sistemas basándose en las peticiones o lineamientos dados por la organización, además incluyen evaluaciones prácticas en la seguridad.

- Revisión de mejores prácticas

  Determina el correcto uso de políticas de seguridad acorde a la razón de la empresa y los estándares que maneje. Esto es posible con entrevistas dirigidas a los encargados del departamento técnico y autoridades de la organización para determinar si las políticas se cumplen y son adecuadas para la entidad.
- Escaneos

  Se determina que sistemas o redes están vulnerables, con fallos en el hardware o software, con virus o intrusos ingresados anónimamente por medio de escáner. Además, se realizan pruebas de penetración que consisten en atacar el sistema de la organización para detectar las vulnerabilidades. Esto se le puede realizar con la aprobación de los encargados del sistema.
- Configuración de herramientas de seguridad, aplicaciones, infraestructuras y servicios

  El CSIRT proporciona a sus miembros manuales o guías sobre las adecuadas configuraciones, actualizaciones, mantenimiento y mejores prácticas para mantener los equipos, aplicaciones, infraestructura y servicios de forma segura.

2.2.2.2. Servicios reactivos

Orientados a brindar apoyo a entidades que están sufriendo amenazas o ataques por terceras personas mediante la aplicación de ciertos procesos que ayudan a que dichas personas no cumplan con su objetivo (Van Der Heide, 2020).

Se dan los siguientes servicios:

- Alertas y avisos

  Busca distribuir contenidos en el que se explique sobre los ataques y vulnerabilidades dentro de las organizaciones, brindando ciertas recomendaciones que deben ser tomadas a corto o largo plazo; además dicho contenido podrá ser compartido con otros CSIRT que estén enfocados a dar sus servicios a la misma entidad o entidades.
- Manejo de incidencias

  La respuesta al incidente se puede presentar en dos formas, la in-situ que trata del análisis presencial de la información y equipos afectados, y se da recomendaciones en el lugar de los hechos y la respuesta de forma remota que provee apoyo vía telefónica, correo electrónico u otros medios de comunicación.

  El equipo realiza el análisis del incidente, que consiste en la recolección de evidencia, revisar y examinar la información generada de la infraestructura y sistemas que fueron

afectados, con el fin de evaluar el alcance y hasta donde o que parte el intruso pudo cumplir con su objetivo.

Al momento de la coordinación se destacan aspectos fundamentales como es el apoyo por parte de uno o más miembros del equipo para poder ayudar en la mitigación del incidente, pedir apoyo a otros equipos que están enfocados en la misma área y compartir recomendaciones de seguridad, después el equipo CSIRT proveerá la ayuda necesaria de manera más eficiente y puntual.

- Análisis de vulnerabilidades

  El equipo se encarga de realizar un examen y análisis de las vulnerabilidades en hardware y software y así determinar comportamientos sospechosos en los sistemas, en ciertos casos es necesario revisar códigos fuente mediante el uso de software, para determinar el verdadero problema y así prevenir incidentes, proporciona recomendaciones u otros criterios de solución.

2.2.2.3. Servicios en mejoras de la calidad

Orientados en la retroalimentación de conocimientos adquiridos como resultado de la experiencia en el área de respuesta a incidentes (Van Der Heide, 2020).

Se dan grandes beneficios al proporcionar los servicios en gestión de calidad para la seguridad:

- Análisis de riesgos

  El equipo realiza la valoración y análisis de riesgos de la infraestructura y sistemas de gestión, permitiendo tomar acciones para el manejo de vulnerabilidades.

- Continuidad del negocio

  De acuerdo a la planificación para tratar incidentes y dar recomendaciones para evitarlos y mejorar el modo de respuesta a las organizaciones, busca mantener un gran porcentaje de funcionamiento de las operaciones, su continuidad y modo de restauración de las actividades frente a vulnerabilidades y ataques.

- Consultoría en seguridad

  Provee y ayuda con guías para mejorar la aplicación y desarrollo de políticas de seguridad, instalación y configuración adecuada de nuevos sistemas, software, dispositivos de red y gestiones de negocio para las organizaciones.

- Concientización tecnológica

  El CSIRT determina donde se necesita mayor información y apoyo para realizar buenas prácticas en políticas de seguridad informática y procesos operacionales, aportando en

la mejora constante de las actividades, capacidad en detección de fallas o ataques, acelerando el modo de recuperación de las operaciones y minimizando daños.

- Capacitación y entrenamiento

  El equipo provee capacitaciones sobre los incidentes o vulnerabilidades actuales a través de reuniones, cursos, talleres o tutoriales que aporten en el desarrollo de acciones de respuesta, procesos de mitigación, modos de prevención y cómo actuar ante reportes y respuestas a incidentes de seguridad informática.

- Evaluación o certificación de productos

  Se evalúa herramientas, aplicaciones, software u otros servicios que requiera la organización para determinar su seguridad; su evaluación se realiza en softwares u otras herramientas de evaluación que detallan y proporcionan características y funcionamiento para determinar si es apto y congenia con normas y políticas que aplica la organización.

Los CSIRTs adquieren los servicios para sus operaciones de acuerdo al tipo de institución a la que se orienten y los que resulten principales para iniciar las actividades, por lo tanto, el proyecto de investigación selecciona la el manejo de incidentes y alertas – avisos para los servicios reactivos, la publicación de anuncios como servicio proactivo, y concientización tecnológica como aporte al servicio de mejoras de la calidad para unidades educativas y gobiernos seccionales de la provincia del Carchi.

2.2.3. Tipos de CSIRT

En el establecimiento de un CSIRT, Van Der Heide (2020) menciona que existen equipos de respuesta a incidentes para organizaciones de tipo: académico, comercial, sector púbico, militar, nacionales, de pequeñas y medianas empresas, proveedores, gubernamental y de infraestructuras críticas.

2.2.3.1. CSIRT académico

Enfocado en brindar ayuda a unidades educativas y universidades públicas y privadas, institutos, centros estudiantiles de investigación o cualquier otra organización que se dedique a la educación. Se basa en aportar recomendaciones que permitan aumentar la seguridad de la información e infraestructura. Además de forjar el interés por la investigación en la seguridad de la información (Van Der Heide, 2020).

Tabla 2. CSIRTs del sector académico en Ecuador

Nombre	Descripción
CSIRT CEDIA	"Equipo de Respuesta a Incidentes de Seguridad Informática de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia".
CSIRT UTPL	"Equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Técnica Particular de Loja".
CSIRT-EPN	"Centro de respuesta a incidentes informáticos de la Escuela Politécnica Nacional".

La tabla 2 muestra el listado de los equipos CSIRTs académicos registrados por CEDIA. Adaptado de "Proyecto-Listado de CSIRTs del Ecuador" de CEDIA, 2020.

El proyecto de investigación se enfoca en el presente ámbito para la creación del equipo CSIRT que ayude a unidades educativas de la provincia del Carchi que cuenten con una red establecida. Listado de las unidades educativas de la provincia del Carchi:

Tabla 3. Lista de unidades educativas del distrito de educación 04D01 Tulcán - San Pedro de Huaca

Institución	Dirección de sitio web
"Unidad Educativa Huaca"	No identificado
"Unidad Educativa Santa Mariana De Jesús"	No identificado
"Unidad Educativa Mariscal Sucre"	No identificado
"Unidad Educativa Isaac Acosta Calderón"	No identificado
"Unidad Educativa Consejo Provincial Del Carchi"	No identificado
"Unidad Educativa Vicente Fierro"	https://vicentefierro.edu.ec/
"Unidad Educativa Tulcán"	http://uetulcan.edu.ec/
"Unidad Educativa San Antonio De Padua"	https://www.sanantoniodepaduatulcan.edu.ec/
"Unidad Educativa Municipal 1ro De Mayo PCEI"	No identificado
"Unidad Educativa Fiscomisional Monseñor Leonidas Proaño PCEI"	No identificado

“Unidad Educativa Hermano Miguel La Salle"	http://www.lasalletulcan.org/
“Unidad Educativa Sagrado Corazón De Jesús”	http://www.bethlemitastulcan.com/
“Unidad Educativa Bolívar”	http://carchidigital.com/bolivar/index.php
“Unidad Educativa Fiscal Coronel Luciano Coral Morillo"	No identificado
“Unidad Educativa Del Milenio Carlos Romo Dávila”	No identificado
“Unidad Educativa El Carmelo”	No identificado
“Unidad Educativa César Antonio Mosquera”	No identificado
“CECIB Juan Bautista Aguirre”	No identificado
“Unidad Educativa Ecuador”	No identificado
“Unidad Educativa Maldonado”	No identificado

Tabla 4. Lista de unidades educativas del Distrito 04D02 Montúfar – Bolívar

Institución	**Dirección de sitio web**
“Unidad Educativa Los Andes”	No identificado
“Unidad Educativa General Julio Andrade”	No identificado
“Unidad Educativa Del Milenio San Gabriel De Piquiucho”	No identificado
“Unidad Educativa Medalla Milagrosa”	No identificado
“Unidad Educativa Monte Olivo”	No identificado
“Unidad Educativa Carlos Montúfar”	https://sites.google.com/view/uecarlosmontufar/p%C3%A1gina-principal
“Unidad Educativa García Moreno”	No identificado
“Unidad Educativa Pusir Grande”	No identificado
“Unidad Educativa San Vicente”	No identificado
“Unidad Educativa Jorge Martínez Acosta”	No identificado

“Unidad Educativa José Julián Andrade”	http://jjandrade.edu.ec/saaminet/web/site/
“Unidad Educativa Pablo Muñoz Vega”	https://uepamve.webnode.es/
“Unidad Educativa Pio XII”	No identificado
“Unidad Educativa Mario Oña Perdomo”	No identificado
“Unidad Educativa Cristóbal Colón”	No identificado
“Unidad Educativa Piartal”	No identificado
“Unidad Educativa La Paz”	No identificado

Tabla 5. Lista de unidades educativas Distrito 04D03 Mira – Espejo

Institución	**Dirección del sitio web**
“Unidad Educativa Libertad”	No identificado
“Unidad Educativa Alfonso Herrera”	No identificado
“Unidad Educativa El Ángel”	No identificado
“Unidad Educativa San Isidro”	No identificado
“Unidad Educativa Eugenio Espejo”	https://ueee.education/index.html
“Unidad Educativa 19 De Noviembre”	No identificado
“Unidad Educativa Juan Montalvo”	https://uejmcarchi.jimdosite.com/
“Unidad Educativa Carlos Martínez Acosta”	No identificado
“Unidad Educativa León Ruales”	No identificado
“Unidad Educativa Especializada Manuela Espejo”	No identificado

De acuerdo con el artículo científico de Hidalgo (2017), al menos el 50% de estudiantes de la ciudad de Tulcán, disponen de un teléfono inteligente para recibir clases, redes sociales, video juegos e ingresar a video conferencias, por ello, el uso de internet se ha incrementado un 9,1 % en zonas rurales y un 37% en zonas urbanas. Docentes necesitan capacitaciones en el uso de las TICs porque realizan operaciones con información educativa, además, servirá de interés por adquirir herramientas que contribuyan a su desempeño laboral.

Se acoge la importancia del uso de las tecnologías como un aporte fundamental para el aprendizaje, y con ello también se presenta el incremento de vulnerabilidades e incidentes de los sistemas. El presente proyecto brinda sus servicios al sector académico de la provincia del Carchi, porque están en constante incremento de aplicación de la tecnología para sus

actividades, se apoya con buenas prácticas y concientización tecnológica para el correcto uso de sus sistemas, siempre con el objetivo de cuidar su información.

2.2.3.2. CSIRT comercial

Enfocado en brindar apoyo en la seguridad de la información e infraestructuras a una persona o grupo de personas dedicadas al comercio nacional e internacional (Murquincho, 2019).

Tabla 6. CSIRTs del sector comercial en Ecuador

Nombre	**Descripción**
Blue Hat CERT	"Equipo de respuesta a incidentes de seguridad cibernética de Blue Hat".
CERT Radical	"Empresa especializada en brindar soluciones de Ciberseguridad e Infraestructura".
CSIRT-GMS	"Equipo de respuesta para Clientes GMS y partners de Seguridad de la Información".
CNT - Grupo de Ciberseguridad	"Servicios convergentes de telecomunicaciones y TICs".
CSIRT Telconet	"Centro de Respuesta a Incidentes de Ciberseguridad de Telconet".
CSIRT Telefónica Ecuador	"Equipo de Respuesta a Incidentes de Seguridad (CSIRT) Global Telefónica".
DataProtect CSIRT	"Servicios de alerta y respuesta a incidentes para diferentes tipos de clientes, así como para el público en EMEA. (Europa, Oriente Medio y África)".
MAINTLATAM CSIRT	"Equipo de Respuesta ante Incidentes de Seguridad, responsable del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad".
NodoVIP CSIRT	"Equipo de respuesta a incidentes informáticos para clientes privados de servicios NodoVIP".
PUNTONET CSIRT	"Equipo de respuestas a incidentes de seguridad informática PuntoNet".

SECURITYLOGIC	“Empresa Especializada en Consultoría, Diseño, Implantación y Gestión de Soluciones de Seguridad Informática y de Comunicación”.
SSCorp-CSIRT	“Equipo de respuesta a incidentes de seguridad informática de SecureSoftCorp”.

La tabla 6 muestra el listado de los equipos CSIRT comerciales registrados por CSIRT CEDIA. Adaptado de "Proyecto- Listado de CSIRTs del Ecuador" de CEDIA, 2020.

2.2.3.3. CSIRT de sector público

Enfocado en la prestación de servicios para agencias públicas y ciudadanos en general.

2.2.3.4. CSIRT de sector militar

Brinda sus servicios a todo tipo de institución militar que trabajan en la protección de la información con ejecución de actividades cibernéticas. Ayudan a resolver problemas de seguridad en información digital y equipos de uso militar.

Tabla 7. CSIRT del sector militar en Ecuador

Nombre	**Descripción**
CSIRT FFAA	“Centro de Respuesta a Incidentes de Seguridad Cibernética del Ecuador”.

La tabla 7 muestra el CSIRT de sector militar registrado por CEDIA. Adaptado de "Proyecto- Listado de CSIRTs del Ecuador" de CEDIA, 2020.

2.2.3.5. CSIRT nacionales

Equipos conformados dentro del país, orientados en la prestación de servicios para diferentes organizaciones nacionales y que resultan de gran apoyo para la protección de los sistemas en hardware y software.

Tabla 8. CSIRTS nacionales de Sudamérica

País	**Nombre CSIRT**
Panamá	CSIRT – Panamá
Venezuela	VenCERT
Ecuador	EcuCERT

Perú	PeCERT
Brasil	CERT.Br
Bolivia	CERT-BO
Paraguay	CERT-Py
Uruguay	CERTuy
Argentina	ICIC-CERT
Chile	ORT-CL
Guyana	CSIRT.GY
Suriname	OIC_CERT

2.2.3.6. CSIRT de pequeñas y medianas empresas

Presta servicios a las empresas que debido a su tamaño o naturaleza les resulta difícil conformar su propio CSIRT. Es por ello que se crean estos equipos con el fin de aportar con servicios dirigidos a la protección de sistemas e información, de esta manera podrán solicitar ciertas peticiones para mejorar su sistema informático.

2.2.3.7. CSIRT de proveedores

Son equipos que prestan sus servicios a fabricantes de productos específicos con el propósito de proteger la información y mitigar los riesgos que tengan relación con los productos y su distribución.

2.2.3.8. CSIRT gubernamental

Equipos que brindan servicios para que la infraestructura en telecomunicaciones y servicios del gobierno que brindan a la ciudadanía sean seguros, confiables y se encuentren disponibles. Funcionan de manera dependiente o independiente, unen criterios y conocimientos a los diferentes sistemas del estado ubicados en todas las provincias y colaboran en la resolución de incidentes. El proyecto de investigación se enfocó en el presente ámbito para la creación de un CSIRT que ayude a los gobiernos seccionales presentes en la provincia del Carchi.

Tabla 9. Lista de los gobiernos seccionales de la provincia del Carchi

Institución	Dirección del sitio web
"Prefectura del Carchi"	https://carchi.gob.ec/2016f/
"Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar"	https://www.gadbolivar.gob.ec/
"Gobierno Autónomo Descentralizado Municipal de Espejo"	https://www.gadme.gob.ec/
"Gobierno Autónomo Descentralizado del Cantón Mira"	http://www.mira.gob.ec/
"Gobierno Autónomo Descentralizado Municipal de Montúfar"	http://www.gadmontufar.gob.ec/index.php
"Gobierno Autónomo Descentralizado Municipal San Pedro de Huaca"	https://www.gob.ec/gadmsph
"Gobierno Autónomo Descentralizado Municipal de Tulcán"	https://www.gob.ec/gadmt

2.2.3.9. CSIRT de infraestructuras críticas

Equipos encargados de proteger los datos, información delicada e infraestructura sin importar si la organización es pública o privada o a que se dedique (comercialización, transporte, comunicaciones, administración de empresas, fabricación, entre otras).

Tabla 10. CSIRTs del sector de infraestructuras críticas en Ecuador

Nombre	Descripción
CSIRT Energía	"Equipo de Respuesta para Recursos y Energía del Ecuador".
CSIRT CELEC EP	"Equipo Multidisciplinario de la Corporación Eléctrica del Ecuador CELEC-EP".

La tabla 10 muestra el listado de los equipos CSIRT orientados al sector de infraestructuras críticas registrados por CSIRT CEDIA. Adaptado de "Proyecto- Listado de CSIRTs del Ecuador", de CEDIA, 2020.

2.2.4. Beneficios de un CSIRT

Desde el criterio de Ramírez (2016), al contar con un CSIRT en una provincia, empresa o país y sin importar su tipo, los beneficios son los siguientes:

- Funciona como un equipó que genera recomendaciones para tratar incidentes informáticos y aspectos de seguridad.
- Concientiza sobre el uso de infraestructura y con las mejores prácticas en cuanto a prevención y mitigación de incidentes.
- Ofrece asesoramiento para el análisis de vulnerabilidades y protección de todas las actividades informáticas que están en constante funcionamiento.
- Contiene su sitio web que proporciona información sobre alertas, vulnerabilidades y formas de actuar para prevenir incidentes y en caso de presentarse mitigarlo y darle un correcto seguimiento.
- Realiza publicaciones y charlas efectivas sobre la seguridad de la información con el fin de concientizar sobre las buenas prácticas y aplicaciones de políticas, normativas, estándares y además dar recomendaciones de aplicación de nuevas tecnologías para el manejo y administración de la seguridad.
- Busca relacionarse con otros CSIRTs, para compartir información y ser partícipe de experiencias en el tratado de incidentes de seguridad informática.
- Entre equipos CSIRT establecen apoyo remoto y presencial constante con el fin de elaborar estrategias para la seguridad informática de manera más amplia.
- Brinda capacitaciones a otros CSIRT que requieren conocer más sobre la prevención y mitigación de incidentes, al igual que la aplicación de buenas prácticas de seguridad a los sistemas computacionales.
- Tienen a miembros del equipo preparándose constantemente para ayudar a las organizaciones con eficiencia y generando confianza sobre los servicios prestados.
- Crea material interesante sobre entrenamiento en seguridad informática para proporcionar a sus miembros por medio del sitio web o charlas presenciales.

Sin embargo, De La Torre & Parra (2018) mencionan que los beneficios de un CSIRT se constituyen en 3 aspectos:

- Económicos porque aporta en el correcto funcionamiento de los sistemas que operan las instituciones, evitando la pérdida de productividad por incidentes o vulnerabilidades
- De relaciones porque como equipo mantiene la responsabilidad de fomentar buenas prácticas y conocimientos a las instituciones, y aportando un buen servicio en la gestión de los servicios con el objetivo de ayudar a minimizar incidentes potenciales y lograr un cambio en un sector de la sociedad.

- Legales porque aporta con procesos o regulaciones del estado, gestionando aspectos normativos y legales para la protección de la información.

Ante lo expuesto anteriormente, el resultado del proyecto de investigación aporta en el ámbito social porque está orientado a unidades educativas y gobiernos seccionales de la provincia del Carchi, aporta en lo económico porque reduce incidentes en los sistemas de las instituciones al realizar concientización tecnológica, alertando de nuevos ataques informáticos, colaborando en la solución de incidentes y notificando de buenas prácticas para la seguridad de la información a través del sitio web del equipo, además, se rige por normativas y procesos que aportan en las operaciones y protección de la información que maneja el CSIRT.

2.2.5. Modelos organizacionales de un CSIRT

Se resalta el aporte de Van Der Heide (2020) porque menciona que la estructura organizacional se establece de acuerdo a la comunidad a la que se orienta y recursos tecnológicos y de infraestructura. Existe equipos nacionales localizados en organizaciones gubernamentales, mientras que los demás pueden asociarse con entidades comerciales, universidades o unidades de investigación.

Por otra parte, Quiroz (2017) mencionan que el modelo organizacional la define el equipo, su criterio le permite escoger por operar de manera independiente, asociarse o formarse dentro de una organización. De acuerdo a los resultados encontrados, se mencionan los modelos organizacionales que un CSIRT puede adoptar por elección o de acuerdo a la disponibilidad de recursos y comunidad objetivo:

2.2.5.1. Modelo de negocio independiente

El CSIRT se desarrolla como una organización independiente, manejando sus propias directrices, estructura, personal y equipo. Este modelo puede ser aplicado a los CSIRTs comerciales.

2.2.5.2. Modelo incrustado

Usualmente son colocados en el área de TI porque se relacionan perfectamente con la organización, ya que la ubicación del CSIRT debe ser la ideal para que los departamentos de la organización puedan estar contacto fácilmente y atender cualquier inconveniente o incidente. De acuerdo con la estructura organizacional se toman en cuenta los modelos del CSIRT:

- Centralizado
  El equipo CSIRT está conformado en la misma oficina.
- Distribuido
  Los miembros del equipo están ubicados en más de una oficina por lo que requieren más coordinación para trabajar.
- Distribución en zonas horarias
  Se considera un modelo de distribución avanzado porque las horas operacionales del equipo se mantienen, pero el mando es rotativo con otros equipos de otra provincia o país.

2.2.5.3. Modelo campus

Modelo usado por equipos de investigación y en ciertos casos las fuerzas armadas y pymes. Los miembros pueden o no tener un CSIRT propio debido al presupuesto tamaño, por lo que crean equipos pequeños o forman parte de un equipo central ya sea independiente o conformado dentro de una organización.

2.2.5.4. Modelo matricial

Combina las estructuras vertical y horizontal, comparte recursos de trabajo, mejora dudas y opera para organizaciones medianas.

2.2.5.5. Modelo voluntario

Conformado por un grupo de expertos que se reúnen de forma voluntaria para colaborar en gestión de incidentes y no dependen de ninguna organización, equipo o asociación, únicamente operan por motivación de los participantes.

2.2.5.6. Modelo hibrido

Se crea de acuerdo a productos - función y productos - geografía para otorgar diversos enfoques, funcionan en empresas que controlan productos o mercados, por lo que facilita la detección de fortalezas y debilidades.
Con el análisis de varias fuentes, y tomando a las anteriores como las principales, se acoge el modelo organizacional incrustado (centralizado) porque el CSIRT se conforma en el laboratorio de Ciberseguridad de la Carrera de Computación de la “Universidad Politécnica Estatal del

Carchi", por lo que dispone de recursos tecnológicos y docentes investigadores de la Carrera de Computación para el inicio de sus actividades.

2.2.6. Estructura organizacional de un CSIRT

Se toma en cuenta el aporte de la OEA (2016), porque explica que dependiendo del modelo organizacional del CSIRT, se determinan las funciones de cada área de trabajo y que deben ser ejecutadas por el personal designado, también incrementará su estructura organizacional conforme aumenten sus miembros y su gestión en servicios y manejo de incidentes.
Por otra parte, Van Der Heide (2020) explica que para la correcta gestión de operaciones del CSIRT, se debe tomar en cuenta la participación, apoyo y colaboración entre áreas. De acuerdo a los resultados encontrados, se mencionan las áreas o departamentos principales de un CSIRT para la gestión correcta de sus operaciones.

2.2.6.1. Dirección

Dentro de esta área el director gestiona las tareas de promoción y publicidad de los servicios, administración del presupuesto, vinculación con otros CSIRT, asociaciones para asesoría, supervisar el trabajo de cada área y determinar estrategias.

2.2.6.2. Operaciones

Se considera el centro crítico del equipo porque se trata los incidentes en base a las peticiones realizadas por las organizaciones, se los clasifican y se procede a brindar el servicio. Además, se monitorea dichos incidentes llevando un análisis de los mismos; los técnicos de esta área recibirán incrementos en incidentes conforme el CSIRT se dé a conocer.

2.2.6.3. TI.

Área que se encarga de la implementación y arreglo de la arquitectura CSIRT, control y manejo del servidor de correos, archivos y web. Gestionan los turnos y las revisiones del sistema, servidores y la red.

2.2.6.4. I&D.

Denominada "Área de Investigación y Desarrollo ", encargada de elaborar nuevas herramientas de seguridad, realizar cursos de formación e investigación de nuevas amenazas y seguridades. El personal debe empezar a trabajar conjuntamente con la implementación del CSIRT, ya que

se encargan en gran parte de la planificación y colaboración en la solución de problemas dentro de la organización. El I+D trabaja conjuntamente en colaboraciones con el área de TI.

2.2.6.5. Servicios de apoyo

Dentro de esta área se supervisa el ámbito jurídico, gestión publicitaria, la administración y finanzas, el marketing y comunicaciones. Estos servicios pueden formar parte del CSIRT o adquirirlos de manera externa.

Cada equipo debe constituir primero su modelo organizacional para posteriormente, constituir de manera correcta el tipo de estructura, la presente investigación establece la estructura organizacional del CSIRT con tres departamentos: dirección como departamento al frente en la toma de decisiones del equipo, TI para el manejo de los sistemas y que trabaja conjuntamente con el departamento de operaciones en la gestión de los servicios reactivos, proactivos y mejoras de la calidad.

2.2.7. Tamaño y cantidad de recursos humanos

La OEA (2016), menciona que el directo del equipo se encarga de contratar al personal con los conocimientos y habilidades para trabajar independientemente del cargo designado, ya que no es necesario que dedique el 100% a una sola actividad principalmente luego de consolidar el equipo. Muchos casos exitosos han iniciado con un director, un gerente TI y un líder en operaciones y otras funciones, modelo utilizado en la investigación; y a medida que el equipo sea reconocido, crecerá la gestión de incidentes y con ello el personal. Con la investigación de varias fuentes acerca de la constitución de un CSIRT, se estructura el tamaño y cantidad de recursos como un modelo referencial.

Tabla 11. Tamaño y cantidad de recursos humanos en fase inicial y madurez del CSIRT

Departamento	**Personal**	
	Inicios del CSIRT	**Madurez del CSIRT**
Dirección	- 1 director o un coordinador	- 1 director - 1 coordinador - 1 líder
Apoyo de TI	- 1 líder - 2 especialistas técnicos	- 2 especialistas técnicos (administrador de redes, administrador de sistemas)

Investigación y Desarrollo	- 1 líder - 1 especialista técnico	- 1 líder - 2 especialistas en seguridad (analista/investigador, custodio de registros)
Operaciones	- 1 líder - 1 especialista técnico	- 1 líder - 3 especialistas en incidentes (clasificación, triage, manejo)
Servicios de apoyo	- 1 abogado (apoyo legal) - 1 reportero (comunicaciones) - 1 analista financiero	- 1 abogado (apoyo legal) - 1 reportero (comunicaciones) - 1 analista

En la tabla 11 se muestra el modelo ejemplo para la constitución de los recursos humanos del CSIRT en su fase de constitución y madurez. Información extraída de "buenas prácticas CSIRT" de OEA, 2016.

2.2.8. Recursos tecnológicos de un CSIRT

Desde el punto de vista de Ramírez (2016), los recursos tecnológicos tienen un papel importante en el desarrollo de las actividades de un CSIRT, por lo que se debe adquirir los equipos, sistemas y recursos tecnológicos que sean necesarios, estos deben adquirir seguridades para la protección de la información y evitar incidentes se seguridad física y lógica. Se completa el análisis la lista de requerimientos tecnológicos con el trabajo de maestría de Hurtado & Chuquiguanca (2020) y el proyecto de investigación De La Torre & Parra (2018).

2.2.8.1. Sitio web público

Es considerado el contacto esencial que tiene el equipo CSIRT para dar a conocer su misión, visión, servicios que presta, información sobre incidentes que se dan en el día a día o vulnerabilidades más comunes. Además, presenta un formulario que les permitirá a sus miembros reportar un incidente informático y solicitar ayuda referente a ello, el sitio web debe cumplir con todas las medidas de seguridad.

2.2.8.2. Correo electrónico

Es muy importante para que los miembros del equipo CSIRT puedan emitir los respectivos informes de los incidentes tratados, también es un medio para el intercambio de documentación, para dar o recibir ayuda de otros equipos en el manejo de incidentes o ciertas vulnerabilidades

presentes en las organizaciones, también realiza la función de usar listas de correos con los miembros para emitir noticias acerca de temas de seguridad u otros temas afines a tecnologías de la información.

2.2.8.3. Teléfono

Es necesario contar con un teléfono como una fuente central de comunicación con las entidades que necesitan ayuda y que puedan ser atendidos sin ninguna restricción por el CSIRT. Además, funciona como un medio de comunicación para tratar incidentes o vulnerabilidades.

2.2.8.4. Herramientas de manejo de incidentes

Es muy importante el uso de herramientas que permitan llevar un registro de los procesos y acciones tomadas por el CSIRT ante incidentes informáticos.

2.2.8.5. Sistemas operativos

Existe una variedad de sistemas operativos como Microsoft Windows, GNU/Linux, OSX, Chrome OS, entre otros, cada uno de ellos con sus propias características. Se debe seleccionar un sistema operativo de acuerdo al tipo de red establecida, características de los equipos y la disponibilidad de recursos ya que algunos tienen licencia.

2.2.8.6. Respaldo de datos

El respaldo de datos se debe realizar periódicamente con los procesos y aprobaciones necesarias, esto permitirá regresar a la documentación original en caso de que el sistema tenga graves problemas. Se debe realizar el almacenamiento fuera del equipo y en cualquier medio como CD, DVD y discos duros; el respaldo a través de la nube no es recomendada porque la información se encontraría en manos de un tercero.

2.2.8.7. Herramientas forenses

Muy útil para la recuperación de datos como evidencia o en caso de fallas en los sistemas de las organizaciones, es uno de los servicios que los CSIRT brindan en el transcurso de la ampliación de los mismos.

2.2.8.8. Servidor DNS

Es un sistema de nombre de dominio conformado por computadoras y recursos conectados a una red privada o a la internet para localizar y dirigir peticiones.

2.2.8.9. Tecnologías de acceso remoto

Mediante el acceso remoto, el CSIRT puede administrar o brindar los servicios a sus organizaciones. Por ello, se puede hacer uso de las tecnologías como telnet o SSH para la administración remota.

2.2.8.10. Caja fuerte

Se trata de una caja elaborada con metal y que contiene una combinación para que solo él o las personas autorizadas, puedan acceder a información de vital importancia que allí se resguarda como documentos, USBs, discos, CDs o DVDs con información extremadamente sensibles, firmas, tratados, entre otros.

2.2.8.11. Firmas electrónicas

Se trata de un método de cifrado que reconoce la identidad de una persona, usado para gestionar y asegurar la integridad de mensajes y documentos que se envían o reciben a través de la red.

2.2.8.12. Conexión a internet

Al tener una conexión a internet el equipo puede gestionar incidentes e información del sitio web, la velocidad de conexión dependerá de los requerimientos del equipo para realizar sus operaciones.

2.2.8.13. Sistemas SIEM

Gestión de Evento e Información de Seguridad, es una herramienta que monitorea aspectos de seguridad que se relacionan con las TI de la organización y analiza los sucesos de seguridad de varias fuentes.

La presente investigación establece la creación de un sitio web desarrollado en el sistema operativo CentOS y un servidor de monitoreo con el sistema operativo Kali Linux, los dos alojados en el servidor del laboratorio de Ciberseguridad. Se tiene un correo electrónico solicitado a la universidad para enviar información requerida por los miembros del CSIRT y

como otro medio de comunicación aparte del sitio web. Además, adopta el sistema de tickets "Centro de Respuesta y Soporte a Incidentes de Seguridad" para configurar el servicio de reportar incidentes y concientización tecnológica, y dispone de una conexión a internet por parte de la universidad.

2.2.9. Estructura de las políticas de seguridad de un CSIRT

De acuerdo con la investigación realizada por De La Torre & Parra (2018), el establecimiento de políticas y procesos resultan de la cantidad de servicios y recursos para el inicio de las actividades del CSIRT. Por otra parte, la OEA (2016) afirma que el funcionamiento del CSIRT también depende de las políticas de seguridad como directrices para ser cumplidas, ayudan en la gestión de incidentes y aseguran la integridad, confidencialidad y disponibilidad de los recursos que tiene el CSIRT, principalmente el servicio de calidad.

Se tomó como referencia la estructura de políticas de la organización FIRST, que deben aplicarse de forma obligatoria por los equipos que deseen formar parte de la comunidad CSIRT. Las políticas principales son:

- Política de clasificación de información
  Ordena la información tomando en cuenta el nivel crítico.
- Política de protección de datos
  Se define el tipo o modelo de protección de la información de acuerdo a su nivel crítico.
- Política de destrucción de información
  Permite la destrucción de informes, registros, dispositivos o cualquier otro objeto que haya culminado con su ciclo de vida, por lo que es una forma garantizada de que la información no sea divulgada o lleguen a manos equivocadas.
- Política de divulgación de información
  Especifica cuando el CSIRT puede compartir y distribuir cierta información en caso de ser necesaria, al igual de indicar la manera en la que se debe divulgar.
- Política sobre el acceso a la información
  Determina que personal puede acceder a cierto tipo de información de acuerdo a su área de desempeño dentro del equipo.
- Política de uso de los sistemas del CSIRT
  Define el uso correcto y medible en hardware y software.
- Política de gestión de incidentes
  Define los procedimientos tomando en cuenta el tipo y tiempo para dar respuesta.

- Política de cooperación

  Explica el modo de apoyo con otros CSIRT.

Por otra parte, se pueden aplicar adicionalmente otras políticas que ayudan en el correcto funcionamiento del CSIRT:

- Política de contraseñas.
- Política de control de cambios.
- Política de segregación de funciones.
- Política de copias de seguridad.
- Política de seguridad de equipos de telecomunicaciones.
- Política de uso de dispositivos móviles.
- Política de uso de correo electrónico.
- Política de seguridad de la red.
- Política de seguridad del computador personal.
- Política de capacitación y entrenamiento.
- Política de comunicación del CSIRT.
- Política de notificación de incidentes.
- Política de uso de internet.

Ramírez (2016) menciona que la estructura de las políticas debe ser sencillas y claras, ya que es un canal para el trabajo en equipo, buen uso de recursos y gestión de servicios tomando en cuenta la seguridad de la información en general.

2.2.10. Acuerdo de nivel de servicio (SLA)

De acuerdo con la investigación realizada en la Corporación IBM (2017), es un contrato que contiene los compromisos de servicio con la comunidad objetivo, se miden de forma cualitativa y cuantitativa, pueden adoptar varios tipos de valores, usarse en el registro de tickets y ordenes de trabajo, especificar fechas de actividades relacionadas con el servicio y restringir el acuerdo a nivel de equipo o departamento.

2.2.10.1. Tipos de SLA

Motadata (2021) afirma que existen tres tipos de acuerdos :

- Basado en el cliente

  Acuerdo don los servicios relevantes, requeridos por el cliente y que se encuentran establecidos en un solo contrato.

- Basado en servicios

  Su contrato se establece para todos los clientes y se convierte en un modelo estándar para todos los servicios de la organización
- Multinivel

  El cliente redacta el informe en base a sus necesidades y puede agregar las condiciones que crea necesarias para sus servicios.

2.2.10.2. Composición de un SLA

De acuerdo con la Corporación IBM (2017) , se ppuede incluir cualquiera de los siguientes aspectos:

- El resumen para explicar de forma puntual acerca de lo que trata el acuerdo (servicios y partes involucradas)
- La definición de los servicios y como se llevan a cabo, horas de cumplimiento, sistemas de mantenimiento, entre otros.
- El rendimiento de los servicios para garantizar el cumplimiento por medio de supervisiones
- Problemas de servicio y solución, donde se menciona a los involucrados en el caso y los pasos para resolver el problema.

2.2.10.3. Métricas que miden un SLA

Las métricas varían de acuerdo al tipo de SLA con el que trabaja la organización, en este caso se menciona el tipo basado en servicio porque aporta al proyecto de investigación. Quintero & Peña (2017), mencionan que en este tipo de servicio se siguen las prácticas y recomendaciones dadas por la “Biblioteca de Infraestructura de Tecnologías de Información – ITIL”, porque es utilizada para la gestión de servicios de TI y sus operaciones en general.

2.2.10.4. Componentes de un informe SLA

- Declaración de objetivos

  El contrato debe mencionar el objetivo de su creación de cuerdo a los servicios que presta al cliente.

- Especificar servicios

  Mencionar cada uno de los servicios para explicar sus condiciones de prestación en general o individual, se incluyen métricas, indicadores o valores que ayuden a identificar las condiciones del servicio y su disponibilidad.
- Gestión de servicios

  Se aporta con métodos y estándares de referencia necesarios para el acuerdo del servicio, su informe, procesos, condiciones, formas de solución y acciones para actualizar, terminar o renovar el contrato.

De acuerdo a la investigación realizada, el acuerdo de nivel de servicio recoge datos y condiciones que debe cumplir el CSIRT por medio de un contrato, los SLA ayudan a garantizar la correcta prestación de servicios con el fin de asegurar un buen nivel de calidad; y se pueden modificar los acuerdos porque se requiere un cambio de métricas conforme el equipo crece en servicios, recursos y comunidad objetivo.

2.2.11. Seguridad de la información

Castillo (2017) menciona que la seguridad de la información representa a una entidad, por ello se gestionan acciones, leyes o normativas para proteger dicho activo, pues la información es poder y no debe estar vulnerable. La seguridad de la información es correcta si cumple con los tres pilares:

Los tres pilares fundamentales en la seguridad de la información son:

- Confidencialidad

  Tiene como objetivo no divulgar la información de la organización, empresa o institución a personal no autorizado.
- Integridad

  Tiene como objetivo evitar cambios o modificaciones de la información sin autorización por parte del encargado o personal competente.
- Disponibilidad

  Su objetivo es mantener los sistemas y equipos sin interrupciones, ya que al dañarse un equipo es lo mismo que estar fuera de servicio.

El artículo de investigación de Bone, Saltos, Figueroa, & Rodríguez (2017), menciona que la seguridad de la información es una disciplina a cargo de la constitución técnica en protección de la información y de los equipos que la almacenan, controlan los puntos de fallos totales o

parciales, traza planes de acción y corrección de amenazas, riesgos y aplicación de buenas prácticas.

La seguridad de la información se apoya en la política de seguridad que crean las organizaciones como una medida necesaria para evitar la vulnerabilidad de la información.

Por otra parte, Figueroa (2019), afirma que la seguridad de la información es asegurar todos los recursos con los que opere una organización, esto incluye la información y los límites de control de acceso, su finalidad es asegurar los activos y mantenerlos fuera del alcance de terceras personas.

La segunda variable del proyecto de investigación va de la mano con la gestión de la información del CSIRT, pues la creación de la política de seguridad de la información del CSIRT colabora en la confidencialidad, integridad y disponibilidad de la información; permite que la comunidad objetivo facilite su información para atender sus incidentes o vulnerabilidades con tranquilidad y confianza porque conocen de las políticas que maneja el equipo.

2.2.12. ISO/IEC serie 27000

El aporte de investigación de Ramírez (2016) da a conocer que la serie ISO 27000 se publicó en el año 2009, registra ediciones en los años 2012 y 2014 y es una normativa que aporta a los "Sistemas de Gestión de la Información (SGSI)", en su constitución, monitoreo, mantenimiento y mejora.

- Norma ISO 27001

  Normativa principal de la ISO serie 27000, creada en el año 2005 y con revisión en 2013, se encarga de la gestión en criterios importantes de la seguridad de la información. Su objetivo es generar un modelo para instaurar, implementar, ejecutar, formalizar el seguimiento, revisar, conservar y mejorar un SGSI. Elabora objetivos para el control de áreas o departamentos que trabajan en políticas de seguridad, manejo de activos, organización de información, recursos humanos, gestión de control de acceso, operaciones y comunicaciones, controles de adquisición, elaboración y mantenimiento de los sistemas, gestión de incidentes, mejora continua y cumplimiento del servicio.

- Norma ISO 27002

  Es una normativa creada en el año 2005 con 133 controles, 39 objetivos distribuidos en 11 dominios, se derivó de la normativa 17799 en el año 2007. Facilita guías que proporcionan buenas prácticas, objetivos de control y recomendaciones para asegurar la información. Únicamente los objetivos de control que se derivan del 10.9 de la

normativa no son aplicables en un CSIRT ya que están orientadas a la sección de comercio electrónico.

Por otra parte, Figueroa (2019) menciona que basándose en la ISO 27001, la seguridad de la información trata la confidencialidad, integridad y disponibilidad en general de todos los datos de una organización, sin importar sus medios de almacenamiento (audio, video, papel, discos duros, entro otros), y su complementación con la ISO 27002 que permite la integridad, confidencialidad y aseguramiento de los datos y de los procesos que se gestionan. Los controles de seguridad que maneja son: ambiental, física. acceso, cifrado, continuidad del negocio, recursos humanos, gestión de incidentes, correcto uso de los sistemas de información y cumplimiento.

Dentro de la conformación del CSIRT, se toma en cuenta la familia ISO 27000 con la serie 27001 y 27002 que permiten determinar políticas y procesos que aportan en la seguridad de la información, se tienen políticas que aportan a la seguridad de la información, cuidado ambiental en la destrucción de información, el control de acceso, la protección en gestión y uso adecuado de los sistemas del equipo, además de procesos para la gestión de servicios que contienen acuerdos para la confidencialidad y no divulgación de la información.

2.2.13. Normativa de directrices y principios para gestionar el riesgo de las organizaciones ISO 31000

ISOTools (2017) menciona que la gestión de riesgos bajo la normativa internacional ISO 31000, aumenta la probabilidad de cumplir los objetivos de la organización, coopera con la gestión de recursos y operaciones y concientiza sobre la importancia de identificar y gestionar los riesgos de forma correcta.

Pasos para establecer un plan de gestión de riesgos:

- Evaluar si el riesgo es leve o de gran impacto para luego tomar desiciones adecuadas.
- Tratar el riesgo tomando acciones para prevenirlo, detenerlo, cambiar su rumbo, entre otos.
- Investigar las características y formas de eliminar el riesgo con el personal involucrado
- Realizar monitoreso constantes para identificar cambios en el riesgo y en base tomar otras medidas de estión.
- Y realizar la implementación de un estanadar que permita identificar todos los acontecimientos y realizar la gestión respectiva.

Todo proceso o servicio gestionado por una organización va a tener riesgos implicados, por lo tanto, el CSIRT utiliza la ISO 31000 para detectar eventos indeseados que ponene en peligro el correcto funcionamiento de las operaciones del equipo.

2.2.14. "Biblioteca de infraestructura de tecnologías de información" ITIL

La empresa de capacitación de tecnologías de información de Latinoamérica NETEC (2019) menciona que se encarga de establecer buenas prácticas, servicios, desarrollo y operaciones con respecto a tecnologías de la información.

Los principales lineamientos que determina ITIL son:

- Gestión de operaciones TI donde se da el control de operaciones.
- La gestión técnica donde se trata la administración de redes, sistemas y servicios.
- Gestión del proceso en elaboración de productos de software y aplicaciones.

No es necesario llevar el proceso ITIL dentro de las etapas que plantea, ya que se las muestra a modo de sugerencia dando a conocer la forma de designar responsabilidades. Dentro de la gestión de servicios TI se dan procesos que juegan un papel importante, estos son:

- Gestión del servicio

  Donde el encargado cumple con todo el ciclo de vida para mejorar los servicios de la organización.
- Propietario del servicio

  Presta servicios específicos, siendo el último responsable frente al cliente y organizaciones TI.
- Gestión del proceso

  El encargado realiza procesos operativos relacionándose con un proceso en particular.

Al efectuar buenas prácticas en el manejo de la información con el proceso ITIL, se tiene grandes beneficios como el contar con un modelo de liderazgo TI, reducir costos y mejorar el servicio, mantener una estrecha comunicación con las demás áreas y buena gestión en tratos con proveedores.

2.2.15. "Ley orgánica de educación intercultural" LOEI

"Garantiza el derecho a la educación determinando principios para una buena convivencia en el sistema educativo". Dicha ley debe ser acatada por el sistema educativo del país, posee 8 títulos, 143 artículos, 14 disposiciones generales y 42 disposiciones transitorias, mismos que van en beneficio de la educación (Merizalde, 2020).

El título 6 de la “Regulación, control, infracciones, sanciones y recursos administrativos”, trata ciertos puntos que están relacionados con la gestión de la información y que resulta útil para el desarrollo del proyecto de investigación, pues la implementación de un CSIRT aportará a la seguridad de los recursos físicos y digitales que las instituciones educativas poseen. El artículo 130 trata sobre el control interno en todas las áreas y procesos que llevan las instituciones por medio de auditores designados por parte del Ministerio de Educación.

Dentro del artículo 132 de prohibiciones, se menciona que está prohibido oponerse a las actividades de control, auditoría y evaluación pedagógica, también está el no emitir informes claros y oportunos acerca de los sistemas que gestionan los servicios de la institución; y está el generar alteraciones en documentos oficiales de las instituciones, elaborar información falsa y ocultar información importante para las autoridades de educación.

2.2.16. “Consorcio de gobiernos autónomos provinciales del Ecuador” CONGOPE

Es una entidad que apoya en la gestión de las prefecturas del país, trabajan en la creación de modelos de gestión justos, democráticos, participativos, incluyentes y descentralizados, todo esto lo realizan ofertando soluciones prácticas e innovadoras brindando asistencia técnica, jurídica, financiera, tecnológica y administrativa, articulando a las prefecturas con otros niveles institucionales nacionales e internacionales que ayuden a potenciar la autonomía y el rol a los 23 GADS provinciales del país. Vinculan a todos los agremiados en una asamblea general de prefectos para asegurar una participación más libre y democrática, forjando el bienestar de las provincias y el gobierno ecuatoriano, tratando al máximo de trabajar con eficiencia, transparencia, ética y honestidad (CONGOPE Ecuador, 2015).

2.2.17. Transparencia de un CSIRT bajo los estándares de referencia RFC2350

2.2.17.1. Definición

RFC 2350 es un documento con estándares de referencia donde se detalla los canales de comunicación, roles, responsabilidades, políticas y procesos operacionales de un CSIRT para dar a conocer a su comunidad objetivo. No se puede mencionar los requisitos de información correctos para todos los equipos, pero RFC 2350 maneja un formato general con asuntos que son de interés para sus miembros.

Para la conformación de un CSIRT, es importante el desarrollo del marco de trabajo, mismo que menciona los puntos para notificar el correcto funcionamiento del equipo, incluyendo la seguridad de la información; de acuerdo al marco de trabajo, para demostrar transparencia y

confiabilidad ante la comunidad objetivo se toma en cuenta el proyecto de establecimiento de un CSIRT realizado por Browndle y Guttman (citado en ECNO CSIRT, 2019).

2.2.17.2. Relaciones entre diferentes CSIRTs

Las relaciones de entre otros equipos son para llevar acuerdos de trabajar en conjunto y compartir información delicada y por cooperación, donde se ponen en contacto para pedir ayuda o un consejo, sim embargo, existen equipos que trabajan bien por sí solos ya que se constituyen por un objetivo menor o porque manejan personal y sistemas en gran escala, es por su madurez o constitución.

2.2.17.3. Establecimiento de comunicaciones seguras

Se deben establecer seguridades en los medios de comunicación del CSIRT con la comunidad objetivo e instituciones de cooperación, esto con la finalidad de evitar intromisiones maliciosas y así asegurar su confidencialidad, integridad y autenticidad. Mas allá de plasmar este punto en el documento, es aplicar a todos los medios de comunicación del equipo con la finalidad de demostrar el uso de mecanismos que ayuden a su protección.

2.2.17.4. Publicación de políticas y procedimientos de un CSIRT

Un CSIRT debe conocer de los servicios que requieren las instituciones y adelantarse en las interacciones que se pueden dar al brindarlos, independientemente del tipo de orientación, todos los equipos tienen la responsabilidad de informar sobre las políticas y procedimientos que realmente debe conocer la comunidad objetivo.

2.2.17.5. Información, políticas y procesos

Anteriormente se trató de la publicación de políticas y procesos en el sitio web del CSIRT, en este punto se menciona la importancia de plasmar la información que estos contienen de manera clara y específica, describiendo los temas relevantes que abordan las políticas y procesos, cada equipo es libre de establecer un formato, lo importante es que la comunidad objetivo pueda acceder a esto y entenderlo.

2.2.17.6. Obtención del documento

La plantilla del documento que se genera debe contener la fecha en la que se lo actualizó por última vez para evitar malentendidos o información errónea, realizar distribuciones por correo

para notificar a sus usuarios si existen cambios, y reemplazar la versión actual del documento apenas se realicen actualizaciones.

2.2.17.7. Información de contacto

Se deben registrar los detalles de contacto del CSIRT incluyendo nombre del equipo, dirección de envío, horarios de atención, número de teléfono, correo electrónico, claves de cifrado, integrantes del equipo, horario de atención y alguna información de contacto.

2.2.17.8. Carta

Es considerado un estatuto en el que se menciona las actividades que realiza el equipo y bajo que autoridad las ejecutan, esto incluye:

- La misión que describe las actividades principales del equipo, es considerada un elemento principal para conformar un CSIRT.
- La circunscripción que consiste en mencionar los integrantes que conforman el equipo y sus respectivas ocupaciones, en caso de no mencionarlos se deben explicar las razones de esta decisión.
- La afiliación que consiste en mencionar la autoridad que permite el funcionamiento del equipo y dentro de que perímetro está ubicado, esto permite ganar la confianza entre el lector y un CSIRT
- La autoridad que consiste en identificar el control y alcance que tiene sobre los sistemas que utiliza el equipo dentro de su perímetro.

2.2.17.9. Políticas

La definición de las políticas de seguridad es fundamental para la gestión operativa de un CSIRT, se recomienda incluir las siguientes:

- Políticas de cooperación y divulgación de la información a través de vendedores, fuerzas de orden mayor, prensa u otros medios siempre sujetos a restricciones.
- Política de comunicación y autenticación que explican los métodos aplicados para la seguridad en comunicaciones que realiza el CSIR, y con ello también las firmas o contraseñas para acceder a la información.

2.2.17.10. Servicios

Un CSIRT proporciona sus servicios como actividades en tiempo real cuando se trata de respuesta a incidentes, actividades proactivas en tiempo no real y cooperación, y por otro lado se encuentran los servicios opcionales porque no todos los equipos van a brindar los mismos servicios.

2.2.17.11. Formulario de notificación de incidentes

Permiten la recolección de información de los incidentes que presentan la comunidad objetivo para proceder de manera eficiente. Proporcionarlos a través del sitio web conjuntamente con las indicaciones apropiadas resulta eficaz en la gestión del incidente.

2.2.17.12. Renuncias

La constitución de un CSIRT no depende de un contrato jurídico, resulta importante mostrar las descripciones de servicios, responsables y finalidades, además, se debe tener un documento que explique las limitaciones, como un reglamento que todos los integrantes del CSIRT deben conocer. Cuando se presentan más procesos y convenios con el CSIRT, se debe realizar un descargo de limitaciones con un abogado.

De acuerdo con los puntos investigados de las fuentes mencionadas anteriormente, se identifica a la estructura del estándar RFC 2350 como guía para dar a conocer la razón de ser, personal, servicios, contactos y las políticas que se gestiona para el correcto funcionamiento del CSIRT, con este documento se genera transparencia, por lo que se encuentra en el sitio web del equipo para conocimiento de la unidades educativas y gobiernos seccionales de la provincial del Carchi que requieran de los servicios.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

3.1.1.1. Cualitativo

El enfoque es cualitativo; según (Hernández, Fernández, & Pilar, 2014) afirma que se basa en la obtención de información mediante la formulación de preguntas como un preámbulo para poder indagar en hechos e interpretaciones de forma interactiva. Resulta de un proceso redundante y con una secuencia que va a ser diferente a otros estudios cualitativos.

Nos involucramos en la problemática que está presente en el diario vivir de la sociedad, se trata de los incidentes informáticos que provocan la inestabilidad operativa de las personas. Es por ello que recolectamos información en base a medidas y procesos que realizan las unidades educativas y gobiernos seccionales de la provincia del Carchi para proteger su información; generando diálogos interactivos formales e informales para conocer criterios propios y experiencias que permitieron establecer un catálogo de servicios reactivos, proactivos y de mejoras de la calidad para el equipo CSIRT.

Adoptamos un aspecto holístico, es decir, nos basamos en experiencias o acciones sobre seguridad de la información, se obtuvo datos de observación no medibles, por lo que el proyecto de investigación se adaptó a realidades investigativas y no de estadísticas. Por otra parte, el enfoque cualitativo nos permitió mantener una comunicación abierta con las organizaciones para acoger y asimilar la información necesaria en base a modalidades, opiniones, acciones, comportamientos o actitudes referentes a la seguridad de la información y equipos que la procesan.

3.1.2. Tipo de investigación

3.1.2.1. Documental

Se aplicó la investigación documental porque se basa en el análisis e interpretación de información de libros, artículos, videos y documentos físicos o digitales con sus respectivas citas y referencias. Con ello establecimos la recolección de información de acuerdo a los requerimientos del proyecto de investigación, para el proceso de implementación obtuvimos una mayor organización y en gran parte un análisis propio.

Por otra parte, se obtuvo nuevas perspectivas sobre el manejo de las variables "equipo de respuesta a incidentes informáticos" y "seguridad de la información", esto llevó a formular preguntas sobre el tema, establecer el proceso de desarrollo del documento y generar fases de implementación requeridas para llegar al resultado esperado.

3.1.2.2. De campo

Tiene la finalidad de recolectar información acerca del tema a investigar, mediante el contacto directo con las fuentes de información para acoger opiniones, testimonios y puntos de vista. Se tomó en cuenta la investigación de campo para recopilar información en unidades educativas y gobiernos seccionales de la provincia del Carchi; con ello se obtuvo datos de fuentes originales para la toma de decisiones teniendo en cuenta los resultados encontrados. Por otra parte, se recopiló información de las unidades educativas vigentes en los distritos de la provincia.

3.1.3. Técnicas

3.1.3.1. Revisión de literatura

Se usó fuentes con la misma temática para hacer uso de conceptos, opiniones, métodos y procesos de forma analítica para aumentar nuestro nivel de conocimiento en el área de estudio.

3.1.3.2. Entrevistas

La entrevista semiestructurada permitió recolectar información mediante el uso de una guía de preguntas abiertas, además de mantener un diálogo interactivo y dar la atención necesaria para apreciar cada opinión, experiencia o criterio del entrevistado. El formato de las entrevistas aplicadas para la recolección de información en las unidades educativas y gobiernos seccionales de la provincia del Carchi se encuentra en el anexo 8.

3.1.3.3. Validación de instrumentos

La validación de instrumentos es considerada fundamental dentro del proceso de recolección de información, pues de ello se garantiza la validez y confiabilidad de nuestras preguntas. Para validar se requiere de especialistas que tengan conocimientos sobre el área de investigación que se está desarrollando, lo recomendable es pedir ayuda a docentes porque tienen la experiencia en métodos y análisis para llevar el proceso de evaluación (Hernández, Fernández, & Pilar, 2014).

- Primera aplicación

  La validación del instrumento de investigación la realizó el Msc. Jairo Hidalgo docente investigador de la Carrera de Computación e Ingeniería en Informática de la Universidad Politécnica Estatal del Carchi. Se muestran los resultados en la siguiente tabla:

Tabla 12. Validación de instrumentos primera aplicación

Experto	**Pregunta**	**Observación**	**Corrección**
Msc. Jairo Hidalgo	Pregunta 1: ¿Qué políticas o normas de seguridad utilizan en la institución para la seguridad de la información y los equipos que la procesan?	Poner de referencia las normativas internacionales COBIT-ISO 27000, etc. Puntuar mejor la pregunta y no debería ir primera.	¿Qué políticas o normativas internacionales utilizan en la institución para la seguridad de la información y los equipos que la procesan (Ejemplo: COBIT, ITIL, ISO/IEC serie 27000, etc.)?
	Pregunta 2: ¿Qué medidas toman para evitar que la información y los equipos sean vulnerados?	No debería ir entre las primeras preguntas.	Ninguna. ¿Qué medidas toman para evitar que la información y los equipos sean vulnerados?
	Pregunta 3: En caso de presentarse un incidente informático ¿Qué procedimientos aplican para dar seguimiento a dicho incidente y mitigar su riesgo?	Indicar que tipo de incidente informático para que el entrevistado nos responda en si incidentes informáticos que se deban a ciertos fallos de seguridad.	En caso de presentarse un incidente informático (filtrado, alteración o pérdida de información, hackeos, denegación de servicios y caída del sitio web, introducción de código malicioso como virus, troyanos, gusanos y malware en general) ¿Qué procedimientos aplican para dar seguimiento a

		dichos incidentes y mitigar sus riesgos?
Pregunta 4: Cuál es el personal a cargo de generar políticas, normas y recomendaciones para la seguridad de la información y equipos.	Realizar la pregunta de manera general conjuntamente con la quinta y sexta pregunta. Cambiar el sentido de la pregunta, hacer que el entrevistado explique más sobre el tema relacionado con las políticas que ellos manejan.	¿Cómo llevan a cabo el proceso para la implementación o creación de políticas de seguridad, actualización de las mismas y generar recomendaciones sobre la seguridad informática?
10. ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información?	Pregunta que debe ir al principio como una apertura para confirmar si la institución cuenta con infraestructura y si es así para continuar.	Ninguna. ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información?
11. Ustedes como departamento de tecnología de la institución. ¿Qué servicio requerirían en cuanto a seguridad de la información?	No es necesaria la pregunta ya que con las demás preguntas de la entrevista sabremos los servicios que ellos requieren.	Reemplazar y llegar a preguntas que se responda a nuestros requerimientos. En caso de necesitar otra información formular más preguntas si es necesario o ver si se puede fisionar con alguna pregunta ya existente.

- Segunda aplicación

  Hernández, Fernández, & Pilar (2014) mencionan que, si se tiene la validación del instrumento de investigación por más de un experto, más confiable y efectiva puede llegar a ser. La segunda validación del instrumento de investigación la realizó en Msc. Marco Yandún docente investigador de la carrera de Computación e Ingeniería en Informática de la Universidad Politécnica Estatal del Carchi. Se muestran los resultados en la siguiente tabla:

Tabla 13. Validación de instrumentos segunda aplicación

Experto	**Pregunta**	**Observación**	**Corrección**
Msc. Marco Yandún	Pregunta 1: ¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos?	Añadir un conector que le motive al entrevistado a detallar su infraestructura.	¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos? ¿Cuáles?
	Pregunta 2: ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información?	Se puede tratar de una pregunta de afirmación y negación (si/no), añadir un conector para obtener información de que tipo de normativas o reglamentos tienen.	¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información? ¿Cuáles?
	Pregunta 4: ¿Qué medidas toman para evitar que la información y los equipos sean vulnerados?	Hacer énfasis de que están tratando la entrevista referente a la institución.	¿Qué medidas toman para evitar que la información y los equipos de la institución sean vulnerados?

	Pregunta 7: ¿De qué manera se informan sobre las nuevas formas de ataques y explotación de vulnerabilidades?	Explicar que la información que reciban sea a los que conforman la institución, que sea formal y especialmente para la institución.	¿De qué manera se informan los miembros de la institución sobre las nuevas formas de ataques y explotación de vulnerabilidades?
	Pregunta 10. ¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan?	Añadir algún aviso, comentario o formular la pregunta en la que mencionen que la actualización debe ser con sus permisos y licencias para que esta sea correcta.	¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan? Teniendo en cuenta que la actualización incluye permisos y licencias respectivamente.

3.2. IDEA A DEFENDER

Un Equipo de Respuesta ante Incidentes Informáticos CSIRT en la Universidad Politécnica Estatal del Carchi, aumentará la capacidad de prevención y respuesta ante incidentes informáticos que atenten contra la seguridad de la información en unidades educativas y gobiernos seccionales de la provincia del Carchi.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

Tabla 14. Operacionalización de variables

Variables	Definición	Dimensiones	Indicadores	Técnica	Instrumento	Informantes
Reporte y seguimiento ante incidentes informáticos	Es recibir, revisar y responder a notificaciones de actividades sobre incidencias informáticas	Servicios reactivos Servicios proactivos Servicios de gestión de la calidad de la seguridad	Medidas para mitigar incidentes informáticos Medidas parar la prevención de incidentes informáticos Acciones para mejorar en la protección de la información	Entrevista	Guía de entrevista, grabadora de audio, cámara fotográfica y software de reuniones virtuales	Encargado del centro de TICS y Laboratorio de Ciberseguridad
Seguridad de la información	Es la unión de la integridad, disponibilidad y	Seguridad lógica	Políticas de seguridad de la información implementadas	Entrevista	Guía de entrevista, grabadora de	Encargados del área de tecnología en Unidades educativas y gobiernos

	confidencialidad de los datos e información de una organización	Seguridad física	Infraestructura implementada para asegurar la información	audio, cámara fotográfica y software de reuniones virtuales	seccionales que cuentan con una red establecida.

3.4. MÉTODOS UTILIZADOS

3.4.1. Inductivo - deductivo

Rodríguez (2017), menciona que el método inductivo funciona al involucrarse en conocimientos generales para llegar a nuevas expectativas o leyes de menor grado, reajustando lo teórico y metodológico para el desarrollo de la propuesta.

Se empleó el método inductivo – deductivo porque adaptamos el interés por la investigación y adquisición de más conocimientos referentes a la seguridad informática y todo referente a lo que conforma un equipo de respuesta. A partir de ello se llegó a la construcción de elementos específicos a utilizar para llegar a una propuesta de solución; es decir, especificar los tipos de seguridades que se ven influenciados en nuestro caso de estudio y estructura del CSIRT.

3.4.2. Analítico

Según Calduch (2017), el método analítico resulta esencial para encontrar hechos que se relacionan o se complementan entre sí, aportan al tema investigado para que este pueda ser explicado.

Aplicamos el método analítico porque obtuvimos distintas fuentes que aportan al desarrollo del tema de investigación, llegando a encontrar similitudes o conceptos que se complementan con los de otras fuentes. De ello se realizó un análisis de todo lo que constituye de manera esencial para el desarrollo del caso de estudio y se adoptó los requerimientos necesarios para obtener conceptos que permitieron llegar a los resultados esperados.

3.4.3. Sintético

Calduch (2017) afirma que el método sintético es el conocimiento de ciertas temáticas que resultan importantes para la investigación, y de ello hacer la reconstrucción para llegar a una teoría simplificada y necesaria.

Con el método sintético logramos una estructura ideal para realizar el modelo de investigación teórica, aplicando los elementos necesarios, adquiriendo conceptos, procesos y datos válidos.

3.5. POBLACIÓN Y MUESTRA

3.5.1. Muestreo por conveniencia

Martínez (2018) menciona que el muestreo por conveniencia no se lleva a cabo con métodos o estrategias de recolección sistemáticos, este depende de la accesibilidad para llegar a los

informantes. Aplicamos dicho método por lo factible que resulta la interacción con los involucrados en la investigación, para la obtención de información del funcionamiento de su organización y delimitándonos en temas de nuestro interés. Nos permitió identificar aspectos institucionales y gubernamentales que se aplican por organizaciones dedicadas a lo mismo, y acoger y emitir criterios útiles en la recolección de información.

3.6. RECURSOS

3.6.1. Humanos

Tabla 15. Recursos humanos

Integrante	Cargo
Msc. Jairo Hidalgo	Docente investigador de la Carrera de Computación e Ingeniería en Informática - tutor del proyecto de investigación.
Msc. Milton Del Hierro	Docente investigador de la Carrera de Computación e Ingeniería en Informática – lector del proyecto de investigación.
Anderson Chamorro	Estudiante de la Carrera de Ingeniería en Informática – autor del proyecto de investigación.
Silvia Pupiales	Estudiante de la Carrera de Ingeniería en Informática – autora del proyecto de investigación.

3.6.2. Institucionales

Laboratorio de ciberseguridad de la Universidad Politécnica Estatal del Carchi para la conformación de CSIRT UPEC e implementación del servidor web y de monitoreo.

Tabla 16. Recursos institucionales

Recurso	Descripción
Espacio en disco del servidor	Servidor con el sistema operativo CentOS 7, ubicado en el laboratorio de Ciberseguridad de la UPEC. Servidor con el sistema operativo Kali Linux, ubicado en el laboratorio de Ciberseguridad de la UPEC.
Correo institucional	Correo otorgado con el dominio de la UPEC (csirt.computacion@upec.edu.ec).

3.6.3. Materiales de trabajo

Tabla 17. Materiales de trabajo

Recurso	Características	Cantidad	Precio
Computador	- Hp Core (TM) i3 - ACER Core (TM) i3	2	1200,00 $
USB	- HP 12 GB	1	15,00 $
Conexión de internet	- 12 GB	1	30,00 $
Material de oficina	- Libretas - Esferos - Hojas de impresión - Grapas - Otros	2	10,00 $
Celular	- Xiaomi Redmi Note 8	1	180,00 $
Viáticos	- Pasajes - Alimentación	2	100,00 $

IV. RESULTADOS Y DISCUCIÓN

4.1. RESULTADOS DE LA ENTREVISTA

4.1.1. Unidad educativa

a) ¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos? ¿Cuáles?

Se tienen servicios independientes de internet, un sitio web y un sistema de notas montado en la hoja de cálculo de Google. La institución cuenta con laboratorios de cómputo de uso para impartir clases y de uso administrativo.

- **Análisis:** La unidad educativa se da a entender que consta con laboratorios de cómputo y software web y un sistema de notas que les permite desarrollar sus actividades académicas.

  Al mencionar la constancia de servicio de internet, manejo de datos y sitio web por parte de la institución, se entiende que hay una gestión de la información y que por ende permite continuar con la entrevista y con el proceso de investigación.

b) ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información? ¿Cuáles?

Utilizan las políticas de seguridad para el uso de laboratorios, red Wifi, ingreso al sistema de notas y se rigen por la Ley Orgánica de Educación Intercultural (LOEI) que protege la información de los estudiantes y docentes.

- **Análisis:** La institución maneja normativas que son usadas básicamente por todas las instituciones, pero que en si no son en gran porcentaje confiables en protección de información a un nivel físico y digital.

c) ¿Qué políticas o normativas internacionales utilizan en la institución para la seguridad de la información y los equipos que la procesan (Ejemplo: COBIT, ITIL, ISO/IEC serie 27000, etc.)?

No cuentan con ninguna normativa internacional, sin embargo, se conoce acerca de las políticas mencionadas en la pregunta, pero no se utiliza en la institución.

- **Análisis:** El entrevistado afirma conocer sobre las políticas y normativas internacionales que funcionan para el área informática y administrativa empresarial y que son de vital importancia en una organización para la

protección de la información y equipos, pero que no se aplican en la unidad educativa por lo que reconoce que es una falencia que podría pasar factura.

d) ¿Qué medidas toman para evitar que la información y los equipos de la institución sean vulnerados?

Utilizan tecnologías que brinda Google, entre ellas está el doble factor de autenticación para el ingreso a sus sistemas, también una auditoría constante del manejo de los sistemas informáticos e información. Además, se configuraron las redes inalámbricas como ocultas para que las personas que no pertenecen a la institución no las puedan visualizar y se maneja Subneteo y VLANS. La institución cuenta con guardias para la protección de las instalaciones (laboratorios, oficinas), cámaras de vigilancia y controles de acceso.

- **Análisis:** La institución está en un nivel de seguridad bajo por las medidas que han adoptado en su gestión, se entiende que las herramientas que utilizan son adquiridas por instinto de proteger los datos por parte del técnico en informática de la institución pero que, en sí, no saben si son los ideales para el tipo de información que manejan.

e) En caso de presentarse un incidente informático (filtrado, alteración o pérdida de información, hackeos, denegación de servicios y caída del sitio web, introducción de código malicioso como virus, troyanos, gusanos y malware en general) ¿Qué procedimientos aplican para dar seguimiento a dichos incidentes y mitigar sus riesgos?

Se realiza un escaneo de vulnerabilidades, virus y código malicioso en general mediante un script y se procede a dar un seguimiento para saber de dónde proviene el ataque, luego borrar los virus y bloquear las IP y en caso de denegación de servicios levantarlos mediante los respaldos.

- **Análisis:** La institución adquiere una estructura de manejo de incidentes y se entiende que los procedimientos son un registro con datos que creen importantes anotar en el momento que están en la gestión del incidente, porque no se ha mencionado el hecho de contar con un formato o un documento con procesos que aplican los encargados de la seguridad para la gestión de incidentes.

f) ¿Cómo llevan a cabo el proceso para la implementación o creación de políticas de seguridad, actualización de las mismas y generar recomendaciones sobre la seguridad informática?

Se maneja dos factores, uno que es la seguridad física a lo que se refiere el personal con a responsabilidad designada para cuidar las instalaciones, equipos de trabajo de los docentes, laboratorios de informática y se maneja un sistema de alarmas donde se encuentra equipo informático. Otro factor es la auditoría para el correcto uso del sistema y con lo que se refiere al manejo de hojas de cálculo.

- **Análisis:** La institución aplica su seguridad a nivel físico y digital designando la responsabilidad a cada involucrado en el tema de la seguridad. Aquí se determina que realizan la creación y determinación de seguridades, pero que deben adquirir capacitaciones o información para que ellos estén más adentrados en el área de la seguridad, y así dar las responsabilidades en seguridad lógica y física de una manera más correcta y confiable.

g) ¿De qué manera se informan los miembros de la institución sobre las nuevas formas de ataques y explotación de vulnerabilidades?

Es iniciativa propia como docente de mantenerse informado y comunicar a las autoridades sobre ciertos incidentes, y para informar sobre la aplicación de ciertas políticas que resguarden bien la información, se conoce de herramientas de acceso público que ayudan un poco en la protección de los sistemas, pero en sí, no existe información al día sobre cualquier ataque que se esté presentando y una explicación de cómo tratar estos incidentes o prevenirlos.

- **Análisis:** La institución tambalea en receptar información acerca de los nuevos ataques o vulnerabilidades de la información que se presentan en el día a día, se entiende que los docentes del área informática se dan a la tarea de buscar información para estar al tanto de la seguridad e incidentes informáticos que se producen en las instituciones del mismo ámbito que es el educativo. En si esta iniciativa a veces puede resultar asertiva para evitar los nuevos ataques o incidentes, pero otras veces no, por lo que se carecen de una organización o un grupo en general que ayude al sector educativo a informarse de todo lo que pasa en el día a día, esto puede resultar importante para la institución en el tema de seguridades.

h) ¿Con qué frecuencia realizan el escaneo de vulnerabilidades y de qué forma?

Se realiza diariamente mediante la ejecución de un script y generación de ubicación en caso de presentarse más de un inicio de sesión del mismo usuario, permitiendo informar al mismo notificando al correo o celular. Cuando hay fechas de ingreso de notas es

donde más se está alerta y supervisando el uso del sistema, la actualización del sistema operativo CentOS y darle las respectivas seguridades se las realiza una vez al mes.

- **Análisis:** El modo operativo es factible para mantener un nivel de seguridad aceptable en la institución, ya que principalmente protegen su área de gestión que son el sitio web y sistema operativo en actualizaciones, Se analiza que el modo de trabajo es bueno pero que el tiempo de verificación del sistema operativo podría ocasionar inconvenientes en su funcionamiento en menos de un mes; se debe establecer tiempos de escaneos de vulnerabilidades de acuerdo al tipo de sistema conformado en la institución.

i) Según su criterio ¿Por qué ocurre el incumplimiento de políticas de seguridad?

Por el factor humano ya que en ciertas ocasiones anotamos contraseñas para no olvidarnos y están más a la vista de terceros al igual que el ingreso a equipos. Por otro lado, las desactualizaciones de las políticas son el foco de vulnerabilidades.

- **Análisis:** Se detalla el factor humano como la principal falla en cuanto a seguridad de la información, pues por eso se producen introducción de virus a los computadores, mal uso de los equipos y permisos de usar información a personas que no les compete, esto y una infinidad de incidentes que se ven producidos por el factor humano pero que en si son los mismos que pueden protegerla, si se tiene una capacitación y sentido de responsabilidad como una manera de comprometerse con el prestigio de la institución.

j) ¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan? Teniendo en cuenta que la actualización incluye permisos y licencias respectivamente.

Cada mes mediante una revisión, documentación del estado del software y se procede con las actualizaciones respectivas.

- **Análisis:** La institución gestiona el proceso de actualizaciones de acuerdo a las fallas tanto en equipos como en el manejo de información mensual, se determina una actualización no tan efectiva ya que la institución no puede gestionar el reemplazo de equipos al instante: y han mencionado que presentan falencias en el manejo de licencias para el uso de software.

4.1.2. Gobierno seccional.

a) ¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos? ¿Cuáles?

La institución cuenta con tres servidores, infraestructura de red y sistemas informáticos que brinda la AME (Asociación de Municipalidades Ecuatorianas) y equipos como parte de la organización.

- **Análisis:** La institución cuenta con servidores que resultan útiles y se ejecutan en los computadores que forman parte de la organización para otorgar los servicios necesarios y en computadoras dedicadas. Menciona el uso de aplicativos que manejan las instituciones del mismo ámbito en el Ecuador ya que son municipalidades que gestionan información pública y por ello pertenecen al estado. Al mencionar redes, servidores y aplicativos se sabe que se realiza la gestión de información, por lo que resulta útil para llevar a cabo el proceso de implementación de nuestro proyecto de investigación y, por ende, continuar con la entrevista.

b) ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información? ¿Cuáles?

Existe un reglamento del buen uso del servicio de los equipos e internet.

- **Análisis:** La institución ha desarrollado un reglamento en los que detallan el cómo y para que se usan los equipos de cómputo al igual del uso del internet para aspectos únicamente laborales. Se reconoce que al hacer buen uso de los dos factores se está estableciendo un nivel de seguridad importante y que puede evitar ciertas vulnerabilidades en la gestión de la información. Se reconoce que hay una organización interna para fomentar dichos reglamentos, por otra parte, no se menciona el uso de normativas nacionales que puedan ser usadas por las municipalidades ecuatorianas a excepción de la asociación mencionada en la pregunta.

c) ¿Qué políticas o normativas internacionales utilizan en la institución para la seguridad de la información y los equipos que la procesan (Ejemplo: COBIT, ITIL, ISO/IEC serie 27000, etc.)?

No utilizan ninguna política o normativa internacional, pero si se conoce de ello.

- **Análisis:** La institución no cuenta con normativas internacionales que aporten a la seguridad de la información y equipos informáticos, esto puede resultar como

un punto negativo para la organización porque no se está aplicando normativas que ayudan a la seguridad física y lógica, por ello resulta la inestabilidad operacional e interrupción de los servicios. Al ser una institución pública debe estar en mayor porcentaje disponible al público y aplicando las medidas respectivas para que el servicio no decaiga, dichas normativas resultarían útiles para ello.

d) ¿Qué medidas toman para evitar que la información y los equipos de la institución sean vulnerados?

Filtrado por direcciones IP, firewall que es proporcionado por CNT para la seguridad en páginas web y restricciones a los sistemas del municipio.

- **Análisis:** Se menciona el filtrado de direcciones IP, por lo que esto permite la protección de intrusos en la red ya que actúa como cortafuegos y controla el tráfico permitiendo o denegando el ingreso a la red de la organización. Se usan los servicios de firewall de una empresa que se dedica al servicio de internet con la finalidad de proteger las páginas web. Esto da a entender que se enfocan en mantener bien los servicios que tratan la gestión pública, pues manejan información delicada y que puede provocar una infinidad de incidentes si esta llega a manos equivocadas.

  Al mencionar la restricción a los sistemas se refieren tanto a lo digital como a lo físico por lo que son factores fundamentales a proteger ya que ahí se encuentra la información.

e) En caso de presentarse un incidente informático (filtrado, alteración o pérdida de información, hackeos, denegación de servicios y caída del sitio web, introducción de código malicioso como virus, troyanos, gusanos y malware en general) ¿Qué procedimientos aplican para dar seguimiento a dichos incidentes y mitigar sus riesgos?

El municipio contrata una licencia de antivirus cada dos años y trabajan con una empresa privada que les proporciona seguridad. En caso de presentarse un incidente informático la institución saca un registro del ataque y lo reporta a la empresa privada, luego esta se encargará de dar el respectivo seguimiento, rastreo y dar una solución al incidente.

- **Análisis:** En este caso, se obtiene una respuesta en la que la institución determinó la importancia de tener protegida la información con la contratación del servicio por parte de una empresa privada, esto hace que el municipio genere su informe de incidente o ataque generando un acceso a la información que se

maneja. Aquí se toman en cuentas dos puntos sumamente delicados que son: el confiar la información a terceras personas y hasta qué punto son confiables. No se trata de menospreciar el trabajo de empresas dedicadas a brindar servicios de seguridad informática, es una cuestión de ética profesional en el personal que trabaja, por otra parte, se pueden realizar los seguimientos y tratado de incidentes por parte de la institución, pero no se ha mencionado de ello al respecto, por lo que se entiende que no tiene procesos o encargados de realizarlo y por ello contratan de manera externa dichos servicios. En este aspecto se nota la importancia de generar capacitaciones a todos los gobiernos seccionales de la provincia y que el estado otorgue personal especialmente para ello.

f) ¿Cómo llevan a cabo el proceso para la implementación o creación de políticas de seguridad, actualización de las mismas y generar recomendaciones sobre la seguridad informática?

Definen las políticas de seguridad de acuerdo a los roles, y el personal se hace responsable del área designada y uso correcto del sistema de acuerdo a las normas que se deben cumplir como servidores públicos.

- **Análisis:** La manera de la implementación y modificación de políticas de seguridad se la realiza con la iniciativa del encargado del área técnica del municipio y a los roles del personal según lo respondido. Como servidores públicos están encargados de estar al tanto de su área y procurar que esta funcione correctamente; sin embargo, no se menciona la capacitación para que los trabajadores estén más al tanto de las seguridades que se deben acatar y tampoco se menciona el periodo de tiempo para la actualización o modificación de políticas, por lo que se entiende que lo realizan cuando se cree conveniente.

g) ¿De qué manera se informan los miembros de la institución sobre las nuevas formas de ataques y explotación de vulnerabilidades?

La empresa privada les proporciona boletines de información sobre vulnerabilidades que se están dando en el momento.

- **Análisis:** Al contratar el servicio de seguridades para la institución, también reciben boletines sobre las vulnerabilidades que se presentan y ataques nuevos. La empresa privada como tal está brindando dicha información con un valor monetario, pero al ser una empresa que da seguridades a todo tipo de instituciones, no está enfocada totalmente a las vulnerabilidades e incidentes que

el municipio puede contraer, y esto es un factor delicado y que debe ser tomado en cuenta por la institución.

h) ¿Con qué frecuencia realizan el escaneo de vulnerabilidades y de qué forma?

El escaneo de vulnerabilidades se la realiza mediante el antivirus diariamente por lo que se encuentra siempre actualizado y activo.

- **Análisis:** La manera diaria de realizar el escaneo de vulnerabilidades resulta eficiente porque deben emitir un informe a la empresa privada de seguridad en caso de presentar un incidente, y esta se encargará del incidente. En este caso el uso del antivirus es el único método empleado, que puede resultar no tan eficiente para verificar los fallos o inconvenientes en los sistemas de la institución.

i) Según su criterio ¿Por qué ocurre el incumplimiento de políticas de seguridad?

La factibilidad económica afecta al ser un Municipio pequeño y resulta difícil adquirir la seguridad adecuada y la ayuda necesaria por parte de las autoridades, ya que prefieren realizar una obra que la población vea y no invertir en seguridad de la información.

- **Análisis:** En este caso se menciona la despreocupación de las autoridades porque prefieren gestionar obras que sean visibles al pueblo para que aprecien y vean que si se ha hecho algo, todo ello resulta por el desconocimiento de la importancia en seguridad de la información en el municipio, se da falencias en las personas de la provincia que valoran las obras a simple vista y no la seguridad de la información digital y los equipos que procesan dicha información , las personas no hacen válida la inversión en tecnología.

j) ¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan? Teniendo en cuenta que la actualización incluye permisos y licencias respectivamente.

El municipio realiza la adquisición de por lo menos diez equipos para la actualización de hardware, y dentro de lo que es la actualización del software la realizan de acuerdo al avance de la tecnología mediante paquetes libres, ya que la ley determina el uso de software libre en instituciones públicas.

- **Análisis:** Al ser una institución que forma parte del estado, y por lo tanto es pública, realiza la adquisición de los computadores por petición al estado que se encarga de las municipalidades del Ecuador, por lo que se da a entender que la actualización de hardware es en base a los informes de petición por fallos de equipos del municipio. Por otra parte, como reglamento del estado, todas las

instituciones seccionales deben usar software libre y realizar las actualizaciones de acuerdo al avance del mismo en programas o licencias.

4.2. DESARROLLO DE LA PROPUESTA

4.2.1. Planificación

4.2.1.1. Documentos de constitución

a) Misión y visión

- Misión

  Ser un elemento de apoyo para unidades educativas y gobiernos seccionales de la provincia del Carchi en la gestión de incidentes y fomentar una cultura de buenas prácticas en seguridad informática.

- Visión

  Ser un equipo reconocido a nivel nacional e internacional por su dedicación y aporte a la seguridad de la información.

b) Valores institucionales

- Trabajo en equipo

  Manteniendo una estructura organizacional para cumplir con nuestro trabajo de una manera eficiente y demostrando una buena calidad del servicio.

- Impacto social

  Fomentando buenas prácticas sobre la seguridad de la información y equipos en las instituciones educativas y seccionales de la provincia; de esta manera generamos un cambio positivo en el ámbito laboral.

- Compromiso

  Dejando lo mejor en cada servicio brindado y satisfechos por un trabajo que aporta al éxito de las instituciones y a nosotros como equipo.

- Empatía

  Entendiendo las circunstancias por las que pasan las instituciones y demostrar cordialidad y la atención que merecen.

- Mejora

  Al innovarnos como equipo aumentando servicios y mejorando la gestión de los mismos con la finalidad de adaptarnos a las nuevas tecnologías y los problemas que estas presentan, en especial del ámbito de seguridades.

- Integridad

  Al gestionar cada servicio asegurando la información que posee la institución y aumentando nuestra capacidad personal y laboral para generar confianza en nosotros y en lo que hacemos.
- Respeto

  Valorando el esfuerzo de cada integrante de CSIRT UPEC, acogiendo opiniones, escuchando órdenes, ayudando y trabajando con igualdad. Manteniendo una buena relación con las instituciones al no difundir información confidencial y demostrando total transparencia al otorgar nuestros servicios.

4.2.1.2. Comunidad objetivo

CSIRT UPEC es considerado como autoridad nula porque sus servicios son de asesoramiento, brindar información y dar recomendaciones frente a incidentes, sin embargo, no tiene autoridad en la toma de decisiones, estas son tomadas únicamente por las partes afectadas. El equipo gestiona los incidentes dependiendo del tipo de sistemas y operaciones que gestiona cada institución educativa y gobierno seccional, por lo que cada requerimiento es diferente. A continuación, se menciona la comunidad objetivo del CSIRT:

a) Académico
   - Unidades educativas pertenecientes al distrito 04D01 Tulcán-San Pedro de Huaca.
   - Unidades educativas pertenecientes al distrito 04D02 Montúfar-Bolívar.
   - Unidades educativas pertenecientes al distrito 04D03 Mira-Espejo.

b) Gubernamental
   - Gobierno Provincial del Carchi.
   - Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar.
   - Gobierno Autónomo Descentralizado Municipal de Espejo.
   - Gobierno Autónomo Descentralizado del Cantón Mira.
   - Gobierno Autónomo Descentralizado Municipal de Montúfar.
   - Gobierno Autónomo Descentralizado Municipal San Pedro de Huaca.
   - Gobierno Autónomo Descentralizado Municipal de Tulcán.

4.2.1.3. Servicios

CSIRT UPEC provee sus servicios al personal del área técnica de las unidades educativas y gobiernos seccionales de la provincia del Carchi.

a) Servicios reactivos

- Alertas y avisos

  CSIRT UPEC se encuentra al pendiente de eventos sobre seguridad informática a través de diversas fuentes, como: foros, noticias, correo electrónico, sitios web de otros CSIRTs, información publicada en internet, entre otras.

  Esto con la finalidad de dar avisos o alertas a la comunidad objetivo sobre virus, información engañosa, intrusión, vulnerabilidades o ataques que se están presentando en la actualidad. Además, proporciona recomendaciones o medidas preventivas a corto o largo plazo.

- Manejo de incidentes

  CSIRT UPEC apoya en la solución o mitigación de incidentes de seguridad informática a las instituciones educativas y gubernamentales del Carchi. Gestiona el proceso de reportes y solicitudes, realiza el triage en donde lleva a cabo un análisis inicial para determinar el procedimiento y su nivel de criticidad, analiza el evento y genera recomendaciones que ayuden en correcciones o soluciones.

b) Servicios proactivos

- Anuncios

  CSIRT UPEC emite anuncios a sus miembros, para que les permita estar a la vanguardia en temáticas de seguridad informática e información de interés relacionadas con sus operaciones diarias. Entre la temática de los anuncios se incluye: tendencias tecnológicas, seguridad informática, tips de productividad, recomendaciones de mejores prácticas, concientización tecnológica, entre otras.

  Los comunicados permiten a los miembros proteger sus sistemas y redes de nuevos problemas antes de que éstos sucedan.

c) Servicios de mejoras de la calidad

- Concientización tecnológica

  CSIRT UPEC, está comprometido en la concientización de seguridad informática y toma la iniciativa de acercarse a las organizaciones miembro con temas que son de interés y de gran aporte en la gestión laboral, proporcionando información para cumplir mejor las políticas, procesos y actividades en la organización mediante capacitaciones, publicación de artículos y contenido multimedia en el sitio web del equipo. Se pretende reducir significativamente los incidentes y aumentar la

capacidad de detectar vulnerabilidades para que los sistemas sean protegidos o recuperados en menor tiempo.

4.2.1.4. Organización y RRHH

a) Modelo organizacional

CSIRT UPEC adopta el modelo incrustado, pues se encuentra ubicado en las instalaciones del laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi, por lo que hace uso de sus recursos para desarrollar sus actividades relacionadas en la gestión de incidentes.

b) Estructura organizacional

CSIRT UPEC conforma su estructura organizacional con tres departamentos: dirección, tecnología y operaciones tomando en cuenta la comunidad objetivo y los servicios con los que inicia sus operaciones. Consideramos importante el departamento de dirección para que se tenga el control de las operaciones de CSIRT UPEC, el departamento de operaciones quien se encarga de la gestión de incidentes y el departamento de TI que se encarga de la administración de sistemas y brinda soporte a los demás departamentos.

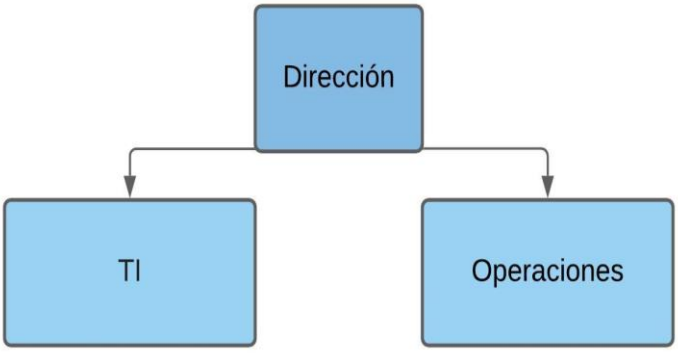


Figura 1. Estructura organizacional de CSIRT UPEC

c) Funciones y responsabilidades

Tabla 18. Funciones y responsabilidades en el CSIRT

Departamento	Funciones	Responsabilidades
Dirección	El director del CSIRT establece metas, objetivos y planes que colaboren en el bienestar de las organizaciones y cumplimiento de la misión del equipo,	- Gestión estratégica. - Control de actividades. - Cooperación externa. - Portavoz.

	supervisar el trabajo y desempeño del equipo asegurando el correcto cumplimiento de procesos y políticas organizacionales, ser el enlace con otros equipos, organizaciones y entidades externas que aporten en el crecimiento operacional, y ser el portavoz en los medios de comunicación.	
TI	El departamento de TI supervisa y administra el sitio web, sistemas tickets, correo electrónico y redes sociales que maneja al equipo CSIRT, incluyendo su infraestructura tecnológica. Además, da soporte y apoyo al departamento de operaciones generando mayor capacidad de respuesta a incidentes.	- Administrador de la infraestructura tecnológica.
Operaciones	El departamento de operaciones se encarga de realizar la gestión de incidentes que son reportados por las instituciones objetivo. Además, se encarga de monitorear y realizar un seguimiento de los incidentes que ya fueron atendidos.	- Gestión de incidentes. - Monitoreo.

4.2.2. Ejecución

4.2.2.1. Instalaciones e infraestructura TI

a) Servidor web

Como se muestra en la figura 2, el sistema operativo CentOS 7 se encuentra instalado y configurado en el servidor del laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi, como espacio que aloja el sitio web de CSIRT UPEC, sistema operativo seleccionado porque opera de forma rápida, con menos vulnerabilidad a virus o ataques, su distribución es gratuita y más seguro. La adecuación y

configuración del servidor CentOS 7 para la implementación del servidor web se encuentra en el anexo 14.

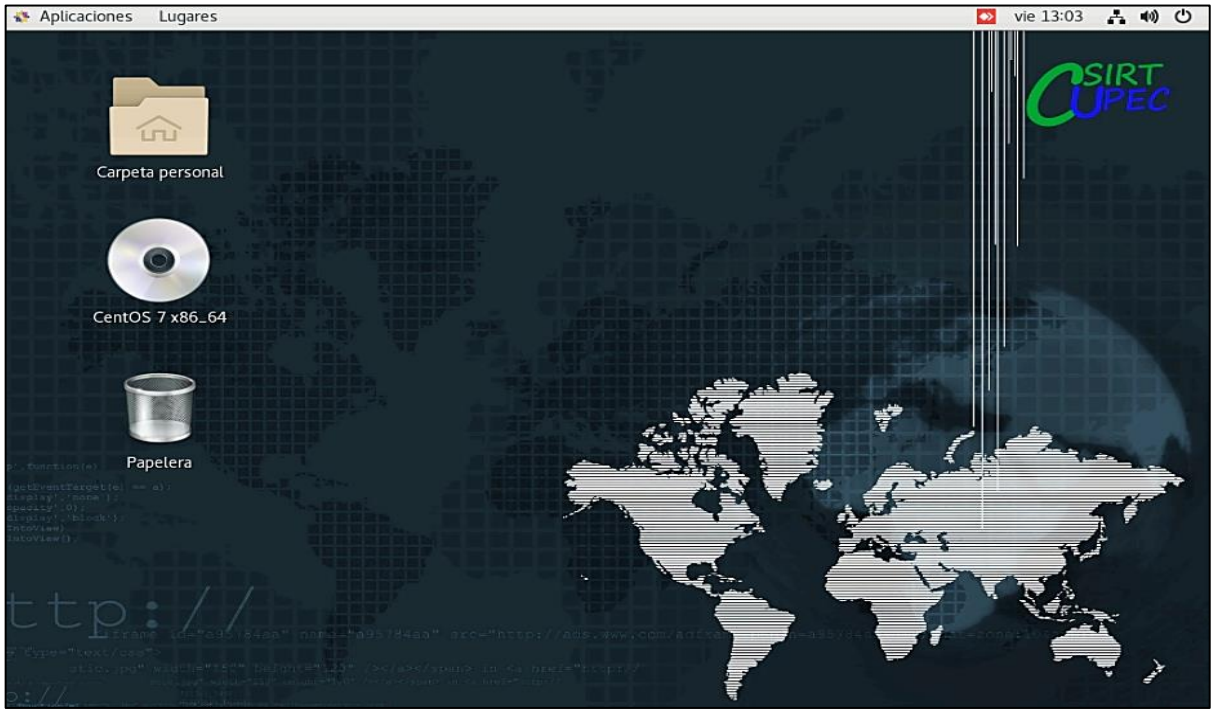


Figura 2. Servidor web con sistema operativo CentOS7

Como se muestra en la figura 3, se utiliza el gestor de contenido WordPress en su versión 5.7 en el desarrollo del sitio web de CSIRT UPEC, seleccionado porque es de código abierto y gratuito, permite la creación de un sitio web elegante, moderno y de alta calidad. La instalación y configuración se muestra en los anexos 15 y 16.

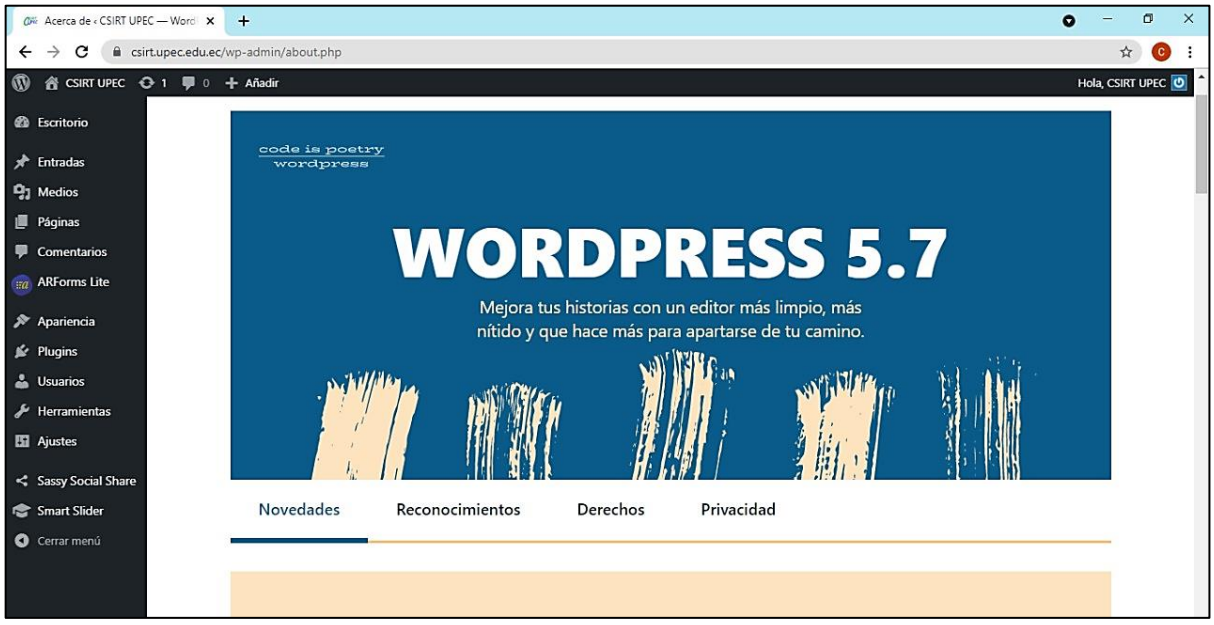


Figura 3. Gestor de contenido WordPress para el sitio web público del CSIRT

Como se muestra en la figura 4, en la cabecera del sitio web se encuentra el nombre del sitio y una descripción, el menú de navegación donde se encuentran los enlaces que direccionan a las diferentes páginas del sitio y una caja de búsqueda para encontrar información de forma rápida, elementos que forman parte de todas las páginas. Además, para la página de inicio se encuentra un carrusel dinámico que muestra imágenes junto con frases sobre seguridad de la información como parte del servicio sobre concientización tecnológica. La creación y configuración de las vistas se muestra en los anexos 17 y 18.

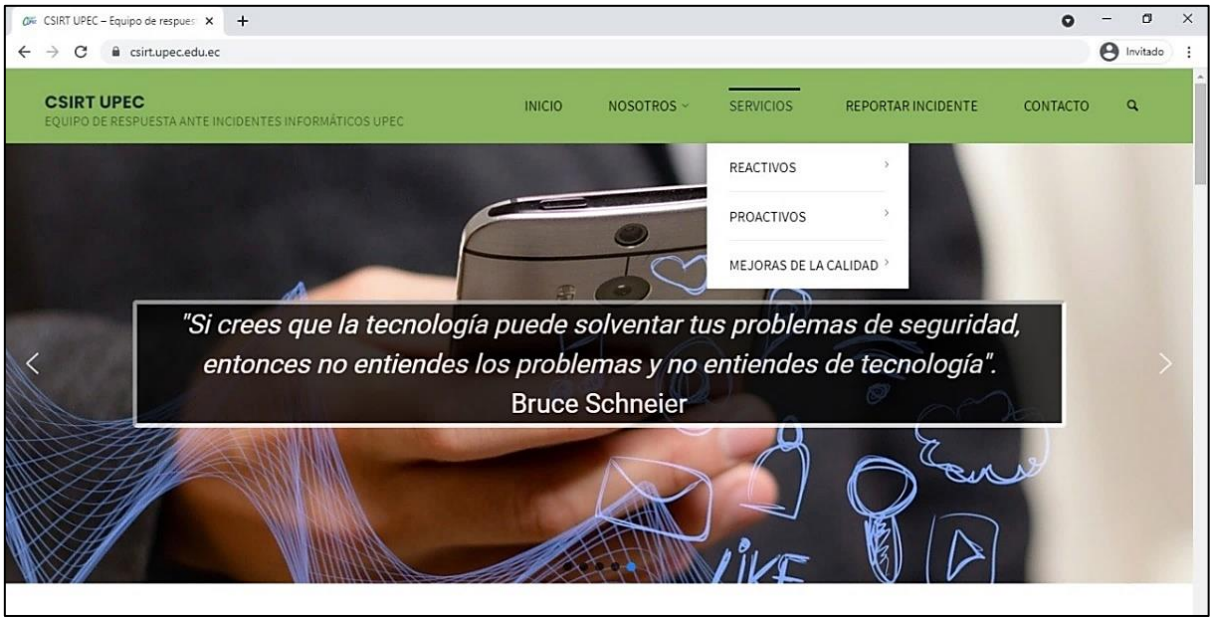


Figura 4. Cabecera página de inicio del sitio web público

En el cuerpo de la página de inicio se encuentran las entradas como parte de los servicios anuncios y concientización tecnológica, muestran información con temáticas en seguridad de la información presentadas dinámicamente en cuadros, donde se observa su categoría, fecha de publicación y un botón que permite conocer más del tema como se muestra en la figura 5.



Figura 5. Cuerpo página de inicio del sitio web público

En la figura 6 se muestra la página nosotros, donde se encuentra el logo de CSIRT UPEC, un resumen de lo que fue trabajar en la conformación del CSIRT con todos los involucrados, la pasión como equipo para cumplir con los servicios que se ofrece, la misión y visión que mencionan el ser un elemento de apoyo para la comunidad objetivo y los valores institucionales que identifican al equipo.



Figura 6. Página nosotros del sitio web público

En la figura 7 se muestra la página norma RFC 2350 donde se publica la información del CSIRT para la gestión de sus operaciones, este comprende de información como equipo, políticas, procesos, involucrados y limitaciones, mismos que son de vital importancia para que un equipo funcione de manera correcta y transparente con la comunidad objetivo.



Figura 7. Página norma RFC 2350 del sitio web público

En la figura 8 se muestra la página manual, donde se publica a detalle las políticas y procesos que forman parte de las operaciones del CSIRT, su publicación permite a los usuarios conocer y los lineamientos con los que se maneja la información y la gestión de sus servicios.



Figura 8. Página manuales del sitio web público

Como se observa en la figura 9, en la página de servicios se da a conocer información sobre los servicios que ofrece CSIRT UPEC a sus miembros y al final se muestra un enlace en el texto que direcciona al formulario de reporte de incidentes. Además, en la parte lateral derecha se exponen los temas de las publicaciones realizadas como enlaces que direccionan a su información, elemento que se visualiza en todas las vistas a excepción de la de inicio.

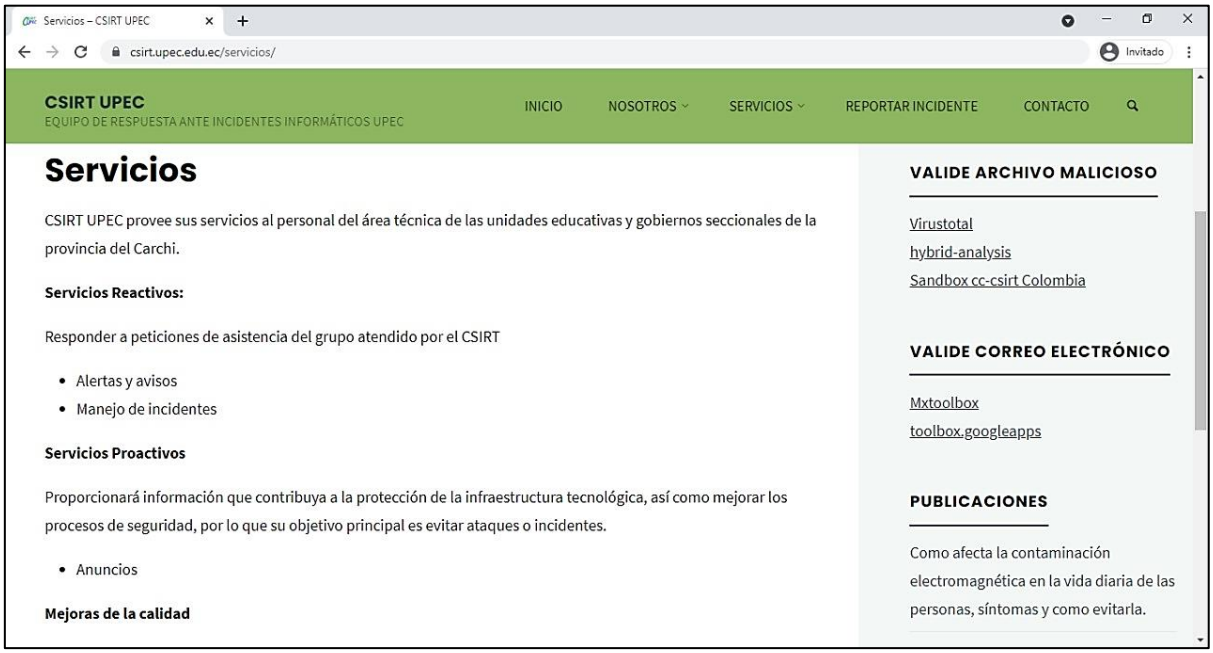


Figura 9. Página de servicios del sitio web público

La figura 10 muestra la página del servicio alertas y avisos, donde se describe detalladamente el servicio y los medios que utiliza el equipo para brindarlo. Además, al final de la página se encuentra un texto con un link que direcciona a la página de contacto en caso de requerir más información o el servicio.

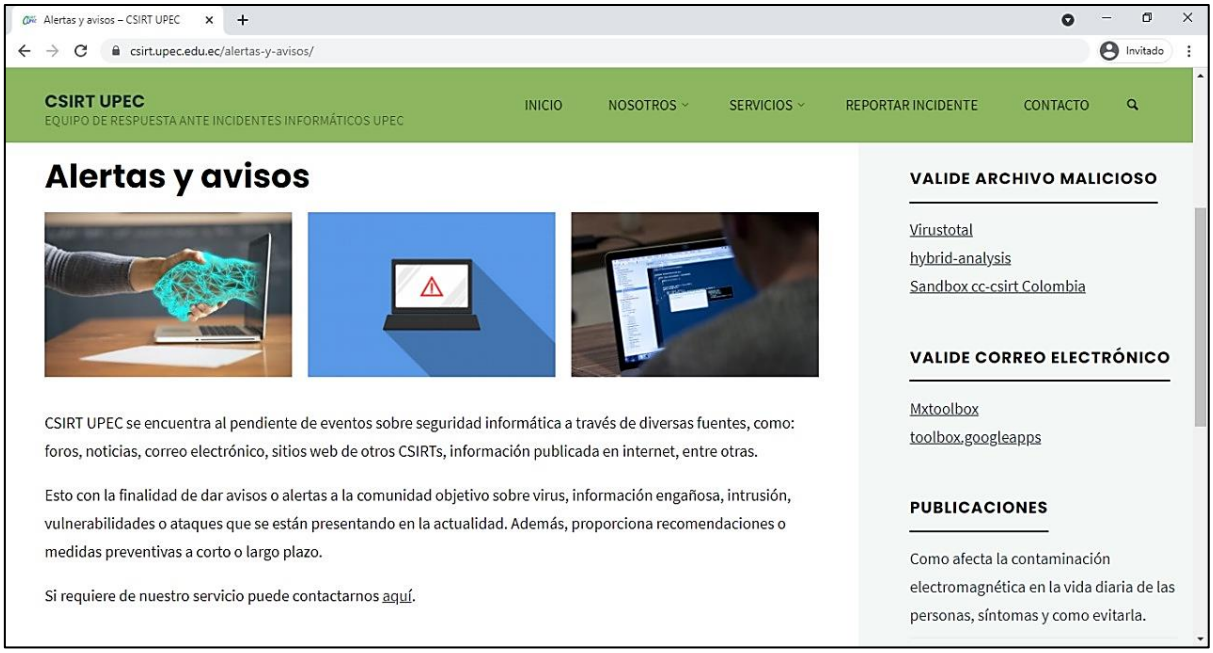


Figura 10. Página del servicio alertas y avisos del sitio web público

En la figura 11 se muestra la página del servicio manejo de incidentes del CSIRT, donde se menciona la comunidad objetivo a la que brinda ayuda en la mitigación o solución de incidentes. Muestra las maneras para reportar un incidente informático, la primera es por medio del formulario del sistema de tickets Centro de Respuesta y Soporte a Incidentes Informáticos, la otra opción es el formulario del sitio web; y mediante el correo electrónico del equipo denominado csirt.computacion@upec.edu.ec, en esta sección también se encuentra el botón de descargar formulario de reporte. Para saber el estado de la gestión del incidente se da clic sobre el botón centro de respuesta y soporte a incidentes de seguridad.



Figura 11. Página del servicio manejo de incidentes del sitio web público

La figura 12 muestra la página del servicio anuncios, donde se da conocer detalladamente información sobre el servicio, destacando información en sus diferentes categorías: tendencias tecnológicas, seguridad informática, tips de productividad, recomendaciones de mejores prácticas, concientización tecnológica y otros puntos que les permitan a las unidades educativas y gobiernos seccionales estar, al tanto en temáticas que se relacionan con los sistemas que manejan u operaciones que realizan, como parte de sus labores diarias, esto como una forma de prevenir incidentes. Además, al final de la página se muestra el link que se direcciona a la página de contacto en caso de requerir más información.



Figura 12. Página del servicio anuncios del sitio web público

La figura 13 muestra la página del servicio concientización tecnológica, donde se da a conocer detalladamente información sobre el servicio, destacando el proceso y mencionando los propósitos al brindar dicho servicio a la comunidad objetivo. Al final se muestra el link de la página de contacto en caso de requerir más información.



Figura 13. Página del servicio concientización tecnológica del sitio web público

En la figura 14 se muestra la página de reporte de incidentes, aquí se encuentra el formulario de reporte que contiene información acerca del servicio y la sección de

información de contacto, donde se pide los nombres completos del solicitante, dirección de correo electrónico como contacto para enviar la recepción del ticket y las recomendaciones de solución, teléfono de contacto, el tipo de organización y su nombre.

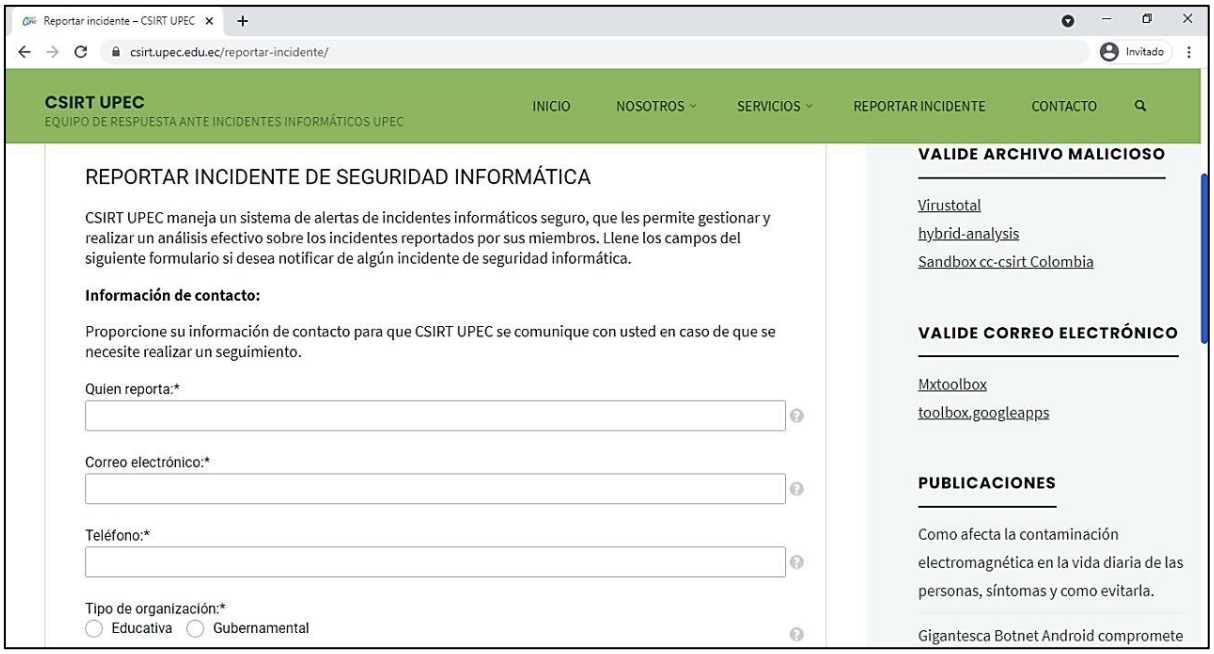


Figura 14. Parte uno de la página reportar incidente del sitio web público

Además, se pide la fecha y hora aproximada en la que ocurrió el incidente y un cuadro de texto donde se pide detallar el incidente para comprender mejor la situación y ser puntuales en las recomendaciones de solución. Antes de enviar el formulario se debe aceptar la política de privacidad que maneja CSIRT UPEC como se muestra en la figura 15.

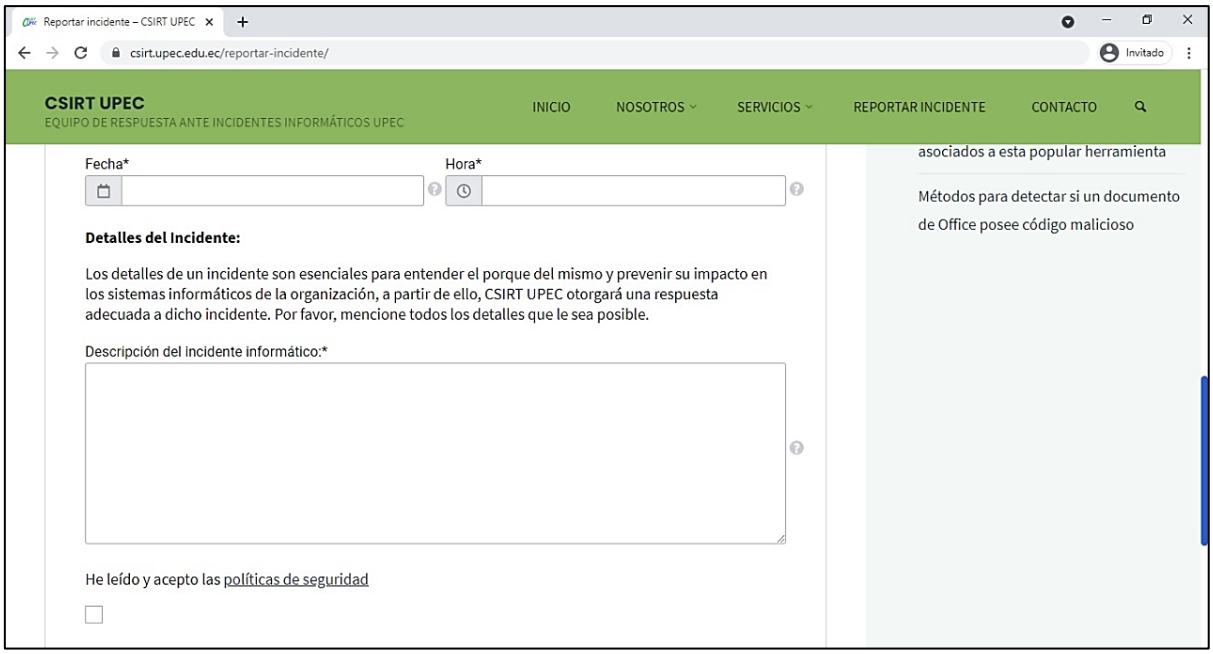


Figura 15. Parte dos de la página reportar incidente del sitio web público

La figura 16 muestra la página de contacto donde se encuentra la dirección de las instalaciones de CSIRT UPEC, correo electrónico institucional, teléfono de contacto, el link que direcciona a la página de manejo de incidentes en caso de requerir reportar un incidente y de la página de nosotros para conocer sobre el equipo; y se tiene el mapa de ubicación para localizar las instalaciones.

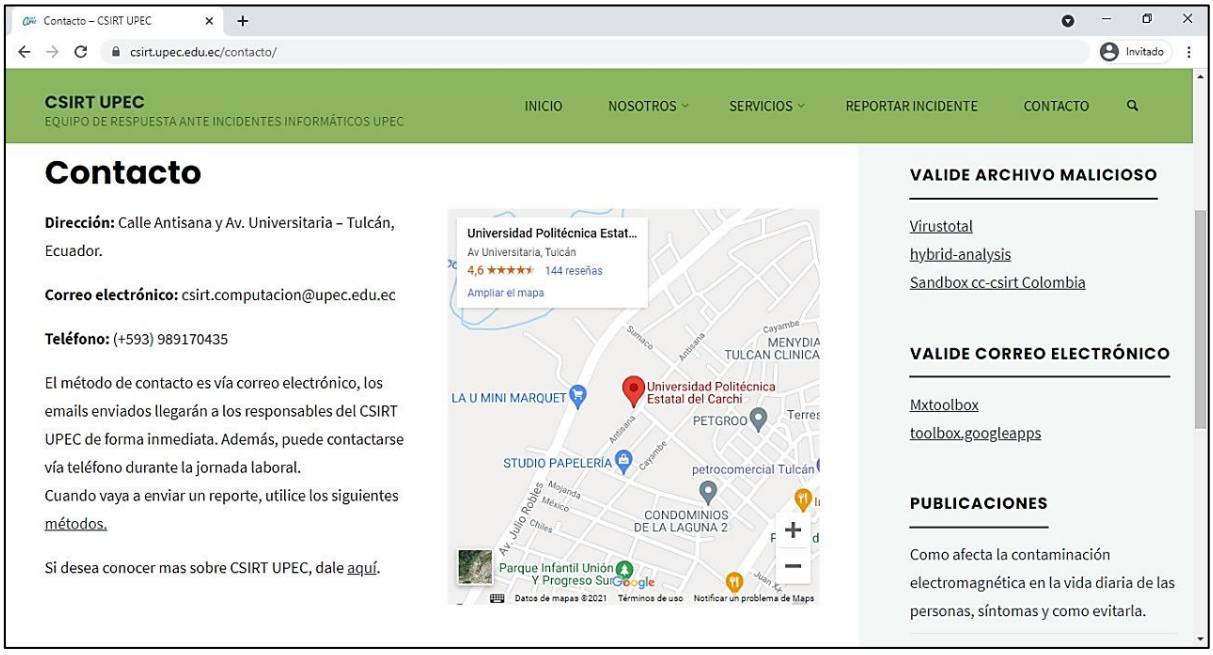


Figura 16. Página contacto del sitio web público

b) Servidor de registro y seguimiento de incidentes

Como se muestra en la figura 17, para realizar el registro y seguimiento de los incidentes informáticos reportados y servicios solicitados a CSIRT UPEC, se utiliza el software de soporte al cliente OSTicket en su versión 1.15-git(cb6766e5). Su página principal muestra el nombre del sistema de tickets "Centro de Respuesta y Soporte a Incidentes de Seguridad", los logos que identifican a la institución, descripción del funcionamiento del sistema en la asignación de tickets, seguido por un enlace que direcciona a la página de CSIRT UPEC y un video tutorial para conocer su funcionamiento. La configuración del servidor de registro y seguimiento a incidentes se encuentra en el anexo 19.



Figura 17. Página principal del sistema de tickets "Centro de Respuesta y Soporte a Incidentes de Seguridad"

En la página abrir un nuevo ticket se encuentra el formulario para crear un ticket, en la sección información de contacto se ingresa el correo electrónico, nombre completo del solicitante y número de teléfono como se muestra en la figura 18. En la sección temas de ayuda se despliegan varias opciones de servicio, CSIRT UPEC gestiona los temas de ayuda: CSIRT- Reportar incidente y CSIRT- Concienciación tecnológica.

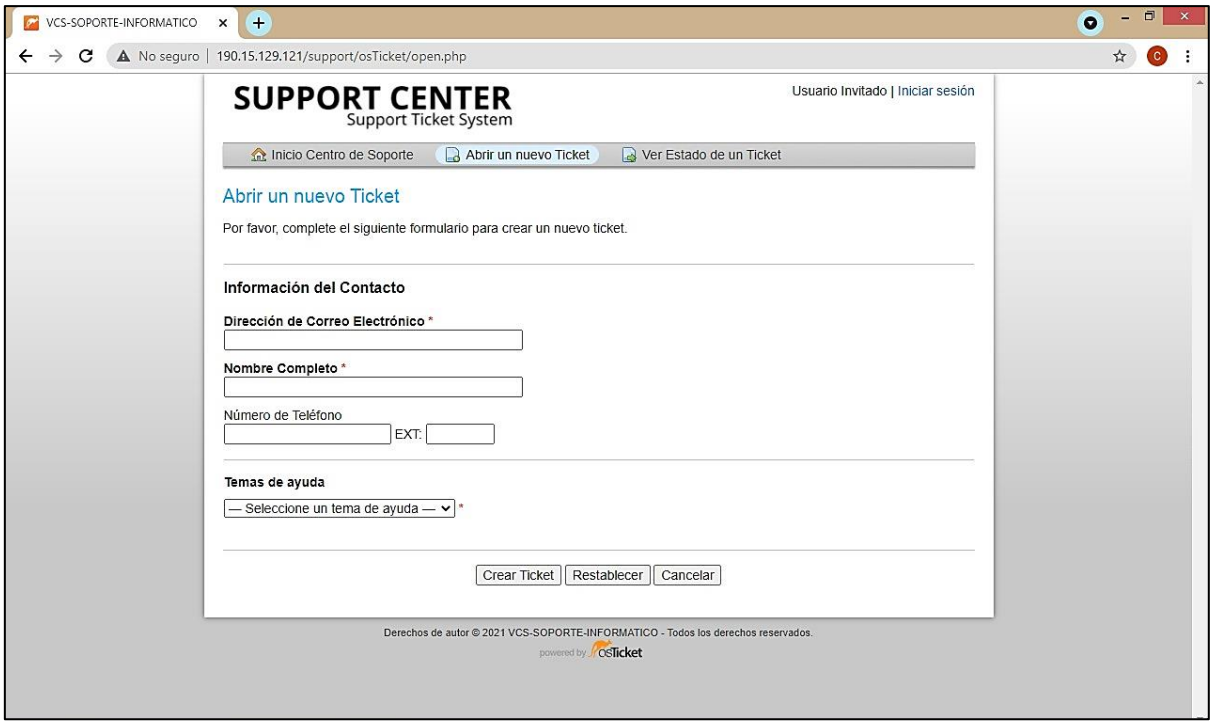


Figura 18. Vista cliente - Página abrir un nuevo ticket con la sección información de contacto y temas de ayuda

Al seleccionar el tema de ayuda < CSIRT- Reportar incidente > se despliega un formulario personalizado, donde se muestra una descripción corta sobre el manejo de incidentes informáticos, los campos tipo de organización donde se despliega las opciones educativa y gubernamental, nombre de la organización, estado actual del incidente donde se despliegan las opciones ya pasó, en curso, amenaza y desconocido y cuando se detectó el incidente donde se debe ingresar la fecha y hora aproximada del incidente. En la sección detalles del incidente, se muestra una descripción en la que se explica el beneficio de facilitar la información que le sea posible sobre el caso y el campo descripción de incidente informático, además se muestra la casilla para aceptar las políticas de seguridad establecidas por CSIRT UPEC y los botones crear, reestablecer y cancelar ticket como se muestra en la figura 19.

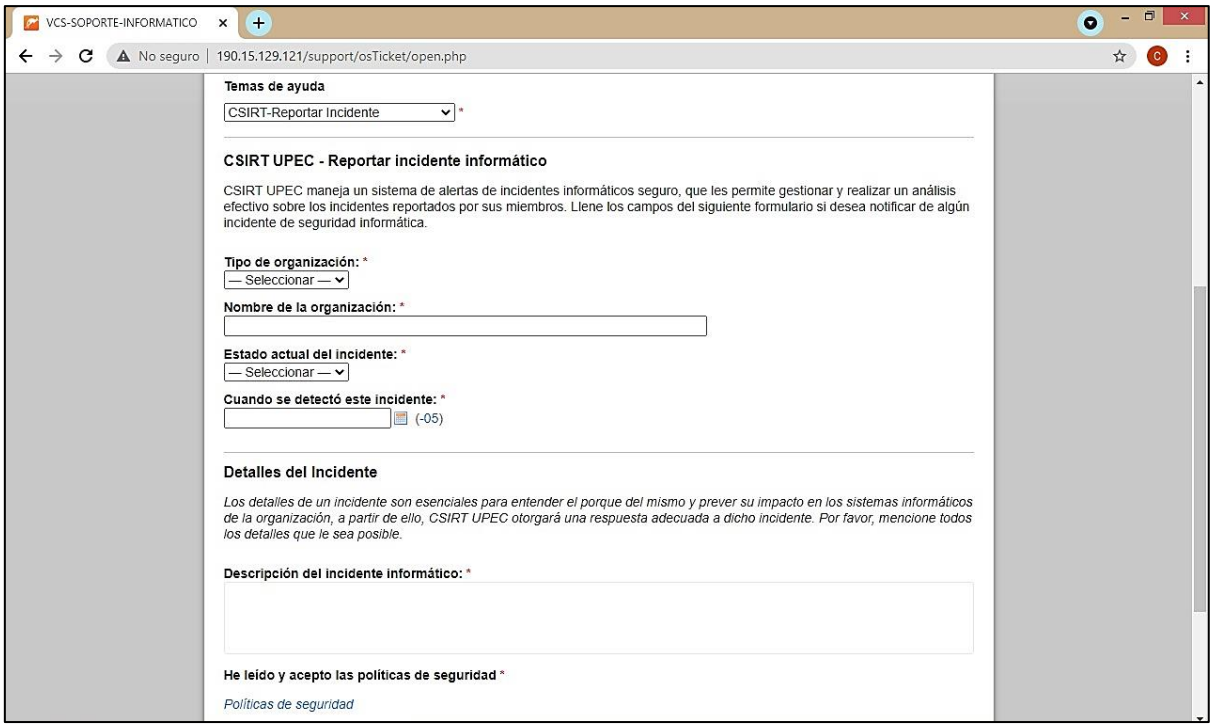


Figura 19. Vista cliente - Formulario del servicio para crear un ticket con el tema de ayuda CSIRT- Reportar incidente

Al seleccionar el tema de ayuda < CSIRT- Concienciación tecnológica >, se despliega un formulario personalizado donde se muestra una descripción corta sobre el servicio, el campo tipo de organización que muestra las opciones educativa y gubernamental y el campo nombre de la organización. En la sección detalles de la concientización se muestran los campos temática requerida, forma de concientización y fecha aproximada para el acercamiento, además, se muestran los botones para crear, reestablecer y cancelar ticket como se muestra en la figura 20.

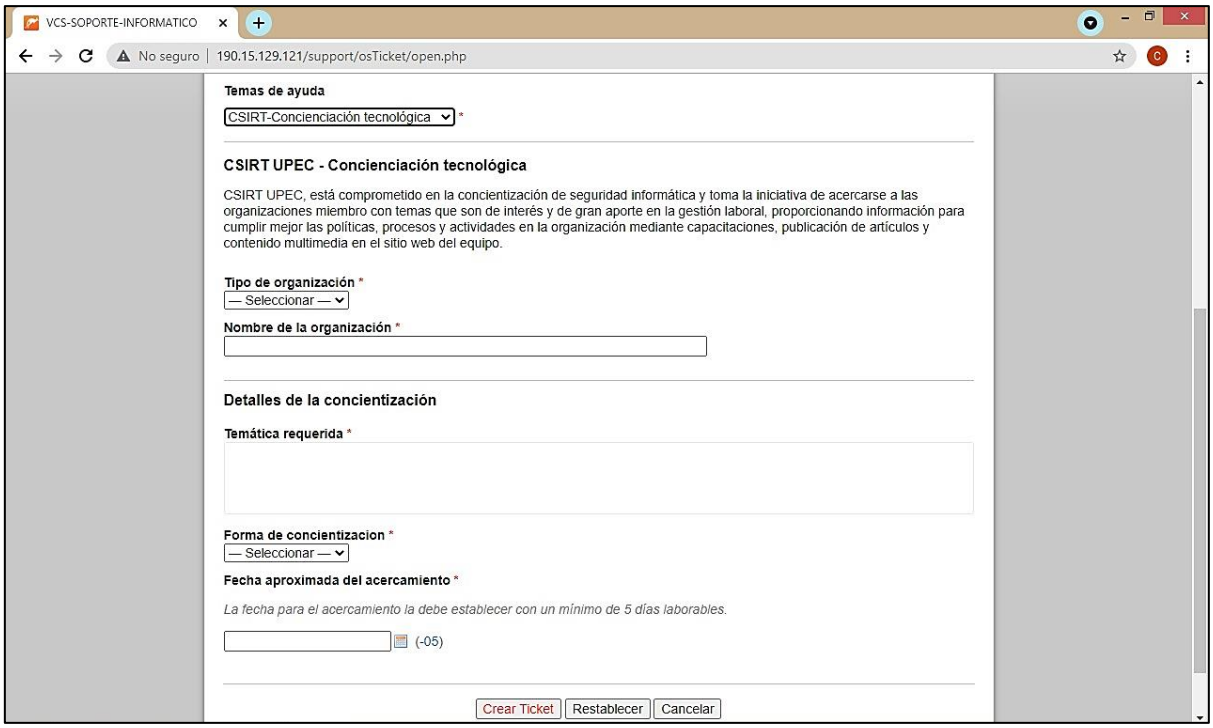


Figura 20. Vista cliente - Formulario del servicio para crear un ticket con el tema de ayuda CSIRT-Concienciación tecnológica

Luego de crear el ticket con el tema de ayuda seleccionado, aparece una página de agradecimiento con el logotipo de CSIRT UPEC, nombre de la persona que generó el ticket, mensaje de solicitud creada con éxito, instrucciones para realizar un seguimiento al ticket creado y la información de contacto con el equipo como se muestra en la figura 21.

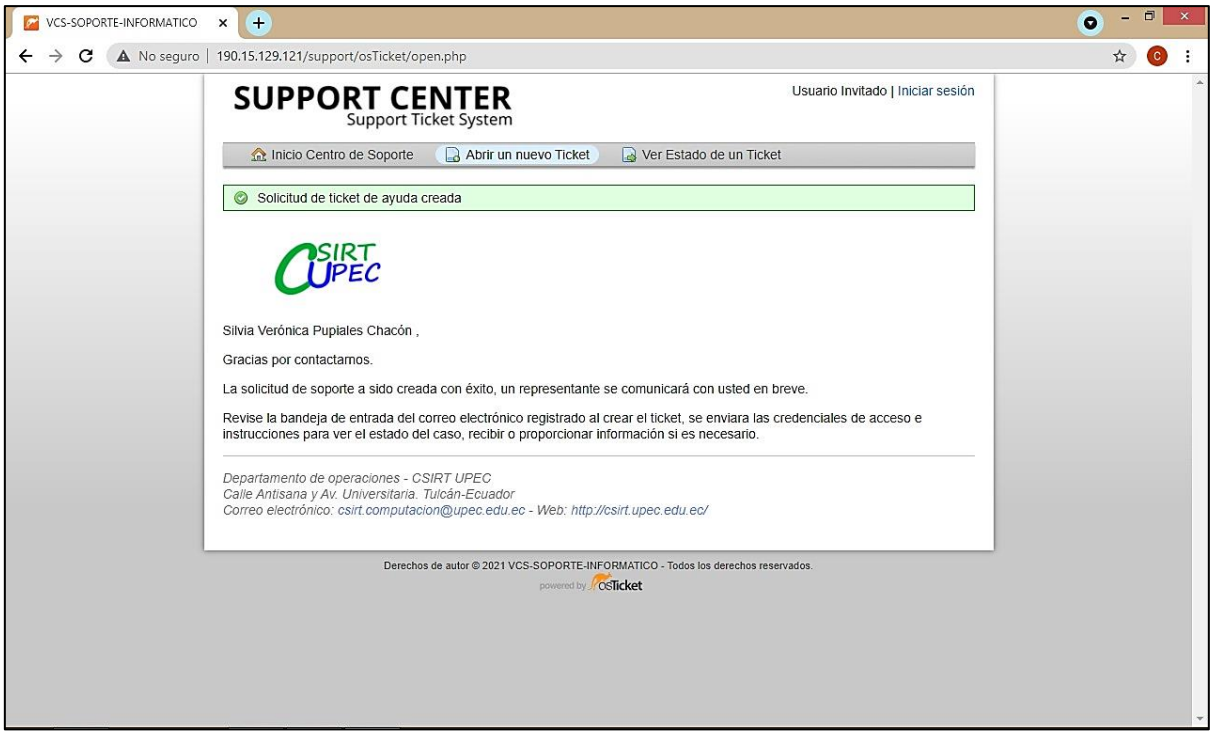


Figura 21. Vista cliente - Mensaje de ticket creado con éxito junto con instrucciones para ver su estado e información de contacto en el sistema de tickets

En la página registro de la cuenta se muestra un formulario para que el usuario que generó el ticket se registre, en la sección información de contacto se llenan los campos correo electrónico, nombre completo y número de teléfono, en preferencias se llena el campo de zona horaria, en la sección credenciales de acceso se registran los campos crear y confirmar contraseña y se encuentran los botones para registrarse o cancelar como se muestra en la figura 22.

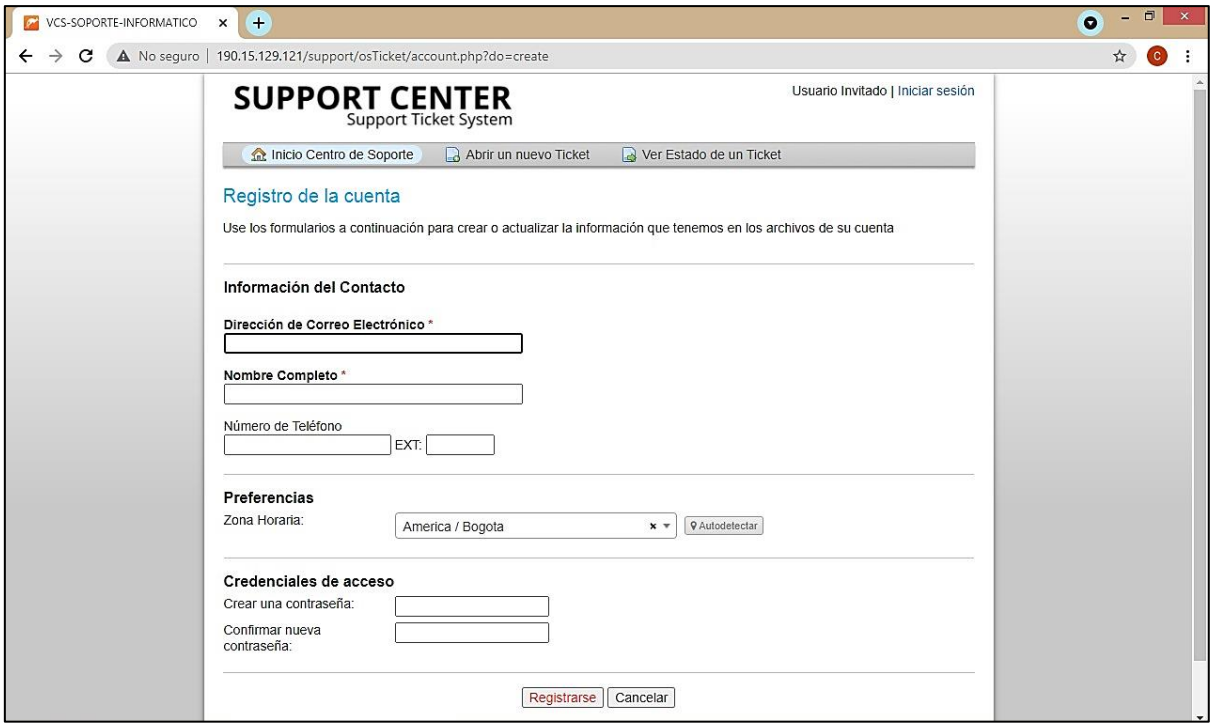


Figura 22. Vista cliente - Formulario de registro de cuenta en el sistema de tickets

Terminado el registro, se presenta una página con instrucciones para confirmar la cuenta y activar su acceso como se muestra en la figura 23.

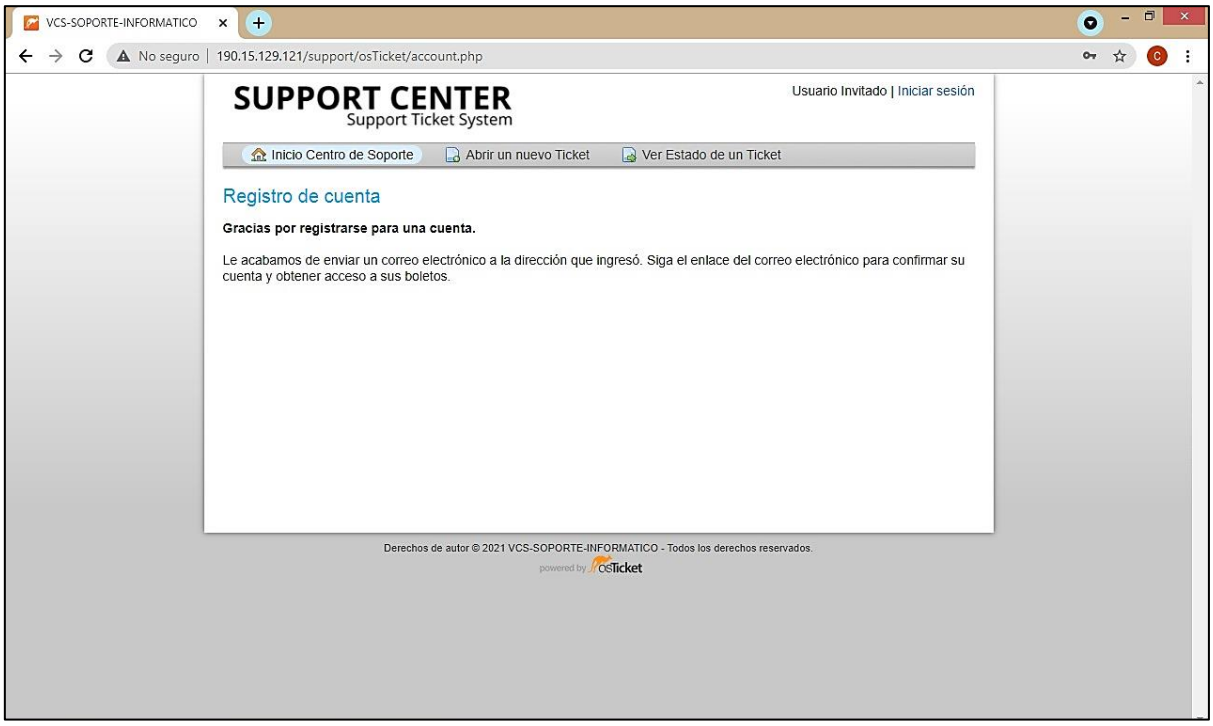


Figura 23. Vista cliente - Página de confirmación de registro del sistema de tickets

Al iniciar sesión como miembro del CSIRT, muestra su área de administración de tickets creados, donde se visualiza el número de ticket, su fecha de creación, estado, asunto (tema de ayuda) y departamento que lleva el caso como se muestra en la figura 24.

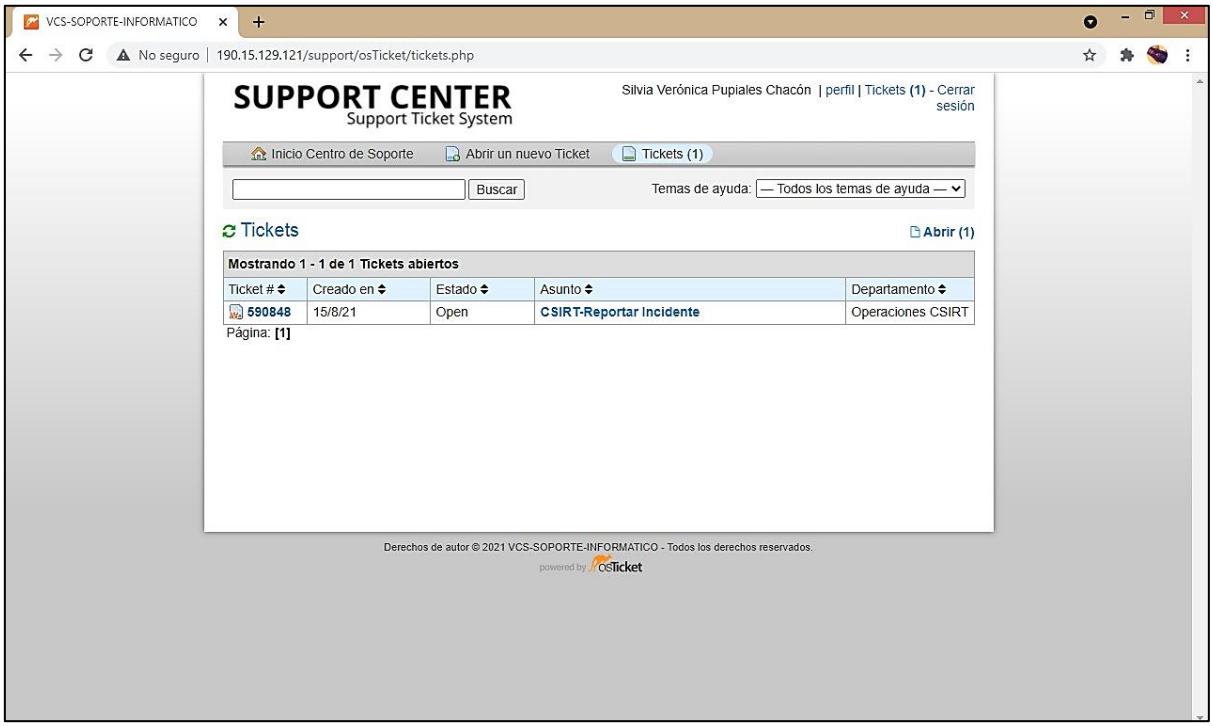


Figura 24. Vista cliente - Página de administración de tickets

Para dar seguimiento al ticket se da clic en número de ticket que se desea revisar y se visualiza su información básica, información de usuario, datos que proporcionó al crear el caso y un espacio para interactuar con el agente a cargo en caso de ser necesario como se muestra en la figura 25.

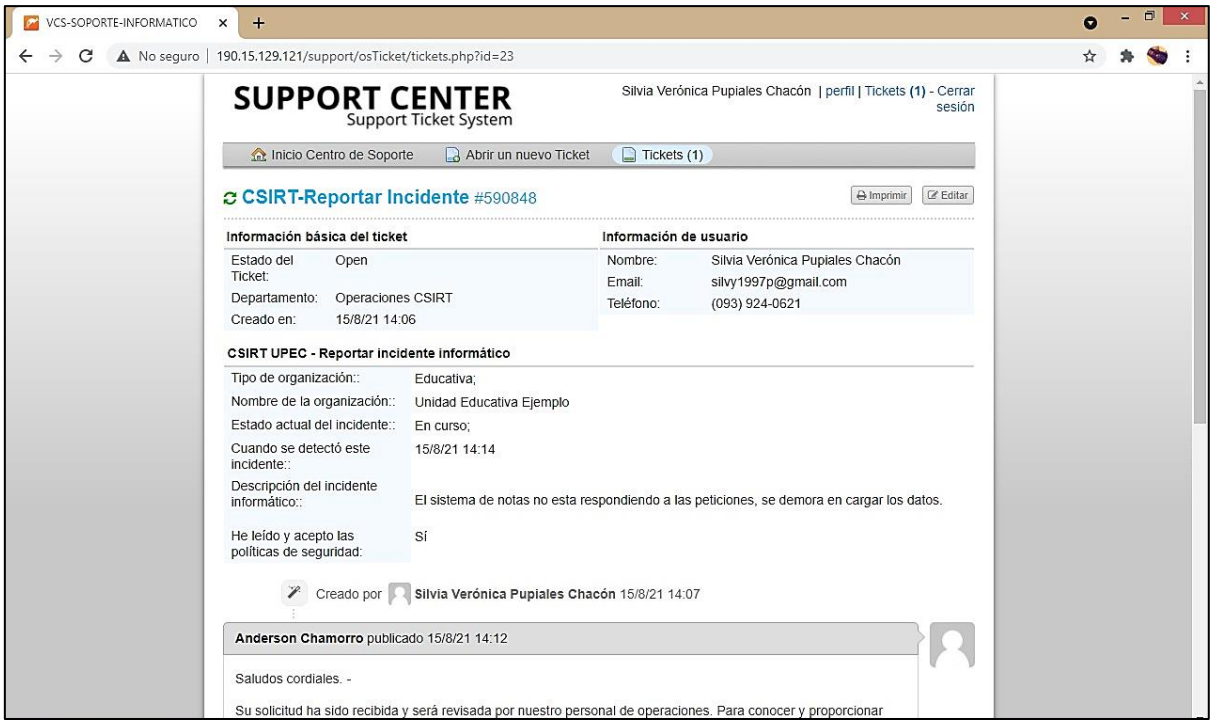


Figura 25. Vista cliente – Detalles del ticket y área de interacción con el agente a cargo del caso

Para le gestión de los tickets por parte del agente, se realiza el inicio de sesión al sistema de tickets con correo electrónico/nombre de usuario y contraseña como se muestra en la figura 26.

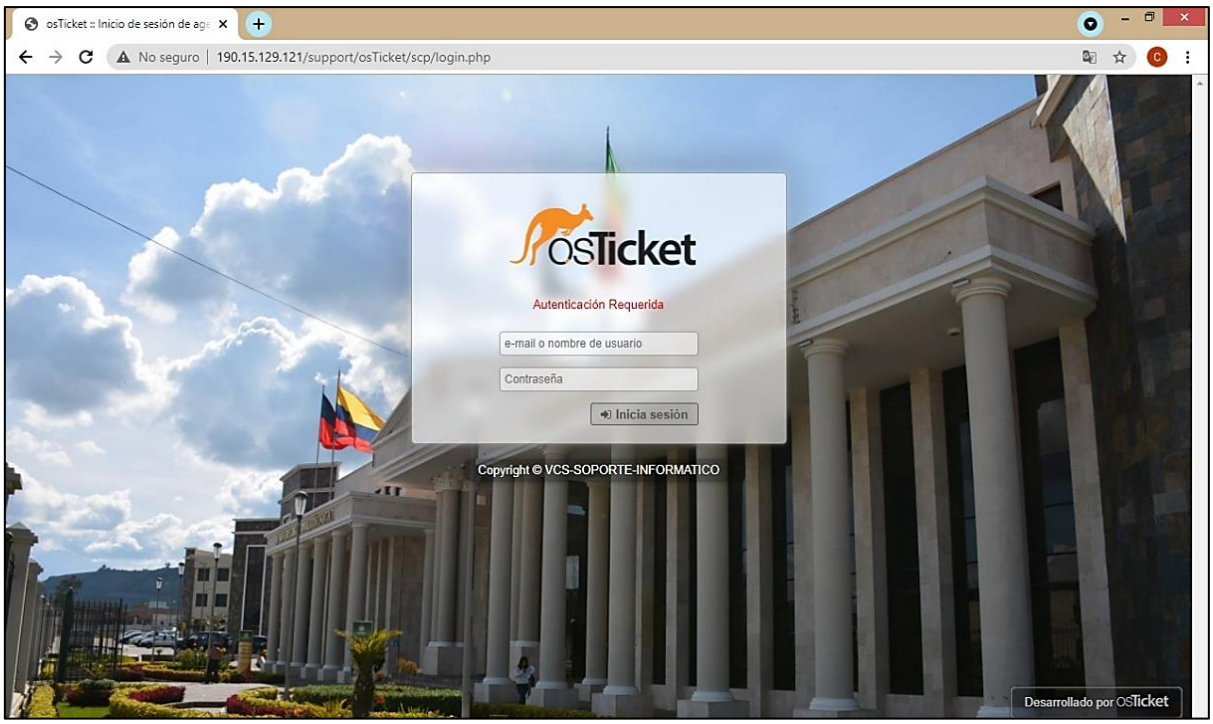


Figura 26. Vista agente – Inicio de sesión en el sistema de tickets

En el menú panel de control se observa las estadísticas de los tickets abiertos, asignados, atrasados, cerrados, reabiertos y borrados mediante una gráfica con líneas de diferentes colores como se muestra en la figura 27.

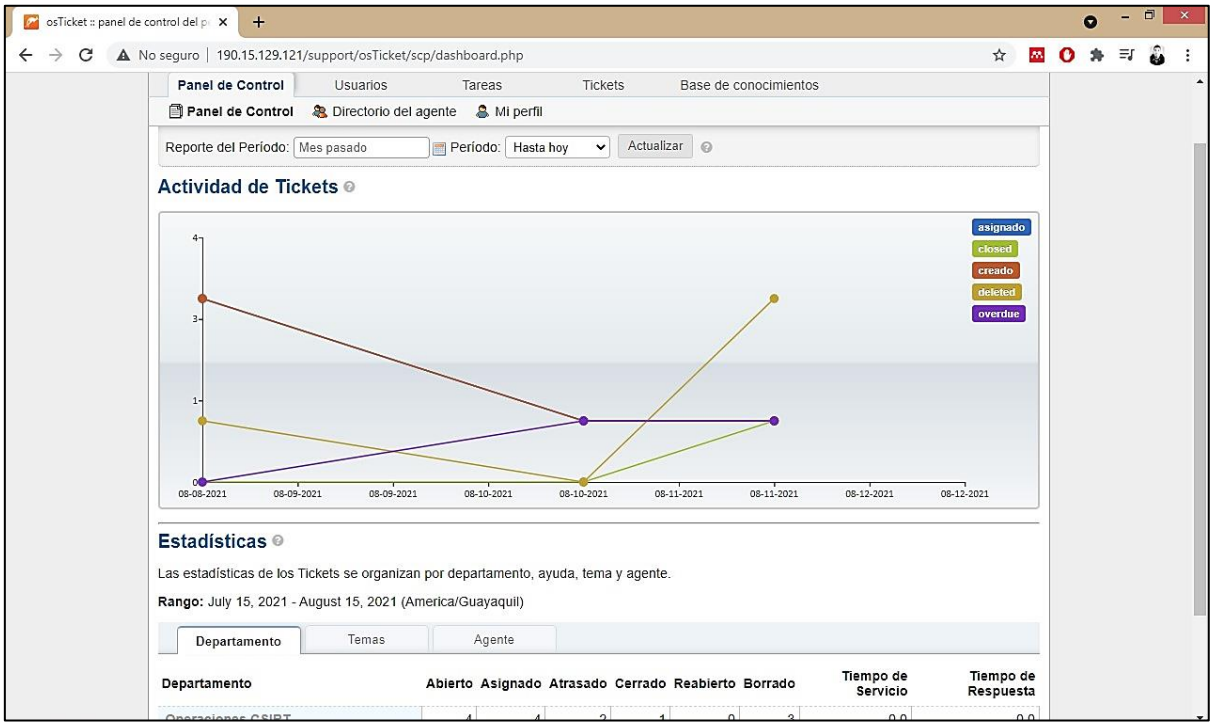


Figura 27. Vista agente – Reporte estadístico de actividad de los tickets en el menú panel de control

En el menú usuarios opción directorio de usuarios, se muestra el registro de todos los usuarios que han generado un ticket, se tiene el nombre, estado, la fecha de creación y actualización del perfil como se muestra en la figura 28.

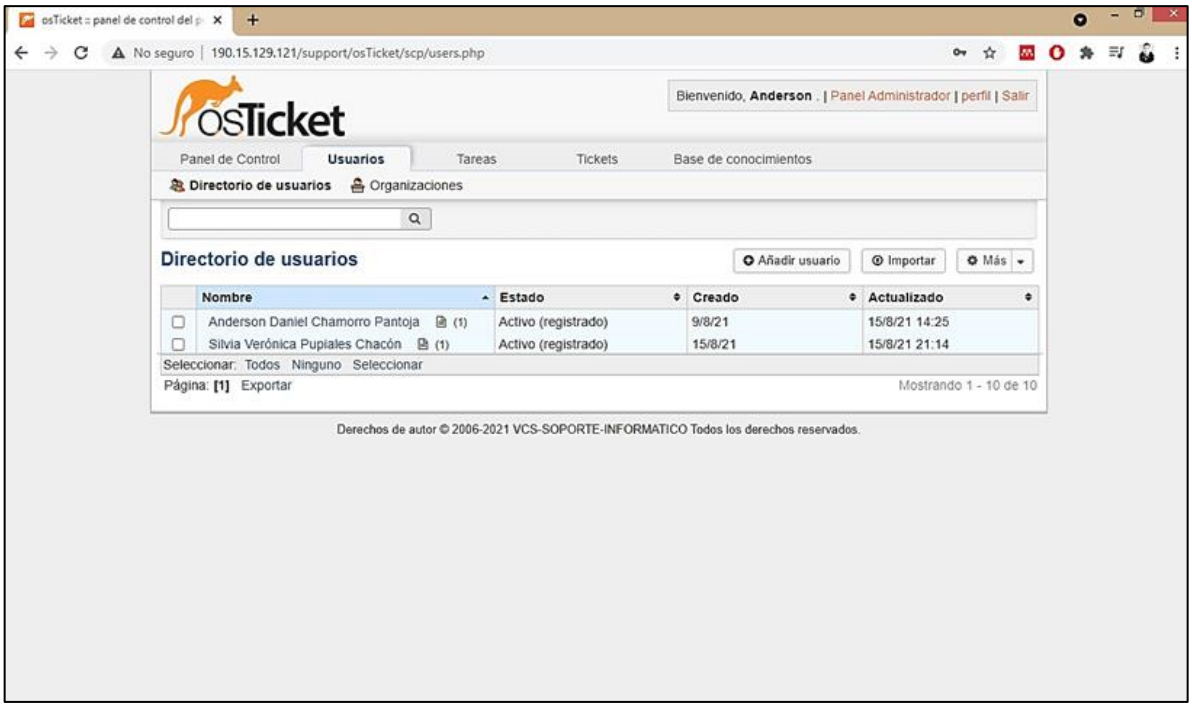


Figura 28. Vista agente – Directorio de usuarios registrados al sistema de tickets en el menú usuarios

En el menú usuarios opción organizaciones, se generan organizaciones para agrupar a los usuarios que solicitaron los servicios de CSIRT UPEC. Para ello se generan las organizaciones gobiernos seccionales provincia del Carchi y unidades educativas provincia del Carchi, en su panel de administración se muestra el nombre, el número de los usuarios y la fecha de creación y actualización de las organizaciones como se muestra en la figura 29.

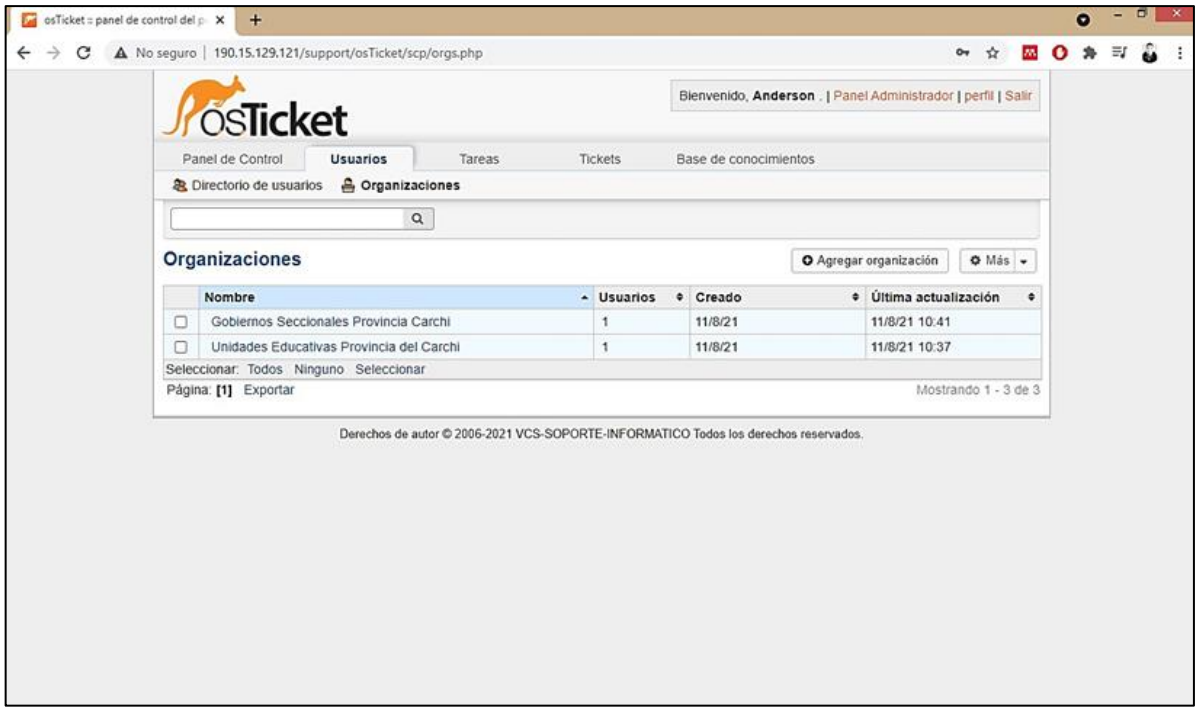


Figura 29. Vista agente – Administrador de organizaciones del sistema de tickets en el menú usuarios

En el menú tickets se muestran las opciones para ver los tickets con estado abierto y cerrado y tickets asignados por agente y equipo, se muestra información del número de ticket, su última actualización, tema de ayuda, usuario, el nivel de prioridad y el departamento encargado del caso, además, se encuentra la opción nuevo ticket para crear un nuevo ticket al usuario por parte del agente como se muestra en la figura 30.

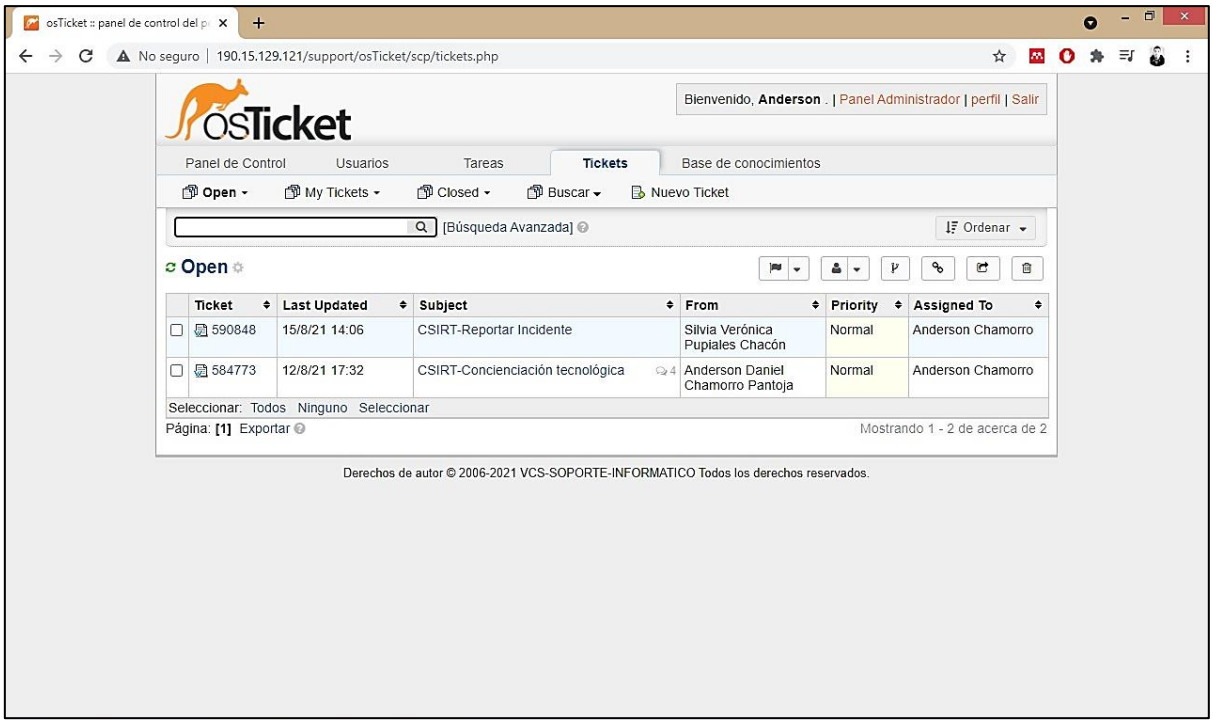


Figura 30. Vista agente – Administrador de tickets

Se da clic en el código de tickets para dar seguimiento al servicio solicitado por el usuario, esto permite gestionar los casos de manera correcta porque se define el estado, prioridad y se da respuesta a las solicitudes de los miembros como se muestra en la figura 31.

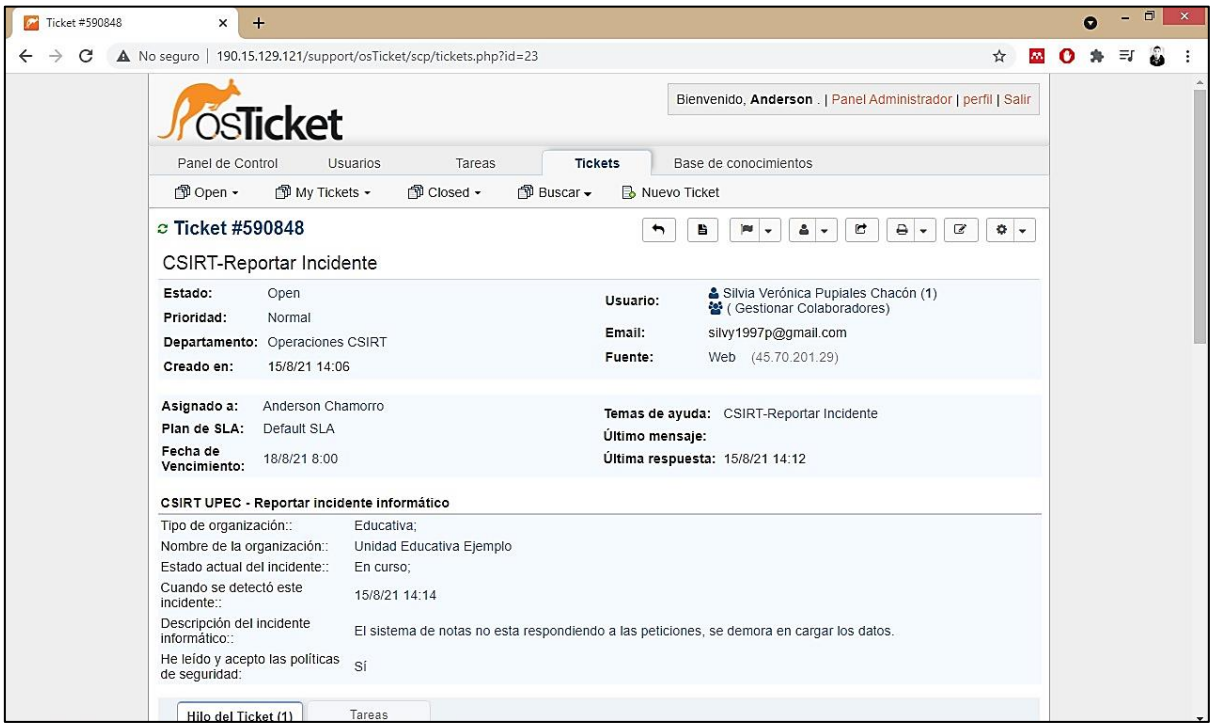


Figura 31. Vista agente – Seguimiento de tickets asignados

c) Servidor de monitoreo

Como se muestra en la figura 32, el sistema operativo Kali Linux 2021.2 se encuentra instalado y configurado en el servidor del laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi, como espacio que permite realizar prácticas de monitoreo de red, evaluación de vulnerabilidades, análisis de información, entre otras; sistema operativo seleccionado porque está diseñado para realizar monitoreo y auditoría informática en general.

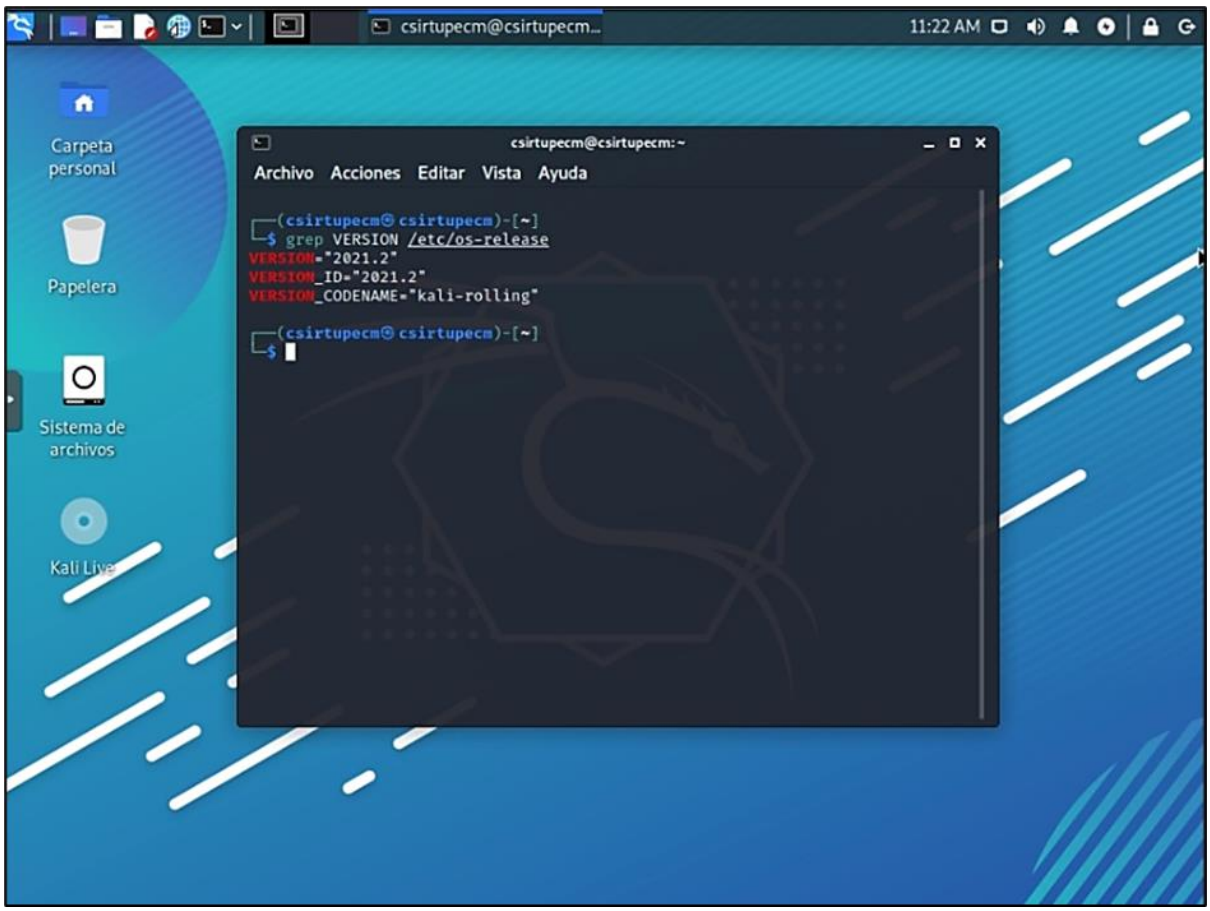


Figura 32. Sistema operativo Kali Linux para el servidor de monitoreo

Entre las herramientas que nos brinda Kali Linux, se encuentran:

La herramienta de código abierto nmap (mapeador de redes) se muestra en la figura 33, se utiliza en la detección de redes y auditoría, inventarios de red, gestión y actualización de programas y monitoreo de actividad del host de servicio. Es una herramienta flexible por sus técnicas avanzadas para trazar obstáculos como redes con filtros IP, cortafuegos o enrutadores, potente para el escaneo de redes con miles de máquinas y amplia en funciones que se adaptan a las preferencias tanto en línea de comandos como gráfica.

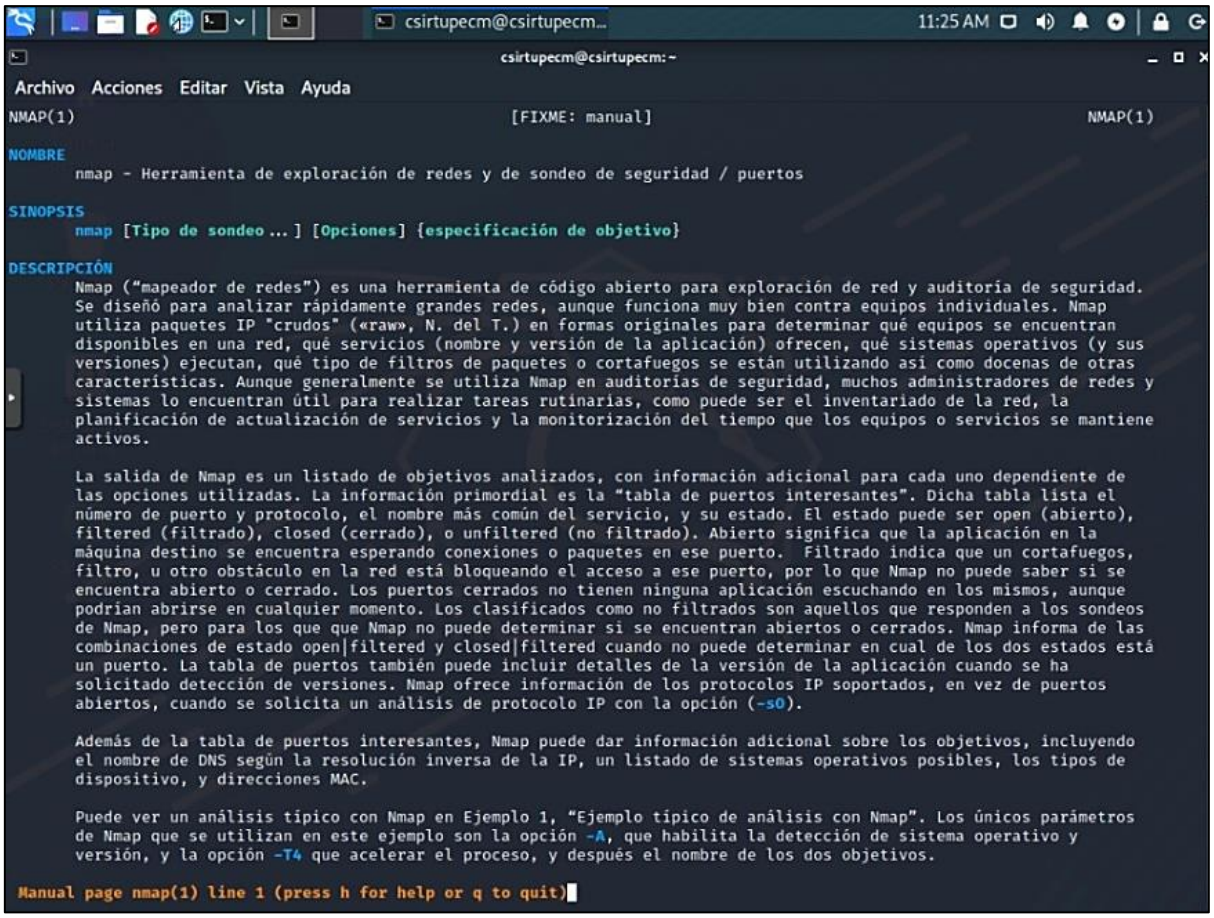


Figura 33. Herramienta de código abierto nmap

En la figura 34 se muestra el analizador de protocolos de red Wireshark que permite ver lo que sucede en la red, aparte de ello, es una excelente aplicación didáctica que ayuda en los problemas de red y estudio de comunicaciones. Se puede mirar cada capa del paquete monitoreado y facilita varias opciones de administración para realizar análisis de tráfico.

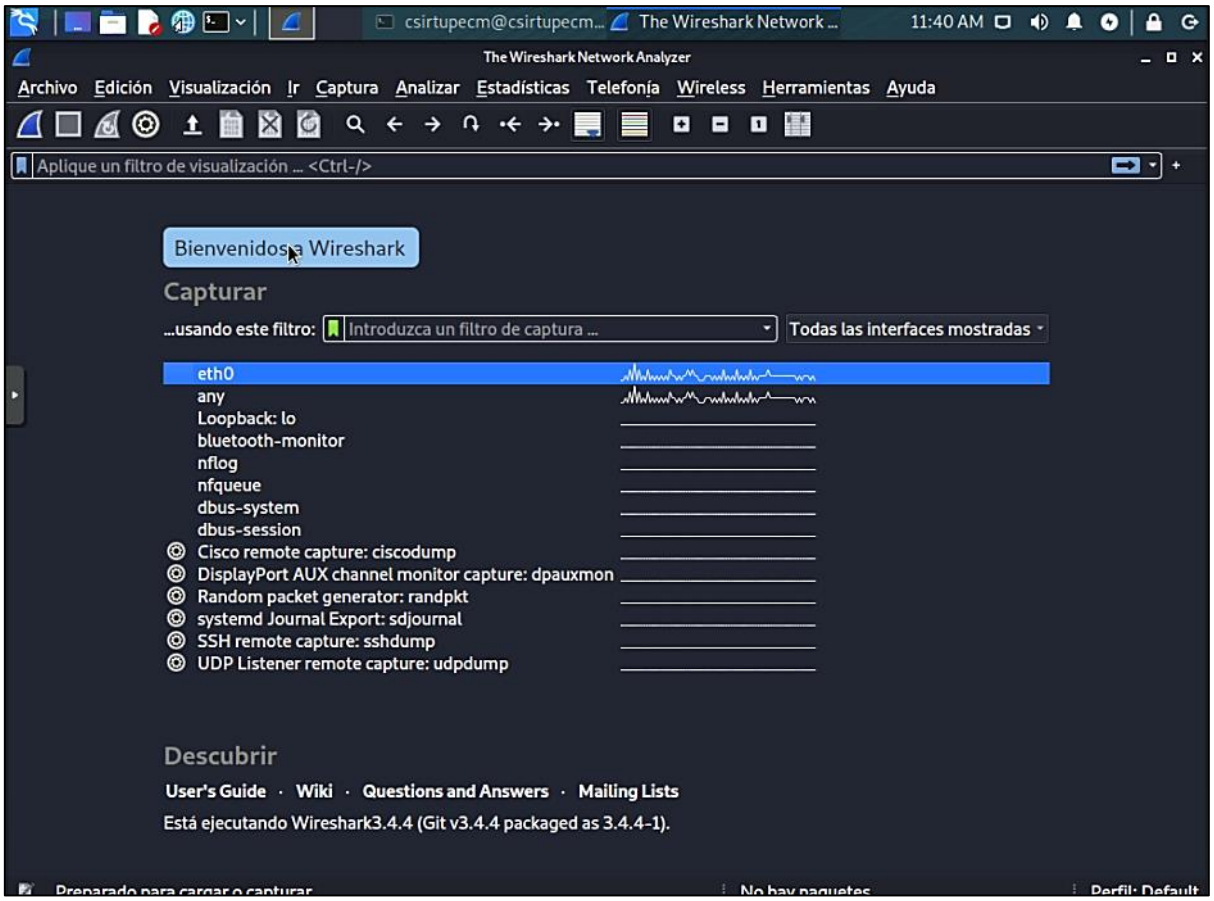


Figura 34. Analizador de protocolos de red Wireshark

En la figura 35 se muestra la herramienta WhatWeb, permite reconocer sitios web de manera cuidadosa y rápida o emitir un informe completo, realiza el equilibrio de confidencialidad y velocidad de resultados al punto de interrogar más a uno o varios sitios web que impulsan el sitio web principal. WhatWeb contiene más de 15 pruebas que incluyen la verificación de favicon, las páginas de inicio de sesión, contenido y los archivos de instalación predeterminados.

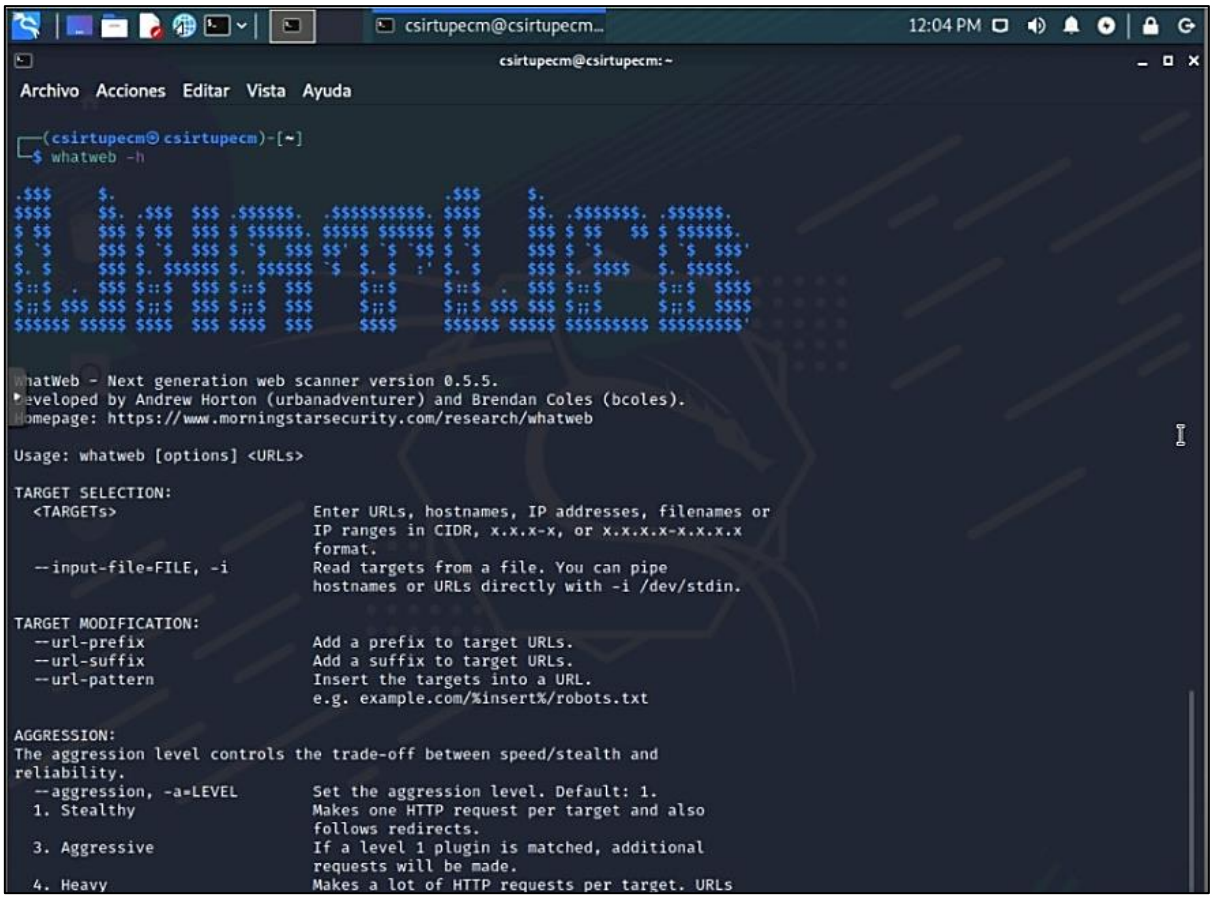


Figura 35. Herramienta WhatWeb

En la figura 36 se muestra la herramienta DMitry con la capacidad de encontrar información que le sea posible de un host, puede recopilar subdominios, información de tiempos de actividades, direcciones de correo electrónico, escaneo de puertos, entre otras. Captura la información de forma rápida y sin necesidad de ejecutar demasiados comandos.

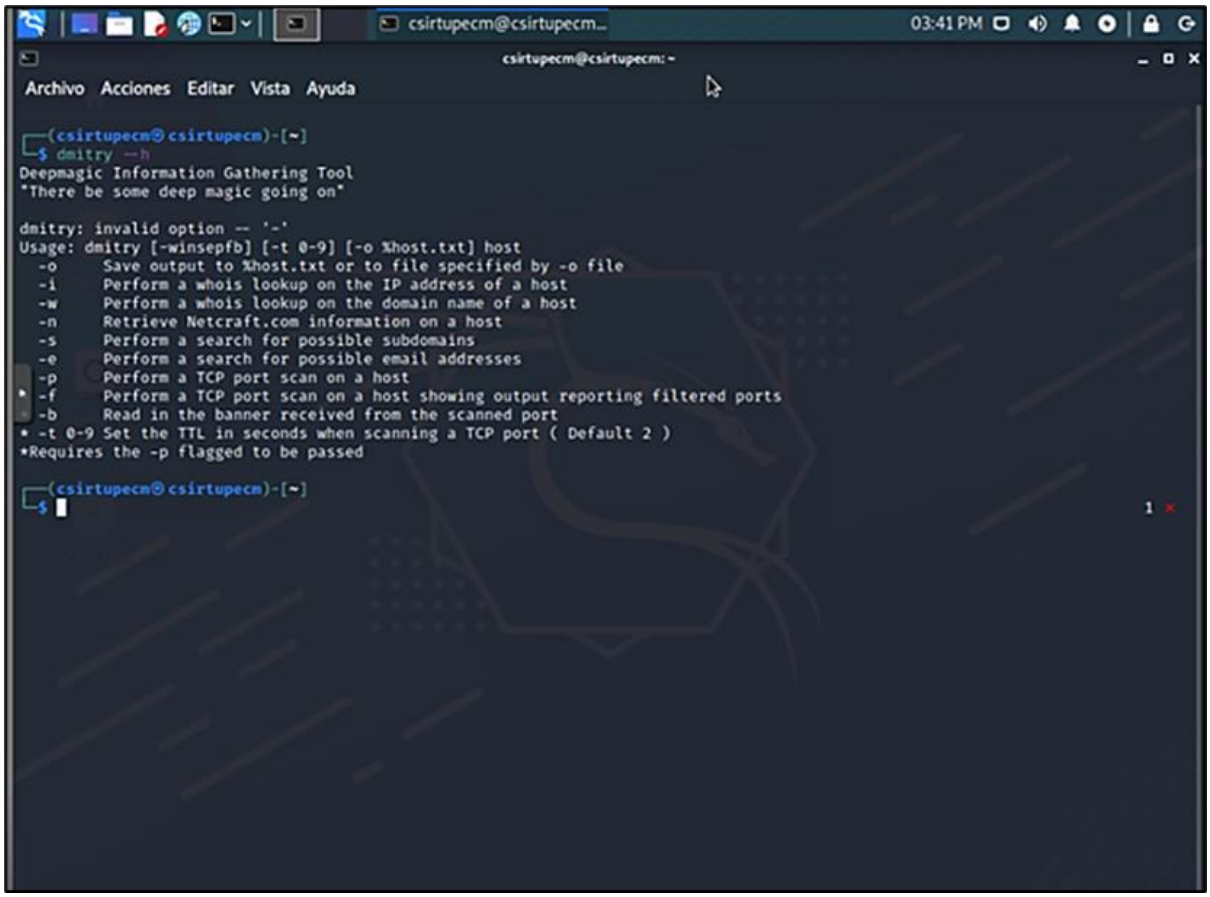


Figura 36. Aplicación de comandos DMitry

En la figura 37 se muestra la herramienta dnsenum, gestiona una secuencia de comandos para listar la información DNS y encontrar bloques de IP sueltos, se obtiene la dirección del anfitrión, dominios y subdominios, rangos de red clase c y subprocesos por consultas whois, obtiene búsquedas inversas y los nombres de dominios y subdominios a través de una consulta en Google con el comando allinurl: -www sitio: dominio.

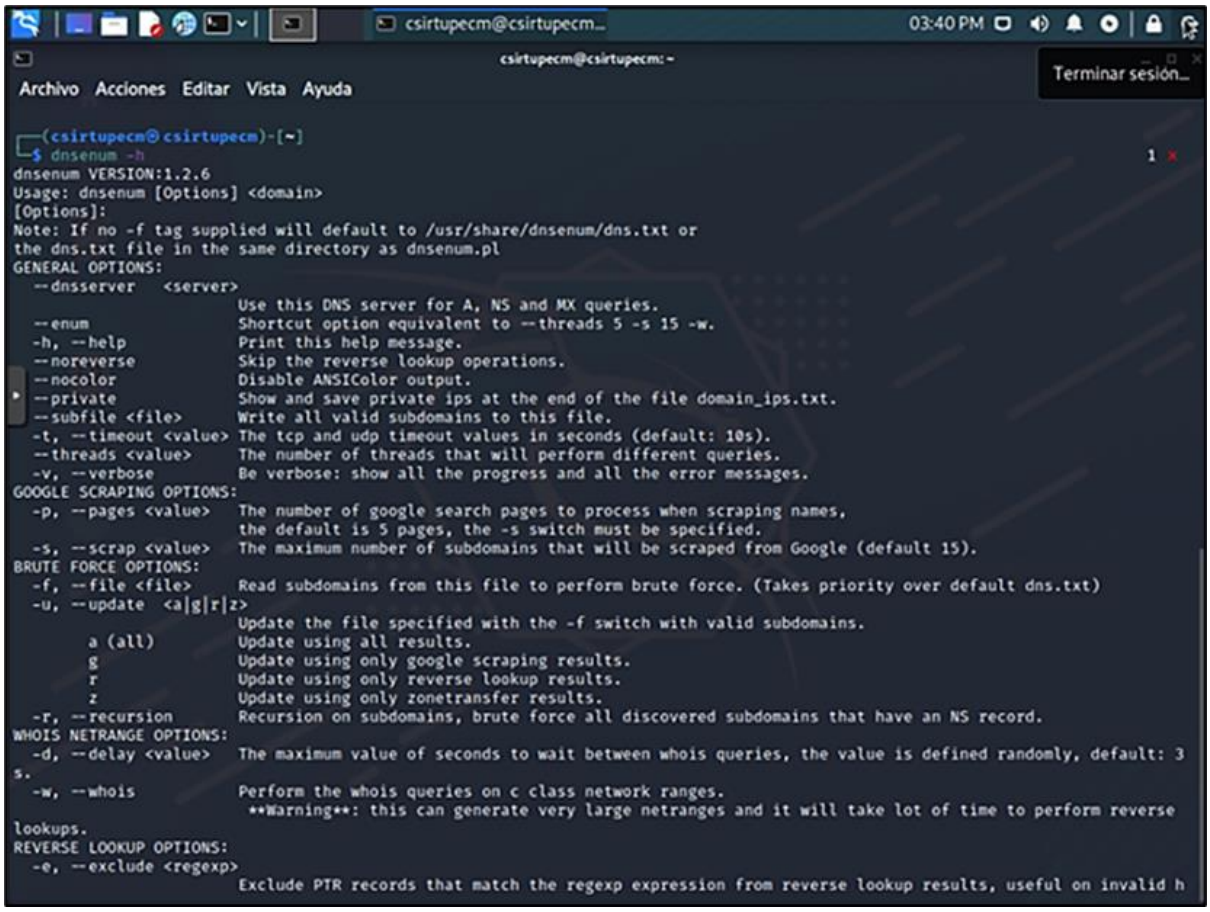


Figura 37. Herramienta dnsenum

En la figura 38 se muestra la herramienta dnstracer, realiza consultas de un nombre de dominio y obtiene un nombre definitivo, continúa y retorna entre servidores hasta encontrar la autorización.

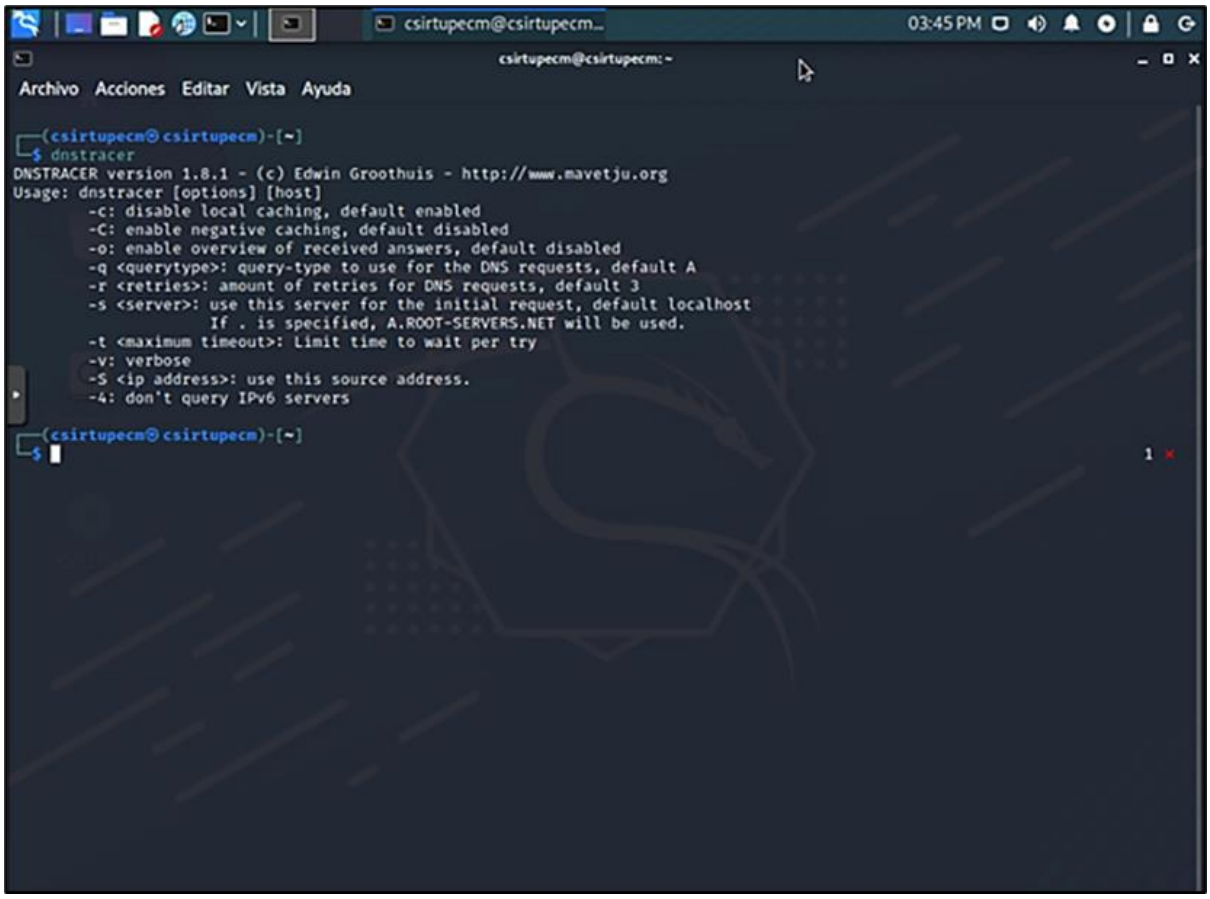


Figura 38. Herramienta dnstracer

En la figura 39 se muestra la herramienta dnswalk, es un depurador DNS que se encarga de realizar transferencias de dominios específicos y comprueba a través de la base de datos su coherencia interna y precisión.

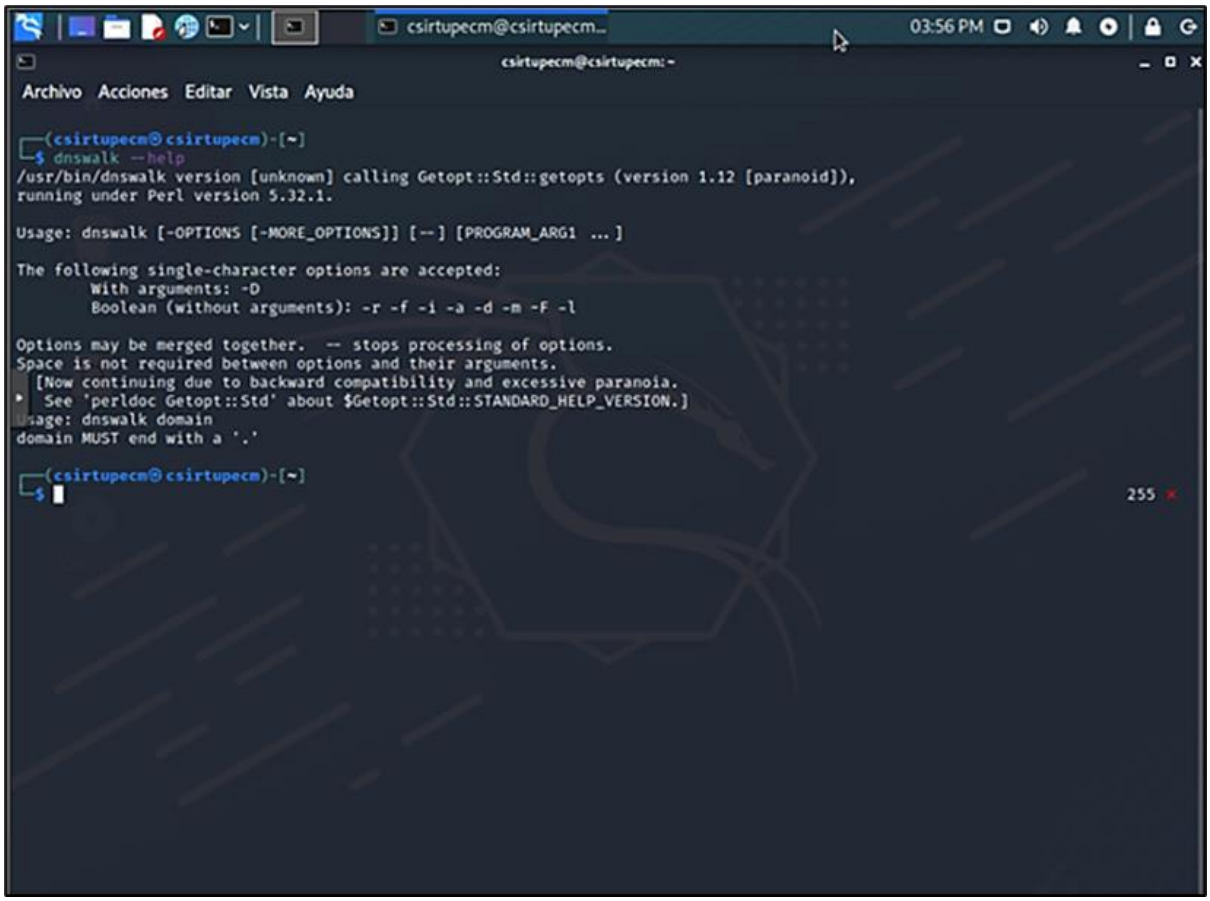


Figura 39. Herramienta dnswalk

En la figura 40 se muestra la herramienta dotdotpwn, ayuda en la detección de vulnerabilidades en cualquier tipo de directorios como HTTP, FTP O TFTP, plataformas web como blogs, ERP, CMS, entre otras; y se lo puede utilizar como script.

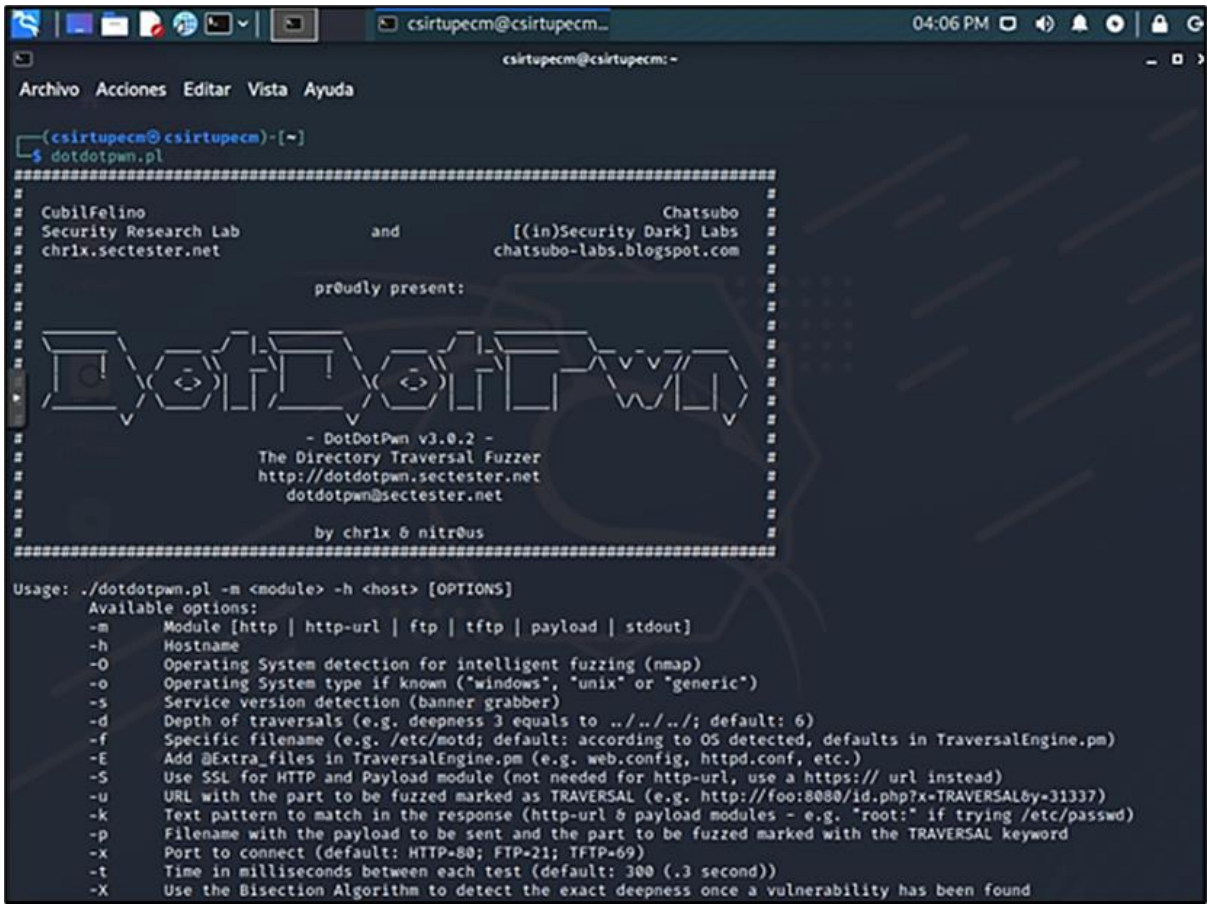


Figura 40. Herramienta dotdotpwn

En la figura 41 se muestra la herramienta de escaneo de vulnerabilidades Nessus en su versión 8.15.1. para diversos sistemas, permite realizar escaneos de manera rápida y garantizando una protección altamente efectiva, ayuda en la protección de amenazas actuales con plugins y se adapta a las necesidades de gestión en vulnerabilidades. La instalación y configuración de Nessus Essentials en Kali Linux se encuentra en el anexo 20.

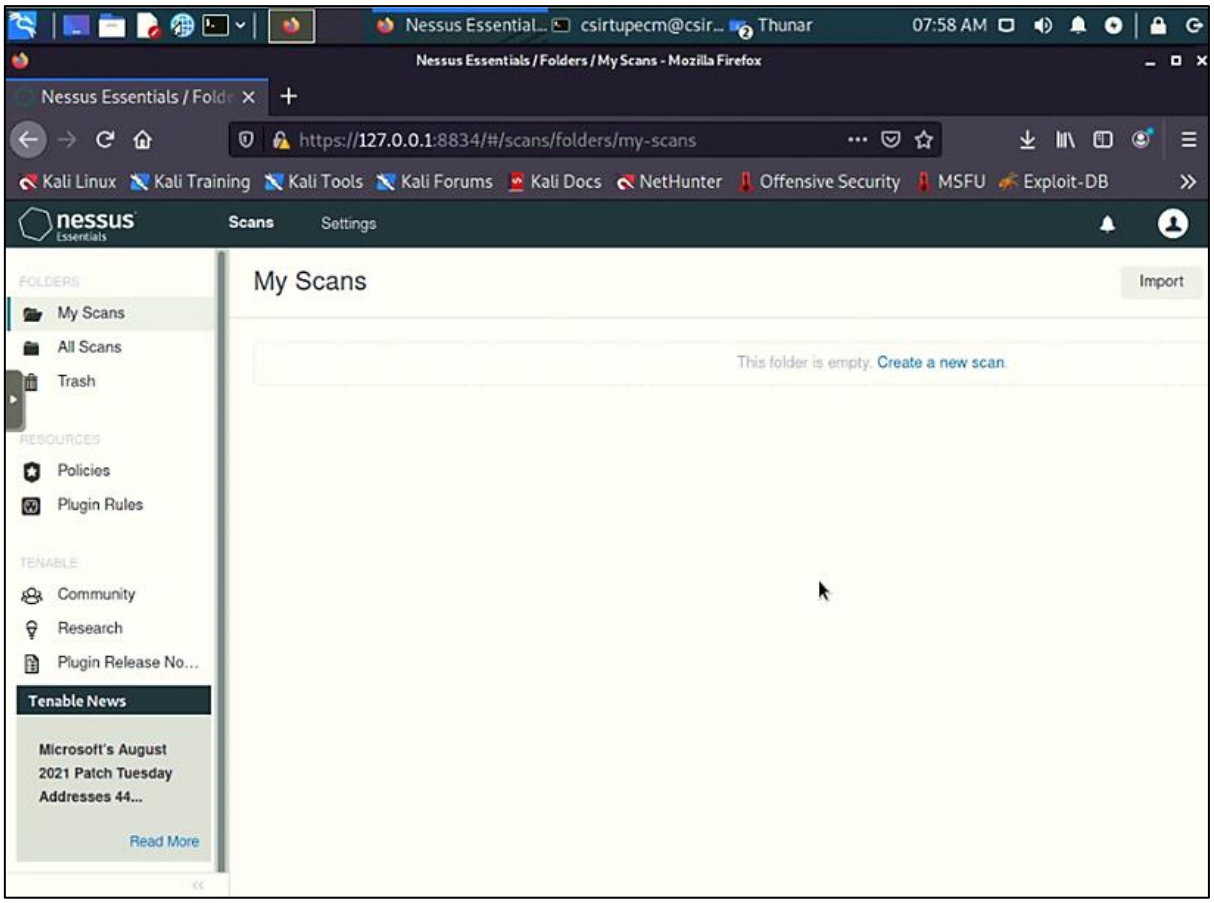


Figura 41. Herramienta de escaneo de vulnerabilidades Nessus

- Herramientas de consulta de IP y dominios

  En la figura 42 se muestra la herramienta Domain Dossier, permite investigar dominios y direcciones IP para la detección de anomalías, genera informes con registros públicos que contiene el ingreso de una dirección donde se registra el nombre de dominio, la dirección IP o una URL y correo electrónico. En el formulario de entrada se muestran casillas de verificación para marcar los datos que se requieren en el informe de las secciones que se muestran a continuación.

  En la búsqueda de direcciones se muestra el nombre canónico que realmente tiene registros de IP, el alias que apuntan al nombre canónico y muestra direcciones IP relacionadas con el alias y nombre canónico, esto incluye nombre de dominio y primera IP encontrada. El registro de dominios whois muestra el nombre del registrante, información de contacto, fecha de registro y su vencimiento y los servidores DNS autorizados para el dominio, el registro de whois en la red muestra el rango de direcciones IP en la asignación, nombre de la organización que las asignó, información de contactos y su fecha de asignación.

Se muestran los registros DNS con dominios relacionados con su entrada, mismos que contienen el dominio asociado con la dirección IP que se ingresó, su registro, el dominio canónico y su ápice de zona y el dominio y ápice de la dirección IP. En traceroute se muestra el número de saltos para la puerta de enlace de entrada, errores en las columnas RTT (tiempo de retardo de ida y vuelta) y el nombre de dominio completo. Por último, en la sección de servicio de escaneo muestra un análisis sobre el tipo de servidor en la dirección y el software que allí se ejecuta.

Dirección de la herramienta Domain Dossier:

https://centralops.net/co/DomainDossier.aspx

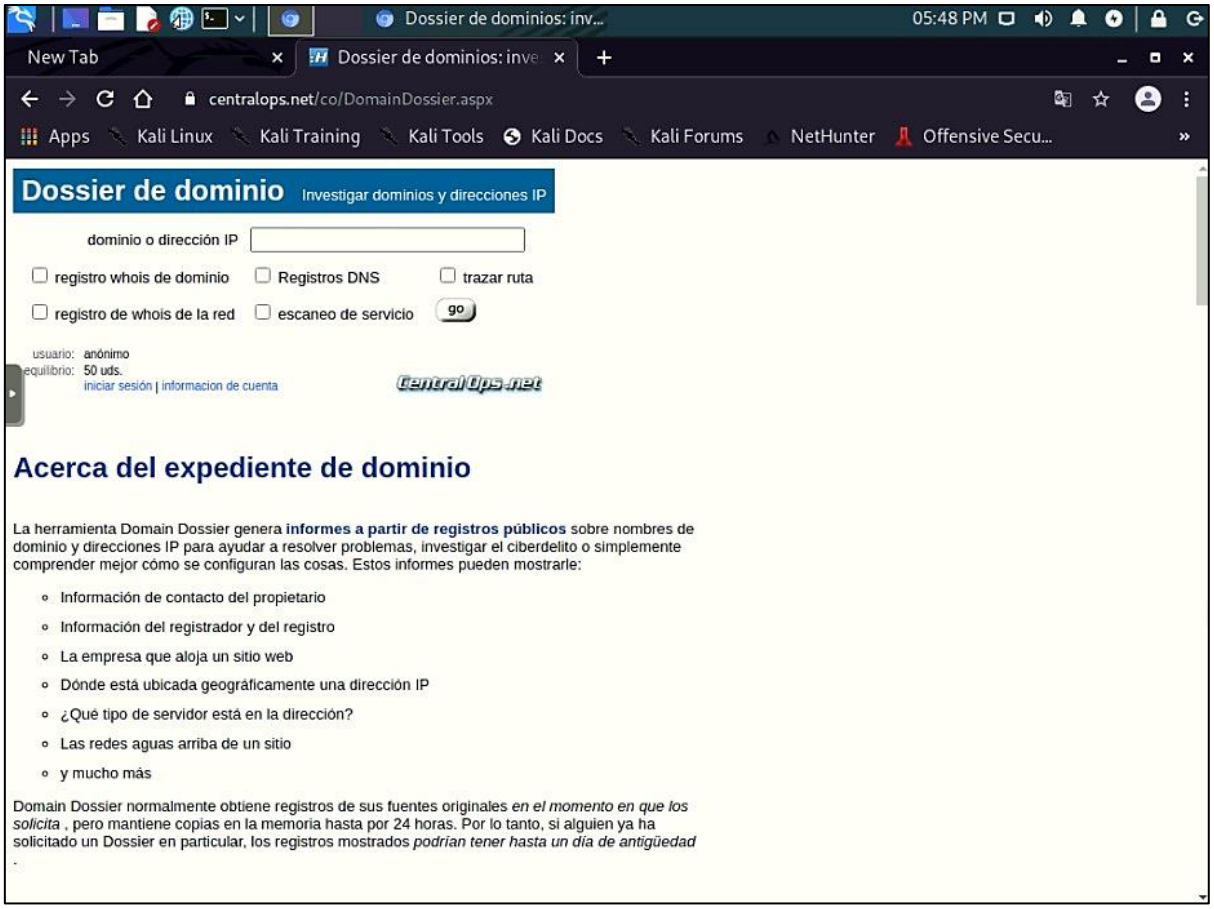


Figura 42. Herramienta Domain Dossier

- Análisis de correos

  En la figura 43 se muestra la herramienta Google Apps Messageheader, permite verificar toda la información del remitente del correo con solo ingresar su cabecera para realizar el análisis, e identificar problemas de enrutamiento, saltos en el servidor, retrasos en mensajes, entre otros.

  Dirección de la herramienta Messageheader:

https://toolbox.googleapps.com/apps/messageheader/

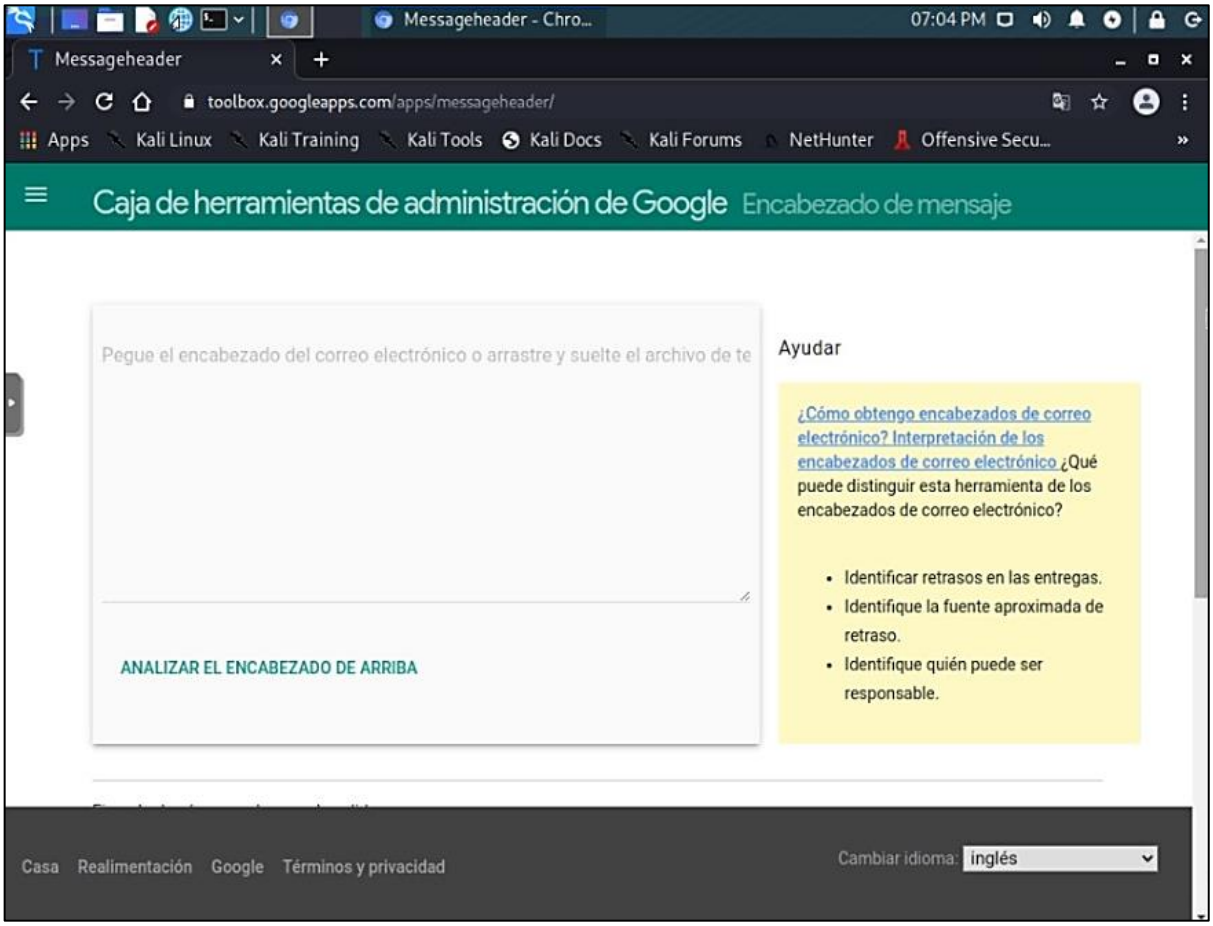


Figura 43. Herramienta Google Apps Messageheader

En la figura 44 se muestra la herramienta de diagnóstico de problemas MXToolBox, permite evaluar el estado del dominio y comprobar direcciones IP con listas negras de correo electrónico.

Dirección de la herramienta MXToolBox:

https://mxtoolbox.com/

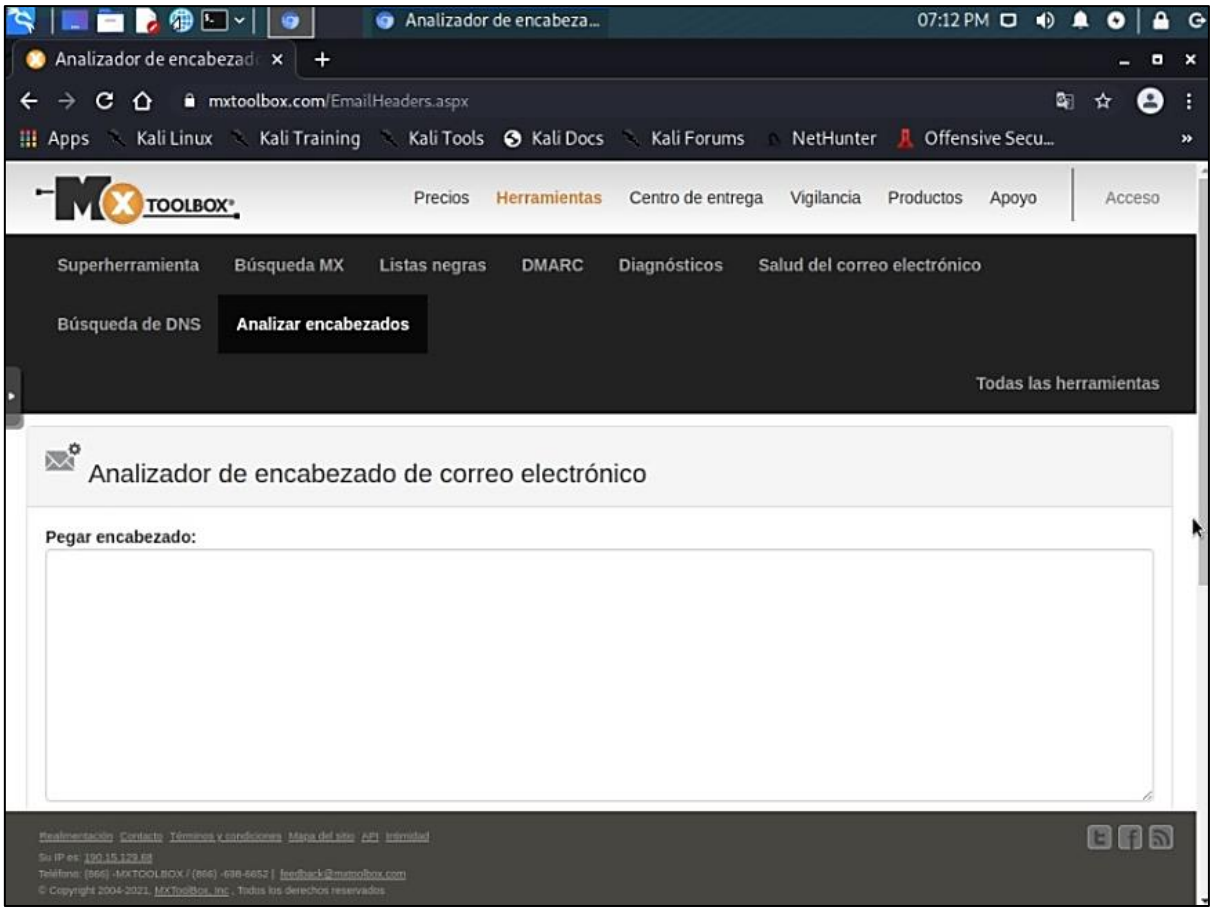


Figura 44. Herramienta de diagnóstico de problemas MXToolBox

- Análisis de malware

  En la figura 45 se muestra la herramienta online Virus Total, su propósito es detectar si un archivo, programa, aplicación o sitio web contiene virus o malware en general, crea rutas para rastrear la dirección de origen de los archivos y determinar si se encuentran elementos sospechosos, y así saber si se los debe usar o eliminarlos de los dispositivos.

  Dirección de la herramienta Virus Total:

  https://www.virustotal.com/gui/home/upload

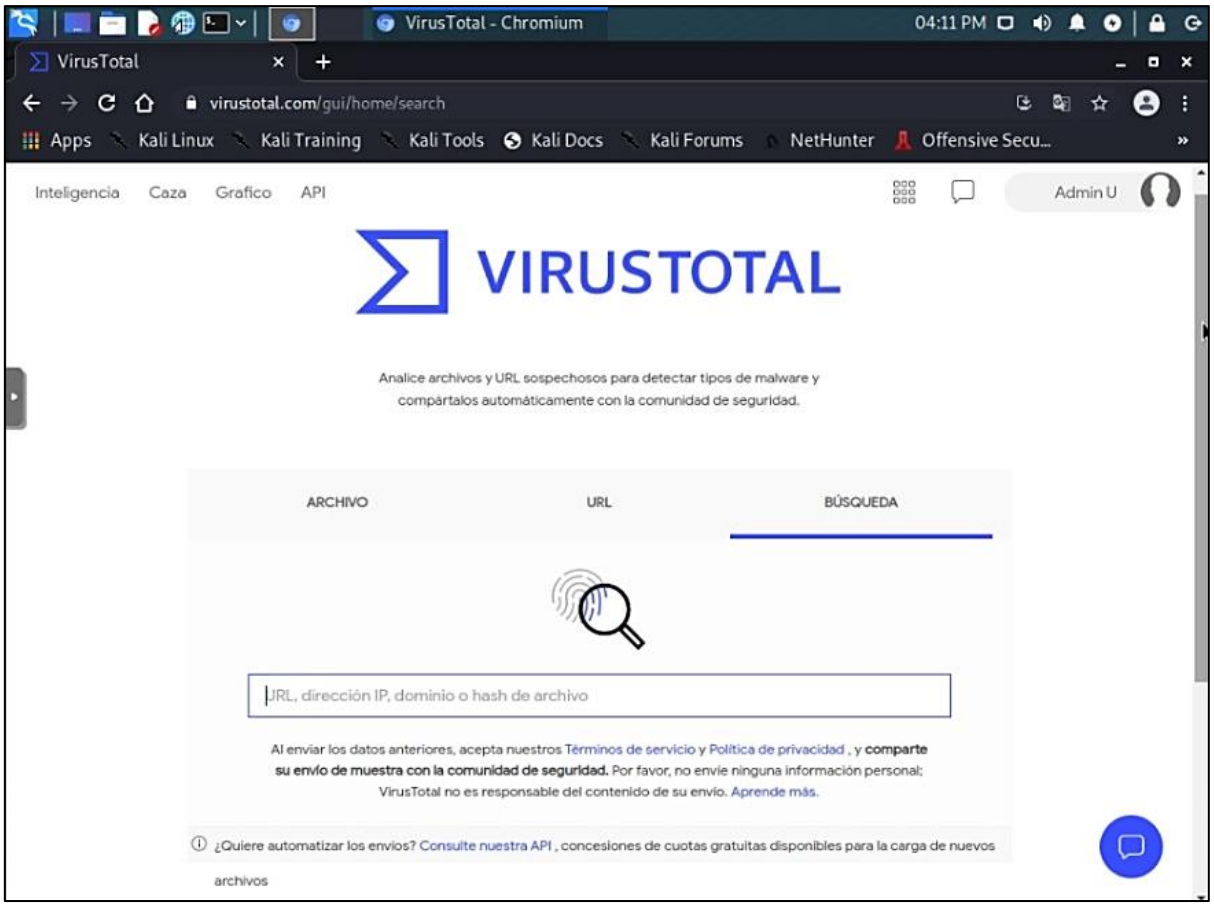


Figura 45. Herramienta online Virus Total

En la figura 46 se muestra la herramienta Hybrid Analysis, otorga un servicio gratuito para detectar y analizar amenazas conocidas o desconocidas de malware en archivos y enlaces, contiene tecnología sandbox (mecanismo para ejecutar software de dudosa procedencia), motores y bases de datos. Realiza detecciones rápidas, análisis estadísticos y a fondo empleando otras herramientas aparte de sandbox para la detección y buscar análisis previos de su base de datos para ver el tipo, información del malware, las detecciones y su nivel de peligrosidad.

Dirección de la herramienta Hybrid Analysis:

https://www.hybrid-analysis.com/

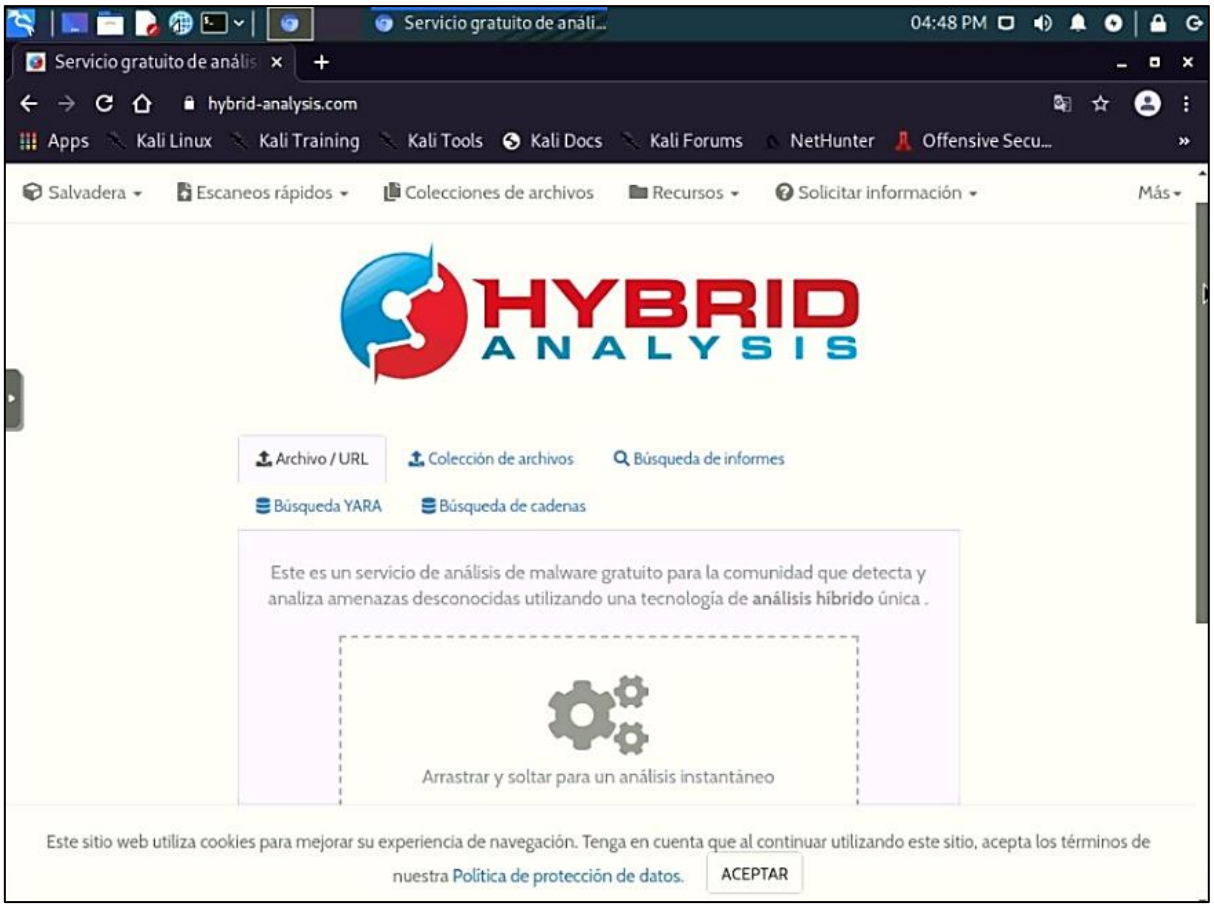


Figura 46. Herramienta Hybrid Analysis

En la figura 47 se muestra la herramienta Sandbox, es un mecanismo de seguridad diseñado para que ciertas acciones o programas que pueden contener código dudoso o malware, no pueda dañar el sistema al ser ejecutados. Se usa en la instalación, configuración y uso de programas que pueden contener malware o comprometer a la seguridad del sistema, como entorno de pruebas, descargar Torrents (información acerca del destino de un archivo), entre otros.

Dirección de la herramienta Sandbox:

https://cc-csirt.policia.gov.co/Sandbox

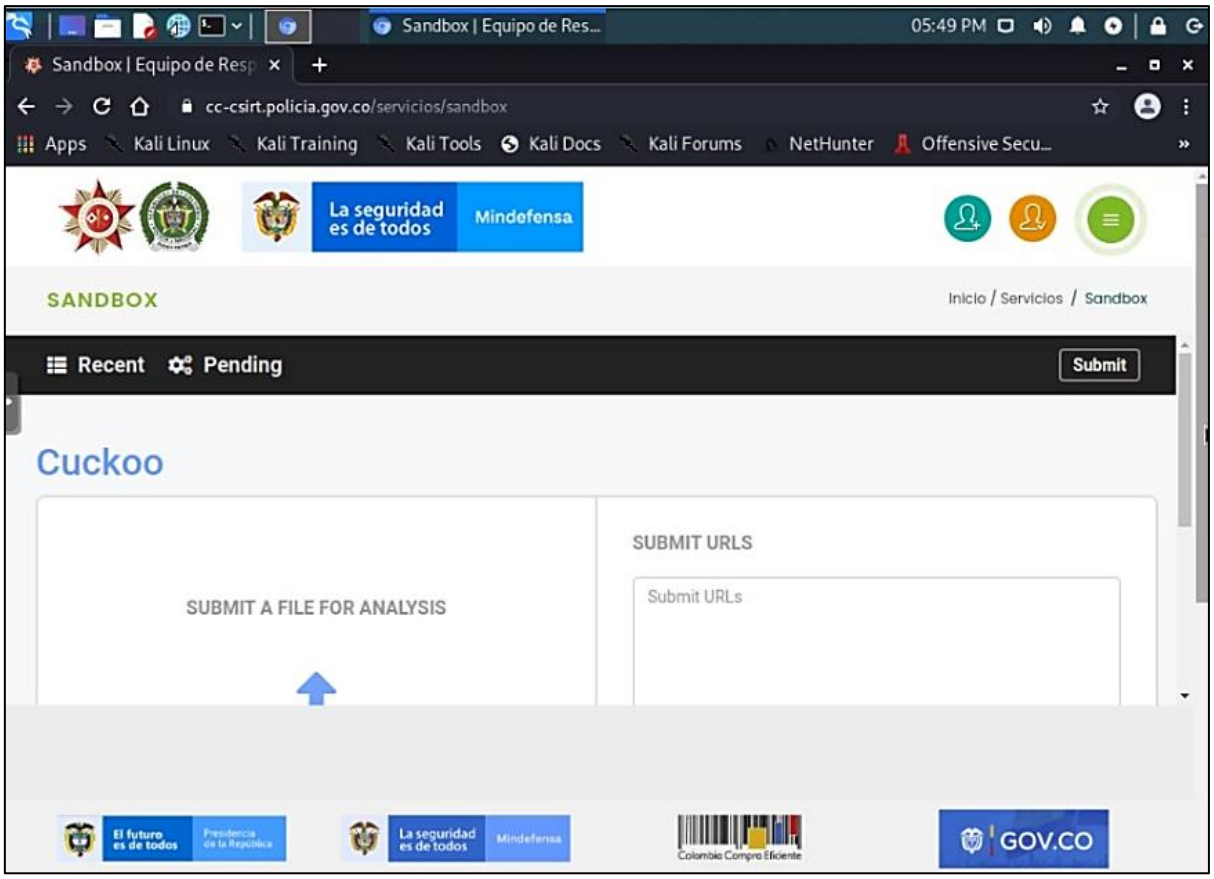


Figura 47. Herramienta Sandbox

En la figura 48 se muestra la herramienta GPG (Privacidad Bastante Buena), se utiliza para cifrar y descifrar datos con el uso de una clave como mecanismos de seguridad para la comunicación y mejora de su privacidad. Realiza la combinación de distintos procesos para el cifrado con una clave privada aleatoria y única para descifrar la información del emisor, asegurando la información de terceras personas, también efectúa la verificación de los datos, su integridad y autenticidad de quien lo envió por medio de las firmas digitales, esto garantiza la consistencia del mensaje asegurando la información transferida.

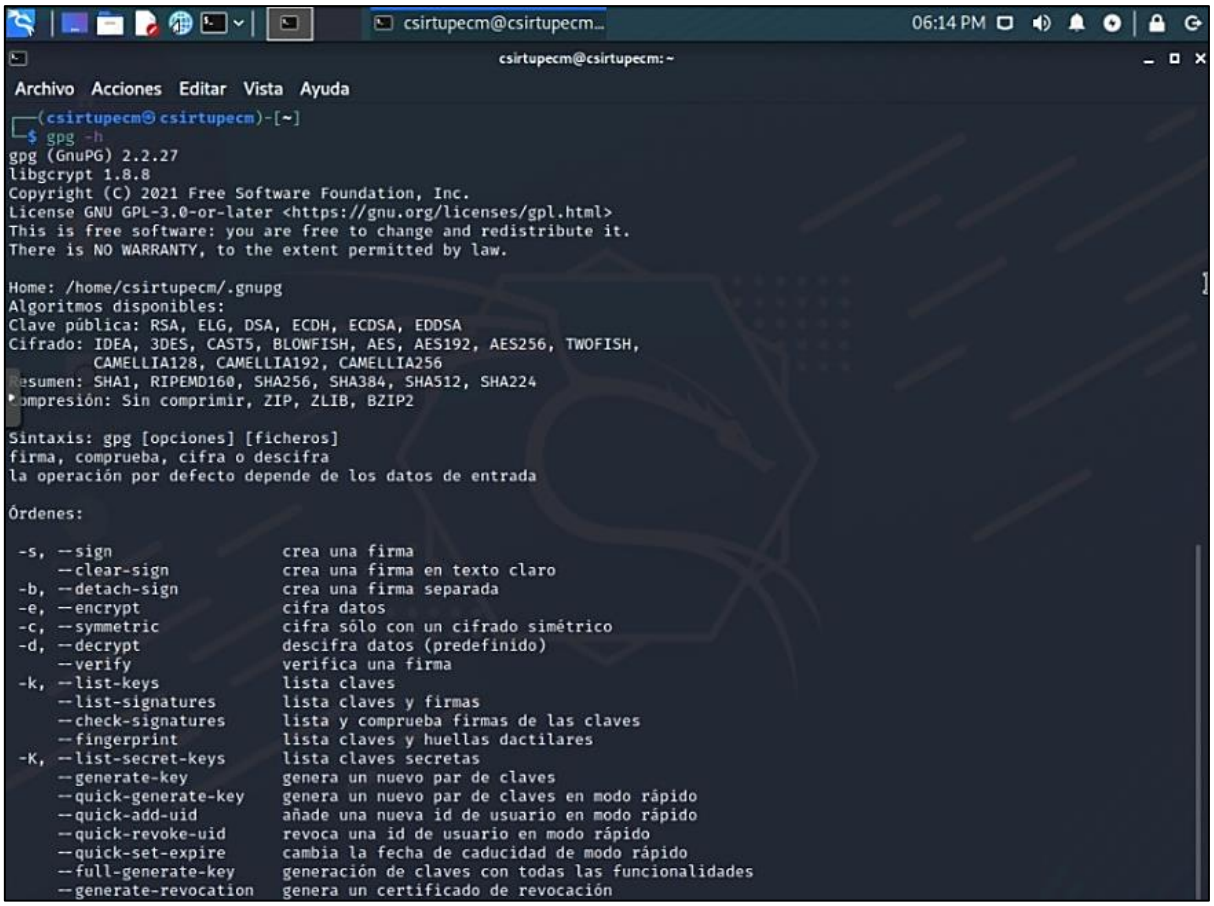


Figura 48. Herramienta GPG

4.2.2.2. Políticas y procedimientos operacionales

a) Política de clasificación de información

Tabla 19. Política de clasificación de información

Objetivo	Definir como clasificar la información en términos de confidencialidad (confidencial, restringido, interno y público).
Alcance	Toda la información generada u obtenida por CSIRT UPEC.
Responsables	El líder del Departamento de Tecnología se encarga de la clasificación de la información tomando en cuenta los niveles de confidencialidad y los activos que manejan el equipo CSIRT.

Declaración de la política

- Información confidencial

La información confidencial es aquella que se la determina como datos sensibles y reservados que no deben ser mostrados sin el consentimiento del propietario.

- Información restringida

La información restringida a diferencia de la clasificación por confidencialidad, algunas personas pueden acceder a ella y otras no. Su clasificación permite limitar su uso y conocer los fines operativos que se llevarían a cabo con esta información.

- Información interna

Su clasificación se basa en identificar la información que puede ser conocida por los integrantes del equipo CSIRT sin el temor de que esta genere un impacto negativo.

- Información pública

Su información se la clasifica como contenido informativo y que puede ser divulgada en los medios con los que opera el equipo CSIRT.

Etiquetado de información

Después de identificar y establecer los criterios para su clasificación, si la información se encuentra en formato digital, se debe etiquetar respetando el siguiente formato:

[CONFIDENCIAL] nombre del archivo

[RESTRINGIDA] nombre del archivo

[INTERNA] nombre del archivo

[PÚBLICA] nombre del archivo

Por otra parte, si la información se encuentra en formato físico, se debe organizar a través de carpetas etiquetadas en su cubierta o porta etiquetas de acuerdo a su nivel de clasificación.

Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.
Glosario de términos	- Departamento de tecnología: Nombre asignado al personal que se encarga del manejo de los sistemas del equipo para su correcto funcionamiento. - Fines operativos de la información: Demostrar los motivos por los que se requiere la información que se encuentra resguardada. - Porta etiquetas: Carpetas grandes para almacenar información que maneja el equipo.

b) Política de protección de datos

Tabla 20. Política de protección de datos

Objetivo	Establecer procedimientos que aseguren la confidencialidad e integridad de los datos al ser almacenados o compartidos.
Alcance	Toda la información generada u obtenida por CSIRT UPEC.
Responsables	El líder del Departamento de Tecnología se encarga de aplicar y hacer cumplir la política para la protección de los datos que maneja CSIRT UPEC. Todos los integrantes y miembros de CSIRT UPEC son responsables de proteger la información que soliciten.

Declaración de la política

- Datos almacenados

  Al almacenar la información digital en servidores, computadoras de escritorio, laptops o medios de almacenamiento portátil, se debe implementar contraseñas de acceso que contengan una mezcla entre mayúsculas y minúsculas, números y caracteres especiales, su longitud debe ser de 8 o más caracteres y no se debe usar los espacios en blanco; por otra parte, los datos en físico deben ser almacenados en sitios o muebles bajo llave o aplicando la debida protección.

- Datos compartidos

  Al momento de compartir información digital se debe utilizar medios de transferencia que proporcionen una conexión segura entre el servidor y cliente, para ello se debe tener en cuenta el uso de protocolos como HTTPS (protocolo seguro de transferencia de hipertexto) en sitios web, SMTP (protocolo de transmisión de datos de correo electrónico) en correos electrónicos y SFTP (protocolo de transferencia segura de archivos) o SSH (Secure Shell – protocolo de administración remota) en acceso remoto. Para compartir información de forma física, se debe asegurar el traslado otorgando la responsabilidad a un integrante del equipo y evitar la manipulación haciendo uso de sobres sellados que serán abiertos únicamente por la persona que solicitó la información.

Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC

Glosario de términos	tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió. - Integridad: Mantener la información sin ningún tipo de alteraciones. - Confidencialidad: Acuerdos que se realizan para que los integrantes del equipo mantengan la información segura de terceras personas. - Conexión segura: Seguridad tecnológica que permite que los datos enviados lleguen únicamente a las personas correctas.

c) Política de destrucción de información

Tabla 21. Política de destrucción de información

Objetivo	Garantizar que la información de CSIRT UPEC sea eliminada de manera correcta y segura
Alcance	Toda la información almacenada por CSIRT UPEC.
Responsables	El director de CSIRT UPEC se encarga de llevar a cabo el proceso de análisis y aprobación de la destrucción de los datos. Cada departamento de CSIRT UPEC se encarga de realizar la valoración de la documentación que posee para su posterior destrucción en caso de que esta ya no tenga valor en las operaciones que realizan. El líder del Departamento de Tecnología se encarga del proceso de destrucción de la información.

Declaración de la política

- Parámetros de eliminación

  Los datos físicos y digitales se deben destruir cuando se realice la valoración de la información almacenada por CSIRT UPEC, donde se determina el fin de su vida útil. Ninguna información debe ser destruida sin la autorización del personal a cargo.

  Se debe evitar intromisiones por terceras personas hasta su total destrucción, el lugar o dispositivos donde se almacenan los documentos que van a ser eliminados deben estar protegidos y contar con medidas de seguridad adecuadas.

- Documentación

	El departamento que requiere destruir información, presenta una solicitud dirigida al director de CSIRT UPEC conforme al anexo 21, para su respectivo análisis y aprobación. El Departamento de Tecnología recibe la notificación, procede a la destrucción y redacta un informe de acuerdo al anexo 22. - Métodos de destrucción Para destruir los datos se debe proceder con un método adecuado, mismo que asegure la completa eliminación y sin posibilidad de recuperación. Cualquier proceso que sea empleado debe aportar al reciclaje y cuidado ambiental. El o los encargados de destruir la información están obligados a proceder con ello de manera segura y adoptar métodos y trajes que los protejan de elementos tóxicos en caso de requerirlo. Papel. -Se da por trituración en tiros verticales y cruzados obteniendo trozos diminutos y difíciles de reconstruir, sus restos se pueden enviar a reciclaje. Documentos electrónicos. -Para la destrucción de documentación electrónica localizada en dispositivos de almacenamiento reutilizables se aplica la técnica de sobre – escritura, para no reutilizables la técnica de destrucción física (triturado y desintegración); y para documentos localizados en correos electrónicos, sitios web, chats u otros, se procede a eliminar y vaciar la información en las fuentes de reciclaje.
Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.
Glosario de términos	- Parámetros de eliminación: Elementos que se deben emplear para realizar la destrucción de la información almacenada en sus diferentes medios. - Sobre escritura: método de añadir texto sobre la información como un método para proceder con una destrucción segura.

d) Política de divulgación de información

Tabla 22. Política de divulgación de información

Objetivo	Establecer la información que puede ser divulgada de acuerdo a quien la requiera, cómo debería ser revelada y las circunstancias para hacerlo. Teniendo en cuenta su nivel de clasificación y protección de la información.
Alcance	Toda la información generada u obtenida por CSIRT UPEC.
Responsables	Todos los integrantes y comunidad objetivo de CSIRT UPEC.
Declaración de la política	
- Información confidencial Los miembros de CSIRT UPEC no pueden divulgar información confidencial, si se debe realizar alguna gestión operativa con terceras personas y se requiere de dicha información, se debe consultar con el propietario para obtener su consentimiento. Si el propietario aprueba el uso de su información con terceras personas, estas deben someterse a un compromiso de confidencialidad de la información que van a recibir, dicho compromiso puede presentarse por parte del propietario o por CSIRT UPEC de acuerdo al anexo 23. - Información restringida La información puede ser divulgada bajo la autorización del director de CSIRT UPEC u otro personal a cargo. Se firma un compromiso de confidencialidad de acuerdo al formato establecido en el anexo 23. - Información interna Es la información clasificada y aprobada para ser usada por los miembros de CSIRT UPEC, salvo unos casos en los que se debe pedir la autorización de divulgación al director. - Información pública La información pública puede ser divulgada a través de los medios establecidos y gestionada como asuntos públicos por parte de CSIRT UPEC.	
Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC

	tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.
Glosario de términos	- Gestión operativa: Conjunto de tareas o procesos que se requieren para brindar los servicios de CSIRT UPEC.

e) Política de acceso a la información

Tabla 23. Política de acceso a la información

Objetivo	Garantizar medidas adecuadas para el acceso a la información tomando en consideración la seguridad y difusión de la información.
Alcance	Toda la información que maneja CSIRT UPEC.
Responsables	El director de CSIRT UPEC se encarga de otorgar o restringir el acceso a la información a cada departamento o integrante del equipo.

Declaración de la política

Todos los integrantes de CSIRT UPEC pueden acceder a la información que se utiliza para la gestión de incidentes.

Se puede acceder a la información relacionada con incidentes finalizados para el entrenamiento del equipo y ayudar en la capacidad de respuesta y formación de personas en la seguridad de la información. También, se la podrá utilizar en la gestión de nuevas alertas, avisos o anuncios de buenas prácticas para las instituciones e integrantes del equipo.

Toda la información es delicada, por lo que se debe hacer buen uso al utilizarla, manteniendo el anonimato de personas que se encuentren involucradas en los documentos. El director del equipo siempre debe estar enterado de los integrantes que acceden a los datos y el uso que le dan.

Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.

Glosario de términos	- Restringir: Poner límites o denegar la libertad de tomar la información del equipo sin la debida autorización. - Anonimato: Información delicada de una institución que no debe ser revelada.

f) Política de uso apropiado de los sistemas del CSIRT

Tabla 24. Política de uso apropiado de los sistemas de CSIRT UPEC

Objetivo	Establecer el uso adecuado de los sistemas de CSIRT UPEC para cumplir con la integridad, confidencialidad y transparencia en todas las actividades.
Alcance	Todos los equipos que utilice CSIRT UPEC.
Responsables	El Departamento de Tecnología es responsable del uso apropiado de los sistemas con los que opera CSIRT UPEC.

Declaración de la política

- Administradores

  El Departamento de Tecnología tiene la obligación de realizar el mantenimiento y gestión de los equipos, manipular los componentes de red como switches, routers, cableado, dispositivos inalámbricos, entre otros; y dar acceso de conectividad a los usuarios que realmente lo necesiten.

  El personal de tecnología tiene la responsabilidad de manejar el centro de datos y restringir el acceso a los servidores de manera local y remota. Ubicar los cables de red y electricidad donde no entren en contacto físico con el fin de evitar incidentes o deterioro de los cables.

  Las instalaciones y equipos de CSIRT UPEC deben ser limpiados minuciosamente por lo menos dos veces al mes y mantener ventilación para evitar humedad, aparición de hongos o malos olores y contar con un extintor cerca o dentro de las instalaciones del equipo.

- Comunidad CSIRT

  Cada integrante debe conocer de las políticas que maneja CSIRT UPEC e incentivar el cumplimiento de las mismas, con ello se garantiza el correcto funcionamiento de los equipos e información para realizar sus operaciones.

  Los sistemas informáticos pueden usarse por los integrantes del equipo que cuentan con la autorización del director.

	Todos los integrantes de CSIRT UPEC deben proteger los sistemas, infraestructura y material de oficina y tienen la responsabilidad de evaluar diariamente el funcionamiento correcto de los equipos a él encomendados que forman parte de su desempeño laboral. Si presenta problemas, su obligación es comunicar al área de tecnología inmediatamente para que se tome las acciones necesarias y evitar desastres. No cambiar de lugar los equipos ni alterar las configuraciones en hardware y software, solo el Departamento de Tecnología puede hacerlo. Los integrantes del equipo pueden usar internet únicamente para gestiones que tengan que ver con las operaciones de CSIRT UPEC. El correo electrónico forma parte de la gestión de incidentes reportados por las instituciones, la información que allí se maneja es confidencial, por lo que el personal que accede a ella, debe regirse a los acuerdos de no divulgación. No divulgar las credenciales otorgadas para el desempeño de sus funciones.
Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.
Glosario de términos	- Integridad: Es la capacidad de tener la información del equipo libre de modificaciones o alteraciones sin antes ser autorizadas por una autoridad competente. - Transparencia: Mostrar ante el equipo e instituciones objetivo los procesos que se realiza y el uso que se le da a la información otorgada por las instituciones que requieren de los servicios. - Router: Dispositivo que permite la conexión a la red a un conjunto de computadoras. - Cableado: Conductor de alambre que se utiliza para la conexión de energía, internet, telefonía, entre otros. - Conectividad local: conexión con los servidores del equipo dentro de las instalaciones en el campus universitario. - Conectividad remota: Acceso a los servidores para el uso de los sistemas fuera de las instalaciones.

g) Política de cooperación

Tabla 25. Política de cooperación

Objetivo	Determinar las organizaciones con las que puede cooperar CSIRT UPEC y de qué forma.
Alcance	CSIRT UPEC y organizaciones que se enfoquen en la misma comunidad objetivo.
Responsables	Director de CSIRT UPEC.
Declaración de la política Se debe dar una interacción constante entre los equipos de seguridad informática para mejorar la calidad de los servicios que brindan a sus comunidades objetivo, su cooperación se basa en una interacción a modo de diálogo para intercambiar opiniones, experiencias, propósitos o recomendaciones en la gestión de incidentes. A continuación, se determinan los puntos de interacción con otros CSIRTs: - Equipos de respuesta a incidentes informáticos Para el crecimiento y madurez de CSIRT UPEC, es de vital importancia la interacción entre equipos sin importar su ámbito de actuación, la cooperación entre ambas partes debe ser comunicativa, en caso de presentarse algún incidente que afecte a todas las instituciones a nivel regional o nacional, se da la necesidad de otorgar ciertos datos confidenciales entre los equipos para poder trabajar en conjunto y así dar solución, para ello se firman compromisos de confidencialidad entre las partes interesadas de acuerdo al formato establecido en el anexo 23. - Organizaciones CSIRT UPEC puede cooperar con diferentes organizaciones que no cuenten con un equipo de respuesta y requieran de orientación en prácticas que ayuden a proteger su información. - Prensa CSIRT UPEC en ocasiones coopera con la prensa donde aborda diferentes temáticas como experiencias al tratar incidentes, para ello se estudia la información que se dará a conocer manteniendo siempre la confidencialidad de datos que no pueden mencionarse públicamente.	
Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC

Glosario de términos	tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió. - Cooperar: Acto de intercambiar información o ideas con otros equipos de seguridad informática. - Compromiso de confidencialidad: Acuerdos de manera verbal o en físico que obliga a un integrante del equipo a no divulgar información delicada que gestiona CSIRT UPEC.

h) Política de privacidad

Tabla 26. Política de privacidad

Objetivo	Demostrar transparencia acerca del uso de la información.
Alcance	Unidades educativas y gobiernos seccionales de la provincia del Carchi que requieran de los servicios de CSIRT UPEC.
Responsables	CSIRT UPEC se encarga de emitir la política de privacidad para que las instituciones se acojan a ellas en el manejo de su información.

Declaración de la política

- Quiénes somos:

  Somos un "Equipo de Respuesta ante Incidentes Informáticos - CSIRT UPEC" que brinda sus servicios a unidades educativas y gobiernos seccionales de la provincia del Carchi, sus instalaciones se encuentran en el laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi. La dirección del sitio web es: https://csirt.upec.edu.ec
- Datos que recogemos:
  - Nombre de la persona que requiere de los servicios.
  - Correo electrónico como un medio de contacto para la gestión de los servicios.
  - Teléfono de contacto con la institución en caso de requerir de alguna información.
  - Dirección de la institución en caso de necesitar acercarnos personalmente para cumplir con nuestros servicios.
  - Nombre de la institución para comprobar si pertenece a nuestra comunidad objetivo.

  La información recolectada es muy importante para reconocer si la institución es verdadera y gestionar sus peticiones de una manera más puntual, la usamos únicamente para fines que van en beneficio de las instituciones y se encuentran protegidos gracias a las políticas que se ejecutan en el equipo.
- Comentarios:

Son un intercambio de ideas u opiniones sobre el contenido expuesto en el sitio web y fomentar más conocimiento sobre el tema, los comentarios son de conocimiento público, por lo que cada usuario es responsable de los datos que expone a terceras personas. No se debe comentar información personal o de la institución a la que pertenece y no promover insultos o cierto tipo de palabras que resulten ofensivas para los demás visitantes del sitio.

- Medios:

  Todos los archivos que sean enviados por medios de contacto que facilita el equipo, son usados únicamente con fines de gestionar los servicios que requieren las instituciones, los datos son protegidos, clasificados y con restricciones adecuadas para el uso correcto de los mismos y así no se encuentren vulnerables.

- Formularios:

  Los formularios de reporte a incidentes por parte de CSIRT UPEC, son usados para ayudar en las recomendaciones de solución a incidentes emitidos por los mismos, se guarda discreción sobre la información que contiene y se trabaja de manera profesional y con la discreción que esto requiere.

- Cookies:

  Las cookies almacenan información del computador del visitante al sitio web, y en caso de registrar información en los formularios o comentarios, el navegador mostrará la información que guardó las cookies para completar la información previamente almacenada. Nos permite generar una experiencia personalizada, almacenando las cookies por lo que no hay posibilidades de incidentes de seguridad por parte del equipo y no contienen virus.

- Con quién compartimos tus datos:

  Los datos son compartidos con los miembros de CSIRT UPEC para la gestión del o los servicios que soliciten las instituciones.

- Información de contacto:

  En el sitio web de CSIRT UPEC se encuentra el número de contacto con el equipo en caso de tratar cuestiones específicas del servicio o de privacidad.

- Como protegemos tus datos:

  Todos los miembros de CSIRT UPEC firman compromisos de confidencialidad de la información, además, se rigen a políticas y procesos que se deben cumplir para la protección de la misma.

Sanciones	Ante la constancia del incumplimiento con los lineamientos establecidos en la presente política. El director de CSIRT UPEC tomará medidas o acciones que considere necesarias de acuerdo al nivel de afectación que se cometió.
Glosario de términos	- Cookies: Archivos que forman parte de los sitios web que mejoran la experiencia del usuario cuando vuelva a visitar el sitio. - Virus: Programa configurado en anonimato con la finalidad de afectar el funcionamiento del hardware y alterar o sustraer información con el fin de obtener un beneficio.

i) Proceso de gestión de incidentes

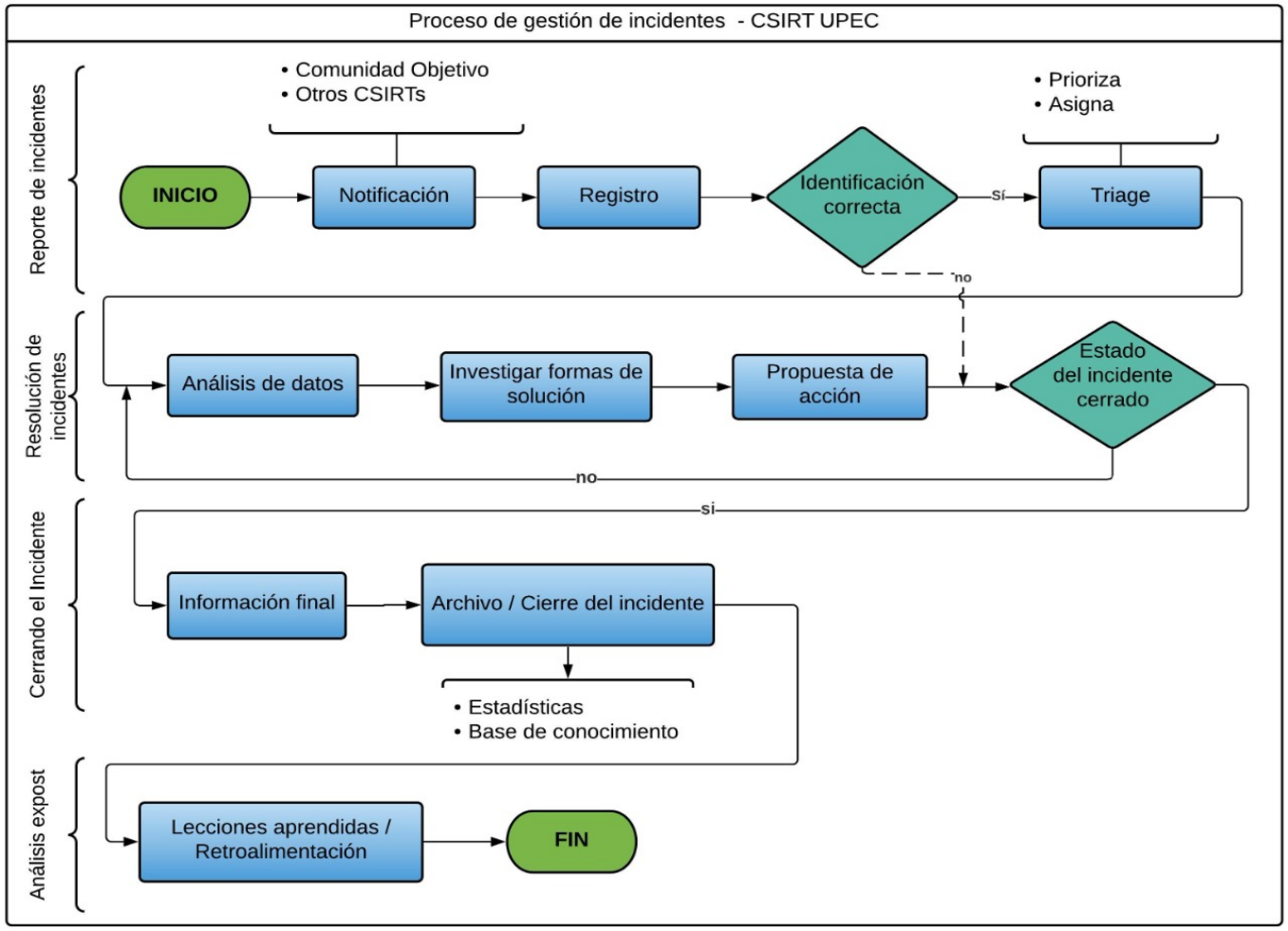


Figura 49. Proceso de gestión de incidentes CSIRT UPEC

- Contexto del proceso

Tabla 27. Ficha de proceso gestión de incidentes

Proceso	**Revisión**	**Fecha revisión**
Gestión de incidentes	1	15/9/2021

Objetivo del proceso

Colaborar con la comunidad objetivo para proveer recomendaciones de solución que les ayude a solventar sus incidentes informáticos.

Alcance

Proveer recomendaciones de solución que ayude en la resolución de los incidentes informáticos presentados en la comunidad objetivo.

Actividades que forman el proceso

- Notificación.
- Registro.
- Identificación.
- Triage.
- Análisis de datos.
- Investigar formas de solución.
- Propuesta de acción.
- Definir estado del incidente.
- Información final.
- Archivado / cierre del incidente.
- Lecciones aprendidas / retroalimentación.

Responsables del proceso

Encargado departamento de operaciones

Entradas del proceso	**Salidas del proceso**
Formulario de reporte a incidentes informáticos por parte del miembro CSIRT UPEC.	Informe final de gestión de incidentes.

Procesos relacionados

Gestión de riesgos

Recursos

- Acceso al sistema de ticket centro de respuesta y soporte a incidentes de seguridad.
- Acceso al sitio web https://csirt.upec.edu.ec/
- Acceso al servidor de monitoreo.
- Acceso al correo electrónico csirt.computacion@upec.edu.ec

Registros/archivos

- Formulario de reporte a incidentes informáticos.
- Correo de notificación al crear el ticket.
- Valoración del incidente.
- Informe final de gestión de incidentes.

Indicadores

- Porcentaje de incidentes acorde con lo establecido en el SLA.
- Porcentaje de tiempo promedio transcurrido para lograr la resolución de incidentes.
- Porcentaje de incidentes por estado.
- Porcentaje de solicitudes complidas dentro del SLA.

Documentos aplicables

- Manual de políticas CSIRT UPEC.
- Acuerdo de nivel de servicios CSIRT UPEC.

- Reporte de incidentes
  - ❖ Notificación. - Los reportes de incidentes pueden provenir de la comunidad objetivo o por notificaciones de otros CSIRTs, mismos que pueden ser notificados mediante el formulario de reportes, sistema de ticket (Centro de Respuesta y Soporte a Incidentes de Seguridad) y correo electrónico (csirt.computacion@upec.edu.ec) del equipo que están ubicados en el sitio web. El formato del formulario de reportes de incidentes se encuentra en el anexo 24.
  - ❖ Registro. - A todos los reportes se les asigna un ticket con un identificador único, mismo que será utilizado durante todo el proceso de gestión del incidente.
  - ❖ Identificación. - Se lleva un proceso de identificación para evitar acciones innecesarias, se determina si el incidente es real, si la institución que emitió el incidente es verídica y pertenece a la comunidad objetivo.

Si no pertenece, se establece el estado del incidente definido en la tabla 28, se notifica al que reportó el incidente dándole a conocer que su institución no forma parte de nuestro ámbito de actuación y recomendándole otros equipos que ayudan a su organización, pero, se analiza el incidente que reporta para determinar si puede afectar a las instituciones objetivo para emitir alertas y avisos.

- Triage. - Se realiza la valoración del incidente acorde al formato establecido en el anexo 25, donde el encargado analiza la información inicial del reporte, mismo que le permitirá priorizar el incidente tomando en cuenta su nivel de criticidad (riesgo alto, riesgo medio, riesgo bajo), después asocia con su tipo y clasificación acorde con la información de la tabla 28, posteriormente, asigna recursos humanos, técnicos y un tiempo aproximado para ser atendido.

Tabla 28. Priorizar incidente

Riesgos		**Analizar riesgo**				**Tiempo de respuesta**
Clasificación	**Tipo**	**Probabilidad**	**Impacto**	**Valor riesgo**	**Nivel de riesgo**	
Código malicioso	Ransomware, malware, spyware, troyano, virus	3	4	12	Alto	30 minutos
Disponibilidad	Ataques DoS/DDoS	2	4	8	Medio	1 hora
	Intercepción de información	2	4	8	Medio	1 hora
Confidencialidad de la información	Acceso a información no autorizada	2	3	6	Bajo	2 horas +
	Modificación de información no autorizada	1	4	4	Bajo	2 horas +
Recopilación de información	Ingeniería Social	2	3	6	Medio	1 hora
Intentos de intrusión	Explotación de vulnerabilidades conocidas	2	2	4	Bajo	2 horas +
	Intentos de acceso	2	2	4	Bajo	2 horas +
	Suplantación de identidad (Phishing)	2	3	6	Bajo	2 horas +
Contenido abusivo	SPAM - En el correo electrónico	3	1	3	Bajo	2 horas +

Por último, se notifica la recepción del reporte a través de un correo electrónico de acuerdo al formato establecido en el anexo 26, donde se le da a conocer el código del ticket asignado y se le proporciona un enlace para poder acceder al sistema por el cual podrá ver el estado, proporcionar información y dar un seguimiento del proceso durante la gestión del incidente.

- Resolución de incidente
  - ❖ Análisis de datos. - Se realiza un análisis de toda la información que se recolectó del formulario de reportes, localizado en el sitio web, sistema de tickets o correo electrónico. En caso de requerir información adicional del incidente se la solicitará mediante el perfil de ticket.
  - ❖ Investigar formas de solución. - Mediante el sistema de monitoreo y herramientas externas que opera CSIRT UPEC, se realiza un análisis de los sistemas para obtener más información sobre el incidente.

    Se lleva un proceso de investigación en foros, artículos, papers y otros que deben ser de fuentes confiables y comprobadas; esto permitirá encontrar una o varias formas de solución al incidente emitido. Otra forma de buscar una propuesta de solución es a través de los equipos CSIRTs con quien se tiene relación, mismos que pueden proporcionar recomendaciones o información sobre casos similares.
  - ❖ Propuesta de acción. - Se propondrá las acciones o soluciones de mitigación del incidente, además de recomendaciones para la erradicación y recuperación de los sistemas.
  - ❖ Estado del incidente. - En este punto se determina el estado del incidente de acuerdo a los lineamientos representados en la tabla 29, mismos que permitirá tomar la decisión de cerrar o seguir con el proceso de resolución.

Tabla 29. Estado de incidente

Estado del incidente	**Descripción**
Cerrado – Incidente no verídico / Fuente no confiable.	No se puedo comprobar la procedencia del incidente.
Cerrado – Incidente no corresponde a la comunidad objetivo.	El incidente reportado proviene de una institución que no forma parte de la comunidad objetivo de CSIRT UPEC.
Cerrado – Falso positivo.	El incidente detectado resultó falso.

Cerrado – Incidente resuelto y sin respuesta.	El incidente fue resuelto, pero no se obtuvo una confirmación de parte de la institución.
Cerrado – Incidente resuelto y con respuesta.	El incidente fue resuelto y la institución confirma al CSIRT.
Cerrado – Incidente sin resolución y sin respuesta.	La institución no ha resuelto el incidente y no contacto con el equipo.
Abierta – Incidente en seguimiento.	Estado con el que empieza y permanece durante todo el proceso de resolución del incidente hasta su cierre.

- Cerrando del incidente
  - ❖ Información final. - Se genera un informe final del incidente acorde al formato establecido en el anexo 27, donde se presenta datos generales sobre el caso, además de una breve descripción de la situación inicial del incidente, los hallazgos encontrados por parte de CSIRT UPEC, las acciones que se realizaron y los resultados obtenidos. Además, se emiten recomendaciones sobre mejores prácticas en seguridad informática y observaciones en caso de ser necesario.
  - ❖ Archivo y cierre del incidente. - Se cierra el caso archivando todo lo relacionado a la gestión del incidente en el ticket otorgado en su registro, esto permitirá su correcto almacenamiento y un buen uso posterior para generar estadísticas o bases de conocimientos.
- Análisis expost

  Lecciones aprendidas / retroalimentación. - De cada incidente gestionado se aprende muchas cosas, como aumentar la capacidad de respuesta, mejorar o aclarar las políticas de seguridad, mejorar la arquitectura de red, mecanismos de detección, uso de herramientas que permitieron un mejor análisis de los incidentes y adelantarse en el reconocimiento de nuevos tipos de ataques.

  Por otra parte, es bueno sacar provecho de cada servicio brindado, pues sirve de diálogo entre otros equipos y estos pueden beneficiarse de nuestras experiencias.

j) Proceso de alertas y avisos

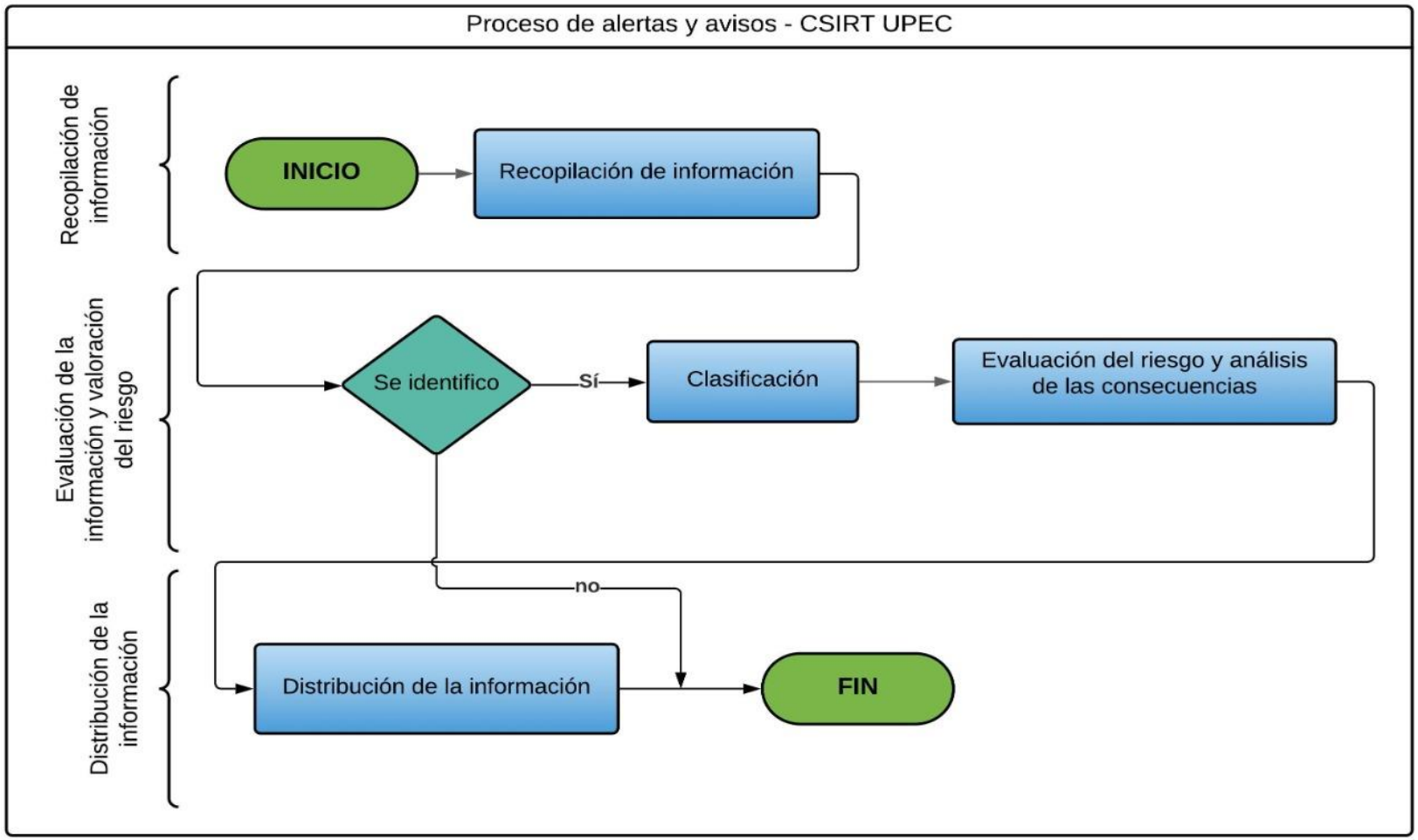


Figura 50. Proceso de alertas y avisos CSIRT UPEC

- Contexto del proceso

Tabla 30. Ficha de proceso alertas y visos

Proceso	**Revisión**	**Fecha revisión**
Alertas y avisos	1	15/9/2021

Objetivo del proceso

Dar a conocer a la comunidad objetivo acerca de incidentes o vulnerabilidades que pueden afectar a sus sistemas.

Alcance

Emitir información acerca del incidente o vulnerabilidad junto con recomendaciones que ayuden a evitarlos.

Actividades que forman el proceso

- Recopilación de información.
- Identificación.
- Clasificación.
- Evaluación del riesgo y análisis de consecuencias.
- Distribución de la información.

Responsables del proceso

Encargado departamento de operaciones

Entradas del proceso	**Salidas del proceso**
- Notificación de Otros CSIRT. - Informe final de gestión de incidentes. - Búsqueda de información.	Documento distribución de alertas o avisos.

Procesos relacionados

Gestión de riesgos

Recursos

- Acceso al sitio web https://csirt.upec.edu.ec/
- Acceso al correo electrónico csirt.computacion@upec.edu.ec

Registros/archivos

- Identificación de información de alertas y avisos
- Distribución de alertas y avisos

Indicadores

- Porcentaje de calificación como información útil.
- Porcentaje de calificación como información no útil.

(Las métricas e indicadores se muestran en el anexo 31)

Documentos aplicables

- Manual de políticas CSIRT UPEC

- Recopilación de información

La información proviene de distintas fuentes, entre ellas, los informes de los incidentes gestionados por parte del equipo, información publicada en sitios web, grupos de tecnología en redes sociales, foros, artículos y noticias a nivel regional, nacional o mundial, además de información sobre casos tratados por otros CSIRTs.

- Evaluación de la información y valoración del riesgo
  - ❖ Identificación. - Antes de hacer pública la información, se debe pasar por la determinación de confiabilidad de acuerdo a las pautas dadas en el formato establecido en el anexo 28, de lo contrario podría crear una mala reputación del equipo y ocasionar malestar, disgustos o tomar medidas innecesarias por parte de las instituciones objetivo.

    Además, se determina si los sistemas (hardware y software) que se mencionan en la información son usados también por la comunidad objetivo y dependiendo de las acciones por las que se dio la vulnerabilidad, conocer si es pertinente la divulgación del contenido por parte de CSIRT UPEC.
  - ❖ Clasificación. - La información entrante podría tener información confidencial o restringida, por lo que para su uso se debe tener en cuenta la política de clasificación.
  - ❖ Evaluación de riesgos y análisis de las consecuencias. - Para evaluar el riesgo que pueden ocasionar las vulnerabilidades, se determina la probabilidad de que estas ocurran en las organizaciones y el impacto que pueden producir si se llegan a presentar. Para su análisis tomar en cuenta el proceso gestión de riesgos establecido por CSISRT UPEC.

    Tras realizar el análisis de riesgo, el aviso se etiqueta con clasificación general de ALTO, MEDIO o BAJO.
- Distribución de la información

  La alerta o aviso se emitirá de acuerdo a la estructura establecida en el anexo 29, a través de los medios con los que opera CSIRT UPEC.

k) Proceso de publicación de anuncios

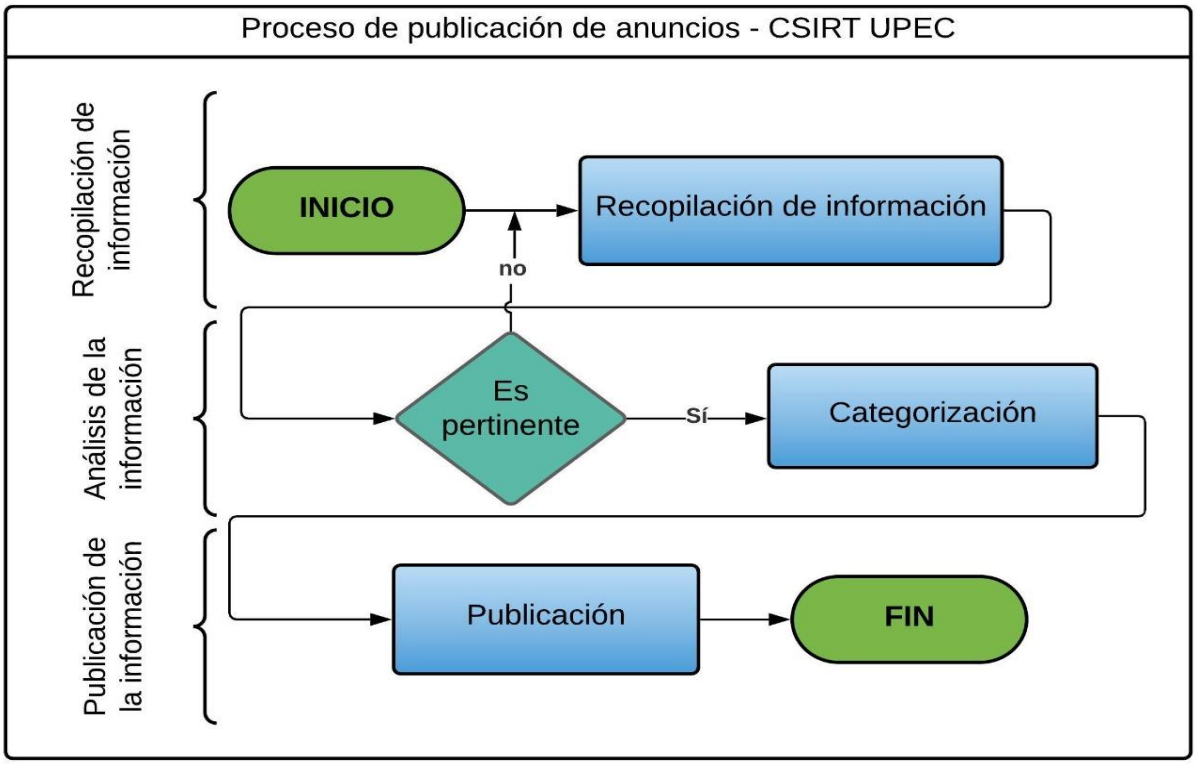


Figura 51. Proceso de Publicación de Anuncios CSIRT UPEC

- Contexto del proceso

Tabla 31. Ficha de proceso publicación de anuncios

Proceso	**Revisión**	**Fecha revisión**
Publicación de anuncios	1	15/9/2021

Objetivo del proceso

Mantener comunicada a la comunidad objetivo con temas de interés y que aportan a la seguridad de la información y de sus equipos.

Alcance

Emitir información que ayude a la seguridad de la información de la comunidad objetivo.

Actividades que forman el proceso

- Recopilación de información.
- Definir pertinencia.
- Categorización.
- Publicación.

Responsables del proceso

Encargado departamento de TI

Entradas del proceso	**Salidas del proceso**
Información nueva en tecnología y seguridad informática pretinen para los miembros.	Publicación de anuncio

Procesos relacionados

No existe

Recursos

Acceso al sitio web https://csirt.upec.edu.ec/

Registros/archivos

Publicación de anuncio

Indicadores

- Número de votos por publicación.
- Promedio de puntuación.
- Tiempo de visualización de publicación antes de la puntuación.

  (Las métricas e indicadores se muestran en el anexo 31)

Documentos aplicables

Manual de políticas CSIRT UPEC

- Recopilación de información
  - ❖ Recopilación en fuentes de información. - Se recolecta información de diversas fuentes, mismos que contienen datos interesantes e importantes para la comunidad objetivo en la seguridad de sus sistemas de información. Las fuentes tienen que ser reconocidas, con autores, contener datos más recientes y que maneje una redacción coherente y con tecnicismos sobre el tema.
- Análisis de la información
  - ❖ Pertinencia. - La información recopilada debe ser analizada para determinar si es pertinente y apropiada para la comunidad objetivo. Se verifica que la información aporte en el desarrollo de las actividades organizacionales y mantenga una relación en los sistemas tecnológicos y procesos que manejan.
  - ❖ Categorización. - La información debe tener categorías de acuerdo a los datos o elementos que intervienen, pero que se enfocan en diferentes secciones de la informática. En base al contenido se determina si se trata de tendencias

tecnológicas, seguridad Informática, tips de productividad, recomendaciones de mejores prácticas y concientización tecnológica.

- Distribución de la información
  - ❖ Publicación. -La información se publica en el sitio web de CSIRT UPEC, de acuerdo al formato establecido en la figura 52, donde se detalla su categoría y la fecha de publicación, título que atraiga la atención del lector, una imagen que represente la temática de la información que se presenta, una descripción puntual y, por último, las fuentes de consulta para que puedan obtener más información acerca del tema.

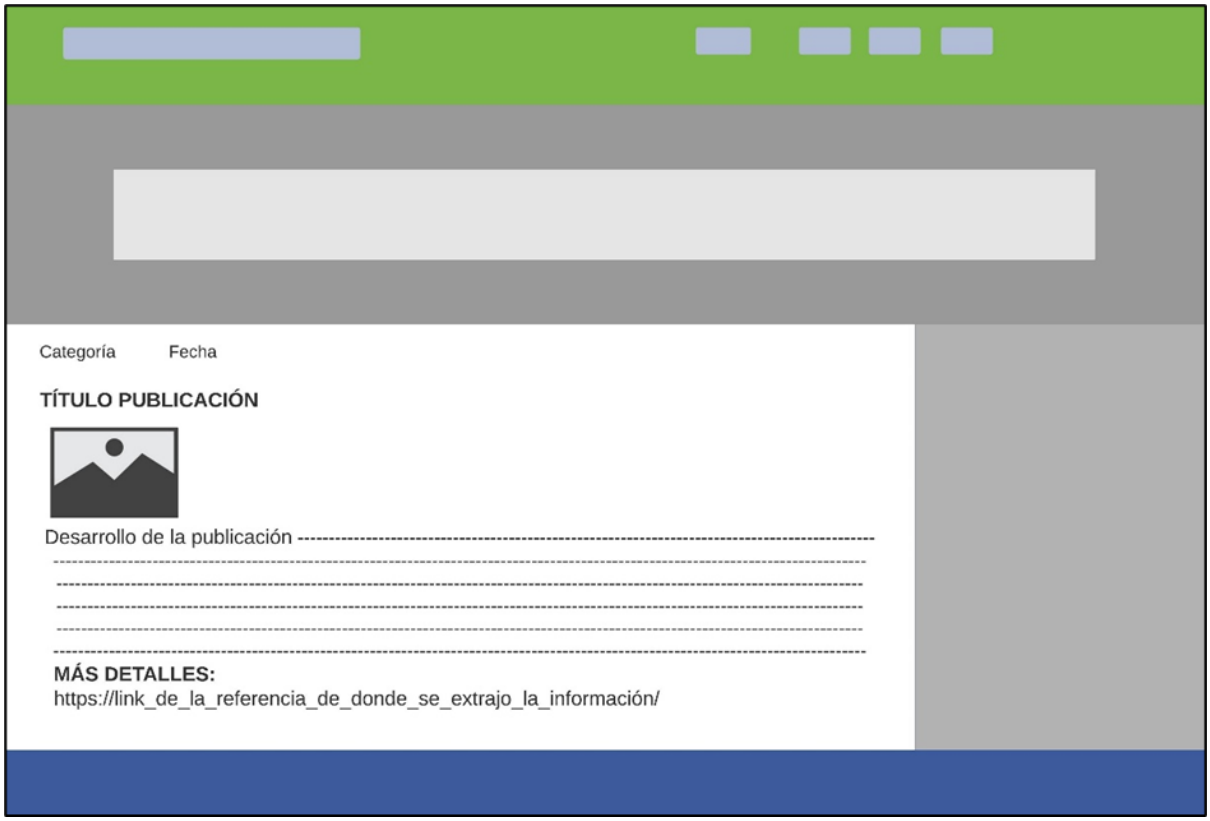


Figura 52. Formato distribución de anuncios CSIRT UPEC

l) Proceso de concientización tecnológica

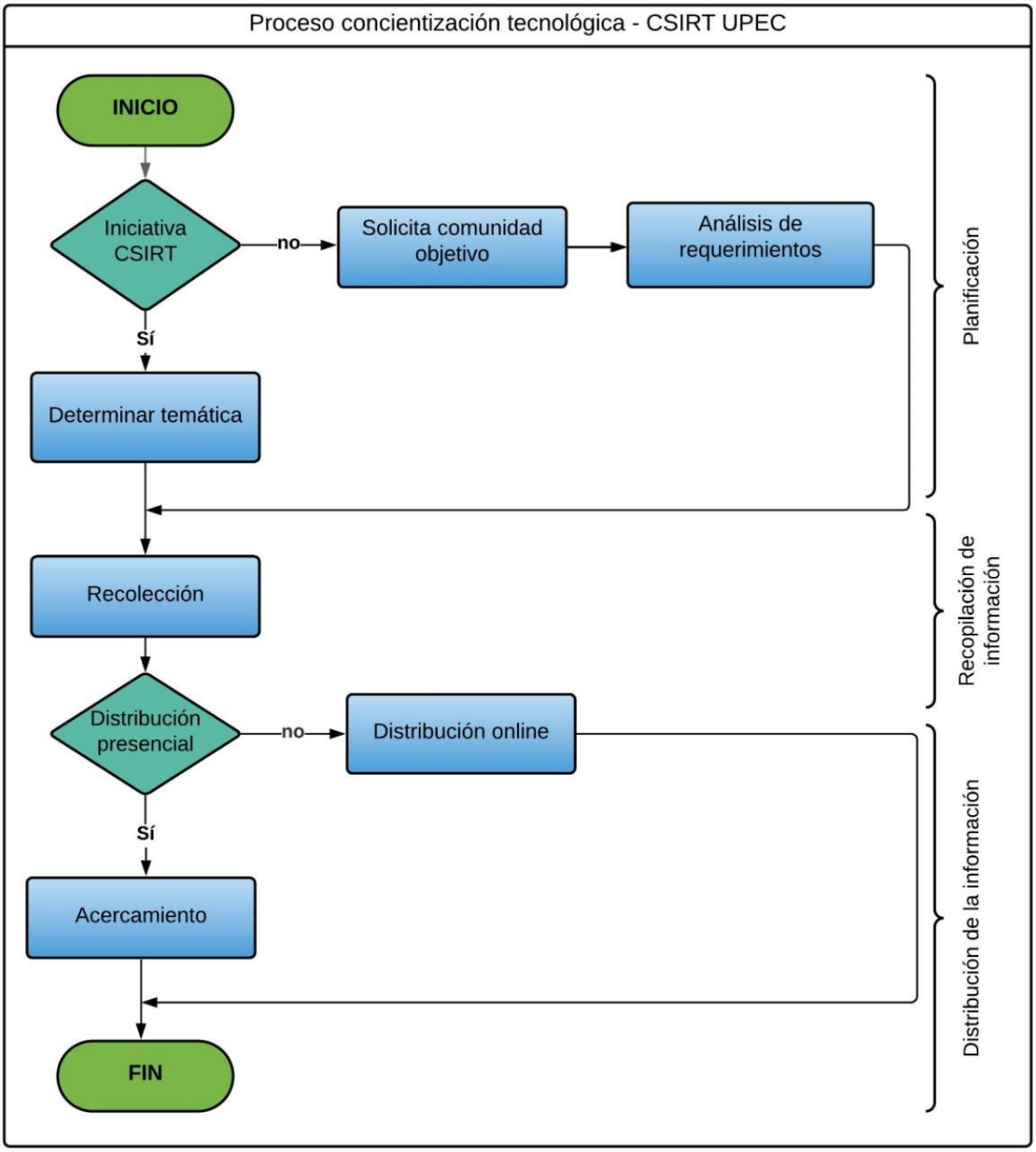


Figura 53. Proceso de concientización tecnológica CSIRT UPEC

- Contexto del proceso

Tabla 32. Ficha de proceso concientización tecnológica

Proceso	**Revisión**	**Fecha revisión**
Concientización tecnológica	1	15/9/2021

Objetivo del proceso

Colaborar en buenas prácticas para la seguridad de la información por iniciativa del CSIRT o comunidad objetivo para crear conciencia sobre seguridad informática e información.

Alcance

Emitir el servicio por el sitio web de parte del equipo o los medios de concientización con el tema requerido por la comunidad objetivo.

Actividades que forman el proceso

- Iniciativa CSIRT.
- Determinar temática.
- Solicitud comunidad objetivo.
- Análisis de requerimientos.
- Determinar temática.
- Recolección.
- Distribución.
- Distribución online.
- Acercamiento.

Responsables del proceso

Encargado departamento de operaciones

Entradas del proceso	**Salidas del proceso**
- Iniciativa CSIRT. - Formulario de solicitud de concientización tecnológica.	Concientización tecnológica.

Procesos relacionados

No existe

Recursos

- Acceso al sistema de ticket centro de respuesta y soporte a incidentes de seguridad.

- Acceso al sitio web https://csirt.upec.edu.ec/
- Acceso al servidor de monitoreo.
- Acceso al correo electrónico csirt.computacion@upec.edu.ec

Registros/archivos

- Formulario solicitud concientización tecnológica.
- Material didáctico de concientización.

Indicadores

- Porcentaje de solicitudes cumplidas dentro del SLA.
- Porcentaje de tiempo promedio transcurrido para lograr la resolución de requerimientos.
- Porcentaje de solicitudes complidas dentro del SLA.

Documentos aplicables

- Manual de políticas CSIRT UPEC
- Acuerdo de nivel de servicios CSIRT UPEC

- Planificación
  - ❖ Iniciativa CSIRT. -CSIRT UPEC, está comprometido en la concientización de seguridad informática y toma la iniciativa de acercarse a las organizaciones con temas que son de interés y de gran aporte en la gestión laboral. Esto genera la capacidad de prevenir y detectar incidentes.
  - ❖ Determinar la temática. -El equipo se encarga de encontrar puntos donde las instituciones necesitan tomar conciencia y aprender de asuntos que ayuden en la protección de la información y sus sistemas. Con ello, se busca mentalizar a las personas sobre ciertas operaciones que se las realiza de manera inapropiada y las consecuencias negativas que se producen, se busca apoyar en el uso de sus sistemas de forma responsable y consciente para evitar vulnerabilidades o incidentes.
  - ❖ Solicitud por parte de la comunidad objetivo. -CSIRT UPEC, está abierto a requerimientos en temáticas de concientización que necesitan las organizaciones para mejorar su desempeño en capacidad de respuesta a incidentes y uso de buenas prácticas para evitar ser vulnerables. La institución objetivo realiza la solicitud con el formato establecido en el anexo 30, donde expone la temática que quieren aprender o conocer mediante el sistema de tickets o correo electrónico del equipo.

- ❖ Análisis de requerimientos. - Se analiza los requerimientos y se define la temática que el equipo brindará para satisfacer las necesidades de la institución.

- Recopilación de información
  - ❖ Recolección. -De acuerdo a los lineamientos requeridos, se realiza la recopilación de la información necesaria que permita explicar y concientizar sobre la temática establecida para que la organización pueda orientarse o tomar decisiones sobre ciertos procesos, las fuentes de consulta deben contar con características como nombre del autor (persona o institución), ser un sitio web reconocido, tener credibilidad y fecha de actualización del contenido. Además, se debe analizar y comparar las fuentes con otras que manejan la misma temática.

    La investigación a presentar debe enfocarse en la comunidad a la que se la va a concientizar, tener objetivos claros sobre el tema, medios y estrategias a aplicar y mensajes claros que se quiere transmitir.
- Distribución de la información
  - ❖ Distribución presencial. -Para la distribución de la información de manera presencial, el equipo debe preparar material que ayude en la charla o capacitación de concientización del tema solicitado, se puede incluir videos, carteles, presentaciones, dinámicas o cualquier otra herramienta o evento que aporte en su desarrollo.
  - ❖ Acercamiento. -CSIRT UPEC se acerca a las instalaciones de la institución para brindar una charla de concientización tecnológica con el tema definido.
  - ❖ Distribución online. -Para generar conciencia en los miembros del equipo, se toman diferentes estrategias, entre ellas se realiza mensajes cortos sobre recomendaciones en seguridad de la información que serán publicados en el carrusel del sitio web, boletines electrónicos distribuidos mediante el correo del equipo y en caso de requerirlo conferencias mediante herramientas de videoconferencia. Además, en la sección de noticias del sitio web se publicarán recomendaciones sobre mejores prácticas en seguridad informática con el formato de anuncios establecido en la figura 52 y categorizados como concientización tecnológica.

m) Proceso para la Gestión de Riesgos

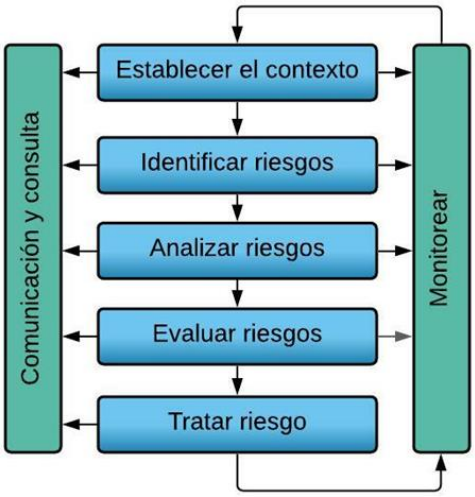


Figura 54. Proceso para la gestión de riesgo

Fuente: ISOTools (2017). 10 pasos para implementar un plan de Gestión de Riesgos de acuerdo a ISO 31000. Página web oficial de normativas ISO.

- Contexto del proceso

Tabla 33. Ficha de proceso gestión de riesgos

Proceso	**Revisión**	**Fecha revisión**
Gestión de riesgos	1	15/9/2021
Objetivo del proceso Identificar y priorizar los riesgos		
Alcance El proceso para la gestión de riesgo permitirá priorizar el riesgo y definir los tiempos de respuesta que serán establecidos en el acuerdo de nivel de servicios (SLA) de CSIRT UPEC. Además de apoyar en la gestión de riesgos del equipo.		
Actividades que forman el proceso - Identificar riesgos - Analizar riesgos - Evaluar riesgos - Tratar riesgo - Comunicación y consulta - Monitoreo		

Responsables del proceso

Encargado departamento de operaciones

Entradas del proceso	**Salidas del proceso**
- Identificación de riesgos. - Triage del reporte a incidentes informáticos.	Priorización de riesgo

Procesos relacionados

- Manejo de incidentes.
- Alertas y avisos.

Recursos

- Acceso al sistema de ticket centro de respuesta y soporte a incidentes de seguridad.
- Acceso al sitio web https://csirt.upec.edu.ec/
- Acceso al servidor de monitoreo.
- Acceso al correo electrónico csirt.computacion@upec.edu.ec

Registros/archivos

- Priorización de riesgo.

Indicadores

- Porcentaje del incremento de riesgos reportados al CSIRT.
  (Las métricas e indicadores se muestran en el anexo 31)

Documentos aplicables

- Manual de políticas CSIRT UPEC.
- Acuerdo de nivel de servicios CSIRT UPEC.

- Establecer el contexto
  - ❖ Alcance. - El proceso para la gestión de riesgo permite priorizar el riesgo y definir los tiempos de respuesta que serán establecidos en el acuerdo de nivel de servicios (SLA) de CSIRT UPEC. Además de apoyar en la gestión de riesgos del equipo.
  - ❖ Organización. - El departamento de operaciones CSIRT UPEC, tendrá la responsabilidad de cumplir el proceso de gestión de riegos.
- Identificar riesgos

  Se identifican los riesgos teniendo en cuenta los procesos de la organización, como se muestra en la tabla 34.

Tabla 34. Identificación de riesgos

Procesos CSIRT relacionados				**Riesgos**	
Manejo de incidentes	**Alertas y avisos**	**Anuncios**	**Concientización tecnológica**	**Clasificación**	**Tipo**
x	x	x		Código malicioso	Ransomware, malware, spyware, troyano, virus - En el sistema web.
x			x		Ransomware, malware, spyware, troyano, virus - En el sistema de ticket.
x		x		Disponibilidad	Ataques DoS/DDoS - En el sistema web.
x			x		Intercepción de información - En el sistema de ticket.
x			x	Confidencialidad de la información	Acceso a información no autorizada - En el sistema de ticket.
x			x		Modificación de información no autorizada - En el sistema de ticket.
x	x	x		Recopilación de información	Ingeniería Social - En el sistema web.
x	x	x		Intentos de intrusión	Explotación de vulnerabilidades conocidas - En el sistema web.
x			x		Intentos de acceso - En el sistema de ticket.

x	x	x			Suplantación de identidad (Phishing) - En el sistema web.
x		x		Fraude	SPAM - En el sistema web.
x	x		x	Contenido abusivo	SPAM - En el correo electrónico.

- Análisis del riesgo

  El Riesgo se lo obtiene mediante el producto de los dos ejes, para ello se utiliza la formula detallada en la tabla 35.

Tabla 35. Fórmula calculo riesgo

Riesgo = Eje de probabilidad * Eje de impacto

Donde el eje de probabilidad y el eje de impacto pueden tomar los valores que se detallan en la tabla 36.

Tabla 36. Valores de los ejes de probabilidad y de impacto

Eje de probabilidad	**Eje de impacto**
1 = Raro	1 = Sin impacto
2 = Baja	2 = Leve
3 = Media	3 = Medio
4 = Alta	4= Grave

Para su análisis se toma en cuenta la matriz de calor análisis de riesgo como se muestra en la figura 55.

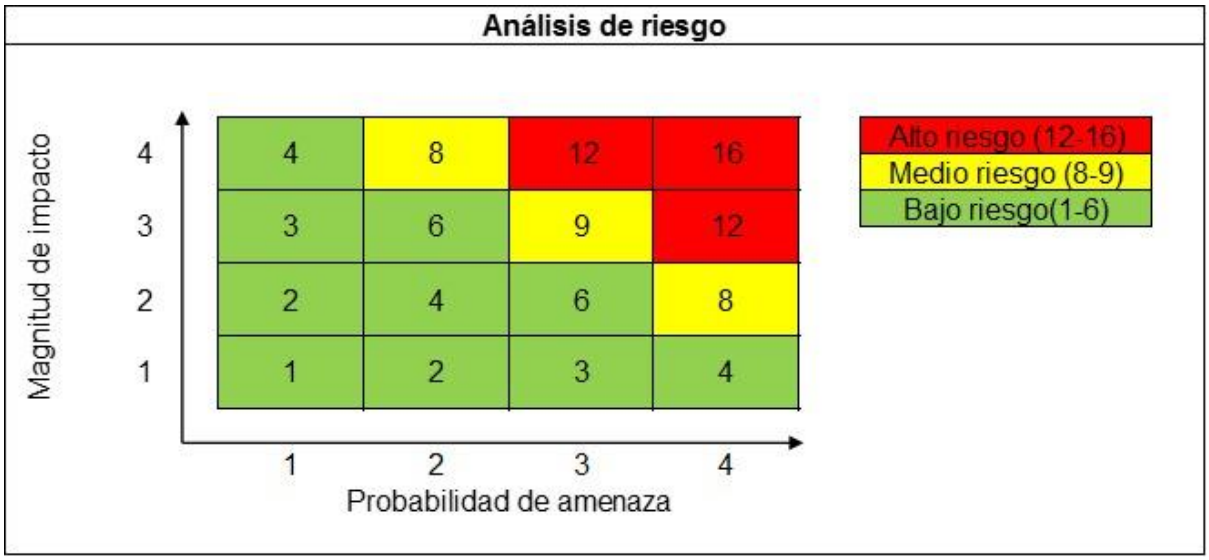


Figura 55. Matriz de calor para el análisis de riesgo

Donde el valor resultante entre el rango de 1 a 6 se considera como un riesgo bajo, de 8 a 9 se considera como un riesgo medio y entre 12 y 16 se considera como un riesgo alto.

- Valorar riesgo

  Se considera el nivel de riesgo para priorizar y definir el tiempo de respuesta al riesgo presentado como se muestra en la tabla 34.

Tabla 37. Prioridad tiempo de respuesta

Nivel de riesgo	**Prioridad tiempo de respuesta**
Riesgo alto	Atención inmediata a 30 minutos
Riesgo medio	31 minutos a 1 hora
Riesgo bajo	1 hora a 24 horas

- Tratar los riesgos
  - ❖ Reducción del riesgo. - CISRT UPEC define los controles que se aplicarán para el tratamiento del riesgo.
  - ❖ Transferencia del riesgo. - Luego de un análisis y dependiendo de la evaluación del riesgo, el equipo decidirá transferir el riesgo hacia agentes externos con mayor capacidad y eficacia.
  - ❖ Aceptación del riesgo. - El equipo asume el riego y define las responsabilidades y formas de control que le permitirán evitar o mitigar el riesgo.
- Comunicación y consulta

  El equipo tiene que estar en contacto con las partes interesadas de forma iterativa en cada punto del análisis del riesgo.
- Monitoreo y revisión del riesgo

  Los riesgos, las amenazas y vulnerabilidades siempre se presentarán, por lo que el equipo está obligado a realizar monitoreo constante de forma iterativa para poder valorizar, tomar medidas de control, mitigación del riesgo y mejora continua.

4.2.2.3. Acuerdo de nivel de servicios (SLA)

a) Introducción

El presente SLA establece como se realiza la entrega de los servicios manejo de incidentes y concientización tecnológica que CSIRT UPEC brinda a sus miembros.

b) Descripción del servicio

Los servicios brindados por CSIRT UPEC a través del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad son:

- Manejo de incidentes. - Apoya en la solución o mitigación de incidentes de seguridad informática a las instituciones miembros a través de recomendaciones de solución.
- Concientización tecnológica. - CSIRT UPEC, está comprometido en la concientización de seguridad informática y toma la iniciativa de acercarse a las organizaciones miembro con temas que son de interés y de gran aporte en la gestión laboral, proporcionando información para cumplir mejor las políticas, procesos y actividades en la organización mediante capacitaciones, publicación de artículos y contenido multimedia en el sitio web del equipo. Se pretende reducir significativamente los incidentes y aumentar la capacidad de detectar vulnerabilidades para que los sistemas sean protegidos o recuperados en menor tiempo.

c) Alcance del acuerdo.

- Cumplimiento de políticas y procesos. -Los servicios manejo de incidentes y concientización tecnológica cumplen las siguientes políticas de seguridad establecidas por CSIRT UPEC:
  - ❖ Política de clasificación de información.
  - ❖ Política de protección de datos.
  - ❖ Política de destrucción de información.
  - ❖ Política de divulgación de información.
  - ❖ Política de acceso a la información.
  - ❖ Política de uso apropiado de los sistemas.
  - ❖ Política de cooperación.
  - ❖ Política de privacidad.

  El servicio manejo de incidentes cumple el siguiente proceso:
  - ❖ Proceso de gestión de incidentes.
  - ❖ Proceso de gestión de riesgos.

  El servicio concientización tecnológica cumple el siguiente proceso:
  - ❖ Proceso de concientización tecnológica.
  - ❖ Proceso de gestión de riesgos.

d) Contacto

Medios de contacto de CSIRT UPEC con sus miembros:

- Correo electrónico: csirt.computacion@upec.edu.ec

e) Horario del servicio

Los servicios manejo de incidentes y concientización tecnológica estarán disponibles en el siguiente horario:

Tabla 38. Horario de los servicios que brinda CSIRT UPEC

Día	**Hora**
Lunes	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm
Martes	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm
Miércoles	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm
Jueves	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm
Viernes	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm
Sábado	Cerrado
Domingo	Cerrado

- Excepciones:
  - ❖ Fines de semana. - CSIRT UPEC no brinda sus servicios los fines de semanas, pero en el caso de que los miembros requieran del servicio manejo de incidentes, y su reporte se clasifique como un RIESGO ALTO, será atendido de acuerdo a los tiempos establecidos en el proceso gestión de riesgos.
  - ❖ Días festivos. - CSIRT UPEC no brinda sus servicios en días festivos, pero en el caso de que los miembros requieran del servicio manejo de incidentes, y su reporte se clasifique como un RIESGO ALTO, será atendido de acuerdo a los tiempos establecidos en el proceso gestión de riesgos.
  - ❖ Extensiones de horarios. - CSIRT UPEC no brinda sus servicios en horarios extendidos, pero en el caso de que los miembros requieran del servicio manejo de incidentes, y su reporte se clasifique como un RIESGO ALTO, será atendido de acuerdo a los tiempos establecidos en el proceso gestión de riesgos.
- Interrupción programada:

  Las interrupciones programadas por CSIRT UPEC, que le permitirán realizar mantenimiento, instalación y configuración de nuevos equipos entre otras actividades de corrección o mejoramiento de los servicios se realizarán en los siguientes horarios (previo aviso):

Tabla 39. Horario para interrupción programada

Día	Hora
Jueves	3:00 pm – 5:00 pm
Viernes	8:00 am – 1:00 pm

- Aviso de interrupción de los servicios

  Si se presenta interrupción programada o no programada en los servicios, el aviso a los miembros del CSIRT se realizará de la siguiente forma:

  - ❖ Interrupción programada. - La notificación al miembro se la realizará con 72 horas de anticipación, mediante el sitio web del equipo.
  - ❖ Interrupción no programada. - La notificación al miembro se la realizará al instante a través del correo electrónico o vía teléfono.

f) Objetivos de nivel de servicios

Los siguientes puntos definen el compromiso de CSIRT UPEC con sus miembros:

- Disponibilidad de los servicios. - Los servicios manejo de incidentes y concientización tecnológica serán brindados en los días y horarios establecidos en el apartado < Horarios del servicio >, con una disponibilidad de 99.0%.
- Desempeño de los servicios. - Se establece el factor crítico de éxito (CSF), indicador clave de rendimiento (KPI), fórmula de cálculo, fuente de datos, meta y la frecuencia de medición, que permiten evaluar la calidad de los servicios.

Tabla 40. Métrica gestión de solicitudes del servicio manejo de incidentes

CSF	KPI	Fórmula	Fuente de datos	Meta	Frecuencia
Resolver los incidentes reportados minimizando su impacto	Porcentaje de incidentes cerrados dentro de lo establecido en el SLA	$\frac{\text{N° de incidentes cerrados que cumplen el SLA}}{\text{Total incidentes cerrados}} \times 100$	Sistema de ticket	45%	Mensual
	Porcentaje de tiempo promedio por adicional por agente para solución de incidentes	$\frac{\text{Tiempo promedio solución de incidentes - tiempo establecido en el SLA}}{\text{Tiempo establecido en el SLA}} \times 100$	Sistema de ticket	N/A	Mensual
Supervisar el estado de los incidentes para la toma de decisiones	Porcentaje de incidentes por estado	$\frac{\text{Número de incidentes no verídicos cerrados}}{\text{Total incidentes cerrados}} \times 100$ $\frac{\text{Número de incidentes que no corresponden a la comunidad onjetivo cerrados}}{\text{Total incidentes cerrados}} \times 100$	Sistema de ticket	N/A	Mensual

$\frac{\text{Número de incidentes falso positivo cerrados}}{\text{Total incidentes cerrados}} \times 100$
$\frac{\text{Número de incidentes resueltos y sin respuesta cerrados}}{\text{Total incidentes cerrados}} \times 100$
$\frac{\text{Número de incidentes resueltos y con respuesta cerrados}}{\text{Total incidentes cerrados}} \times 100$
$\frac{\text{Número de incidentes sin resolución y sin respuesta cerrados}}{\text{Total incidentes cerrados}} \times 100$

Tabla 41. Métrica gestión de solicitudes del servicio concientización tecnológica

CSF	KPI	Fórmula	Fuente de datos	Meta	Frecuencia
Brindar el servicio de forma eficiente cumpliendo las	Porcentaje de solicitudes cumplidas dentro del SLA	$\frac{\text{N° de requerimientos cumplidos dentro del SLA}}{\text{Total de solicitudes cerradas del servicio en el mes}} \times 100$	Sistema de ticket	80%	Mensual

solicitudes dentro del SLA acordado	Porcentaje de tiempo promedio transcurrido para lograr la resolución de requerimientos	$\frac{\text{Tiempo promedio solución de solicitudes - tiempo establecido en el SLA}}{\text{Tiempo establecido en el SLA}} \times 100$	Sistema de ticket	N/A	Mensual

Tabla 42. Métrica gestión de niveles de los servicios

CSF	KPI	Fórmula	Fuente de datos	Meta	Frecuencia
Los servicios se deben brindar de acuerdo a lo establecido en el SLA	Porcentaje de solicitudes complidas dentro del SLA	$\frac{\text{N° de servicios cerrados que cumplen el SLA}}{\text{Total servicios cerrados en el mes}} \times 100$	Sistema de ticket	65.5%	Mensual

g) Soporte al usuario

CSIRT UPEC brindará soporte de los servicios a través de los siguientes medios:

- Sitio web (Página de contacto): https://csirt.upec.edu.ec/contacto/
- Correo electrónico: csirt.computacion@upec.edu.ec

Los miembros del CSIRT, podrán solicitar soporte para sus servicios en el siguiente horario:

Tabla 43. Horario para solicitar soporte a CSIRT UPEC

Día	**Hora**
Lunes a viernes	8:00 am – 1:00 pm, 3:00 pm – 5:00 pm

h) Escalamientos

Si el miembro presenta incumplimiento de los servicios, su caso escalará al siguiente personal a cargo.

El personal asignado se reunirá con el agente que ocasionó el incumplimiento para definir acciones para la continuidad del servicio.

i) Procedimientos de solicitud

Los miembros de CSIRT UPEC, se basarán en los procesos establecidos donde se explica el correcto proceso para la solicitud del servicio, los medios y formatos hasta el cierre del servicio:

a) Proceso manejo de incidentes.
b) Proceso concientización tecnológica.

j) Revisiones.

El presente SLA será revisado entre CSIRT UPEC y el miembro en el caso requerirse.

k) Responsabilidades.

Responsabilidades de CSIRT UPEC y de sus miembros para hacer cumplir la entrega del servicio acorde a lo establecido en este SLA.

- CSIRT UPEC: Verificar el desempeño del equipo al bridar los servicios a sus miembros.
- Miembros: Notificar a CSIRT UPEC sobre las anomalías presentadas al recibir el servicio.

4.2.3. Cierre

Se finaliza el proceso de constitución de CSIRT UPEC para la seguridad de la información en unidades educativas y gobiernos seccionales de la provincia del Carchi. En su constitución se muestra el propósito del equipo en la sociedad, el impacto que se quiere lograr y los valores que lo identifican, menciona los servicios de alertas y avisos, manejo de incidentes, anuncios y concientización tecnológica con autoridad nula porque no participa en la toma de decisiones de la comunidad objetivo. Adopta el modelo organizacional incrustado al ubicarse en el "Laboratorio de Ciberseguridad de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi"; y detalla las funciones de los integrantes del CSIRT de acuerdo a sus departamentos, conformados por dirección, TI y operaciones.

Se conforma de un sitio web y herramientas que ayudan en la gestión de los servicios, estos se encuentran en sistemas operativos menos propensos a incidentes o vulnerabilidades. Para sus operaciones, CSIRT UPEC tiene políticas y procesos que ayudan en el manejo correcto de los servicios e información que se gestiona.

4.2.3.1. Presupuesto referencia para la implementación de CSIRT UPEC

Para llevar a cabo la implementación de CSIRT UPEC se obtuvo recursos facilitados por el Laboratorio de Ciberseguridad de la Carrera de Computación y la Universidad Politécnica Estatal del Carchi, se toma en cuenta un presupuesto referencial para valorar cada recurso brindado para la conformación del equipo al inicio de sus actividades.

- Costos plataforma tecnológica en hardware y software

  Los recursos en hardware y software incluyen componentes de comunicación, almacenamiento y gestión de los servicios del equipo, se realiza el costo referencial en la tabla 44.

Tabla 44. Costo referencial de tecnología hardware y software de CSIRT UPEC

Rubro	**Unidad**	**Equipo**	**Precio unitario**	**Subtotal**
Sistema IDS/IPS	1	IPS-4240-K9	$10.100,00	$10.100,00
Correlacionador de eventos SIM7SIEM	1	CS-MARS-25K9	$12.100,00	$12.100,00
Switch de acceso	1	CISCO WS-C2960-24LCS	$4.900,00	$4.900,00

Router de borde	1	CISCO 19417k9	$1.539,00	$1.539,00
Total				$28.639,00

- Costos operativos

  CSIRT UPEC cuenta con tres técnicos para cada departamento (dirección, TI y operaciones), se toma en consideración la fundamentación teórica, en la que se dice que, para el inicio de las actividades del equipo, se deben establecer los recursos humanos necesarios de acuerdo a la comunidad objetivo, el tipo de incidentes que estas pueden presentar y el número de servicios a disposición. Se realiza un costo referencial para el personal en la tabla 45.

Tabla 45. Costo referencial gastos operativos de CSIRT UPEC

Rubro	**Unidad**	**Sueldo**	**Subtotal/ mensual**	**Subtotal/ anual**
Director CSIRT	1	$2,100,00	$2,100,00	$25.200,00
Personal departamento de operaciones	1	$1.150,00	$1.150,00	$13.800,00
Personal departamento de TI	1	$1.340,00	$1.340,00	$16.080,00
Total			$4.590,00	$55.080,00

- Costos equipos de oficina

  El material de oficina aporta al correcto desarrollo organizacional y siempre será utilizado como apoyo en las operaciones del CSIRT, en este caso, se utiliza las instalaciones del Laboratorio de Ciberseguridad y los recursos que tiene, sin embargo, también se considera un factor económico tomado en cuenta. Su costo referencial se establece en la tabla 46.

Tabla 46. Costo referencia equipos de oficina de CSIRT UPEC

Rubro	**Unidad**	**Precio unitario**	**Sub total**
Estaciones de trabajo	3	$600,00	$1800,00
Archivador	1	$250,00	$250,00
Computador	3	$1.300,00	$3.900,00
Teléfono	3	$300,00	$900,00
Impresora multifuncional	1	$2.100,00	$2.100,00

Artículos de oficina	$2.500,00
Total	$11.450,00

- Costos servicios básicos

  Manejamos un costo referencial, mostrando a CSIRT UPEC como una organización que paga por la infraestructura en la que se ubica, servicio de teléfono, energía e internet de forma independiente, estos elementos se los consideran fundamentales para que el equipo funcione al 100 %. Los costos de referencia se muestran en la tabla 47.

Tabla 47. Costo referencial servicios básicos de CSIRT UPEC

Rubro	**Unidad**	**Precio Instalación**	**Precio mensual**	**Precio anual**	**Subtotal**
Internet (100 MB)	1	$100,00	$18,35	$220,20	$320,20
Teléfono (Línea comercial)	1	$67,20	$13,44	$161,28	$228,48
Energía eléctrica	1	$160,00	$200,00	$2.400,00	$2.560,00
Total					$3.108,68

- Presupuesto referencial

  El costo referencial total para la implementación de CSIRT UPEC, se lo realiza de los totales obtenidos de las anteriores tablas de recursos, el presupuesto se establece para un año y su resultado se muestra en la tabla 48.

Tabla 48. Costo referencial total para la implementación de CSIRT UPEC

Rubro	**Costo**
Costo de tecnología hardware y software	$28.639,00
Costos operativos	$55.080,00
Costos equipos de oficina	$11.450,00
Costos servicios básicos	$3.108,68
Total	$98277,68

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se realizó la fundamentación teórica acerca del reporte y seguimiento a incidentes informáticos y seguridad de la información, donde se concluye que el uso de distintas fuentes de investigación permite determinar los requerimientos necesarios para conformar un CSIRT, ya que cada equipo se enfoca en una comunidad objetivo, y con ello determinan servicios y recursos operacionales para el correcto funcionamiento.
- Se identificó el correcto reporte y seguimiento a incidentes informáticos en la Universidad Politécnica Estatal del Carchi para la conformación de un CSIRT en el Laboratorio de Ciberseguridad, por lo que se concluye que aparte de contar con recursos humanos y procesos operacionales, la aplicación de normativas, procesos o leyes nacionales e internacionales también aportan a la seguridad de la información y disminuyen los incidentes o vulnerabilidades en una organización.
- Se determinó la seguridad de la información requerida por las unidades educativas y gobiernos seccionales de la provincia, a través de una entrevista e interacción con los encargados del área tecnológica y se concluye que, la recolección de información directamente de la fuente beneficiada en el proyecto ayuda a establecer el catálogo con los servicios que necesitan, los procesos correctos para brindarlos y las políticas que ayuden a la protección de la información de las organizaciones por parte del CSIRT.
- Se implementó un Equipo de Respuesta ante Incidentes de Seguridad Informática en el Laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi denominado CSIRT UPEC, está constituido con un servidor web y monitoreo, los servicios reporte de incidentes y concientización tecnológica configurados en el sistema de tickets Centro de Respuesta y Soporte a Incidentes de Seguridad, manual de políticas y procesos operacionales para la gestión de los servicios e información por parte del equipo, documento de constitución bajo el estándar RFC 2350 y un acuerdo de nivel de servicio. En conclusión, la constitución de un CSIRT debe contener los recursos necesarios y que aporten la gestión de sus operaciones, además, cada comunidad presenta diferentes incidentes o vulnerabilidades, por lo que los recursos de implementación de los equipos jamás van a ser iguales.

5.2. RECOMENDACIONES

Finalizado el proceso de investigación y adquirido los conocimientos en la constitución de un CSIRT con los procesos adecuados para tratar incidentes, se recomienda:

- Realizar una investigación meticulosa que permita determinar los requerimientos necesarios para la conformación de un CSIRT.
- Aplicar normativas, estándares y mejores prácticas como aporte al correcto funcionamiento de un CSIRT en la gestión de sus operaciones, calidad de los servicios y seguridad de la información.
- Aplicar métodos de recolección de información que permitan captar las necesidades de la comunidad objetivo, para posteriormente establecer los servicios y procesos necesarios.
- Utilizar el estándar de referencia RFC 2350 para constituir la información principal del CSIRT y manejar una política de privacidad, en la que se dé a conocer a la comunidad objetivo el uso que se le da a la información que emite a través de los medios de comunicación que tiene el equipo.
- Generar documentos pre establecidos y respuestas automáticas que ayuden al correcto proceso de solución de incidentes y concientización tecnológica, para aumentar la capacidad de respuesta y mejorar el servicio.

VI. REFERENCIAS BIBLIOGRÁFICAS

AETecno. (20 de Marzo de 2019). *Los países de Latinoamérica que registran mayor cantidad de Ciberataques*. Obtenido de AETecno: https://tecno.americaeconomia.com/articulos/los-paises-de-latinoamerica-que-registran-mayor-cantidad-de-ciberataques

Agencia AFP. (18 de Marzo de 2020). *Hackers usan coronavirus para realizar ciberataques.* Obtenido de Milenio: https://www.milenio.com/tecnologia/coronavirus-hackers-aprovechan-la-pandemia-para-realizar-ciberataques

BBC News Mundo. (16 de Septiembre de 2019). *Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano.* Obtenido de BBC: https://www.bbc.com/mundo/noticias-america-latina-49721456

Bone, C., Saltos, J., Figueroa, J., & Rodríguez, R. (2017). *La seguridad informática y la seguridad de la información.* Polo del Conocimiento, Manta, Ecuador. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/420

Calduch, R. (2017). *Métodos y técnicas de investigación internacional.* Obtenido de UNIVERSIDAD COMPLUTENSE DE MADRID: https://www.ucm.es/data/cont/docs/835-2018-03-01-Metodos%20y%20Tecnicas%20de%20Investigacion%20Internacional%20v2.pdf

Cano, J. (2020). *Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA (Tesis de pregrado).* Universidad Nacional Abierta y a Distancia UNAD, Cundinamarca, Bogotá DC, Colombia. Obtenido de Universidad Nacional Abierta y a Distancia, Cundinamarca, Bogotá DC: https://repository.unad.edu.co/handle/10596/36488

Castillo, A. (31 de marzo de 2017). *SEGURIDAD LOGICA. Gestión de la información: Confidencialidad, integridad, disponibilidad y estanqueidad*. Obtenido de Cronicaseguridad: https://cronicaseguridad.com/2017/03/31/seguridad-logica-gestion-la-informacion-confidencialidad-integridad-disponibilidad-estanqueidad/

CEDIA. (2020). *CSIRT*. Obtenido de CEDIA: https://www.cedia.edu.ec/es/servicios/tecnologia/infraestructura/csirt

CONGOPE Ecuador. (13 de noviembre de 2015). ¿Qué Hace el CONGOPE? YouTube. Obtenido de https://www.youtube.com/watch?v=UUsqTMr26D0&feature=emb_logo

Corporación IBM. (2017). *Acuerdos de nivel de sevicios*. Obtenido de IBM: https://www.ibm.com/docs/es/mfsp/7.6.1?topic=records-service-level-agreements-slas

De La Torre, H., & Parra, M. (2018). *Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE (Tesis de pregrado).* Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador. Obtenido de http://repositorio.espe.edu.ec/handle/21000/15071

ECNO CSIRT. (13 de 09 de 2019). *RFC 2350*. Obtenido de https://ednon.com/wp-content/uploads/2020/10/rfc2350_enoc-csirt_v1.2_es.pdf

El Comercio. (16 de Septiembre de 2019). *¿Cómo puede afectar a tu familia la masiva filtración de datos personales de millones de ecuatorianos?* Obtenido de El Comercio: https://www.elcomercio.com/tendencias/consecuencias-filtracion-datos-ecuatorianos-estafas.html?fbclid=IwAR0FOu8RyHDA7lsft3o9ogNv-2YPlKS6YR9-oUvJihSLzSxpsn2k6_AgFug

El Comercio. (29 de Julio de 2021). *Ecuador está entre los países con más ciberataques en America Latina*. Obtenido de El Comercio: https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html?fbclid=IwAR2BHbJkFuwS0YMMkNhuk7tNwCTdb5nCFVOZvU6MFfomNrDCtGuVBCy3IW0

Figueroa , J. (2019). *Plan de seguridad informática basado en la norma ISO 27002 y la gestión de la información para el departamento de TIC de la Uniandes extensión Babahoyo [Tesis de pe grado].* Universidad Regional Autónoma de Los Andes- UNIANDES, Babahoyo, Ecuador. Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/9751

Guzmán, K. (30 de Julio de 2019). *México, país con más ciberataques en el mundo.* Obtenido de Milenio: https://www.milenio.com/negocios/mexico-pais-con-mas-ciberataques-en-el-mundo?fbclid=IwAR11j_6wGJleEyGiiZ8TueBmRRqiLY3Zb8GQZDPIgJeX3N_o0VDgyFtfoGY

Hernández, R., Fernández, C., & Pilar, L. (2014). *Metodología de la Investigación* (Sexta ed.). (McGraw-Hill, Ed.) Ciudad de México, México: Interamericana Editores, S.A. Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Hidalgo, J. (2017). *Importancia de las tic en la enseñanza aprendizaje de los estudiantes de la unidades educativas de la ciudad de Tulcán [Artículo científico]*. Universidad Politécnica Estatal del Carchi, Tulcán.

Hurtado, L., & Chuquiguanca, L. (2020). *Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado [Tesis de Maestría]*. Universidad Internacional SEK, Quito, Ecuador.

ISOTools. (2017). *10 pasos para implementar un plan de Gestión de Riesgos de acuerdo a ISO 31000*. Obtenido de Blog Calidad y Excelencia: https://www.isotools.org/2017/05/14/10-pasos-para-implementar-un-plan-de-gestion-de-riesgos-de-acuerdo-a-iso-31000/?fbclid=IwAR3RECwLGJ2P1gcA61iU1u52B0osGsA-8hNBDpbkM54i1LzYt96XgkgarPc

Martínez, C. (2018). *El muestreo en investigación cualitativa. Principios básicos y algunas controversias.* Obtenido de Scielo: https://www.scielo.br/pdf/csc/v17n3/v17n3a06.pdf

Merizalde, C. (21 de noviembre de 2020). UTPL - Ley Orgánica de la Educación Intercultural. YouTube. Obtenido de https://www.youtube.com/watch?v=jswV5k3ot2c

Motadata. (15 de Abril de 2021). *Tipos de acuerdo de nivel de servicio SLA*. Obtenido de Motadata: https://www.motadata.com/es/blog/types-of-service-level-agreement/

Murquincho, D. (2019). *CSIRTS Latinoamérica.* Obtenido de StuDoCu: https://www.studocu.com/ec/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/csirts-latinoamerica/3781244/view

NETEC. (17 de junio de 2019). *¿Qué es ITIL? Beneficios y procesos de ITIL*. Obtenido de NETEC: https://www.netec.com/post/que-es-itil-beneficios-y-procesos-de-itil

OEA. (abril de 2016). *Buenas Prácticas para establecer un CSIRT nacional.* Obtenido de Organización de los Estados Americanos (OEA): https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.sites.oas.org/cyber/Documents/2016%2520-%2520Buenas%2520Practicas%2520CSIRT.pdf&ved=2ahUKEwilyZ7Kl9_tAhWjd98KHZL7C7UQFjAAegQIBBAC&usg=AOvVaw2hUSCavhCxGn9GK7BJxdFV

Palacios, P. (2018). *Equipo de respuesta ante incidentes informáticos para La Universidad Regional Autónoma de Los Andes "UNIANDES" (Tesis de pregrado).* Universidad Regional Autónoma de los Andes UNIANDES, Ambato, Ecuador. Obtenido de http://dspace.uniandes.edu.ec/handle/123456789/8158

Quintero, L., & Peña, H. (2017). *Modelo basado en ITIL para la gestión de los servicios de TI para la Cooperativa de Caficultores de Manizales.* Universidad Autónoma de Manizales [Artículo de maestría]., Pereira, Colombia.

Quiñonez, G. (9 de Diciembre de 2019). *Delincuentes aprovechan temor a virus para estafas, hackeos*. Obtenido de Teleamazonas: https://www.teleamazonas.com/delincuentes-aprovechan-temor-a-virus-para-estafas-hackeos/

Quiroz, B. (2017). *Análisis y gestión de la seguridad en la red del GAD Municipio de Rioverde, mediante el diseño del equipo de respuesta a incidentes de seguridad informática, CSIRT (Tesis de pregrado).* Universidad Politécnica Salesiana Sede Quito, Quito , Ecuador. Obtenido de http://dspace.ups.edu.ec/handle/123456789/14466

Ramírez, H. (2016). *Desarrollo de un Marco de Trabajo para la Protección de un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT) (Tesis de pregrado).* Centro de Investigación en Matemáticas, A.C. CIMAT. Obtenido de http://cimat.repositorioinstitucional.mx/jspui/handle/1008/442

Reyes, M. (23 de Abril de 2018). *Conoce los 10 países de donde provienen más ciberataques en todo el mundo.* Obtenido de FayerWayer: https://www.fayerwayer.com/2018/04/los-10-paises-mas-ciberataques/?fbclid=IwAR2X9GkQW23ByoW6VwwH5Tu025Goc0oMFSUANlveES33IOabdVcPzl03lmI

Rodríguez, A. (2017). *Métodos científicos de indagación y de construcción del conocimiento.* Obtenido de Redalyc: https://www.redalyc.org/articulo.oa?id=20652069006

Van Der Heide, M. (2020). *Establecimiento de un CSIRT.* Obtenido de CEDIA: https://csirt.cedia.edu.ec/wp-content/uploads/2020/08/Estableciendo.un_.CSIRT_.v1.3-es_EC.pdf

VII. ANEXOS

Anexo 1 Acta de pre defensa



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERÍA EN INFORMÁTICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: ANDERSON DANIEL CHAMORRO PANTOJA **CÉDULA DE IDENTIDAD:** 0402042030
NIVEL/PARALELO: 0 **PERIODO ACADÉMICO:** JUN 2020 - SEP 2021

TEMA DE INVESTIGACIÓN: Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. CARLITOS ALBERTO GUANO CÁRDENAS
LECTOR: MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
ASESOR: MSC. GEORGINA GUADALUPE ARCOS PONCE

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: lunes, 6 de septiembre de 2021
HORA: 09H30
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 4.90
2) Trabajo escrito 2.10
Nota final de PRE DEFENSA **7.00**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el lunes, 6 de septiembre de 2021

Firmado digitalmente por CARLITOS ALBERTO GUANO CARDENAS
MSC. CARLITOS ALBERTO GUANO CÁRDENAS
PRESIDENTE

Firmado electrónicamente por: GEORGINA GUADALUPE ARCOS PONCE
MSC. GEORGINA GUADALUPE ARCOS PONCE
TUTOR

MILTON GABRIEL DEL HIERRO MOSQUERA
MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
LECTOR

Adj.: Observaciones y recomendaciones

Figura 56. Acta de pre defensa del proyecto de titulación denominado equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información – Anderson Chamorro



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERÍA EN INFORMÁTICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: SILVIA VERÓNICA PUPIALES CHACÓN **CÉDULA DE IDENTIDAD:** 1003991062
NIVEL/PARALELO: 0 **PERIODO ACADÉMICO:** JUN 2020 - SEP 2021

TEMA DE INVESTIGACIÓN: Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. CARLITOS ALBERTO GUANO CÁRDENAS
LECTOR: MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
ASESOR: MSC. GEORGINA GUADALUPE ARCOS PONCE

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: lunes, 6 de septiembre de 2021
HORA: 09H30
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 4.90
2) Trabajo escrito 2.10
Nota final de PRE DEFENSA **7.00**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el lunes, 6 de septiembre de 2021

Firmado digitalmente por CARLITOS ALBERTO GUANO CARDENAS
MSC. CARLITOS ALBERTO GUANO CÁRDENAS
PRESIDENTE

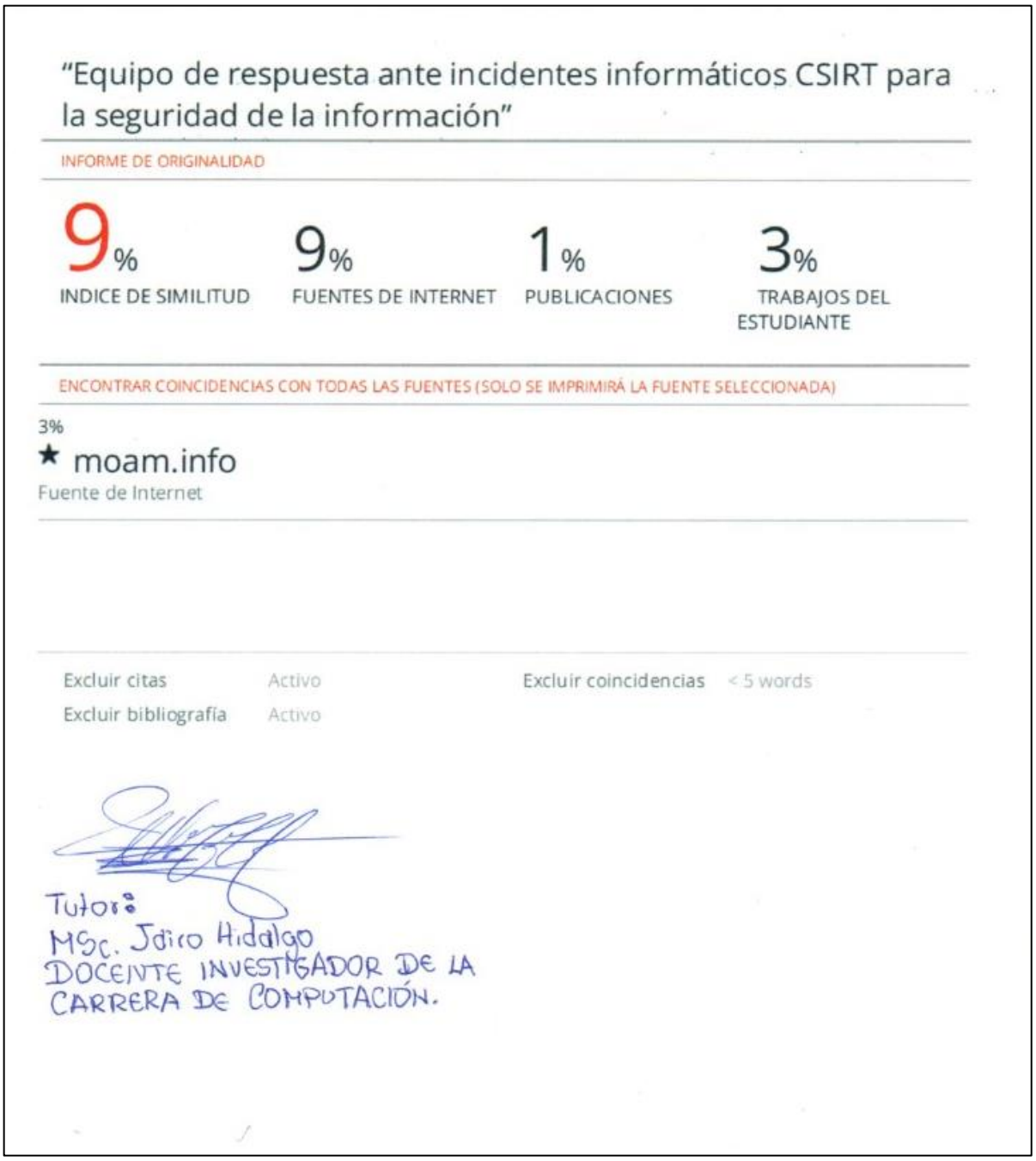
Firmado electrónicamente por: GEORGINA GUADALUPE ARCOS PONCE
MSC. GEORGINA GUADALUPE ARCOS PONCE
TUTOR

MILTON GABRIEL DEL HIERRO MOSQUERA
MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
LECTOR

Adj.: Observaciones y recomendaciones

Figura 57. Acta de pre defensa del proyecto de titulación denominado equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información – Silvia Pupiales

Anexo 2 Informe de turnitin



"Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información"

INFORME DE ORIGINALIDAD

9%	9%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

3%

★ moam.info

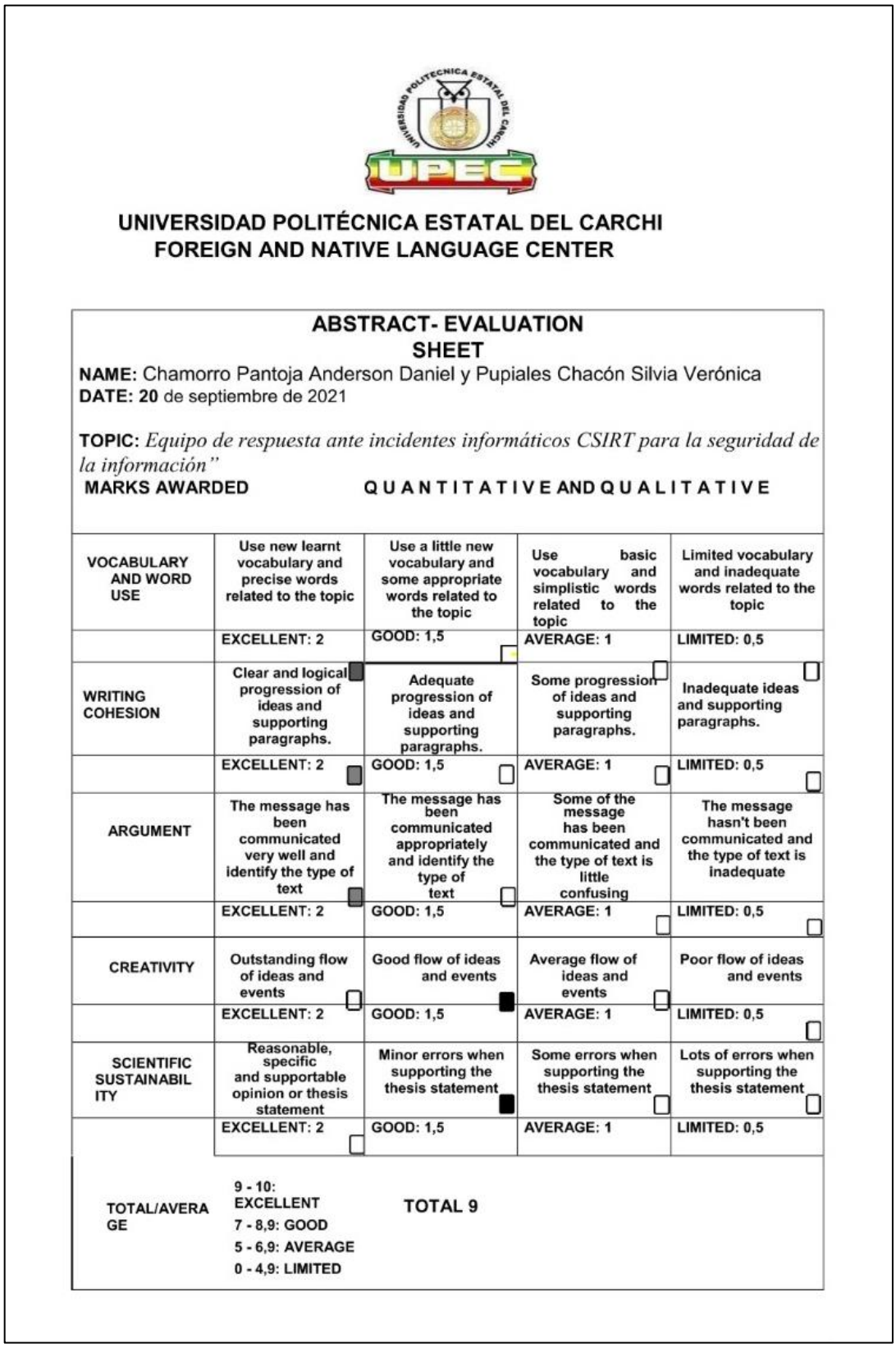
Fuente de Internet

Excluir citas	Activo	Excluir coincidencias	< 5 words
Excluir bibliografía	Activo		

Tutor:
MSc. Jairo Hidalgo
DOCENTE INVESTIGADOR DE LA CARRERA DE COMPUTACIÓN.

Figura 58. Informe de turnitin del documento de investigación

Anexo 3 Validación del abstract



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Chamorro Pantoja Anderson Daniel y Pupiales Chacón Silvia Verónica
DATE: 20 de septiembre de 2021

TOPIC: *Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información"*

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2	GOOD: 1,5	AVERAGE: 1	LIMITED: 0,5
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2	GOOD: 1,5	AVERAGE: 1	LIMITED: 0,5
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2	GOOD: 1,5	AVERAGE: 1	LIMITED: 0,5
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2	GOOD: 1,5	AVERAGE: 1	LIMITED: 0,5
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2	GOOD: 1,5	AVERAGE: 1	LIMITED: 0,5
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	**TOTAL 9**		

Figura 59. Validación del abstract por parte del CIDEN (parte 1)

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Chamorro Pantoja Anderson Daniel y Pupiales Chacón Silvia Verónica

Fecha de recepción del abstract: 20 de septiembre de 2021
Fecha de entrega del informe: 20 de septiembre de 2021

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:
Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

Firmado electrónicamente por:
EDISON BOANERGES PENAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Figura 60. Validación del abstract por parte del CIDEN (parte 2)

Anexo 4 Autorización para el desarrollo del proyecto de investigación en el laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi.



Tulcán, 22 de noviembre de 2019

Msc.
JAIRO HIDALGO
DOCENTE INVESTIGADOR DE LA CARRERA DE COMPUTACIÓN / INFORMÁTICA

Presente. -

De nuestra consideración:

Por medio del presente, reciba un cordial saludo y nos dirigimos a usted, para solicitarle de la manera más comedida se autorice el ingreso al laboratorio de Cyberseguridad con la finalidad de llevar a cabo el proceso de titulación.

El cual será utilizado para el desarrollo de la propuesta denominada **"Equipo de respuesta ante incidentes de seguridad informática CSIRT para la seguridad de la información en unidades educativas y gobiernos seccionales"**, por lo que se requiere de un espacio en el disco del servidor para realizar las respectivas configuraciones. Proceso que se realizará a partir del periodo académico octubre 2019 - febrero 2020 hasta la culminación del mismo.

.

Por la atención que se digne dar al presente, reciba nuestros agradecimientos.

Atentamente,

Anderson Chamorro
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 0402042030

Silvia Pupiales
ESTUDIANTE
INGENIERIA EN INFORMÁTICA
C.I. 1003991062

Autorizado

Figura 61. Oficio para el acceso al laboratorio de Ciberseguridad dirigido al Msc. Jairo Hidalgo – "Docente Investigador de la Carrera de Computación/ Ingeniería en Informática de la UPEC"

Anexo 5 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D01 San Pedro de Huaca – Tulcán".



06 02 982 982
Ext- Oficio

Tulcán, 7 de octubre de 2020

101

Lic.

Oscar Villarreal

DIRECTOR DISTRITAL 04D01 SAN PEDRO DE HUACA -TULCÁN

Presente. –

De nuestra consideración:

Por medio del presente, reciba un cordial saludo y nos dirigimos a usted para solicitarle de la manera más comedida, nos facilite la información de las Unidades Educativas vigentes pertenecientes a su distrito con la finalidad de llevar a cabo el proceso de titulación.

Dicha información será utilizada para el desarrollo de la propuesta denominada "Equipo de respuesta ante incidentes de seguridad informática CSIRT para la seguridad de la información en unidades educativas y gobiernos seccionales".

Por la atención que se digne dar al presente, reciba nuestros agradecimientos

Atentamente,

Anderson Chamorro
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 0402042030

Silvia Pupiales
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 1003991062

DIRECCIÓN DISTRITAL DE EDUACIÓN - TULCÁN
ATENCIÓN CIUDADANA
Nº de Folio: 001
Hora: 07-10-2020 8:43
TULCÁN - ECUADOR

Figura 62. Oficio dirigido al Lic. Oscar Villarreal – "Director Distrital 04D01"

Anexo 6 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D03 Mira - Espejo"



Tulcán, 8 de octubre de 2020

Msc.

Lourdes Del Hierro

DIRECTORA DISTRITAL 04D03 MIRA - ESPEJO

Presente. –

De nuestra consideración:

Por medio del presente, reciba un cordial saludo y nos dirigimos a usted para solicitarle de la manera más comedida, nos facilite la información de las Unidades Educativas vigentes pertenecientes a su distrito con la finalidad de llevar a cabo el proceso de titulación.

Dicha información será utilizada para el desarrollo de la propuesta denominada "Equipo de respuesta ante incidentes de seguridad informática CSIRT para la seguridad de la información en unidades educativas y gobiernos seccionales".

Por la atención que se digne dar al presente, reciba nuestros agradecimientos

Atentamente,

Anderson Chamorro
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 0402042030

Silvia Pupiales
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 1003991062

Recibido
2020-10-07
13:24

Silv41997p@gmail.com
0939240621

Figura 63. Oficio dirigido a la Msc. Lourdes Del Hierro – "Directora Distrital 04D03"

Anexo 7 Oficio de petición del listado de nombres de unidades educativas vigentes en el "Distrito 04D02 Montufar - Bolívar".

Tulcán, 12 de octubre de 2020

Lic.

Washington Mafla

DIRECTOR DISTRITAL 04D02MB MONTÚFAR - BOLÍVAR

Presente. –

De nuestra consideración:

Por medio del presente, reciba un cordial saludo y nos dirigimos a usted para solicitarle de la manera más comedida, nos facilite un listado con los nombres de las Unidades Educativas vigentes pertenecientes a su distrito.

Dicha información será utilizada para el desarrollo de la propuesta denominada "Equipo de respuesta ante incidentes de seguridad informática CSIRT para la seguridad de la información en unidades educativas y gobiernos seccionales de la provincia del Carchi", misma que será desarrollada en la Universidad Politécnica Estatal del Carchi como parte del proceso de titulación.

Por la atención que se digne dar al presente, reciba nuestros agradecimientos

Atentamente,

Anderson Chamorro
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 0402042030

Silvia Pupiales
ESTUDIANTE
INGENIERÍA EN INFORMÁTICA
C.I. 1003991062

Recibido
2020-10-12

Figura 64. Oficio dirigido al Lic. Washington Mafla – "Director Distrital 04D02"

Anexo 8 Formato de entrevista

	Universidad Politécnica Estatal del Carchi **Facultad de Industrias Agropecuarias y Ciencias Ambientales** **Ingeniería en Informática**	
ENTREVISTA A UNIDADES EDUCATIVAS DE LA PROVINCIA DEL CARCHI		
Fecha:		
Hora:		
Lugar:		
Entrevistadores:		
Entrevistado:		
Institución:		

Objetivo de la entrevista

Como parte de nuestra tesis en la carrera de Ingeniería en Informática, estamos realizando una investigación sobre los procedimientos que realizan las unidades educativas para la seguridad de la información y los equipos que la procesan. La información será utilizada en el desarrollo de la investigación denominada "Equipo de Respuesta ante Incidentes Informáticos CSIRT para la seguridad de la información".

Introducción

El uso de las tecnologías para el envío de información por la red, se han vuelto más comunes en el diario vivir de las personas, esto permite mejorar la comunicación en ámbitos laborales desde cualquier lugar o parte del mundo; con ello también se presentan las amenazas o incidentes que buscan que la información no llegue a su destino sin antes haber interferido en ella al igual que provocar daños en los equipos que la procesan.

Es por ello que nace el plan de investigación para la creación de un "Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT en el Laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi". El resultado permitirá a las unidades educativas de la provincia del Carchi que cuentan con una red establecida, tener un equipo que ayude en la prevención y mitigación de incidentes informáticos mediante un sistema web que será creado para pedir ayuda, o ver recomendaciones acerca del uso de las correctas políticas o normas de seguridad.

Características de la entrevista

- Las respuestas obtenidas serán únicamente para el uso de los entrevistadores en el desarrollo de la investigación.
- La duración de la entrevista será de treinta minutos a una hora aproximadamente.

Preguntas

1. ¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos? ¿Cuáles?
2. ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información? ¿Cuáles?
3. ¿Qué políticas o normativas internacionales utilizan en la institución para la seguridad de la información y los equipos que la procesan (Ejemplo: COBIT, ITIL, ISO/IEC serie 27000, etc.)?
4. ¿Qué medidas toman para evitar que la información y los equipos de la institución sean vulnerados?
5. En caso de presentarse un incidente informático (filtrado, alteración o pérdida de información, hackeos, denegación de servicios y caída del sitio web, introducción de código malicioso como virus, troyanos, gusanos y malware en general) ¿Qué procedimientos aplican para dar seguimiento a dichos incidentes y mitigar sus riesgos?
6. ¿Cómo llevan a cabo el proceso para la implementación o creación de políticas de seguridad, actualización de las mismas y generar recomendaciones sobre la seguridad informática?
7. ¿De qué manera se informan los miembros de la institución sobre las nuevas formas de ataques y explotación de vulnerabilidades?
8. ¿Con qué frecuencia realizan el escaneo de vulnerabilidades y de qué forma?
9. Según su criterio ¿Por qué ocurre el incumplimiento de políticas de seguridad?
10. ¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan? Teniendo en cuenta que la actualización incluye permisos y licencias respectivamente.

Esta entrevista ha sido de gran ayuda y hemos obtenido información muy importante para continuar con nuestro plan de investigación. Muchas gracias por su colaboración.

Figura 65. Formato entrevista para unidades educativas de la provincia del Carchi

	Universidad Politécnica Estatal del Carchi **Facultad de Industrias Agropecuarias y Ciencias Ambientales** **Ingeniería en Informática**	

ENTREVISTA A GOBIERNOS SECCIONALES DE LA PROVINCIA DEL CARCHI
Fecha:
Hora:
Lugar:
Entrevistadores:
Entrevistado:
Institución:

Objetivo de la entrevista

Como parte de nuestra tesis en la carrera de Ingeniería en Informática, estamos realizando una investigación sobre los procedimientos que realizan los gobiernos seccionales para la seguridad de la información y los equipos que la procesan. La información será utilizada en el desarrollo de la investigación denominada "Equipo de Respuesta ante Incidentes Informáticos CSIRT para la seguridad de la información".

Introducción

El uso de las tecnologías para el envío de información por la red, se han vuelto más comunes en el diario vivir de las personas, esto permite la mejor comunicación en ámbitos laborales desde cualquier lugar o parte del mundo; con ello también se presentan las amenazas o incidentes que buscan que la información no llegue a su destino sin antes haber interferido en ella al igual que provocar daños en los equipos que la procesan.

Es por ello que nace el plan de investigación para la creación de un "Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT en el Laboratorio de Ciberseguridad de la Universidad Politécnica Estatal del Carchi". El resultado permitirá a los Municipios que cuenten con una red establecida y Gobernación de la provincia del Carchi, tener un equipo que ayude en la prevención y mitigación de incidentes informáticos mediante un sistema web que será creado para pedir ayuda o ver recomendaciones acerca del uso de las correctas políticas o normas de seguridad.

Características de la entrevista

- Las respuestas obtenidas serán únicamente para el uso de los entrevistadores en el desarrollo de la investigación.

- La duración de la entrevista será de treinta minutos a una hora aproximadamente.

Preguntas:

1. ¿La institución cuenta con una infraestructura de red, servidores, sistemas y servicios informáticos? ¿Cuáles?
2. ¿La institución en el momento cuenta con normativas o reglamentos para asegurar la información? ¿Cuáles?
3. ¿Qué políticas o normativas internacionales utilizan en la institución para la seguridad de la información y los equipos que la procesan (Ejemplo: COBIT, ITIL, ISO/IEC serie 27000, etc.)?
4. ¿Qué medidas toman para evitar que la información y los equipos de la institución sean vulnerados?
5. En caso de presentarse un incidente informático (filtrado, alteración o pérdida de información, hackeos, denegación de servicios y caída del sitio web, introducción de código malicioso como virus, troyanos, gusanos y malware en general) ¿Qué procedimientos aplican para dar seguimiento a dichos incidentes y mitigar sus riesgos?
6. ¿Cómo llevan a cabo el proceso para la implementación o creación de políticas de seguridad, actualización de las mismas y generar recomendaciones sobre la seguridad informática?
7. ¿De qué manera se informan los miembros de la institución sobre las nuevas formas de ataques y explotación de vulnerabilidades?
8. ¿Con qué frecuencia realizan el escaneo de vulnerabilidades y de qué forma?
9. Según su criterio ¿Por qué ocurre el incumplimiento de políticas de seguridad?
10. ¿Cómo llevan el proceso de actualización del hardware y software de la institución y con qué frecuencia lo realizan? Teniendo en cuenta que la actualización incluye permisos y licencias respectivamente.

Esta entrevista ha sido de gran ayuda y hemos obtenido información muy importante para continuar con nuestro plan de investigación. Muchas gracias por su colaboración.

Figura 66. Formato entrevista para gobiernos seccionales de la provincia del Carchi

Anexo 9 Evidencia de aplicación de entrevistas a unidades educativas y gobiernos seccionales de la provincia del Carchi.

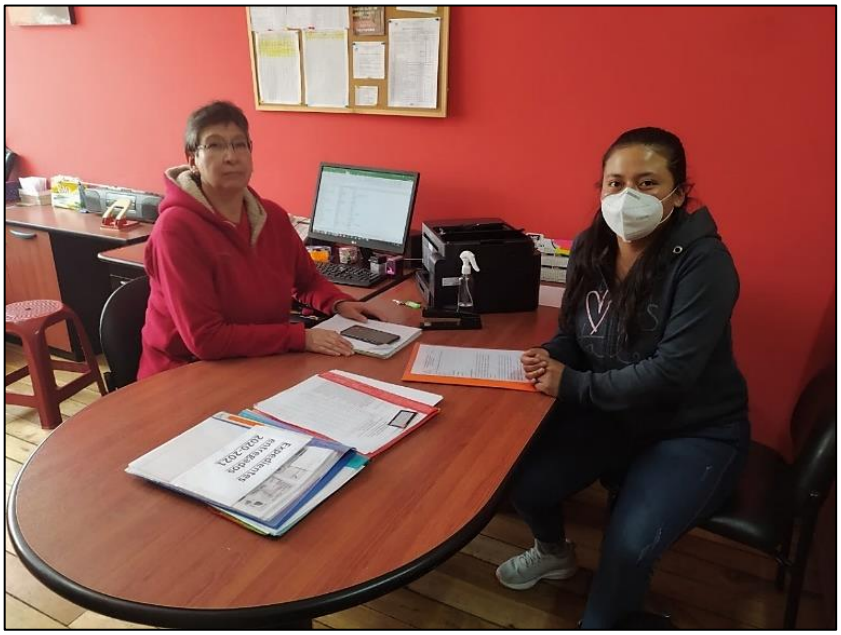


Figura 67. Entrevista a la Lic. Mariela Narváez – "Docente de la Unidad Educativa San Antonio de Padua"



Figura 68. Entrevista a la Lic. Carolina De La Vega - "Docente de la Unidad Educativa José Julián Andrade"



Figura 69. Entrevista al Ing. Diego Rosales - “Docente de la Unidad Educativa Tulcán”



Figura 70. Entrevista al Ing. Diego Erazo - “Encargado del Área de Tecnología del GAD Municipal San Pedro de Huaca”



Figura 71. Entrevista al Ing. Fred Carrera - “Encargado de la Jefatura de Sistemas del GAD Municipal de Tulcán”



Figura 72. Entrevista a la Ing. Doris Arcos - “Encargada del Área de Tecnología del Gobierno Provincial del Carchi”



Figura 73. Entrevista al Msc. Jhony Enríquez - “Director del Centro de TIC de la Universidad Politécnica Estatal del Carchi”

Anexo 10 Oficio de habilitación de correo electrónico institucional para CSIRT UPEC.



Memorando Nro. UPEC-CACO-2021-0152-M.

Tulcán, 09 de julio de 2021

PARA: Sr. Mgs. Wilson Andres Zabala Villarreal
Director de Tecnologías de Información y Comunicación

ASUNTO: Alcance Memorando Nro. UPEC-CACO-2021-0151-M.

De mi consideración:

Por medio del presente y realizando un alcance al Memorando Nro. UPEC-CACO-2021-0151-M., en función al documento suscrito por los estudiantes Sr. Anderson Chamorro y Srta. Silvia Pupiales, me permito solicitar d la manera más comedida la creación de un correo electrónico estructurado de la siguiente forma csirt.computacion@upec.edu.ec, mismo que será utilizado para el desarrollo de la propuesta del proyecto de titulación que será implementado en el Laboratorio de Ciberseguridad de la Carrera.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

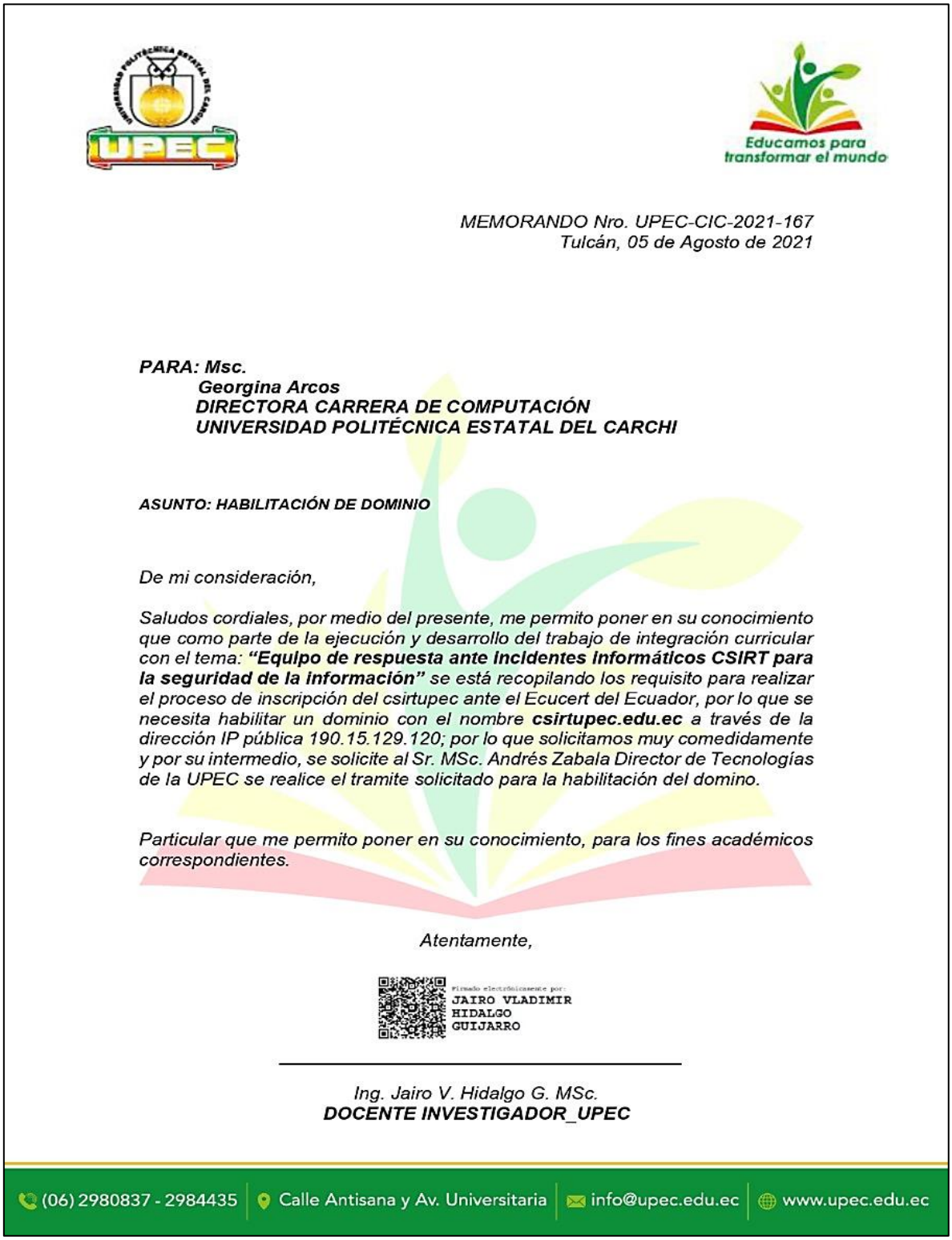
Mgs. Georgina Guadalupe Arcos Ponce
DIRECTORA DE LA CARRERA DE COMPUTACIÓN

GEORGINA GUADALUPE ARCOS PONCE

(06) 2224079 - 2224080 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 74. Oficio de habilitación de correo electrónico dirigido al Sr. Msc. Wilson Zabala - "Director de Tecnologías de Información y Comunicación".

Anexo 11 Oficio de petición de dominio csirt.upec.edu.ec.



MEMORANDO Nro. UPEC-CIC-2021-167
Tulcán, 05 de Agosto de 2021

PARA: Msc.
Georgina Arcos
DIRECTORA CARRERA DE COMPUTACIÓN
UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

ASUNTO: HABILITACIÓN DE DOMINIO

De mi consideración,

Saludos cordiales, por medio del presente, me permito poner en su conocimiento que como parte de la ejecución y desarrollo del trabajo de integración curricular con el tema: **"Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información"** se está recopilando los requisito para realizar el proceso de inscripción del csirtupec ante el Ecucert del Ecuador, por lo que se necesita habilitar un dominio con el nombre **csirtupec.edu.ec** a través de la dirección IP pública 190.15.129.120; por lo que solicitamos muy comedidamente y por su intermedio, se solicite al Sr. MSc. Andrés Zabala Director de Tecnologías de la UPEC se realice el tramite solicitado para la habilitación del domino.

Particular que me permito poner en su conocimiento, para los fines académicos correspondientes.

Atentamente,

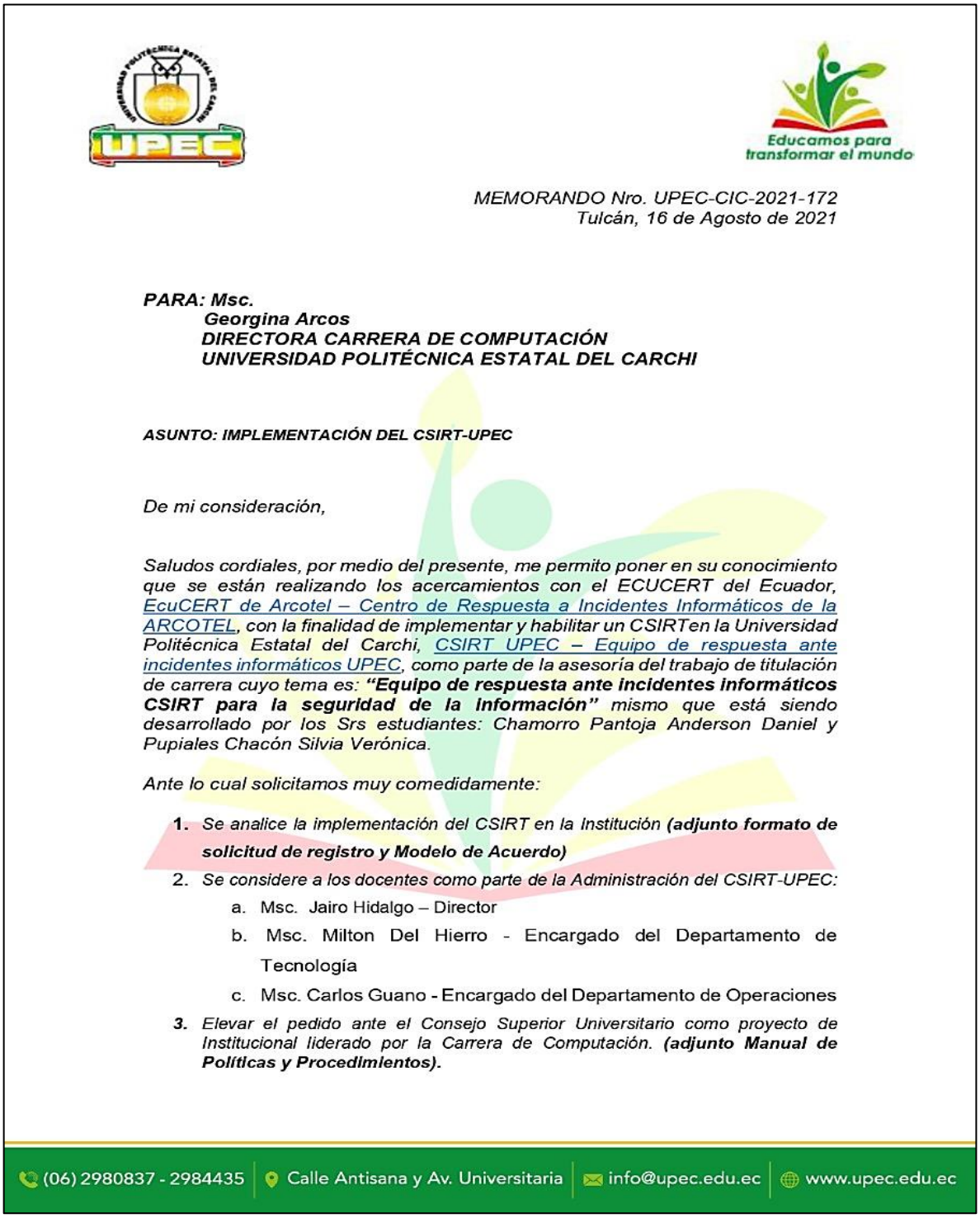
Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

Ing. Jairo V. Hidalgo G. MSc.
DOCENTE INVESTIGADOR_UPEC

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 75. Oficio de habilitación de dominio dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi"

Anexo 12 Oficio de autorización para el funcionamiento de CSIRT UPEC en el Laboratorio de Ciberseguridad de la Carrera de Computación.



Educamos para transformar el mundo

MEMORANDO Nro. UPEC-CIC-2021-172
Tulcán, 16 de Agosto de 2021

PARA: Msc.
Georgina Arcos
DIRECTORA CARRERA DE COMPUTACIÓN
UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

ASUNTO: IMPLEMENTACIÓN DEL CSIRT-UPEC

De mi consideración,

Saludos cordiales, por medio del presente, me permito poner en su conocimiento que se están realizando los acercamientos con el ECUCERT del Ecuador, EcuCERT de Arcotel – Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, con la finalidad de implementar y habilitar un CSIRTen la Universidad Politécnica Estatal del Carchi, CSIRT UPEC – Equipo de respuesta ante incidentes informáticos UPEC, como parte de la asesoría del trabajo de titulación de carrera cuyo tema es: ***"Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información"*** *mismo que está siendo desarrollado por los Srs estudiantes: Chamorro Pantoja Anderson Daniel y Pupiales Chacón Silvia Verónica.*

Ante lo cual solicitamos muy comedidamente:

1. *Se analice la implementación del CSIRT en la Institución* ***(adjunto formato de solicitud de registro y Modelo de Acuerdo)***
2. *Se considere a los docentes como parte de la Administración del CSIRT-UPEC:*
   a. Msc. Jairo Hidalgo – Director
   b. Msc. Milton Del Hierro - Encargado del Departamento de Tecnología
   c. Msc. Carlos Guano - Encargado del Departamento de Operaciones
3. *Elevar el pedido ante el Consejo Superior Universitario como proyecto de Institucional liderado por la Carrera de Computación.* ***(adjunto Manual de Políticas y Procedimientos).***

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 76. Oficio de habilitación de CSIRT UPEC dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi" (parte 1)

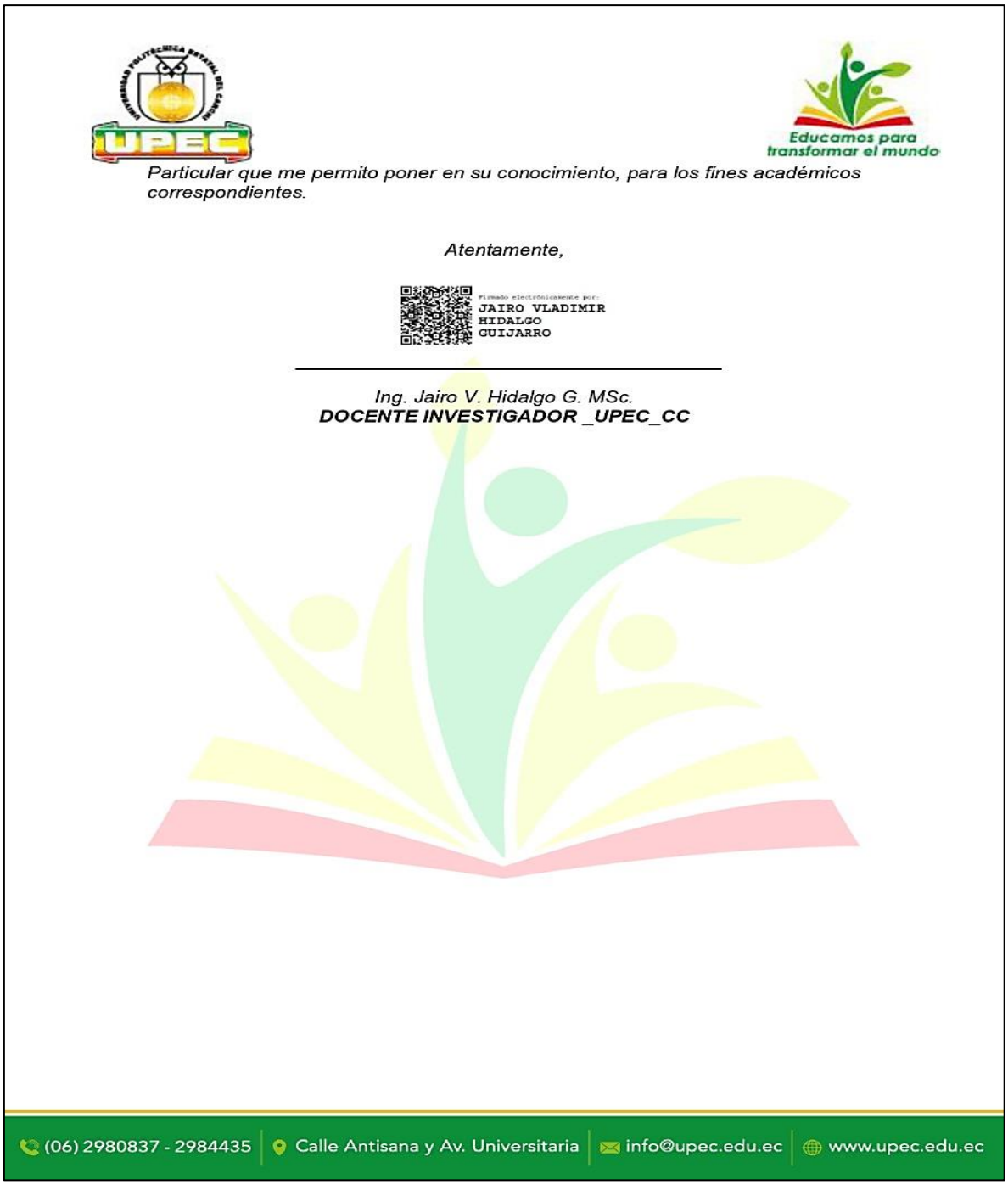
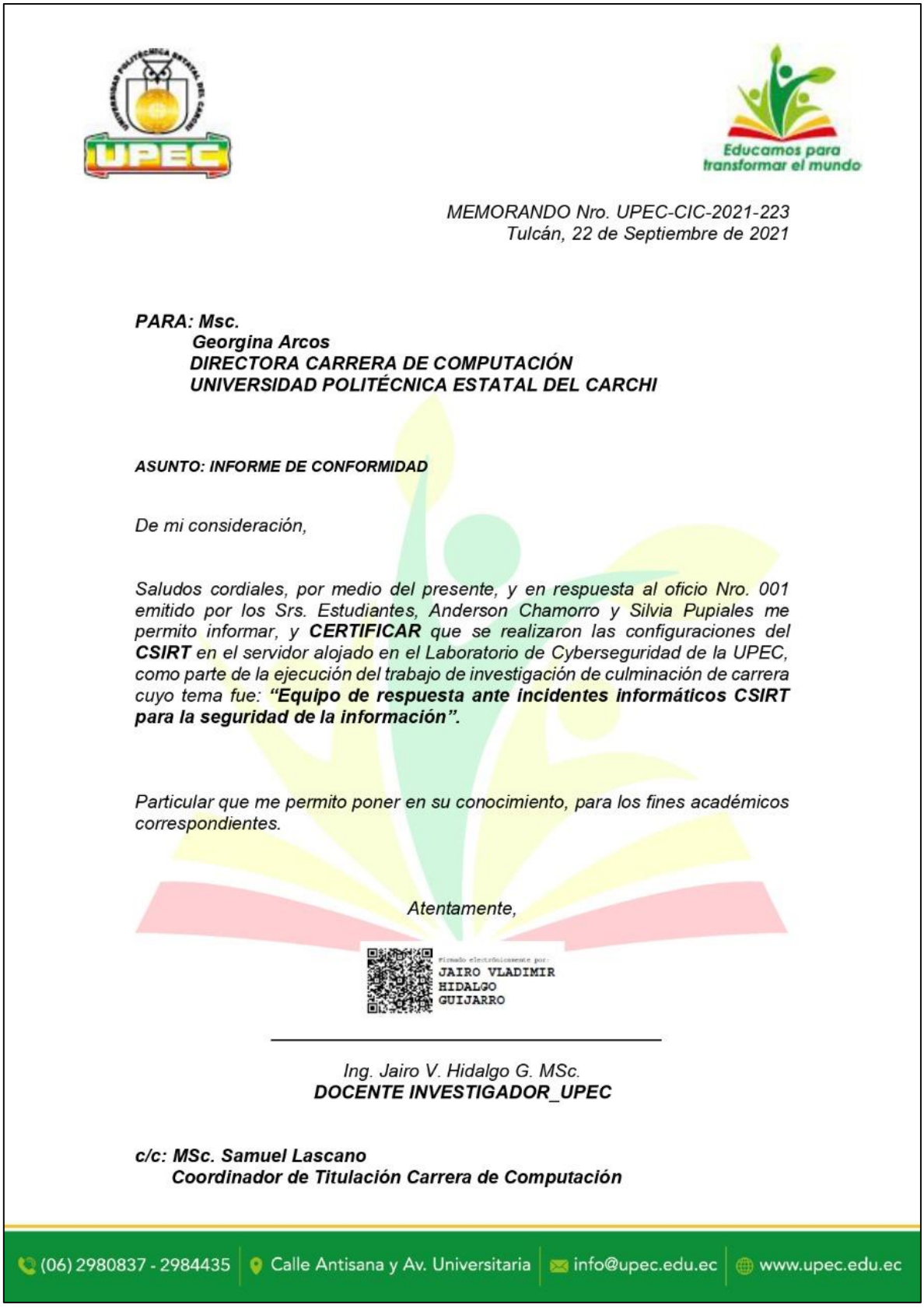


Figura 77. Oficio de habilitación de CSIRT UPEC dirigido a la Msc. Georgina Arcos - "Directora de la Carrera de Computación de la Universidad Politécnica Estatal del Carchi"(parte 2)

Anexo 13 Informe de conformidad



MEMORANDO Nro. UPEC-CIC-2021-223
Tulcán, 22 de Septiembre de 2021

PARA: Msc.
Georgina Arcos
DIRECTORA CARRERA DE COMPUTACIÓN
UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

ASUNTO: INFORME DE CONFORMIDAD

De mi consideración,

Saludos cordiales, por medio del presente, y en respuesta al oficio Nro. 001 emitido por los Srs. Estudiantes, Anderson Chamorro y Silvia Pupiales me permito informar, y **CERTIFICAR** que se realizaron las configuraciones del **CSIRT** en el servidor alojado en el Laboratorio de Cyberseguridad de la UPEC, como parte de la ejecución del trabajo de investigación de culminación de carrera cuyo tema fue: **"Equipo de respuesta ante incidentes informáticos CSIRT para la seguridad de la información".**

Particular que me permito poner en su conocimiento, para los fines académicos correspondientes.

Atentamente,

Firmado electrónicamente por:
JAIRO VLADIMIR
HIDALGO
GUIJARRO

Ing. Jairo V. Hidalgo G. MSc.
DOCENTE INVESTIGADOR_UPEC

c/c: MSc. Samuel Lascano
Coordinador de Titulación Carrera de Computación

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 78. Informe de conformidad en cumplimiento de los resultados de la propuesta CSIRT UPEC

Anexo 14 Adecuación y configuración del servidor CentOS 7 para la implementación del servidor web

- **Instalación del servidor web Apache**

  Se ingresa como usuario root y se actualiza los paquetes de apache con el comando "yum update httpd", como se observa en la figura 79 para instalar la última versión estable y compatible con el servidor. yum es un paquete que permite administrar paquetes de software para sistemas operativos Linux basados en RPM (Red Hat Package Manager).



Figura 79. Actualización de paquetes Apache

Se instala el paquete de apache con el comando "yum install httpd" y se confirma la instalación de todas sus dependencias con la letra "y" como se muestra en la figura 80. httpd es el demonio que se ejecuta al momento que se generan solicitudes al servidor web.

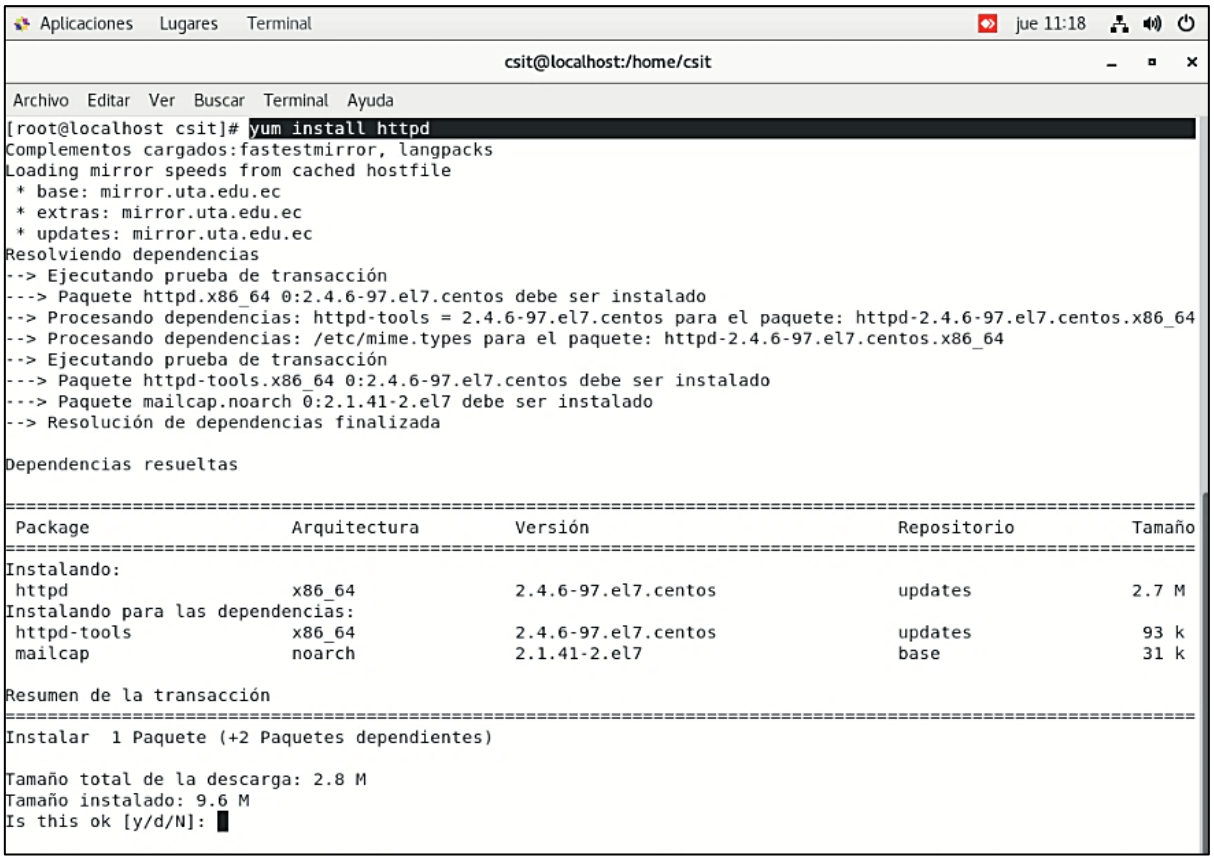


Figura 80. Instalación del servidor web Apache

En la figura 81, se muestra la finalización de la instalación de Apache, en su versión 2.4.6-97 y un listado de sus dependencias instaladas con éxito.

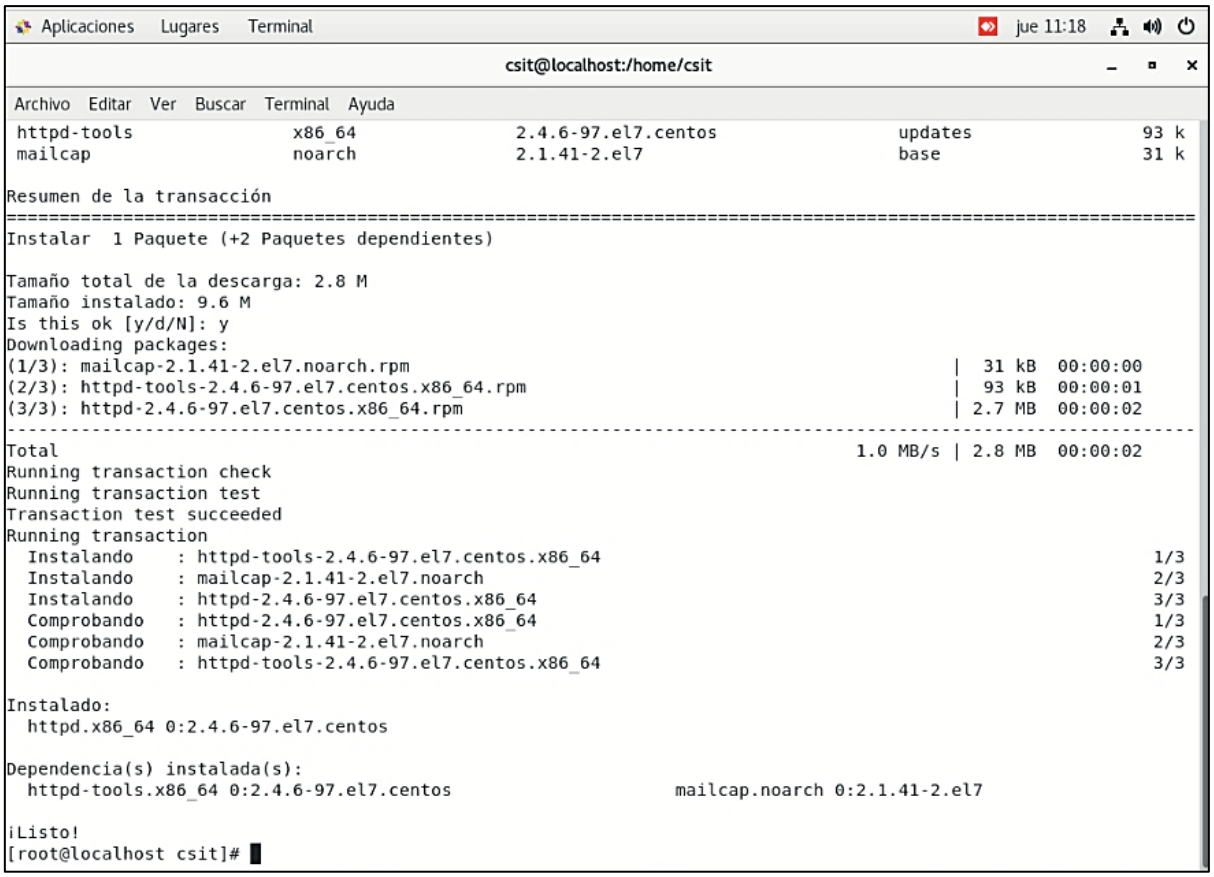


Figura 81. Detalles de la instalación del servidor web Apache

Se abren los puertos 80 y 443 en el firewall con el comando “firewall -cmd --permanent --add-service= {http, https}”, para habilitar la solicitud a través de http y https como se muestra en la figura 82, recargamos el firewall con el comando “firewall -cmd --reload” para cargar las nuevas reglas. Firewall es un controlador que implementa reglas de tráfico de red persistentes.

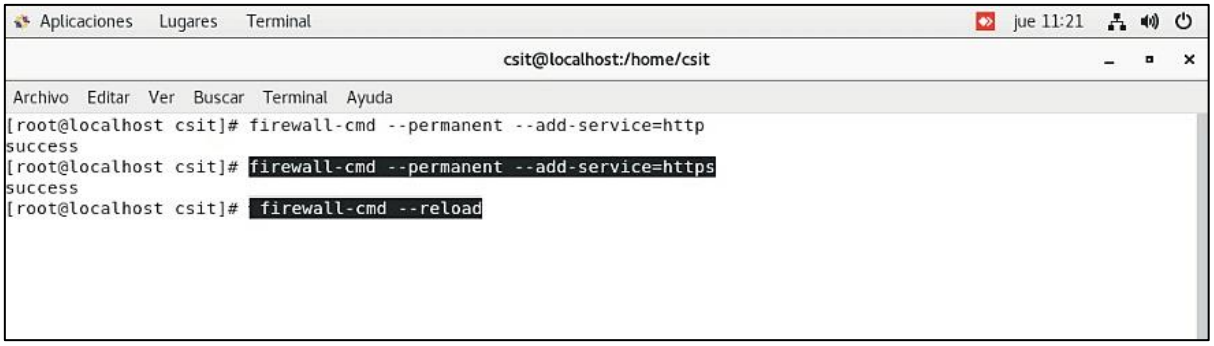


Figura 82. Habilitado de puertos 80 y 443 en el firewall del servidor

En la figura 83, se muestra el inicio de Apache con el comando “systemctl start httpd” y la verificación de éxito del servicio consultando su estado con el comando “systemctl status httpd”. systemctl permite controlar el sistema y servicios en distribuciones Linux.

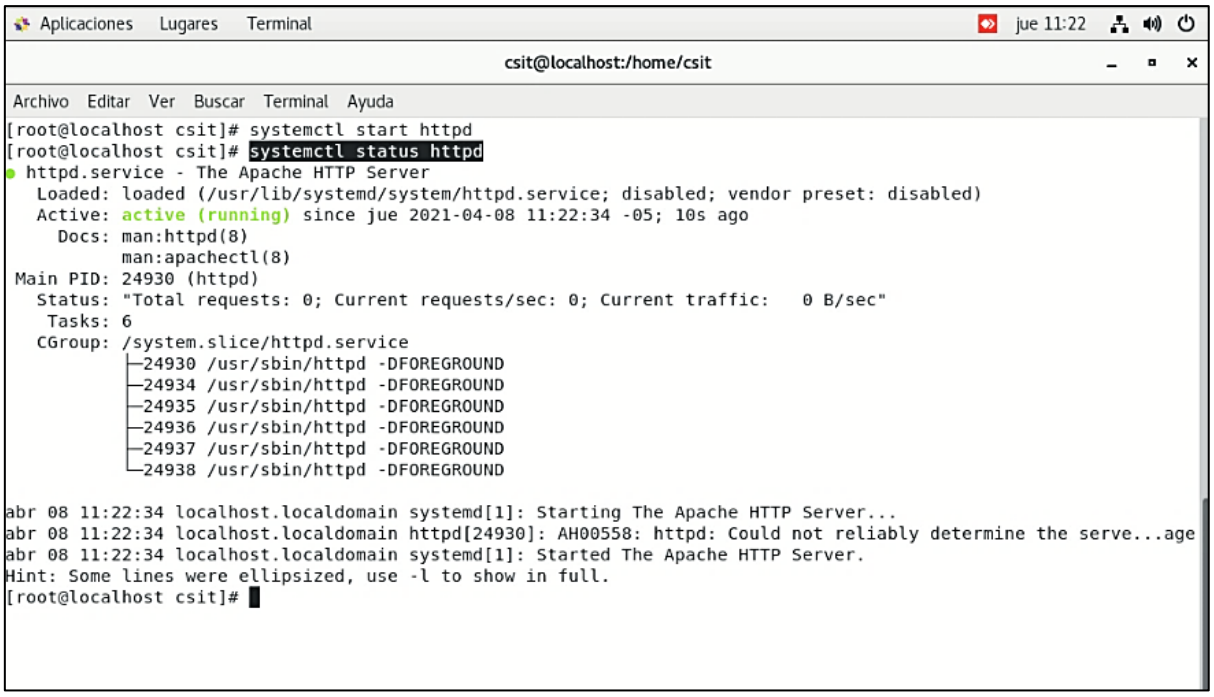


Figura 83. Arranque del servidor web Apache

Al finalizar el proceso de instalación del servidor web Apache, se verifica su funcionamiento colocando la IP pública 190.15.129.120 en el navegador, para visualizar la página predeterminada que se muestra en la figura 84. La IP pública es un número único que distingue nuestra red externamente.

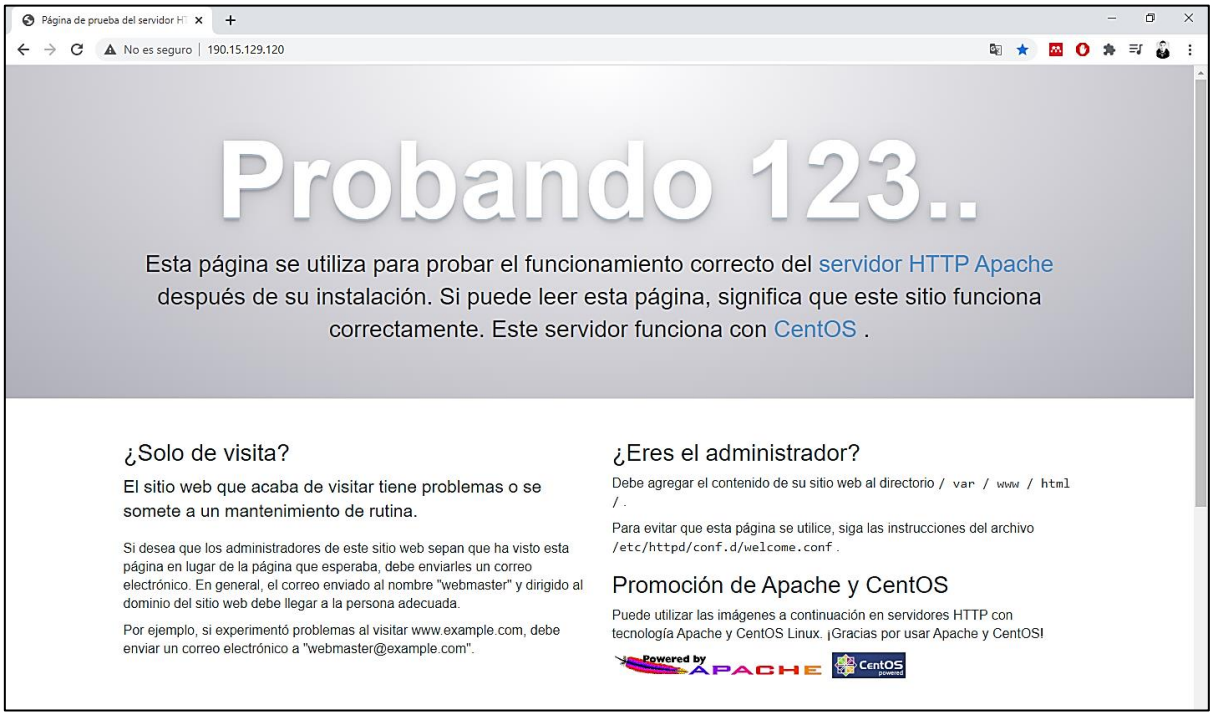


Figura 84. Verificación de la página predeterminada del servidor web Apache

Para obtener el certificado SSL de la autoridad certificadora Let’s Encrypt se utiliza el cliente Certbot (cliente que emite certificados a través de la autoridad certificadora), para ello se ingresa el comando “certbot certonly --webroot --webroot-path /var/www/html --agree-tos -m csirt.upec@gmail.com -d csirt.upec.edu.ec” como se observa en la figura 85.

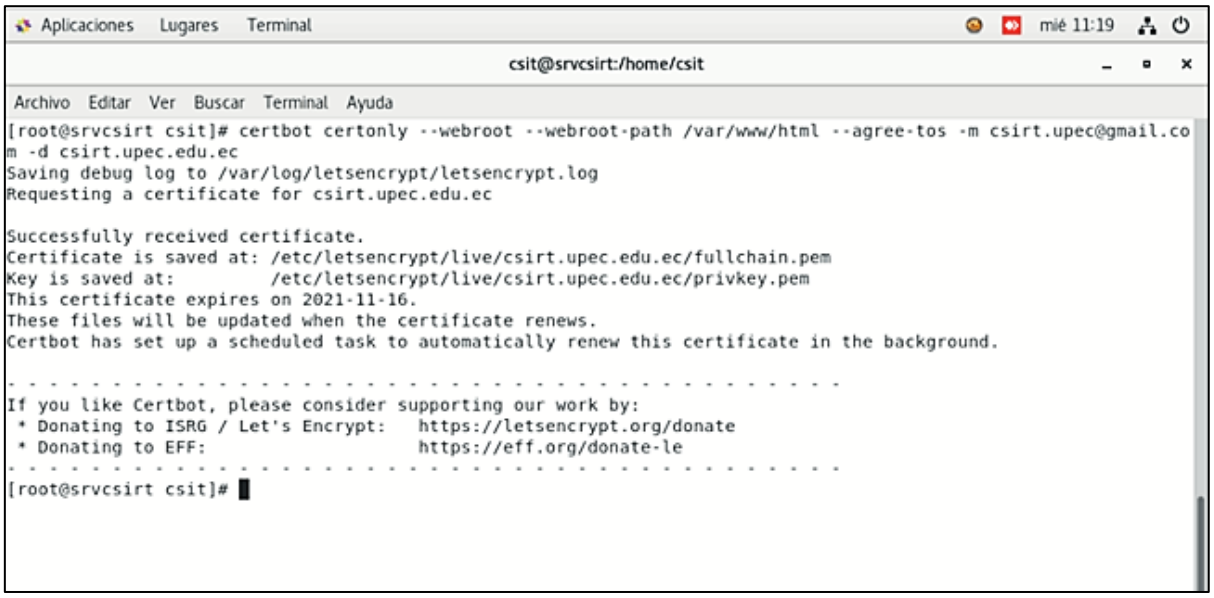


Figura 85. Obtención del certificado SSL utilizando el cliente Certbot

Para instalar los certificados generados al sitio web, se ingresa al Virtual Host correspondiente y se ingresa las rutas donde se encuentran los certificados generados por Certbot como se observa en la figura 86.

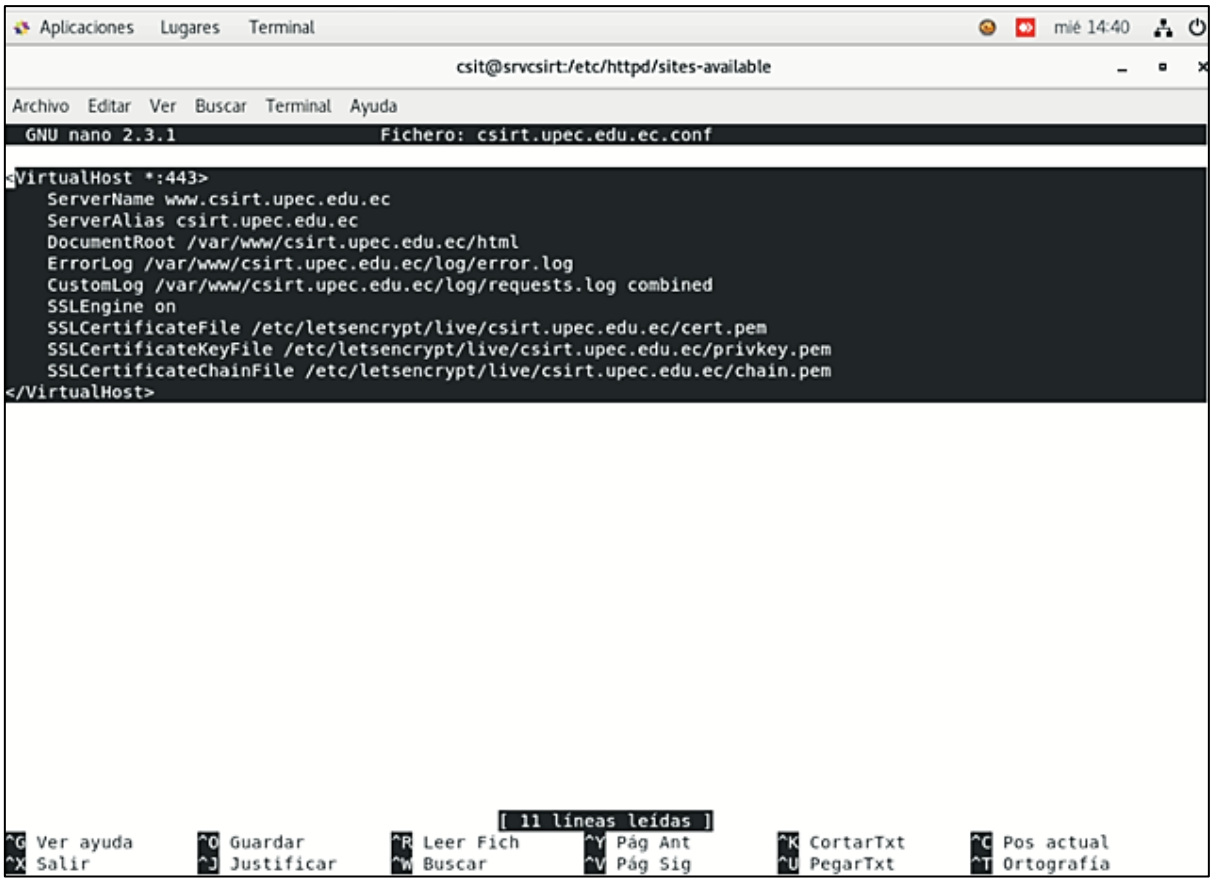


Figura 86. Instalación de certificados SSL para el sitio web

- **Instalación de MySQL Server**

  Para todo el proceso de instalación se requiere el acceso a super usuario (root), para ello ingresamos el comando “su” y su contraseña en la terminal. Se descarga el repositorio de MySQL de la página oficial en su versión más actual y estable para el servidor con el comando “wget https://dev.mysql.com/get/mysql80-community-release-el7-3.noarch.rpm”, como se visualiza en la figura 87. wget es un comando que permite descargar archivos de la web en distribuciones Linux.

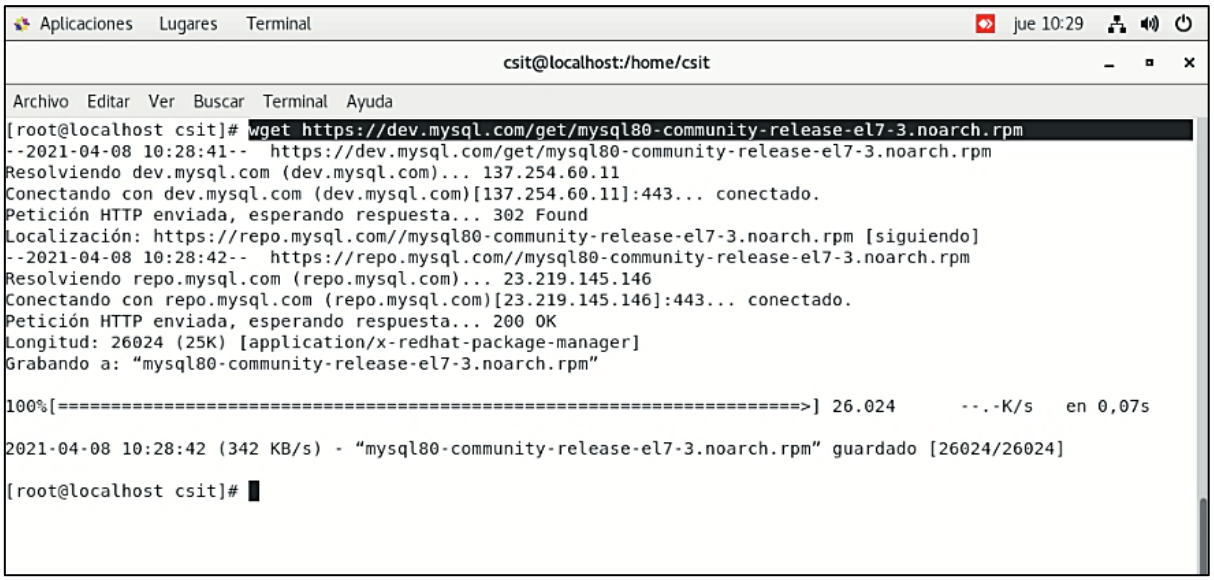


Figura 87. Descarga del repositorio MySQL al servidor

Se prepara el repositorio en el servidor con el comando "rpm -Uvh mysql80-community-release-el7-3.noarch.rpm", para la posterior instalación de MySQL, como se muestra en la figura 88.



Figura 88. Preparación del repositorio MySQL

Iniciamos la instalación del paquete MySQL con el comando "yum install mysql-server", y se confirma la instalación de todas sus dependencias con la letra "s" como se muestra en la figura 89.

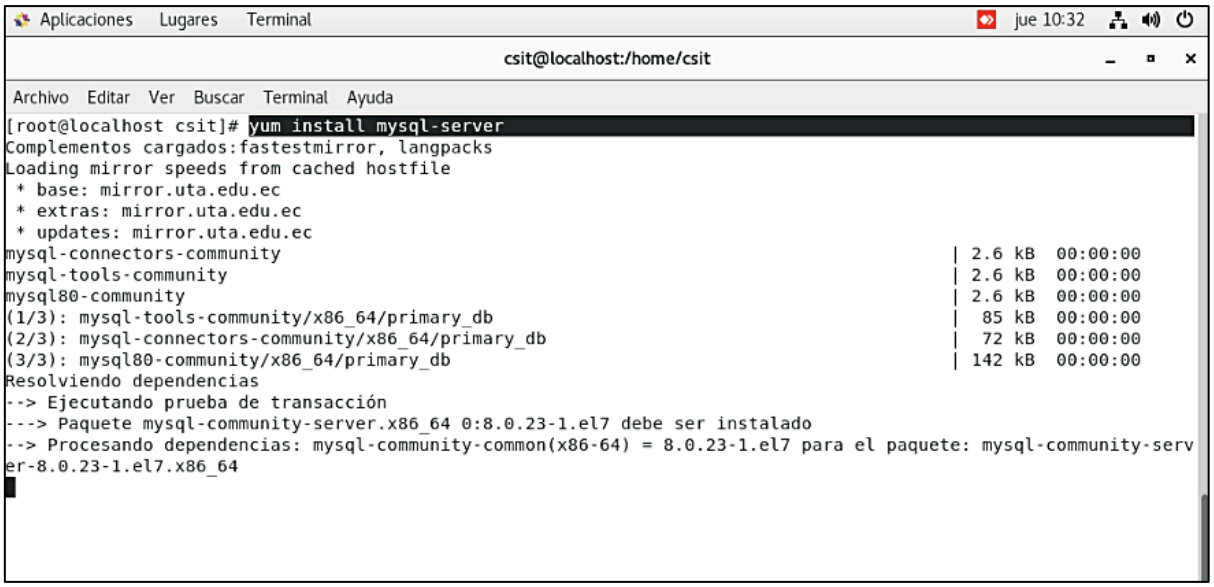


Figura 89. Instalación de MySQL Server

En la figura 90, se muestra la finalización de la instalación de MySQL en su versión 8.0.23 community y un listado de sus dependencias instaladas con éxito.

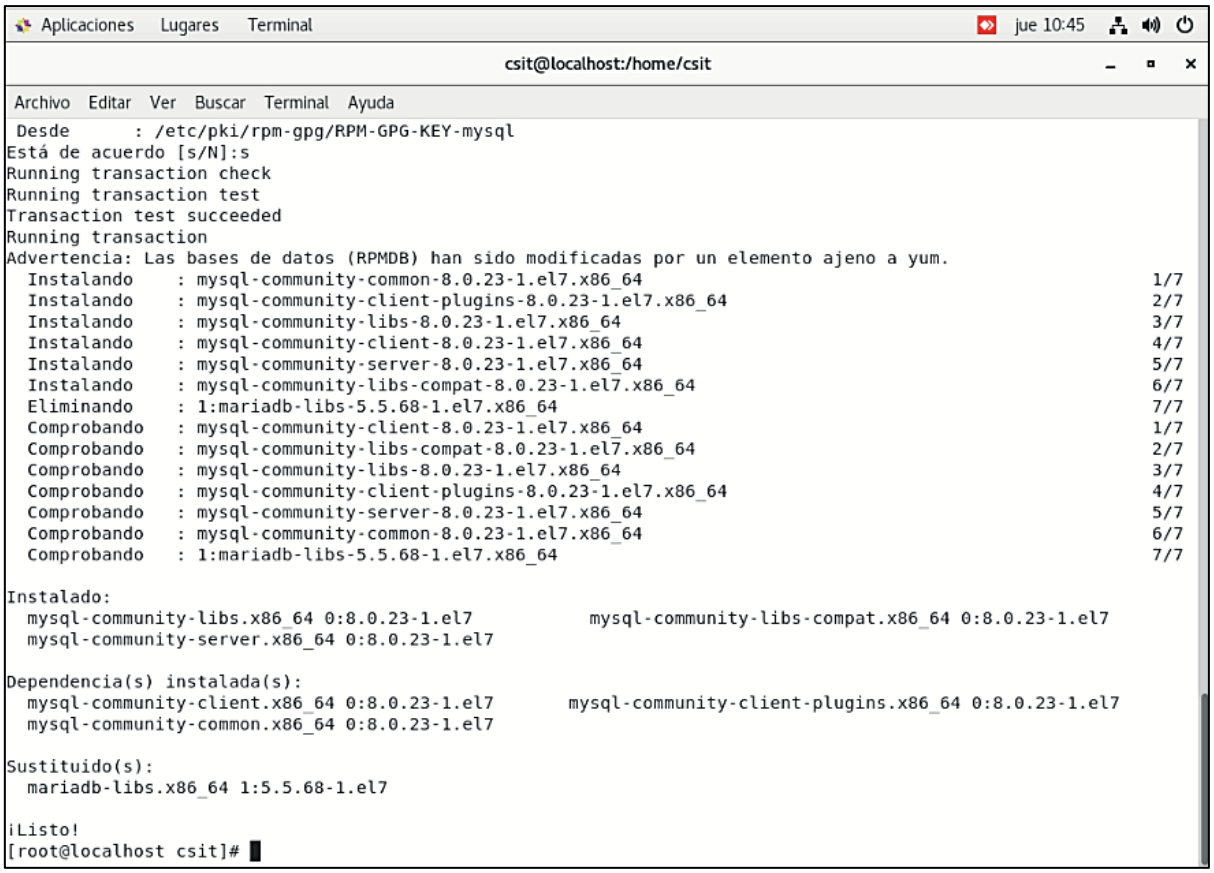


Figura 90. Detalles de la instalación de MySQL

En la figura 91, se muestra el inicio del proceso de MySQL utilizando el comando "systemctl start mysqld" y la verificación de éxito del servicio consultando su estado con el comando "systemctl status mysqld".

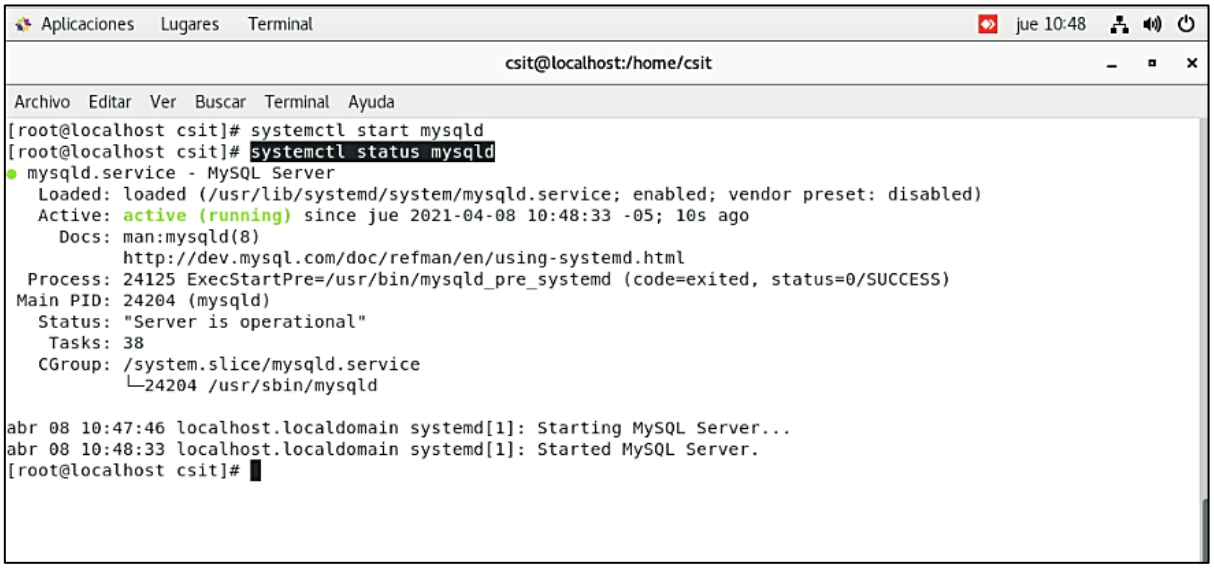


Figura 91. Inicio del servicio MySQL Server

Como se muestra en la figura 92, se consulta la contraseña root temporal de MySQL que se genera por defecto en el proceso de instalación con el comando “grep 'password' /var/log/mysqld.log”. Grep es considerada una utilidad para leer una entrada o lista para imprimirla en pantalla en sistemas operativos Linux.



Figura 92. Consulta de contraseña temporal de MySQL

Como se muestra en la figura 93, se modifica la contraseña de acceso root de MySQL ejecutando el script “mysql_secure_installation”, y se confirma los cambios con la letra “y” para darle seguridad y restringir el acceso. La contraseña debe cumplir entre ocho y doce caracteres, mismos que deben formarse por números, caracteres especiales, letras mayúsculas y minúsculas. Script es un archivo con un conjunto de órdenes que realizan una acción.

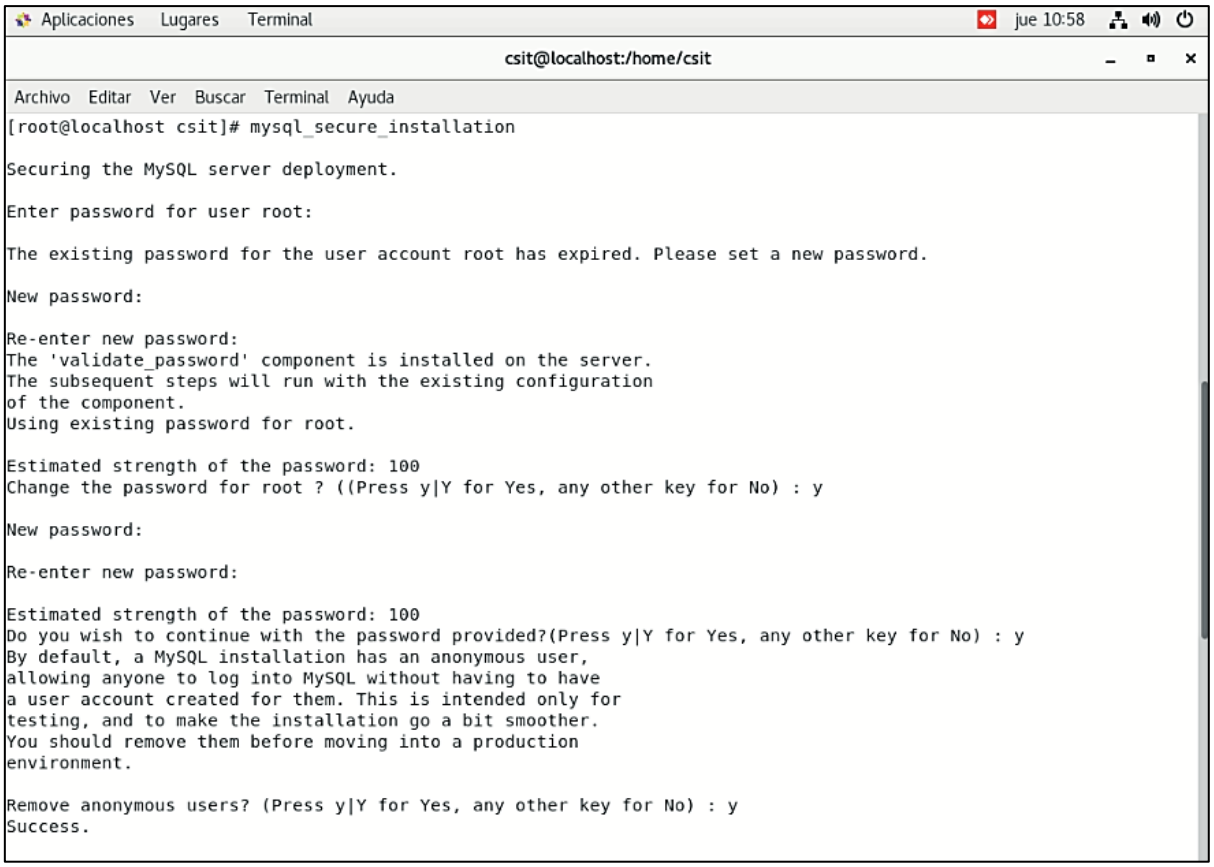


Figura 93. Modificación de contraseña de acceso root en MySQL

Para finalizar, se ingresa como super usuario con el comando “mysql -u root -p”, donde se observa la versión instalada y su área de trabajo como se observa en la figura 94.

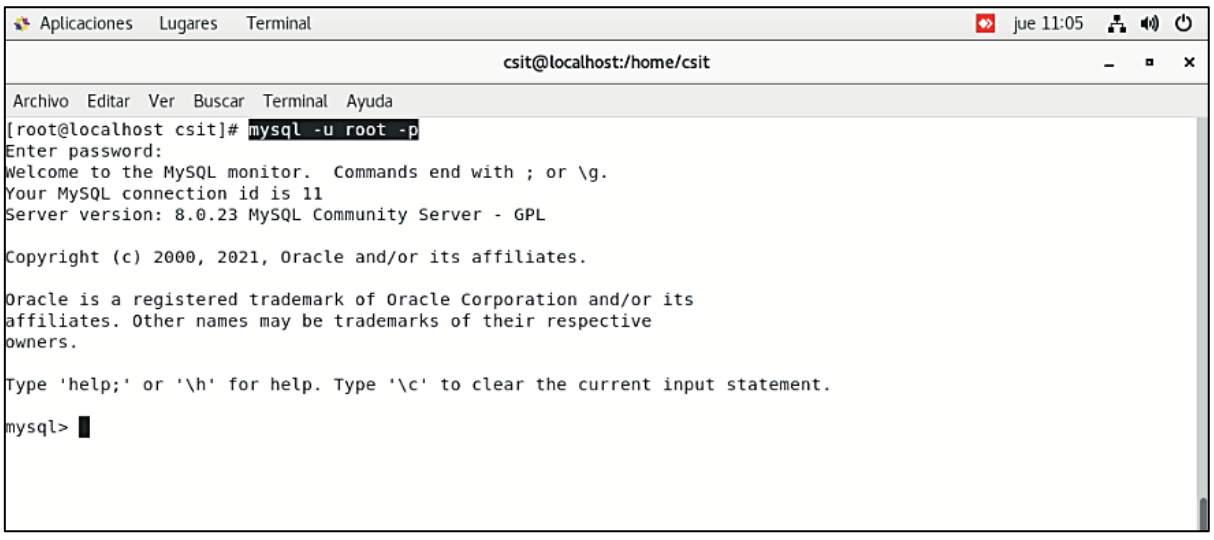


Figura 94. Acceso root a la base de datos MySQL

- **Instalación PHP**

  Para todo el proceso de instalación de PHP se requiere el acceso a super usuario (root), se ingresa el comando “su” y su contraseña. Como se observa en la figura 95, se descarga el repositorio REMI con el comando “wget http://rpms.remirepo.net/enterprise/remi - release -7.rpm” y el repositorio EPEL con el comando “wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm”, al servidor para obtener los componentes necesarios en la instalación. REMI y EPEL son repositorios que permiten instalar paquetes de fuentes externas de software.



Figura 95. Descarga de los repositorios REMI y EPEL

Se prepara los repositorios REMI y EPEL con el comando “rpm -Uvh remi-release-7.rpm epel-release-latest-7.noarch.rpm”, para la instalación de PHP en el servidor como se observa en la figura 96. RPM es una herramienta que se utiliza para la administración de paquetes en Linux.

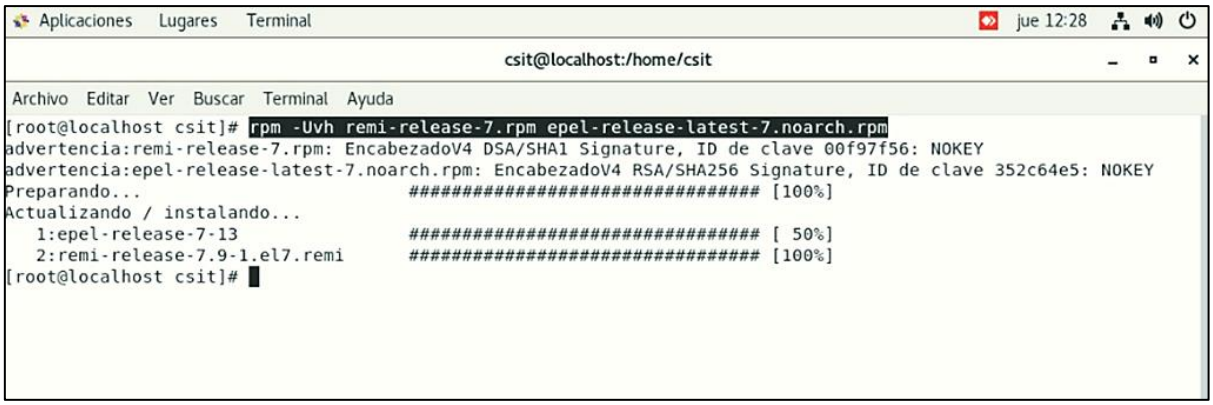


Figura 96. Preparación de los repositorios REMI y EPEL

En la figura 97, se observa el habilitado del repositorio REMI con el comando “yum-config-manager --enable remi-php74”, del cual se obtendrá la versión de PHP estable y compatible con el servidor.

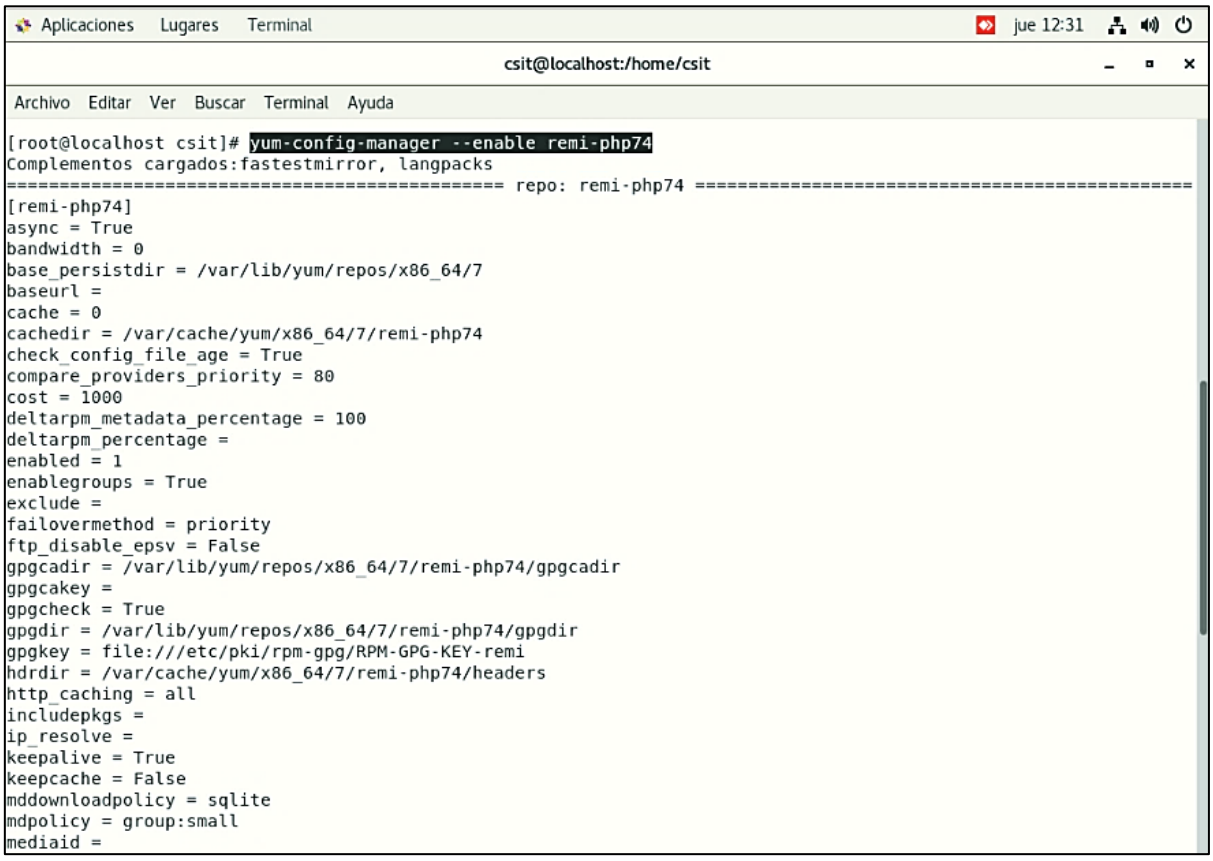


Figura 97. Habilitado del repositorio REMI

Se instala el paquete de PHP y sus dependencias con el comando “yum install php php-opcache php-gd php-curl php-mysqlnd”, como se muestra en la figura 98.

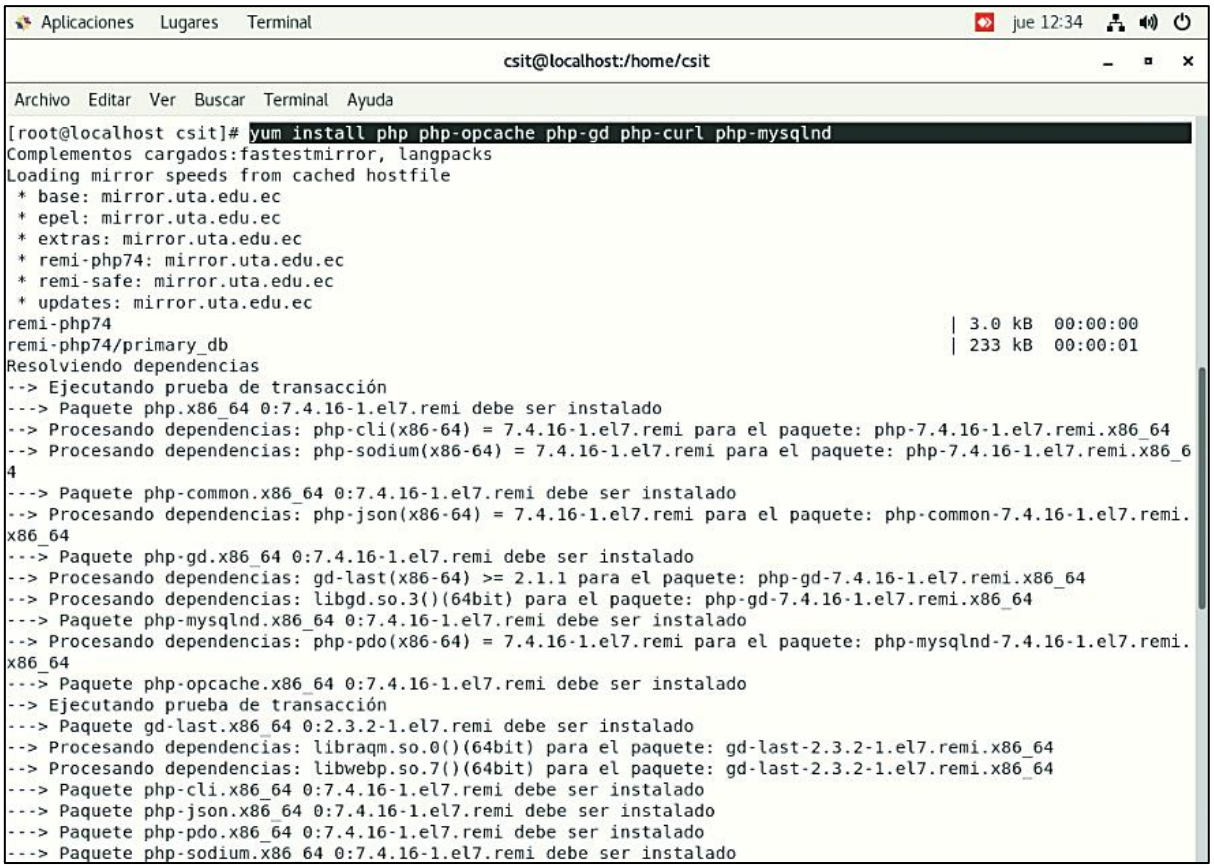


Figura 98. Instalación de PHP y sus dependencias

En la figura 99, se muestra la finalización de la instalación de PHP en versión 7.4.16 y un listado de sus dependencias instaladas con éxito.

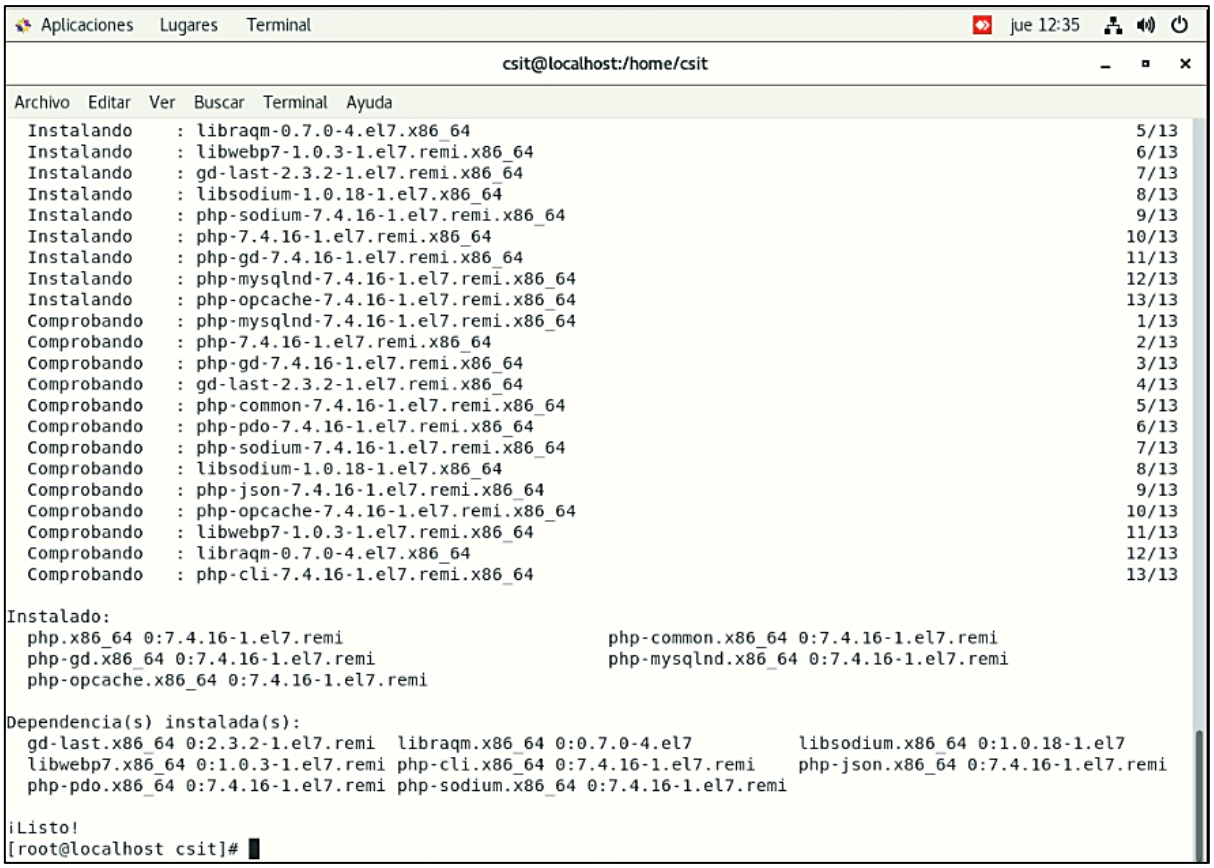


Figura 99. Detalles de instalación de PHP

Anexo 15 Instalación y configuración de WordPress

- **Configurar instalación de WordPress**

  Se ingresa al Shell de MySQL como super usuario con el comando “mysql -u root -p”, y se crea la base de datos utilizando la sentencia SQL “CREATE DATABASE nombre_base_de_datos”, como se observa en la figura 100, es un requisito para la instalación del gestor de contenido WordPress. Sentencia SQL es un lenguaje que se utiliza en el manejo de los datos en la base de datos.

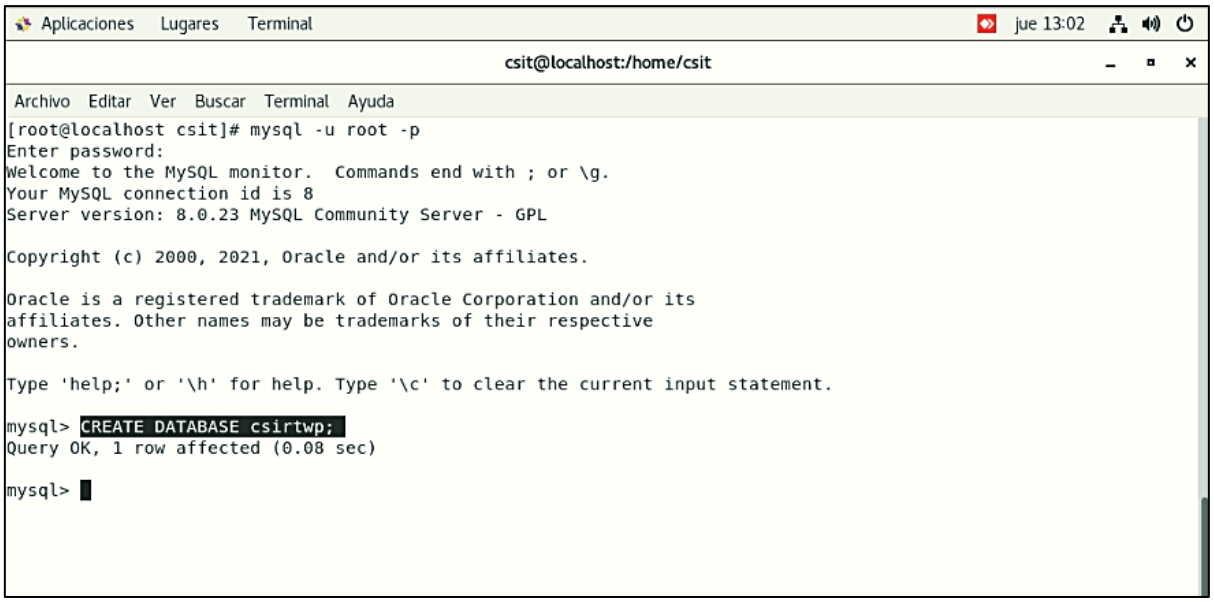


Figura 100. Creación de la base de datos en MySQL Server

Como se muestra en la figura 101, se crea un usuario y contraseña con la sentencia "CREATE USER nombre_usuario @localhost IDENTIFIED BY 'contraseña';", para la administración de la base de datos.

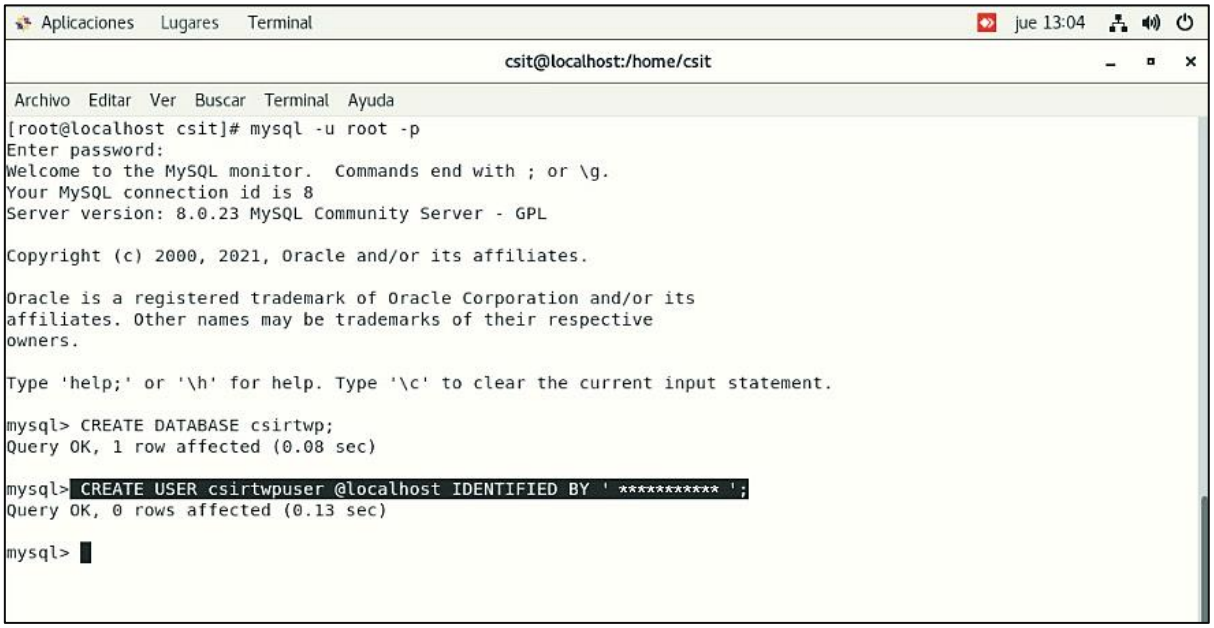


Figura 101. Creación de usuario y contraseña en la base de datos MySQL

Se asignan privilegios de acceso a la base de datos creada con la sentencia "GRANT ALL PRIVILEGES ON nombre_bdd. * TO nombre_usuario @localhost IDENTIFIED BY 'contraseña';", y se recargan los cambios para que surtan efecto con la sentencia

"FLUSH PRIVILEGES;" como se muestra en la figura 102. Grant es un comando que se utiliza para habilitar el ingreso a la base de datos.

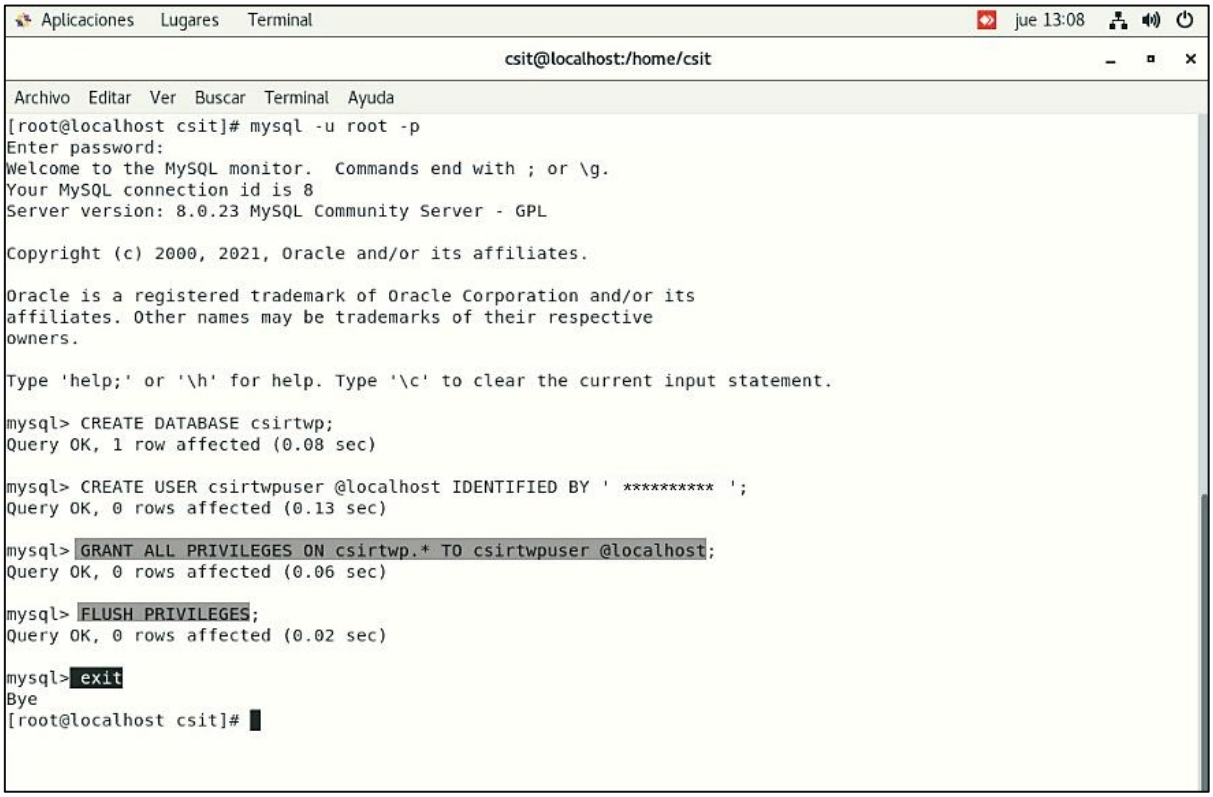


Figura 102. Asignación de privilegios de acceso a la base de datos al usuario

Se descarga el gestor de contenido WordPress en su versión 5.7.0 con el comando "wget http://wordpress.org/latest.tar.gz" como se muestra en la figura 103, última versión estable de su fuente oficial hasta el momento, obteniendo un comprimido con los archivos necesarios para la instalación.

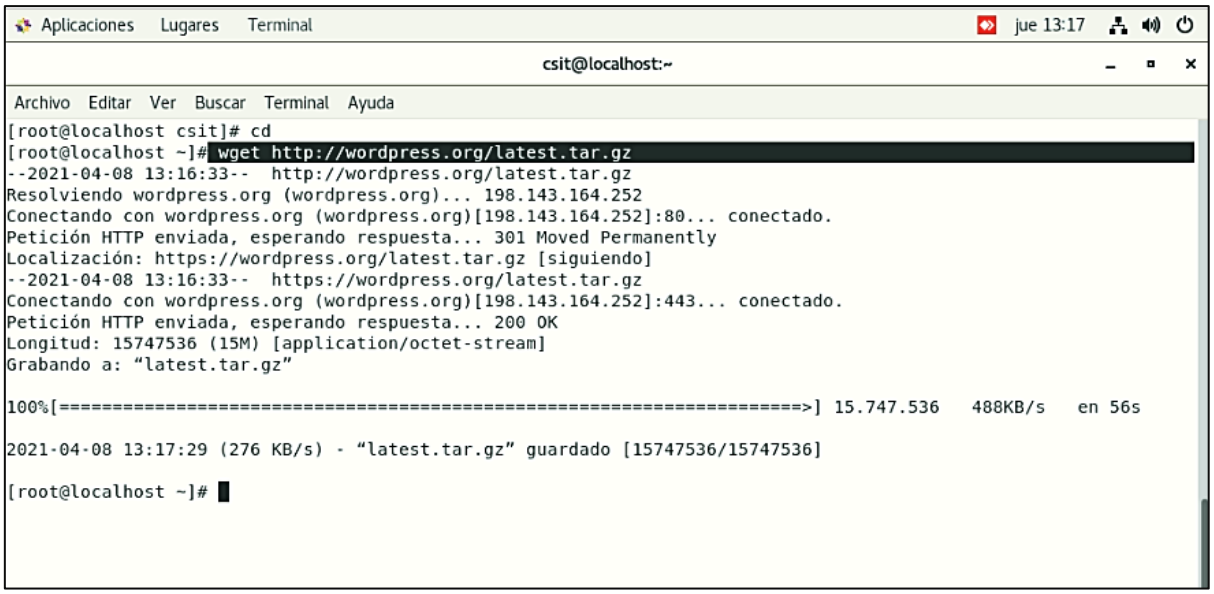


Figura 103. Descarga del gestor de contenido WordPress

Se extraen los archivos del comprimido latest.tar.gz con el comando “tar xzvf latest.tar.gz” como se muestra en la figura 104, se obtiene el directorio WordPress con los elementos de configuración, administración y estructura. Tar es un comando que permite comprimir y descomprimir archivos.

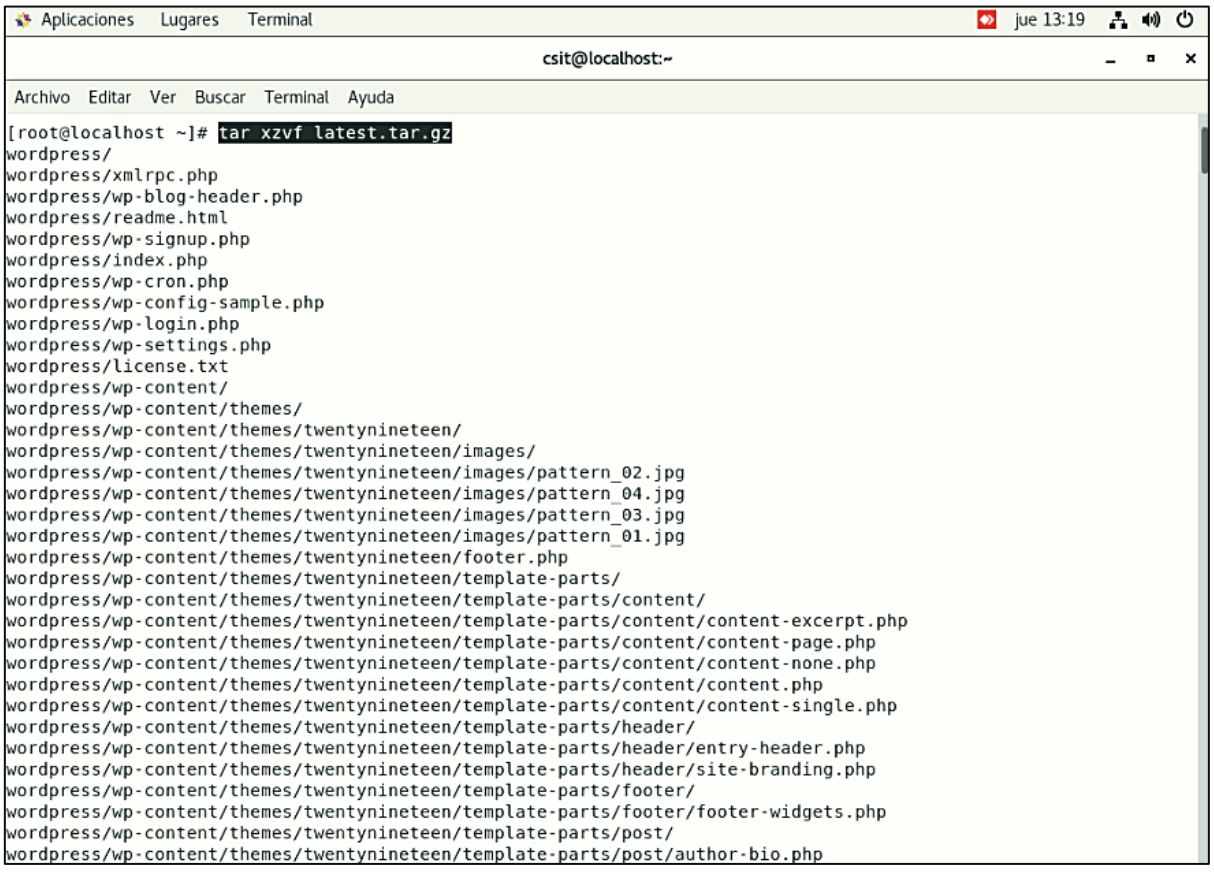


Figura 104. Extracción del directorio WordPress

Como se muestra en la figura 105, se mueve el directorio WordPress a la carpeta public_html del directorio raíz de apache con el comando “rsync -avP ~/wordpress/ /var/www/html/”, manteniendo los mismos permisos para que funcione el contenido del sitio web. Rsync es una aplicación utilizada para la transmisión eficiente de datos.

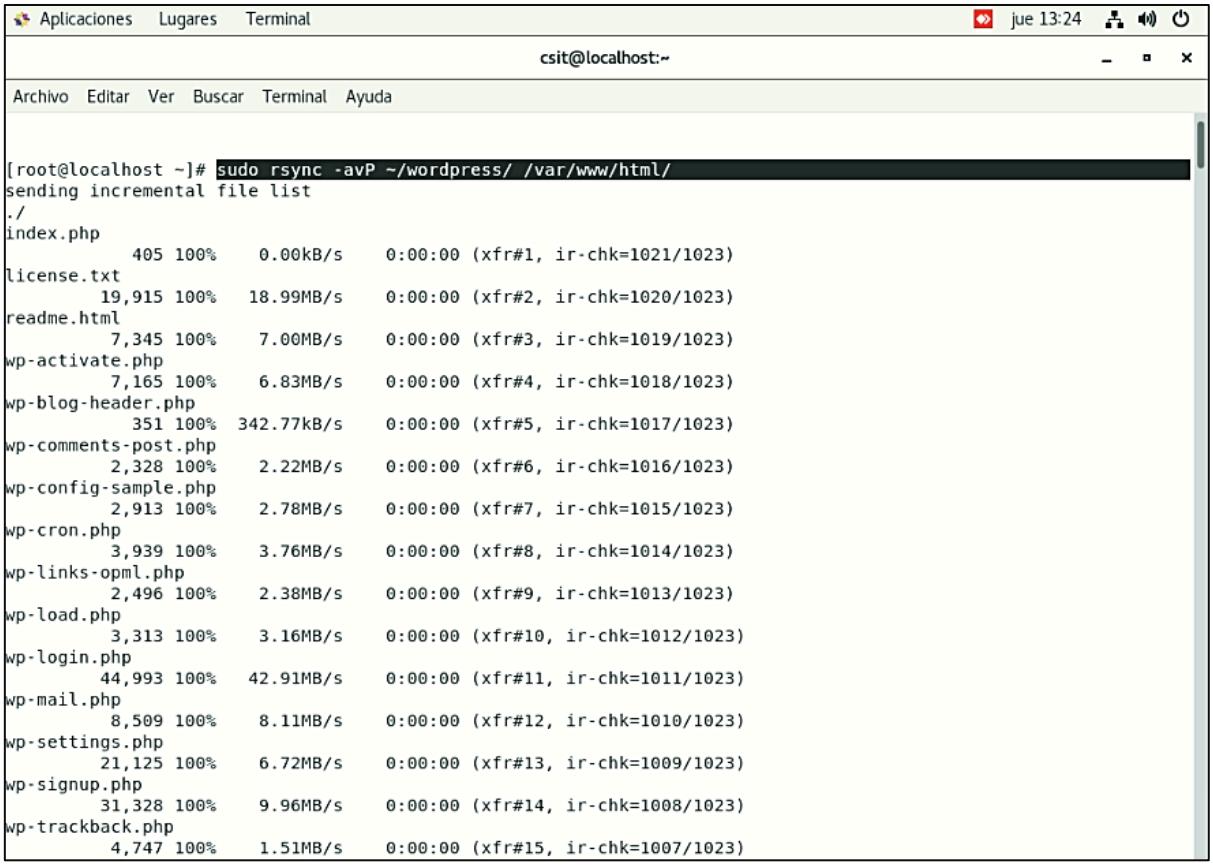


Figura 105. Reubicación del archivo WordPress

Como se muestra en la figura 106, se agrega la carpeta uploads en el directorio WordPress wp-content con el comando “mkdir /var/www/html/wp-content/uploads” para almacenar los archivos que se generan. Mkdir es un comando que permite crear carpetas o subdirectorios.



Figura 106. Agregar carpeta para archivos generados en WordPress

Con el comando “chown -R apache: apache /var/www/html/*”, se otorga permisos y propiedades adecuados a carpetas y archivos como se muestra en la figura 107, esto permite que WordPress gestione sus archivos de manera segura. Chown es un comando que cambia al propietario del directorio o archivos en distribuciones Linux.



Figura 107. Asignar propiedad y permisos al directorio WordPress

Se ingresa a la carpeta HTML con el comando “cd /var/www/html”, donde se encuentra el directorio raíz de WordPress y se copia el archivo por defecto wp-config-sample.php con el comando “cp wp-config-sample.php wp-config.php” como se muestra en la figura 108, para crear el archivo de configuración que utiliza el CMS en su funcionamiento. Cd es un comando que permite mostrar el nombre o cambiar de directorio y el comando cp se utiliza para copiar un archivo o carpeta.



Figura 108. Actualización del archivo wp-config de WordPress

Como se muestra en la figura 109, se modifica el archivo de configuración con el comando “nano wp-config.php”, y se coloca las credenciales (nombre BDD, usuario y contraseña) de la base de datos para su conexión. Nano es un editor de texto para sistemas Unix.

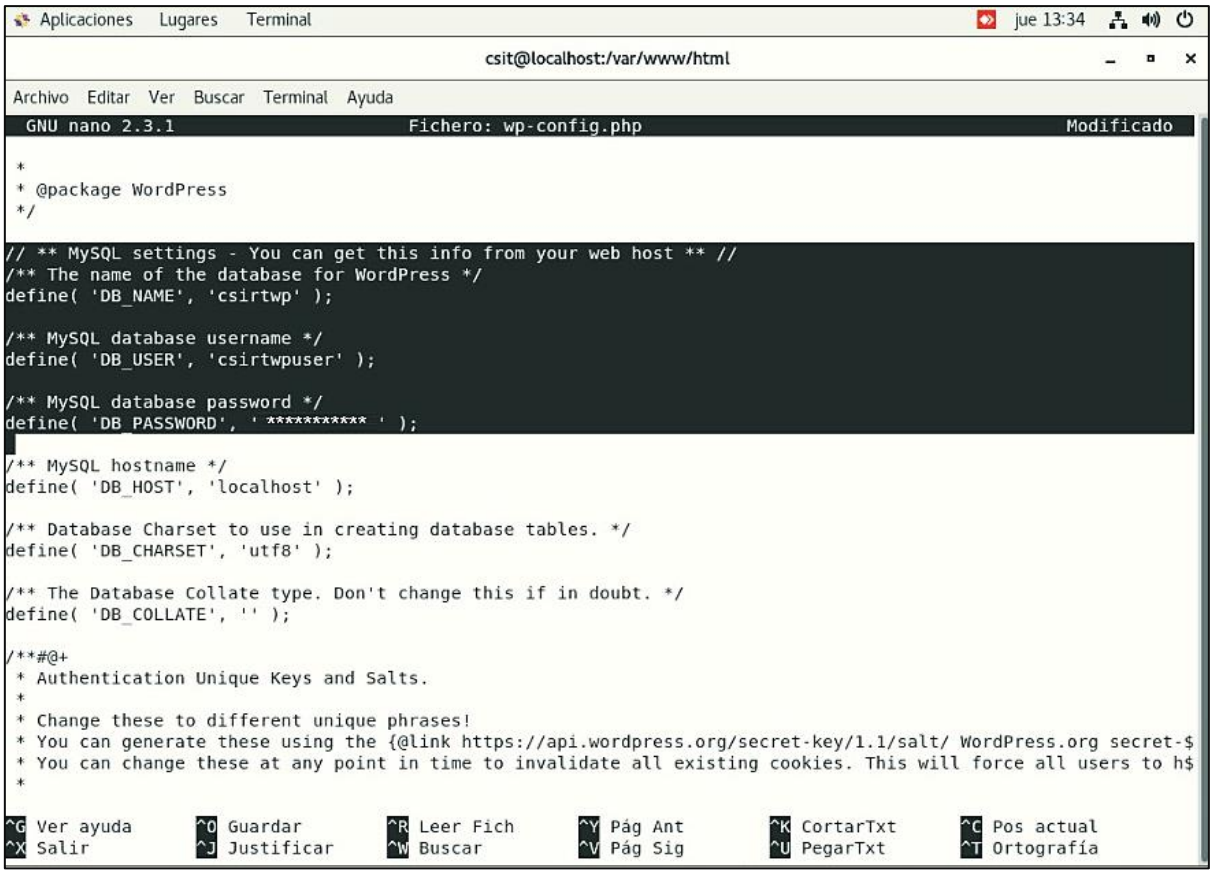


Figura 109. Conexión con la base de datos en el archivo de configuración WordPress

- **Instalación de WordPress**

  Como se muestra en la figura 110, se completa la instalación mediante su interfaz web, para ello se ingresa la dirección IP pública o el nombre de dominio en el navegador.

  Se escoge el idioma con el que se desea instalar WordPress y se da clic en continuar.

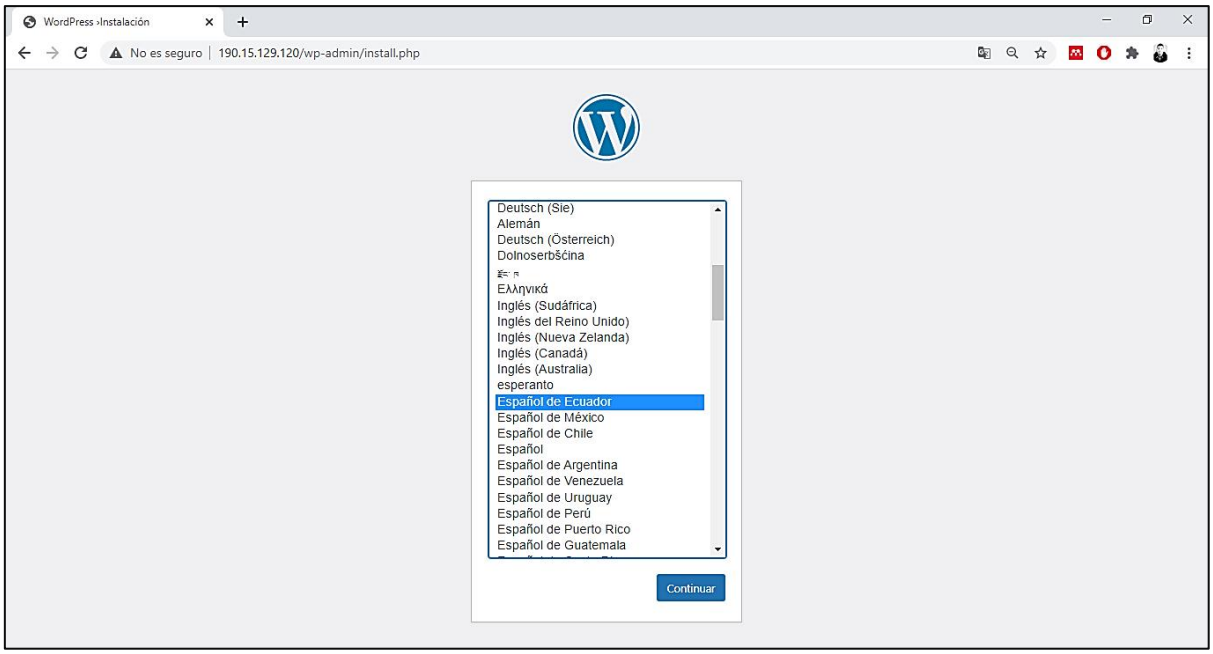


Figura 110. Configuración de idioma para la instalación de WordPress

Para finalizar el proceso de instalación se coloca el título del sitio web y se crea una cuenta de usuario para su administración, para ello se coloca el usuario, una contraseña segura, correo electrónico y se da clic en instalar WordPress como se muestra en la figura 111.

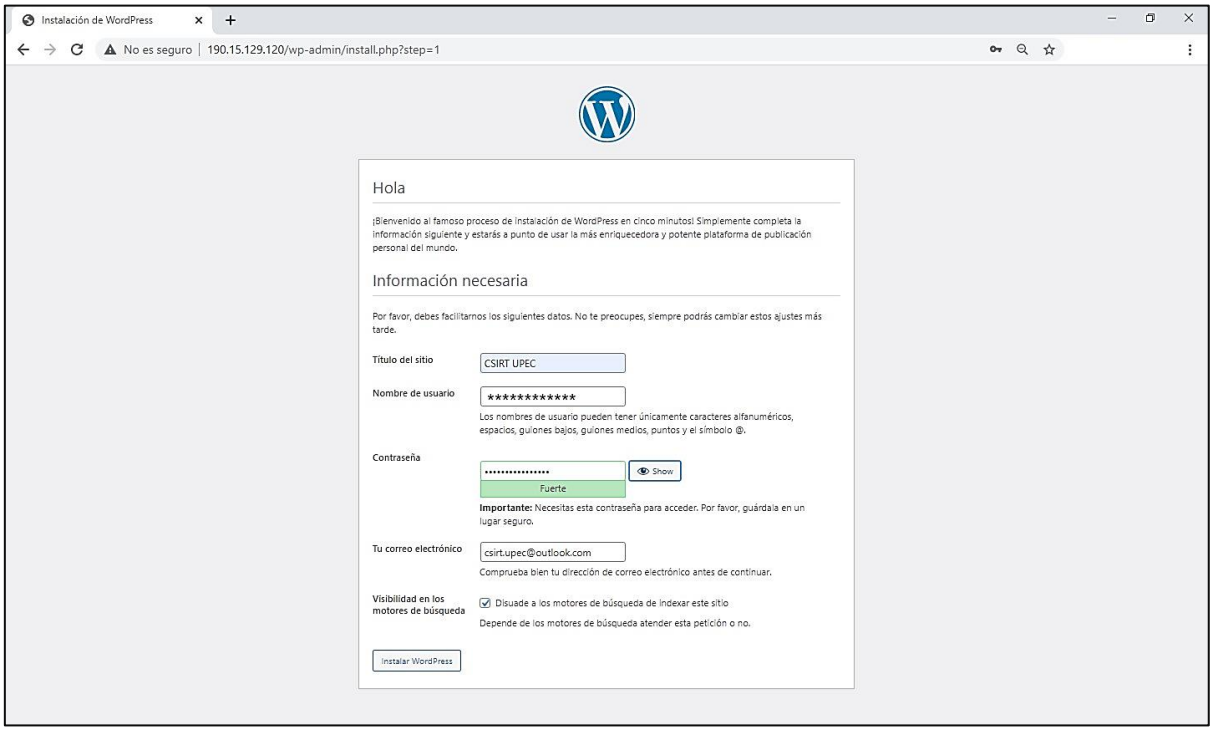


Figura 111. Instalación de WordPress en su interfaz web

Al finalizar la instalación con éxito, se muestra un mensaje con el usuario y contraseña para la administración del sitio como se muestra en la figura 112.

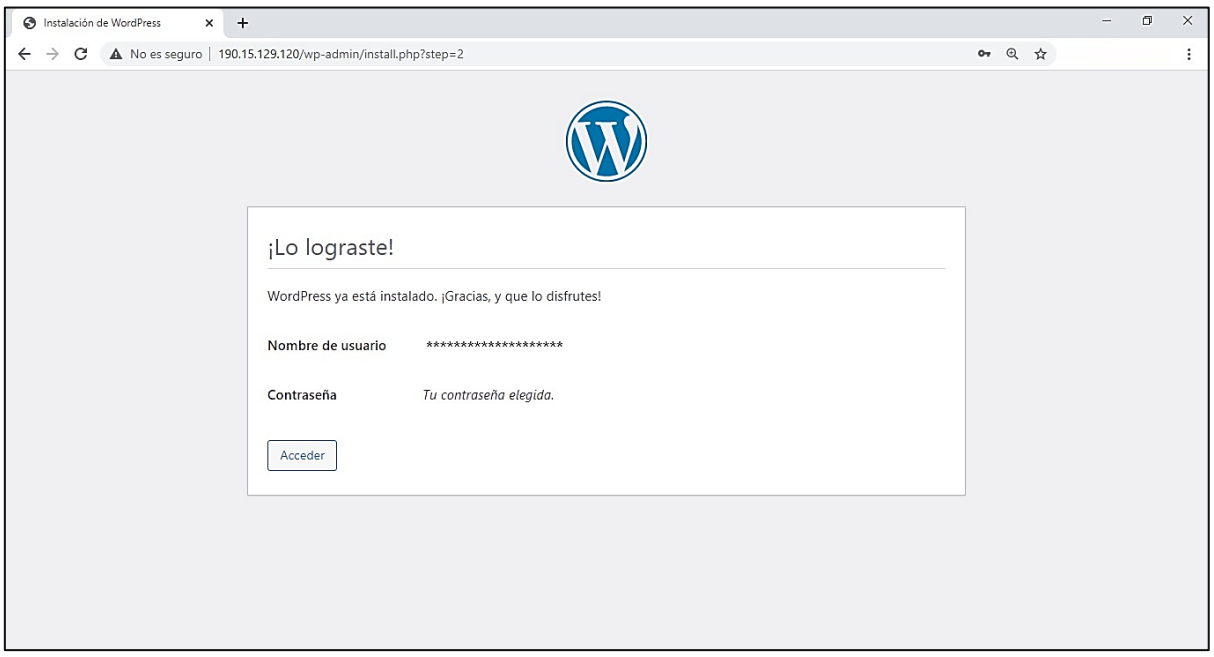


Figura 112. Fin del proceso de instalación WordPress

Como se muestra en la figura 113, para acceder al área principal de trabajo WordPress, se coloca el usuario, contraseña de administrador y se da clic en acceder.

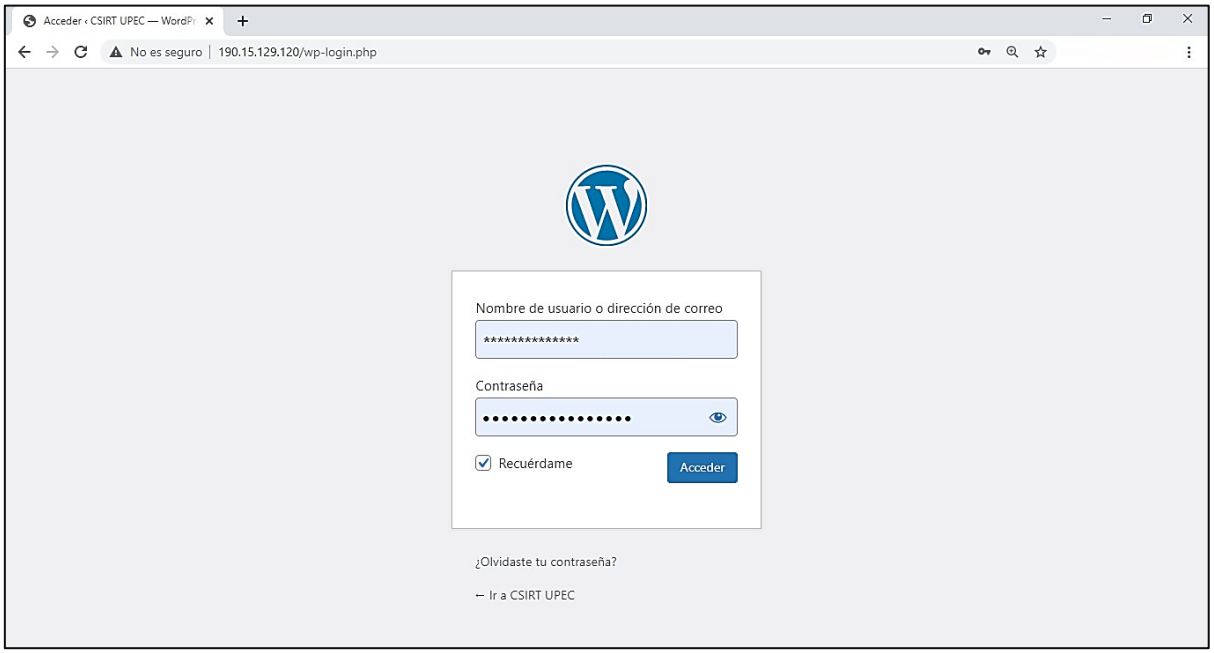


Figura 113. Formulario de inicio de sesión WordPress

Al ingresar como administrador se muestra el menú de navegación en la parte izquierda, la barra de herramientas en la parte superior y el área de trabajo principal como se muestra en la figura 114.

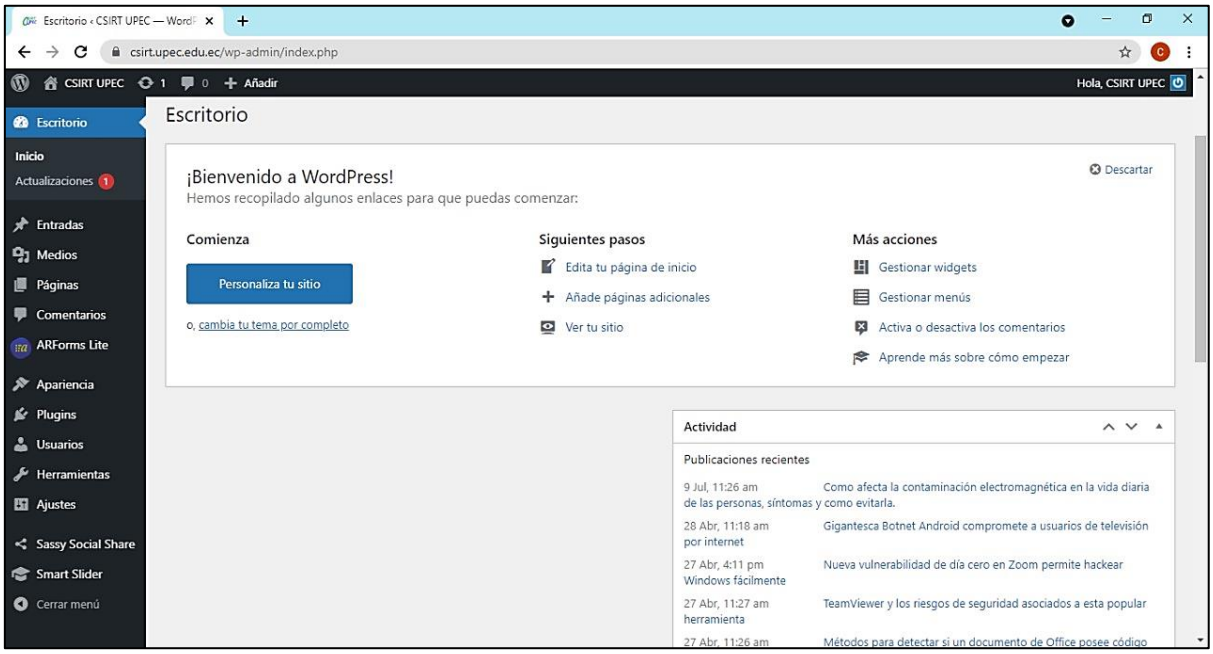


Figura 114. Área de trabajo de WordPress

- **Configuración WordPress**

  Como se muestra en la figura 115, para configurar el gestor de contenido WordPress, se ubica el menú de navegación y clic en ajustes, se elige la opción generales, donde se establece el título del sitio “CSIRT UPEC”, la descripción “Equipo de respuesta ante incidentes informáticos UPEC” que explica la temática que trata, dirección URL de WordPress “https://csirt.upec.edu.ec/” y del sitio “https://csirt.upec.edu.ec/”, dirección de correo electrónico de administración “csirt.upec@outlook.com”, idioma “español de Ecuador”, zona horaria “Bogotá”, el formato de fecha DD/MM/AA y con inicio de semana en lunes, para establecer los cambios se da clic en guardar.

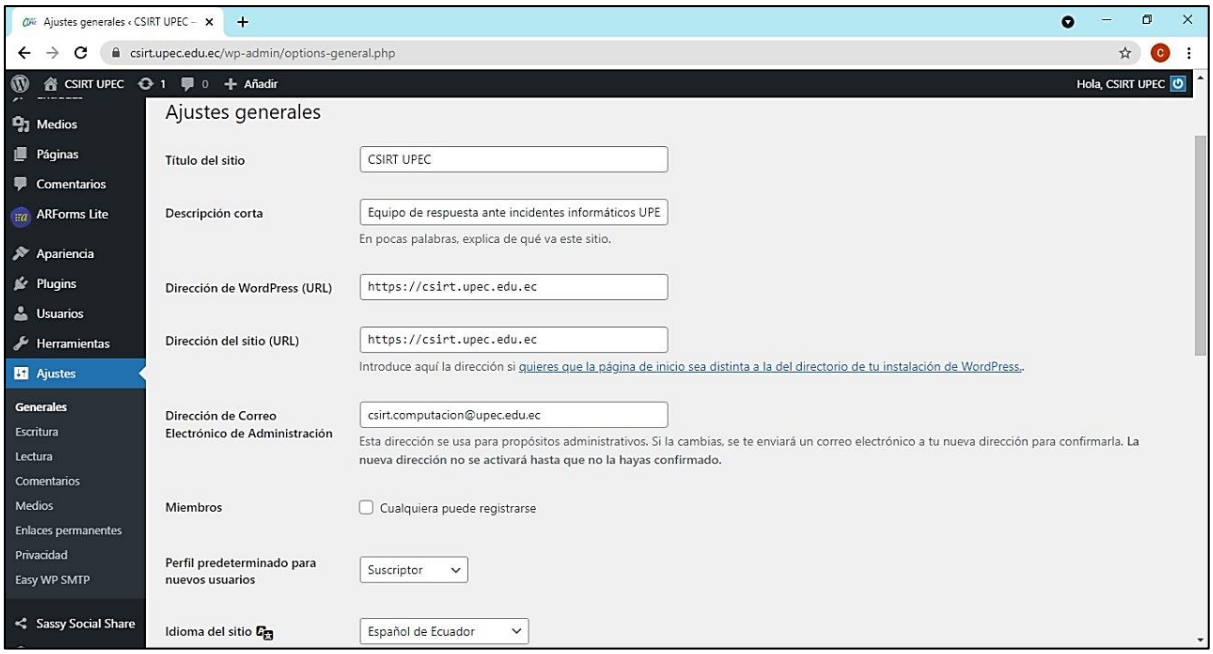


Figura 115 Ajustes generales para el gestor de contenido WordPress

En la opción de escritura se elige la opción sin categoría como predeterminada para las entradas y el formato de entrada por defecto estándar como se muestra en la figura 116.

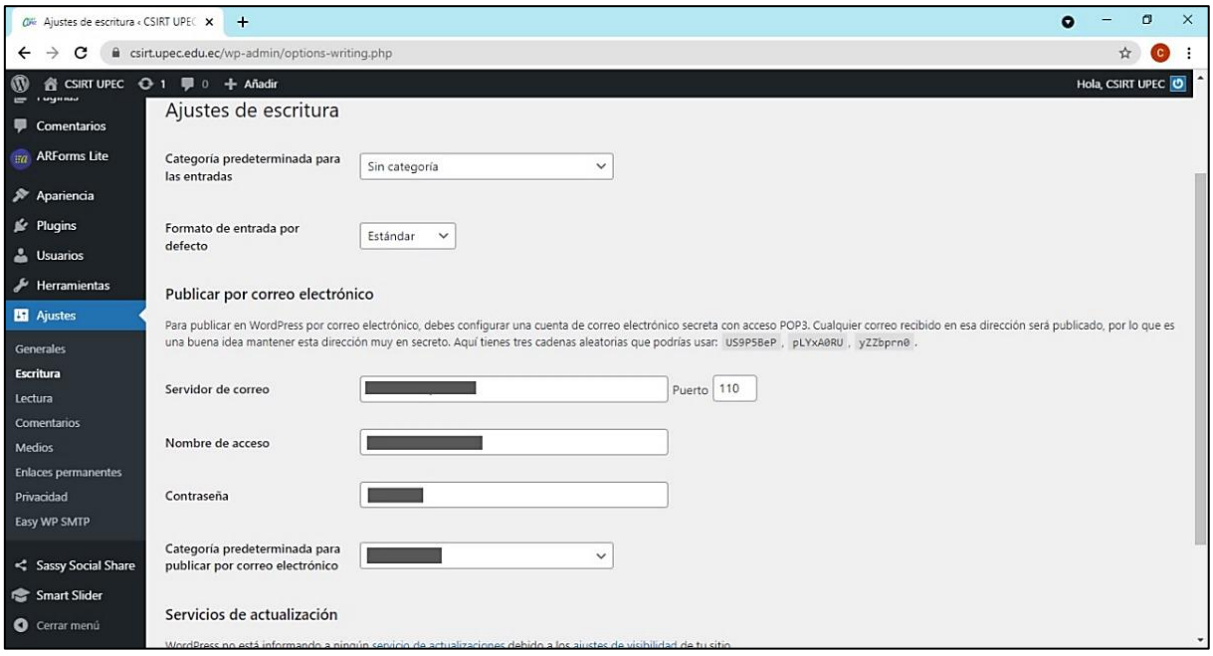


Figura 116. Ajustes de escritura para el gestor de contenido WordPress

En la opción ajustes de lectura se establece una página estática como portada del sitio con un máximo de 10 entradas, además, se activa la casilla para indexar el sitio como se muestra en la figura 117.

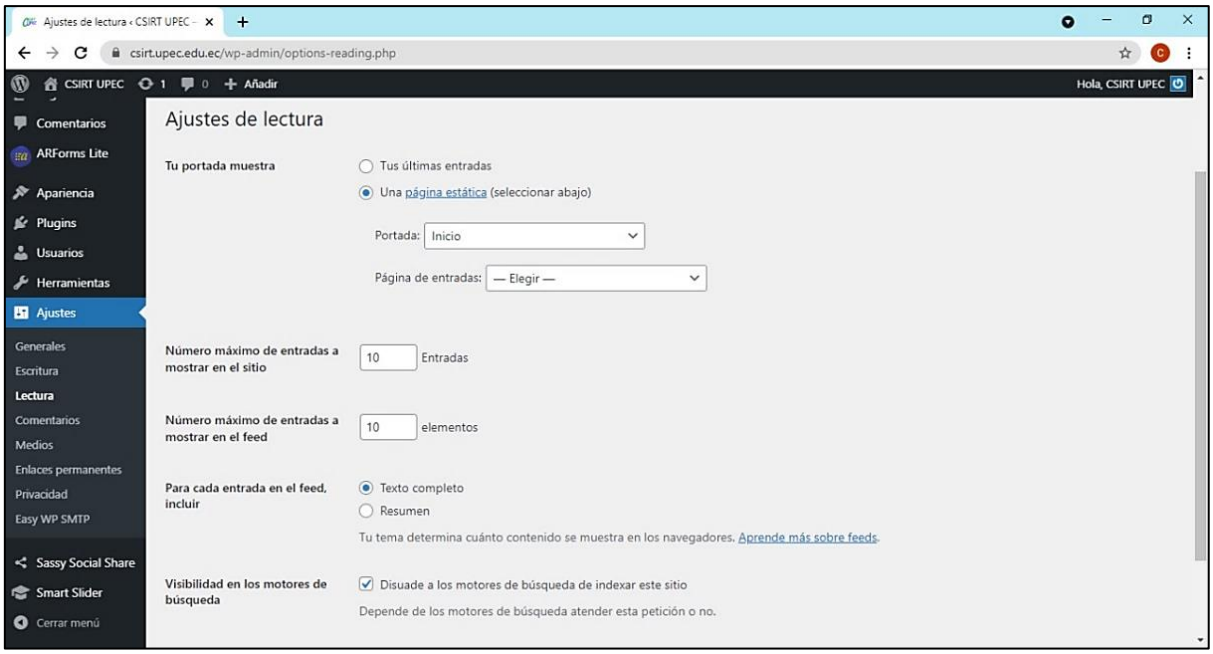


Figura 117. Ajuste de lectura para el gestor de contenido WordPress

En la opción ajuste de comentarios activamos las casillas de permitir avisos de enlaces de otros blogs y envió de cometarios a las nuevas entradas para los ajustes por defecto de las entradas, en otros ajustes se activa la casilla para ingreso de nombre y correo del autor del comentario, mostrar casilla de verificación para establecer las cookies del autor, y permitir cinco niveles de comentarios anidados, recibir notificación por correo cuando alguien comente o exista un comentario para ser moderado, aprobar los comentarios de forma manual y activar casilla para mostrar la visibilidad del avatar con su logotipo gravatar al comentar como se observa en la figura 118.

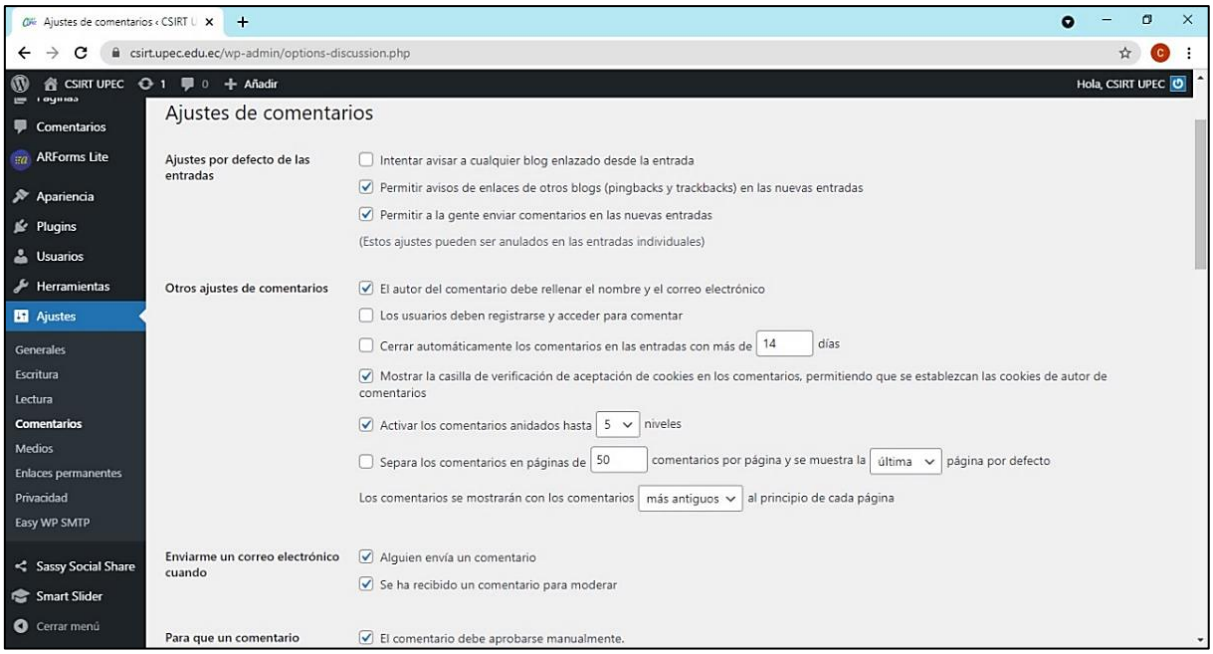


Figura 118. Ajuste de comentarios para el gestor de contenido WordPress

Como se muestra en la figura 119, se establece el tamaño de las imágenes al determinar sus dimensiones, el tamaño miniatura está definido en 150 px de ancho y alto, el tamaño medio en 300 px de ancho y alto y el tamaño grande con un ancho y alto de 1024 px. Se activa la casilla para organizar los archivos de carpetas por mes y año.

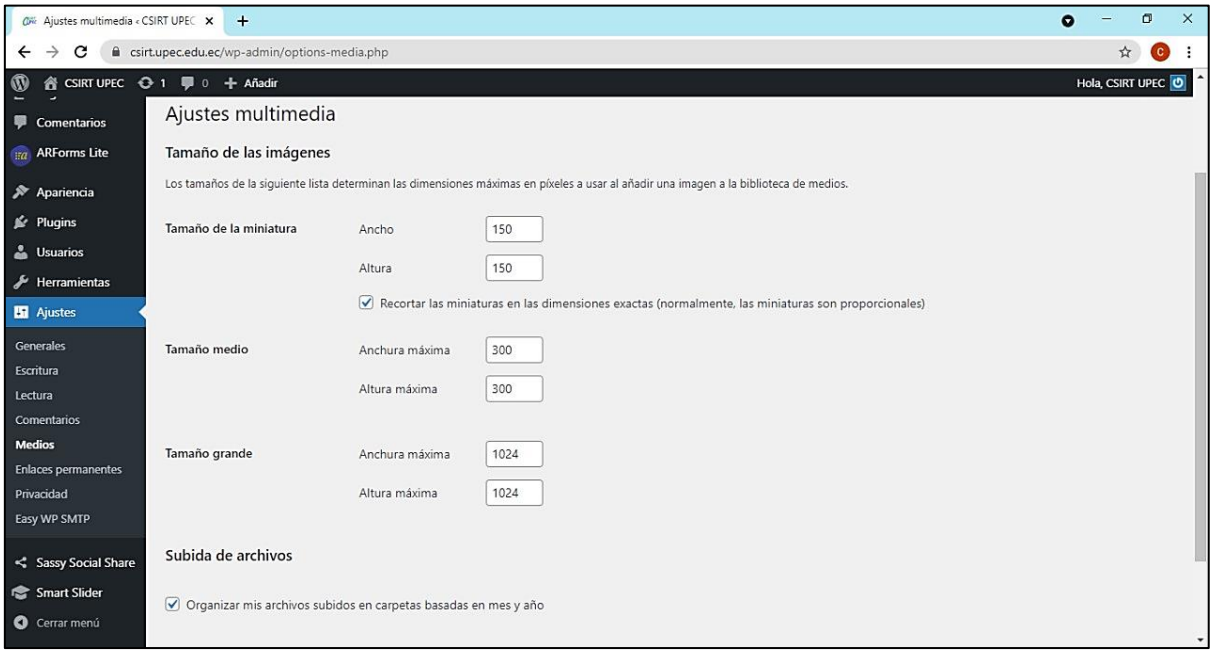


Figura 119. Ajuste multimedia para el gestor de contenido WordPress

En la opción de ajustes para enlaces permanentes se establece una estructura simple para la estética de la URL del sitio como se muestra en la figura 120.

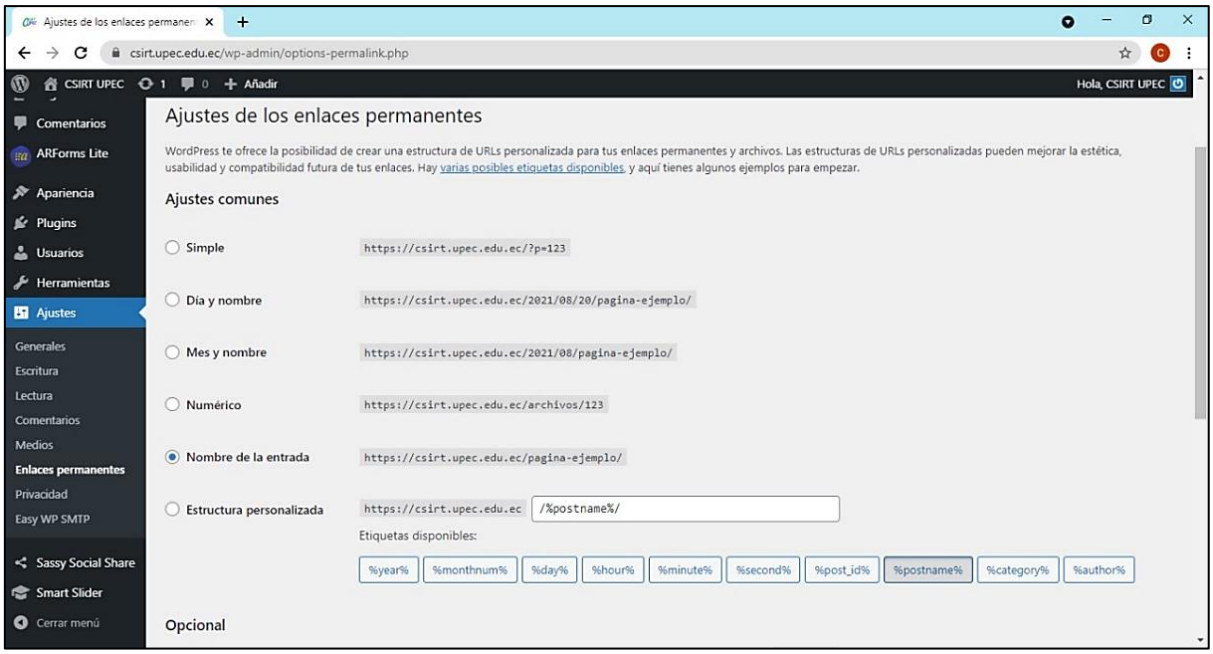


Figura 120. Ajuste de enlaces permanentes para el gestor de contenido WordPress

Como se muestra en la figura 121, en ajustes de privacidad, se selecciona la página denominada política de privacidad y clic en añadir.

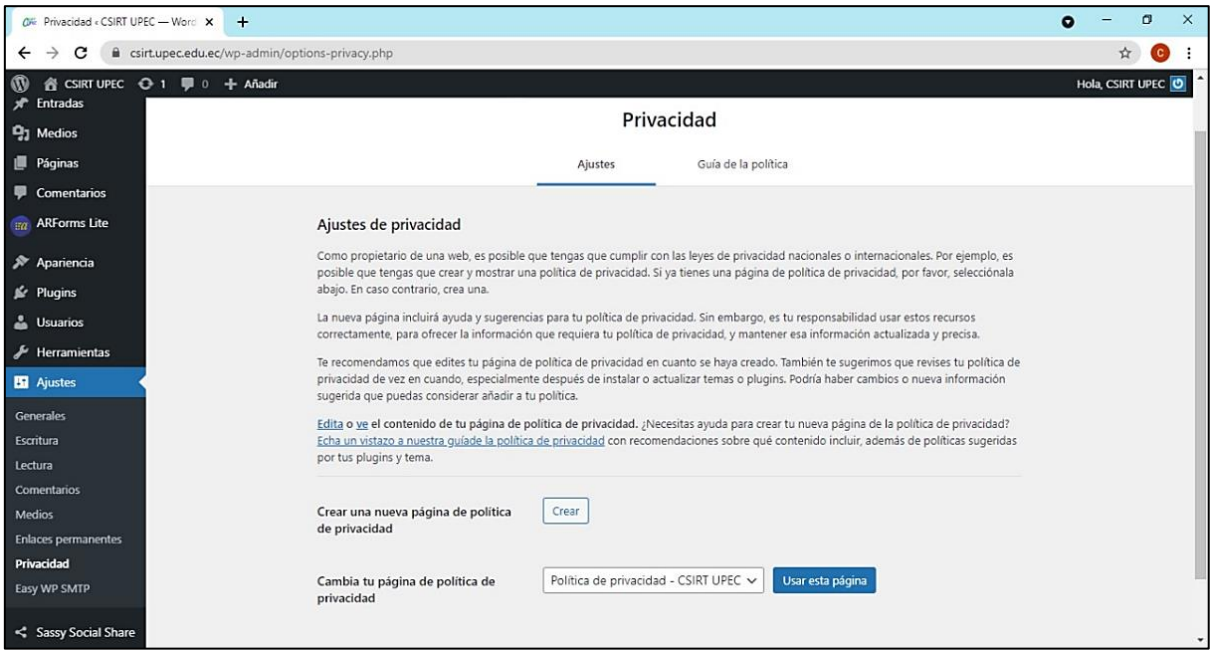


Figura 121. Ajustes de privacidad

- **Plugins**

  En el menú de navegación se encuentra la opción “plugins”, en añadir nuevo se busca el plugin requerido, se muestran búsquedas por destacados, populares, recomendados, favoritos y se encuentra una caja de búsqueda para encontrar plugins por el nombre

como se muestra en la figura 122. Para añadir el plugin al gestor de contenido se da clic en instalar ahora.

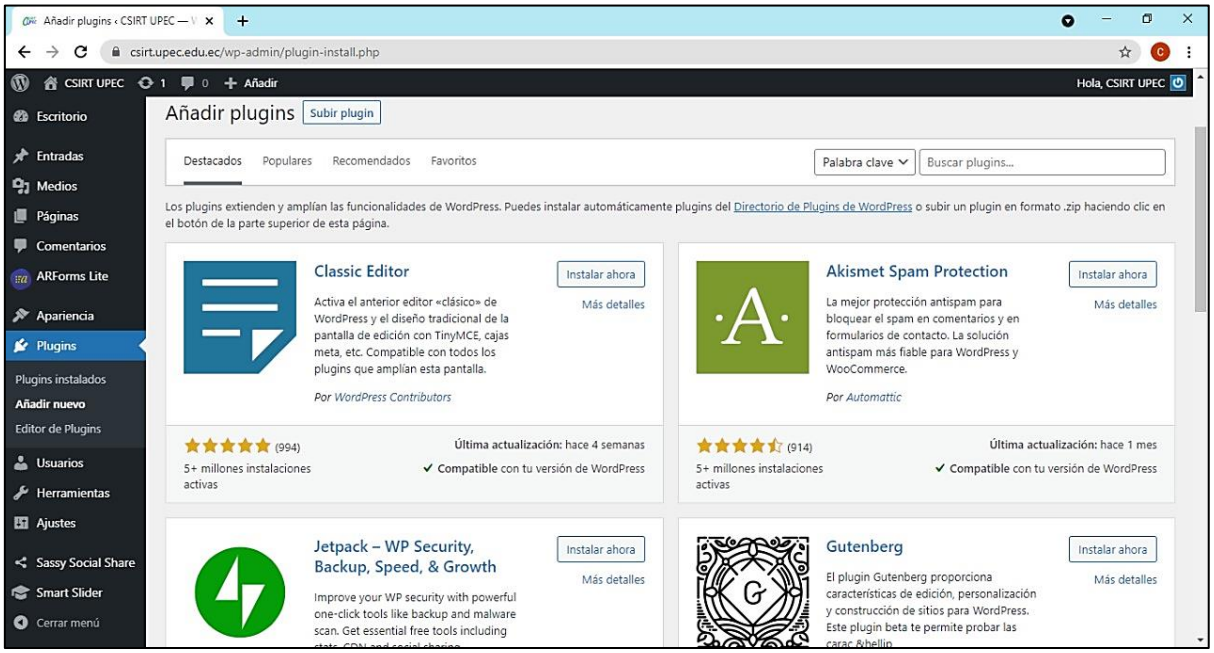


Figura 122. Búsqueda e instalación de plugins requeridos para distintas funcionalidades en el gestor de contenido WordPress

Como se muestra en la figura 123, en la opción plugins instalados se activan los plugins añadidos al gestor de contenido, además, se observa el nombre del plugin con opciones de configuración, en su descripción consta la versión y detalles y su opción de activar actualizaciones automáticas que no se encuentra habilitada.

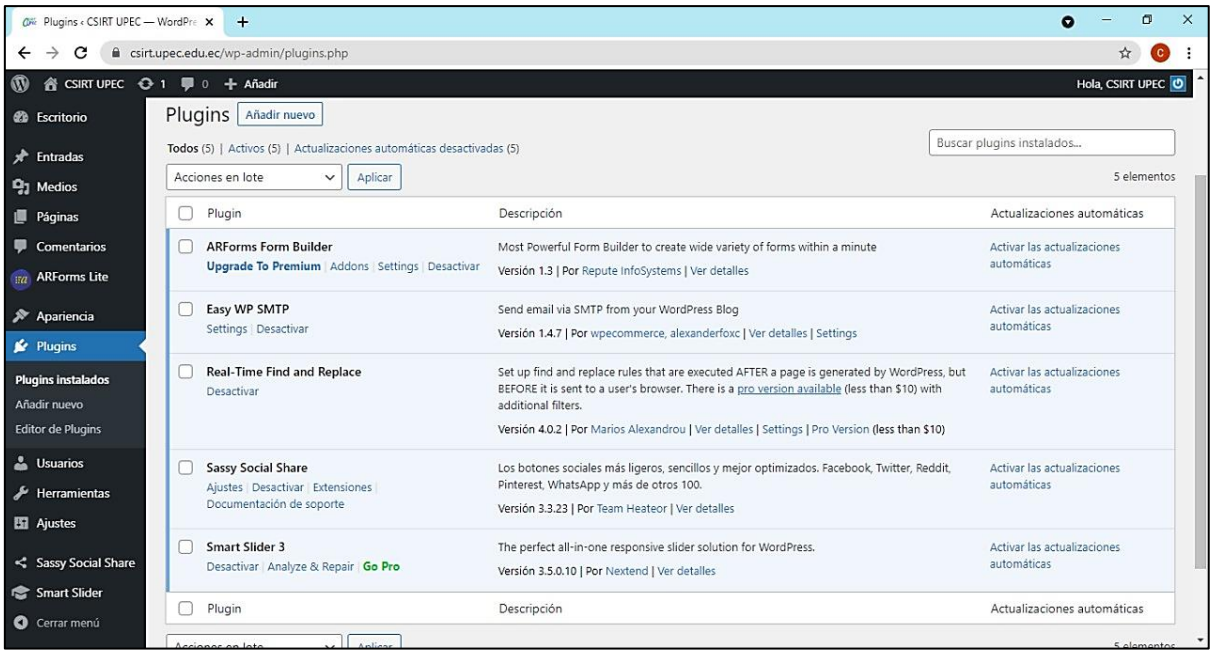


Figura 123.Visualización de plugins instalados

Se instala el plugin ARForm Builder para la creación de formularios, en su configuración se establece los mensajes predeterminados en el formulario que son “este campo no puede estar vacío” cuando el campo está en blanco, “problemas al enviar, los errores se marcan a continuación” cuando el campo esta incorrecto, “”el formulario se envió correctamente, gracias” como un mensaje de éxito, “lo lamentamos, el formulario no se envió correctamente” cuando el envío es fallido y se coloca la palabra “enviar” al botón de envío como se muestra en la figura 124.

En ajustes del correo electrónico se estable CSIRT UPEC para responder, csirt.computacion@upec.edu.ec como correo para recibir mensajes y responder, en envío de correo SMTP se elige el servidor de WordPress y su formato en HTML. En otros ajustes ingresamos 0 para que los mensajes de éxito nunca se oculten y se da clic en guardar.

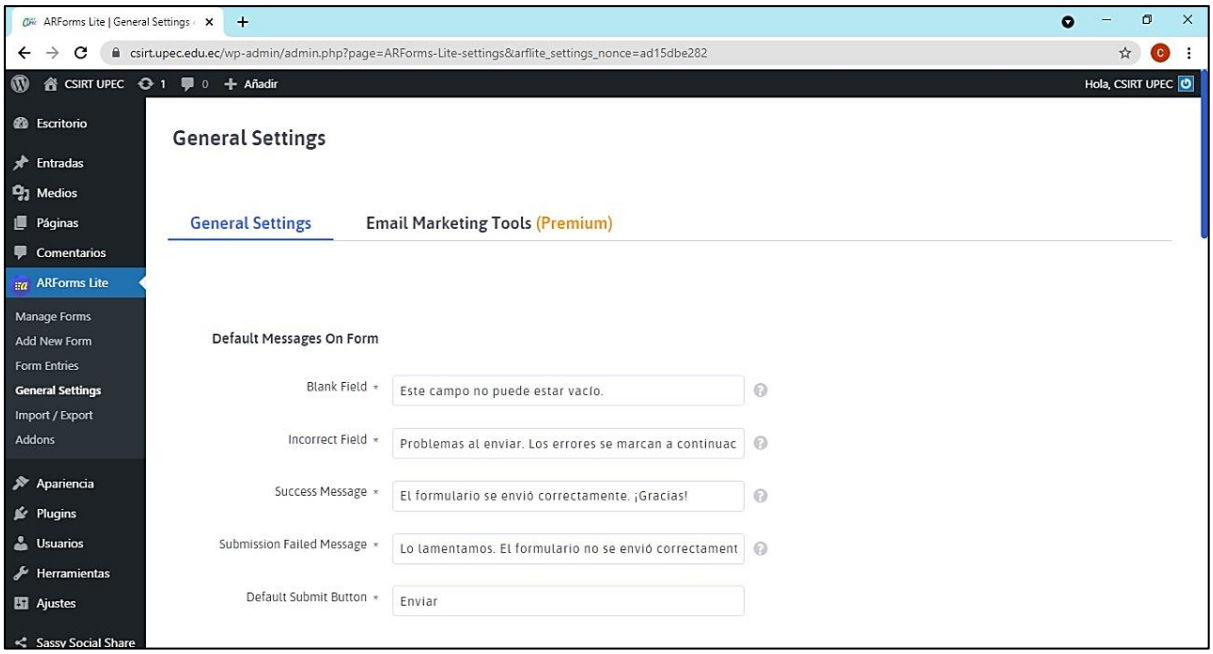


Figura 124. Configuración del plugin ARForm Builder

Se instala el plugin Easy WP SMTP para añadir la funcionalidad de envío de correos, en la configuración se ingresa el correo electrónico para el campo remitente con el nombre CSIRT UPEC, el host SMTP brindado por el servidor de correo, el tipo de cifrado que utiliza, su puerto SMTP, se activa la casilla de autenticación y se ingresa el nombre y contraseña como se muestra en la figura 125.

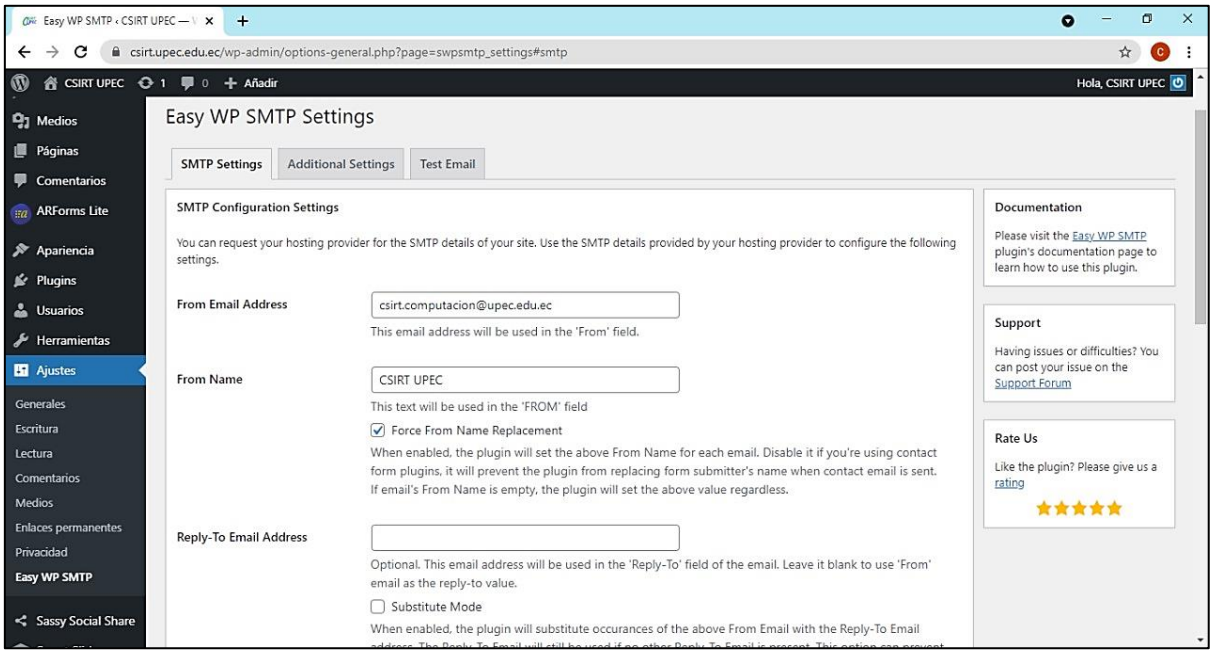


Figura 125. Configuración del plugin Easy WP SMTP

En la figura 126, se muestra la instalación del plugin Real-Time Find and Replace para reemplazar código del tema en tiempo real, para su configuración, en el cuadro de texto encontrar se ingresa el código de tema que se desea cambiar y en el cuadro reemplazar con, se ingresa el código de reemplazo.

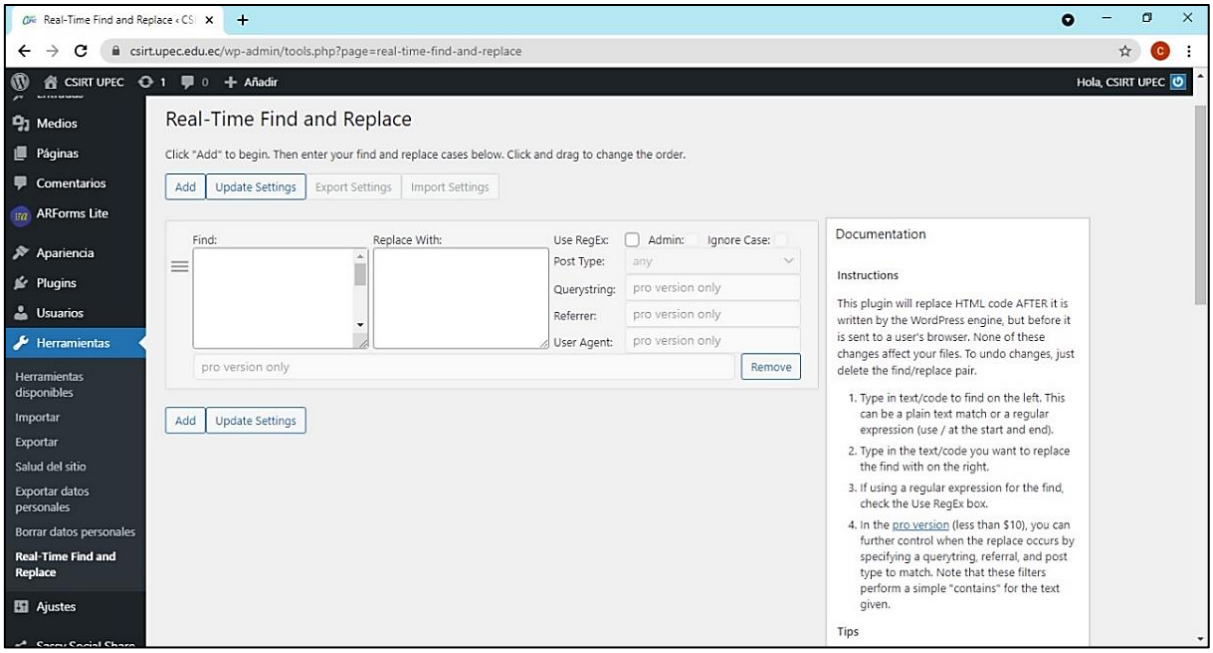


Figura 126. Configuración del plugin Real-Time Find and Replace

Se instala el plugin Sassy Social Share para incluir la funcionalidad de compartir las entradas en redes sociales, en su configuración se establece la forma del icono social, el tamaño en 35 px, color de logotipo por defecto, se añaden Facebook, WhatsApp, Twitter y LinkedIn, se establece su alineación centrada y debajo del contenido de las entradas como se muestra en la figura 127.

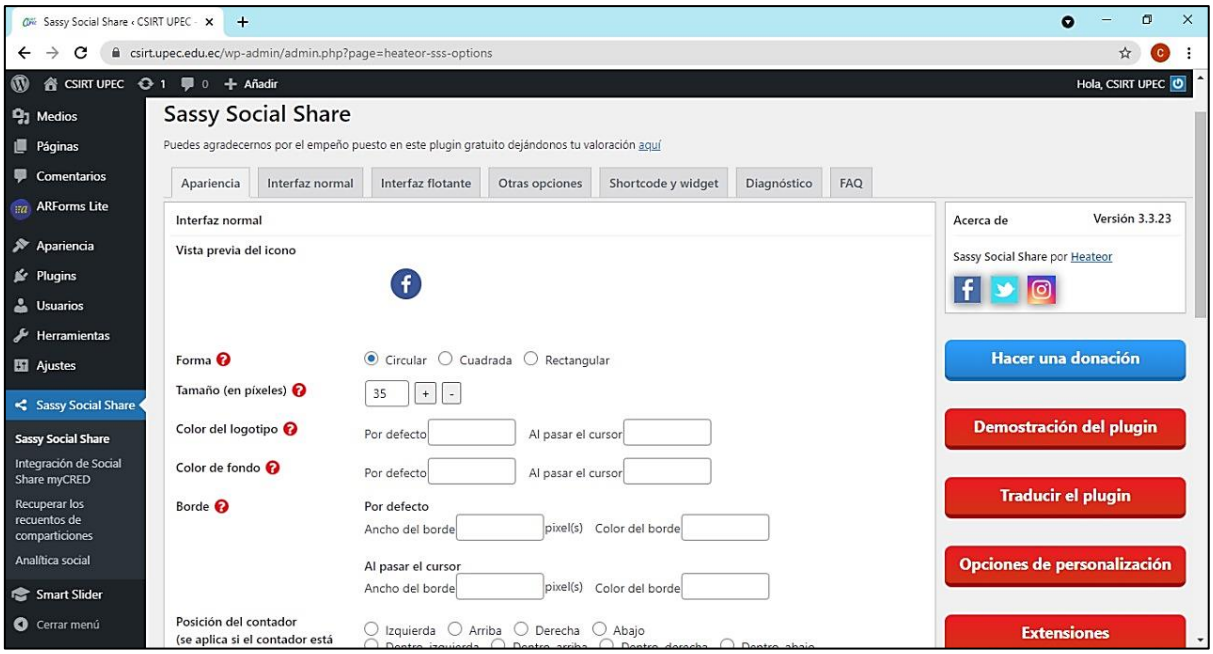


Figura 127. Configuración del plugin Sassy Social Share

En la figura 128, se muestra la instalación del plugin Smart Slider 3 para añadir el carrusel al sitio web, en su configuración, para el texto se define la fuente Arial, tamaño 14, formato normal y con una altura de línea de 1,5 de espacio, para las imágenes opacidad al 100% y 0 px para el relleno, frontera y radio de borde; y para los botones, la fuente de texto Robot, color blanco, tamaño de 14 px y en formato normal.

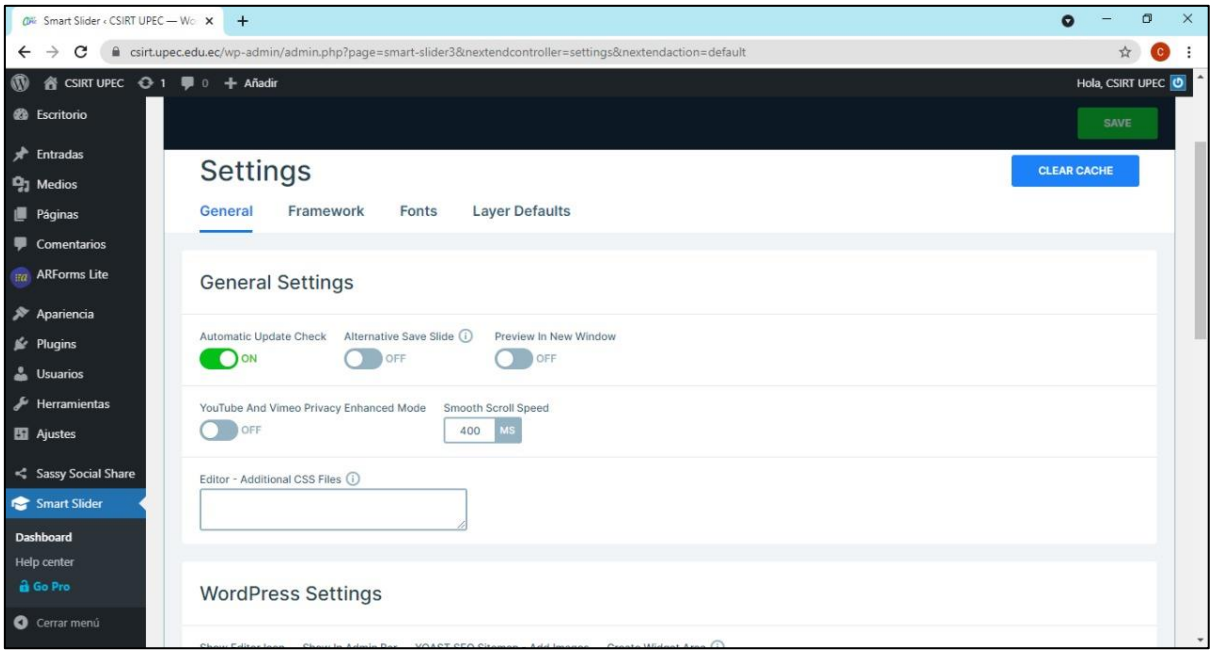


Figura 128. Configuración del plugin Smart Slider 3

- **Usuarios**

  Para añadir un usuario a WordPress se ubica el menú de navegación usuario y añadir nuevo como se muestra en la figura 129, se ingresa el usuario, correo electrónico y contraseña como campos obligatorios, nombre, apellidos, web e idioma, se establece el rol que va a cumplir el usuario, se activa la casilla de notificación por correo al usuario y se da clic en añadir nuevo usuario.

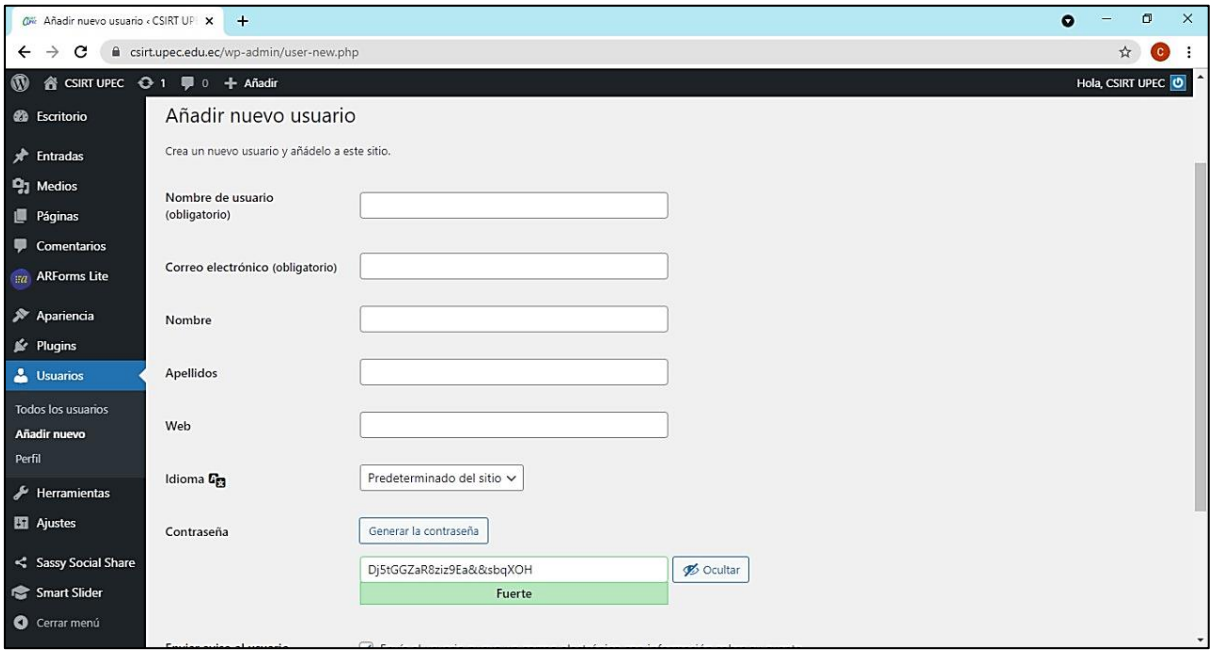


Figura 129. Creación de usuario para la administración del sitio web

Como se muestra en a figura 130, para la administración de los usuarios creados, se dirige al menú de navegación usuarios y clic en todos los usuarios, su área de trabajo permite editar, borrar, ver su perfil, enviar restablecimiento de la contraseña, además, se mira la tabla con nombre de usuario, nombre, correo electrónico, el perfil que desempeña y el número de entradas que ha creado cada usuario.

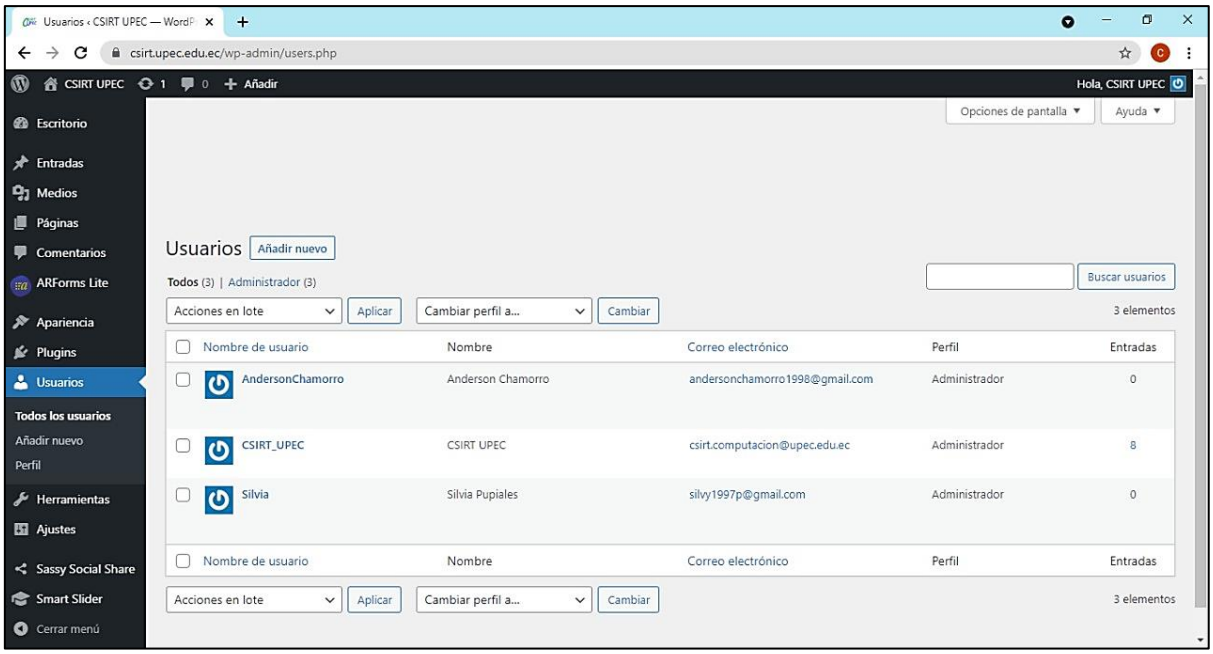


Figura 130. Administrador de usuarios del gestor de contenido WordPress

Anexo 16 Configuración diseño sitio web

- **Diseño del sitio web**

  Se añade un tema para darle estructura al sitio web, para ello se da clic en la opción apariencias donde se despliega varias opciones, se elige la opción temas y en añadir nuevo como se muestra en la figura 131.

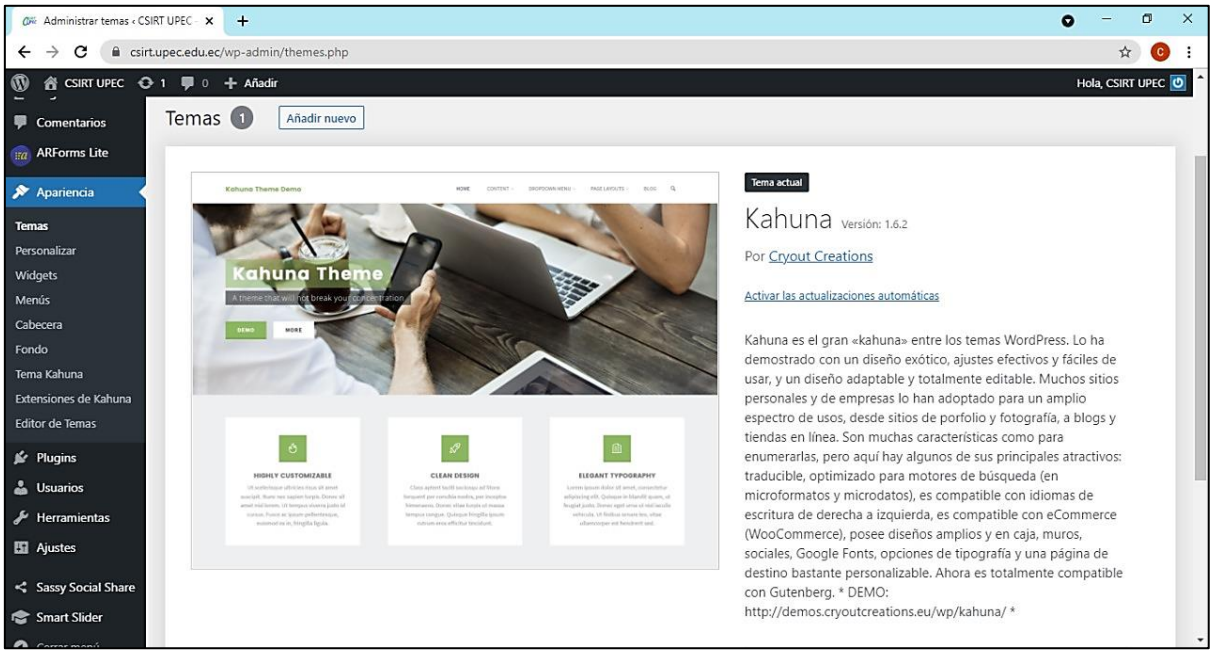


Figura 131. Añadir tema al gestor de contenido WordPress

Se muestra los temas disponibles clasificados en las categorías destacados, populares, recientes y favoritos como se observa en la figura 132, además se tiene las opciones de filtrar por características para obtener sugerencias de temas que cumplan con los requerimientos seleccionados, la opción subir tema que permite añadir un tema en formato .zip y la caja de búsqueda para buscar los temas por sus nombres. Se da clic en instalar el tema seleccionado.

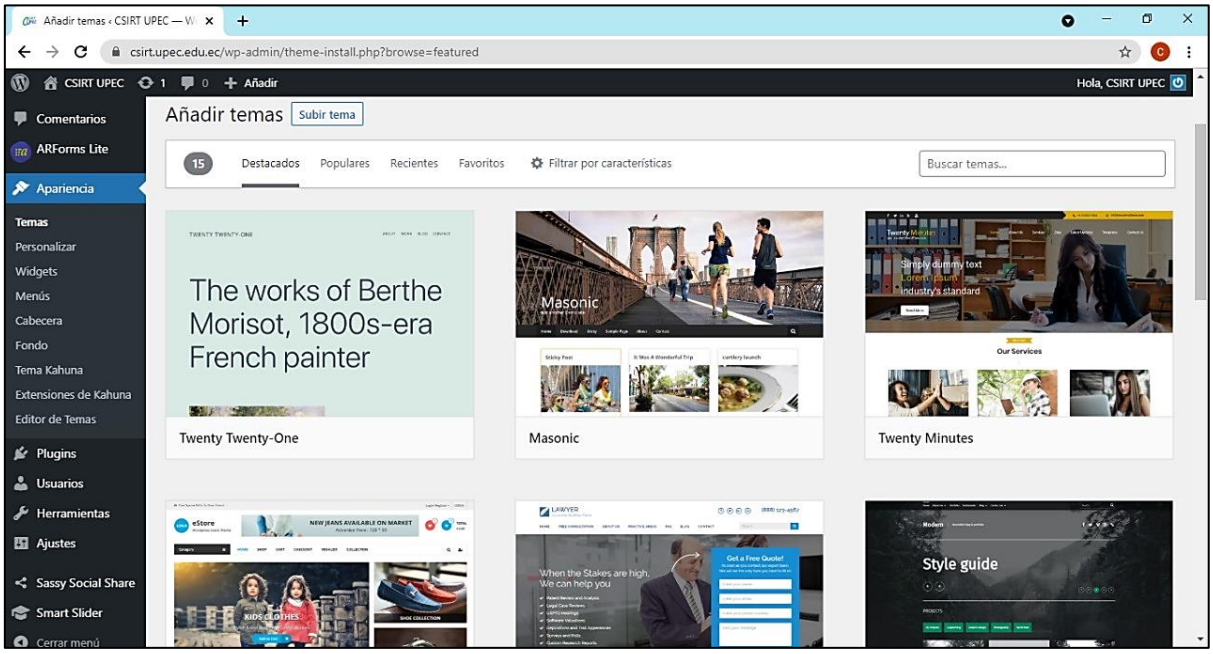


Figura 132. Selección e instalación del tema para el gestor de contenido WordPress

Como se muestra en la figura 133, se activa el tema instalado, el cual dará su estilo y diseño a todo el sitio. El tema seleccionado es “kahuna” en su versión gratuita 1.6.2.

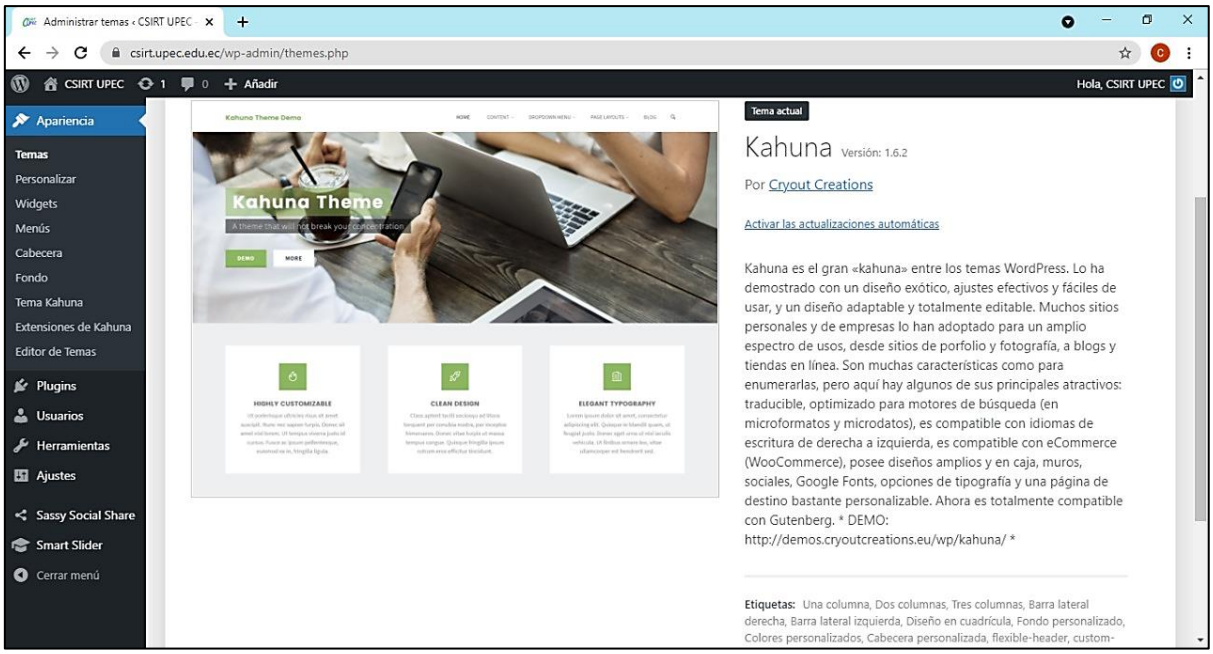


Figura 133. Activación del tema Kahuna en WordPress

Para dar un diseño y un estilo apropiado al sitio, en el menú de navegación, se ubica la opción apariencias y clic en personalizar como se muestra en la figura 134. Se encuentran varias opciones que permiten configurar y dar un diseño, estructura, animación y funcionalidad al sitio.

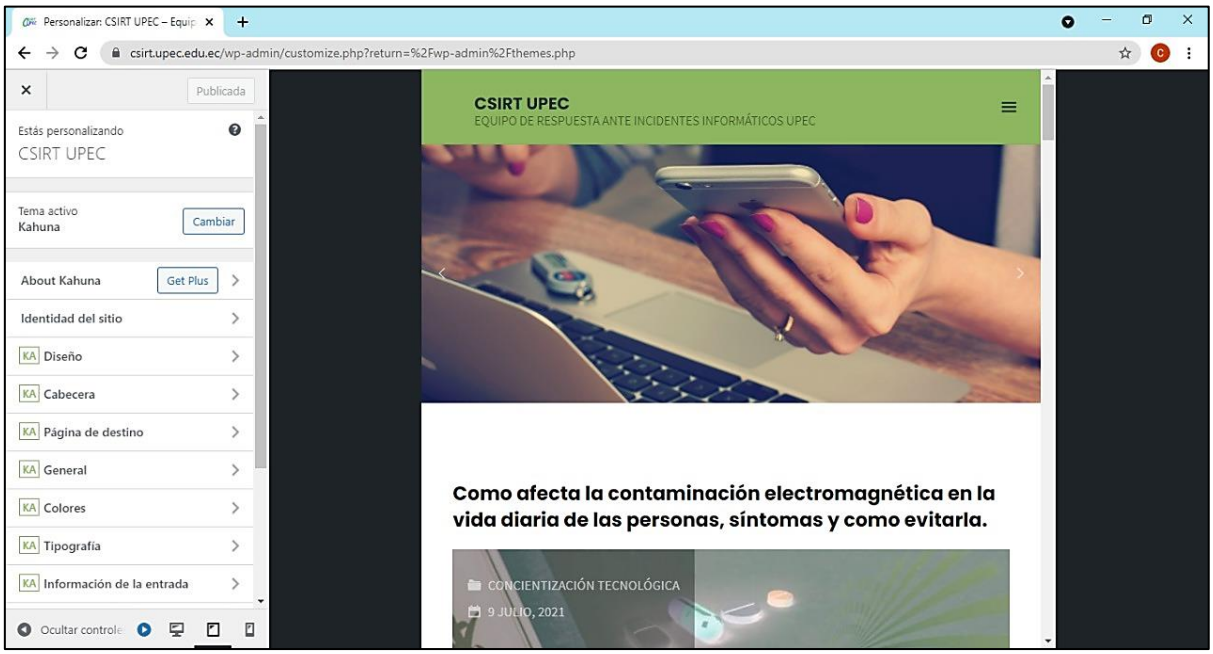


Figura 134. Opción personalizar el menú de navegación WordPress

- **Identidad del sitio**

  En la opción identidad del sitio se encuentran tres opciones que permiten adecuar las características principales para el reconocimiento del sitio web, cómo se muestra en la figura 135, las opciones a configurar son identidad del sitio y cabecera multimedia.

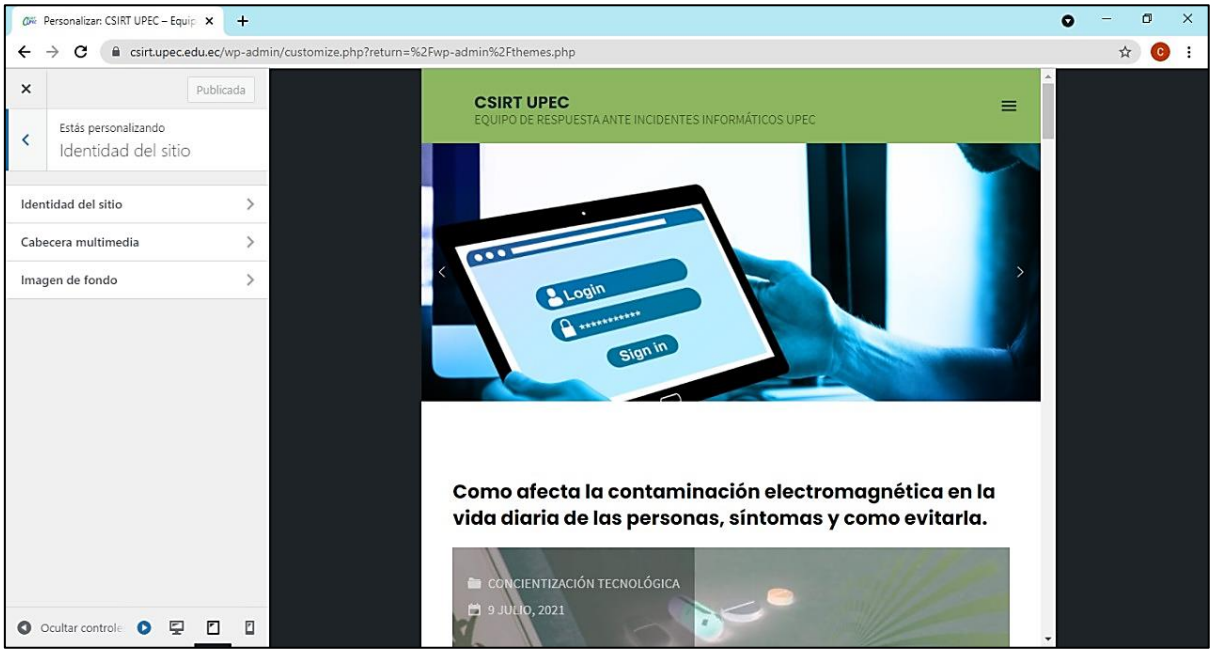


Figura 135. Personalizar identidad del sitio en WordPress

En la opción identidad, como título del sitio se coloca “CSIRT UPEC” y como descripción corta el significado de sus siglas “EQUIPO DE RESPUESTAS A INCIDENTES INFORMÁTICOS UPEC”, se activa la casilla para obtener visibilidad de estos en la cabecera del sitio y se añade el icono como se observa en la figura 136, para que se visualice en las pestañas del navegador al momento de ingresar al sitio.

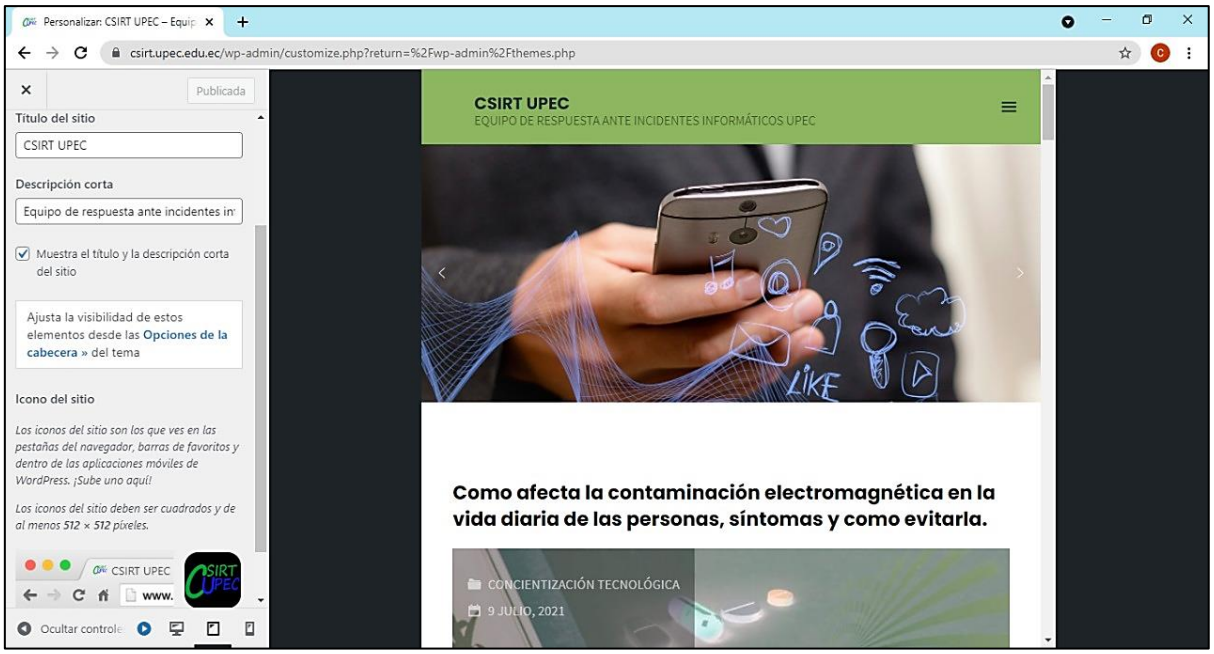


Figura 136. Opción identidad del sitio para agregar título, descripción y favicon al sitio web

Como se muestra en la figura 137, en la opción cabecera multimedia, se añade una imagen que se visualizará en la cabecera de cada página a acepción de la página de destino o inicio.

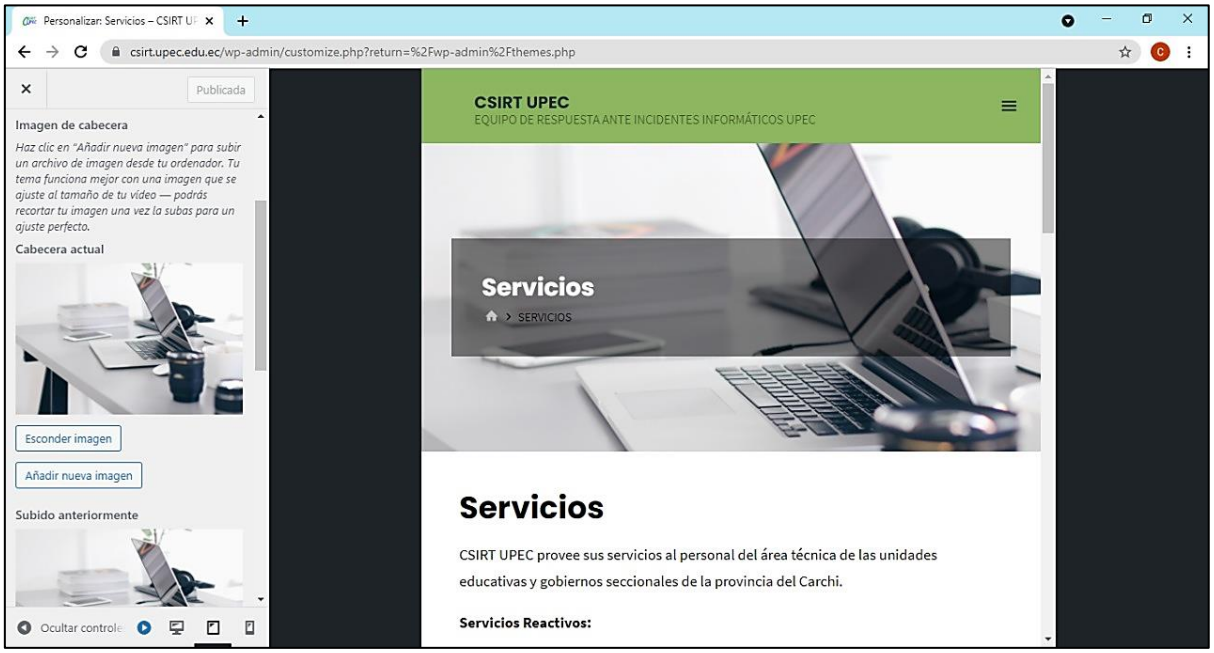


Figura 137. Inserción de imagen como cabecera para las páginas del sitio web

- **Diseño**

  En el menú diseño se establece los modelos de estructura que tomará el sitio web, donde se define la ubicación de los elementos y su contenido, las opciones de configuración son diseño general y otros diseños como se muestra en la figura 138.

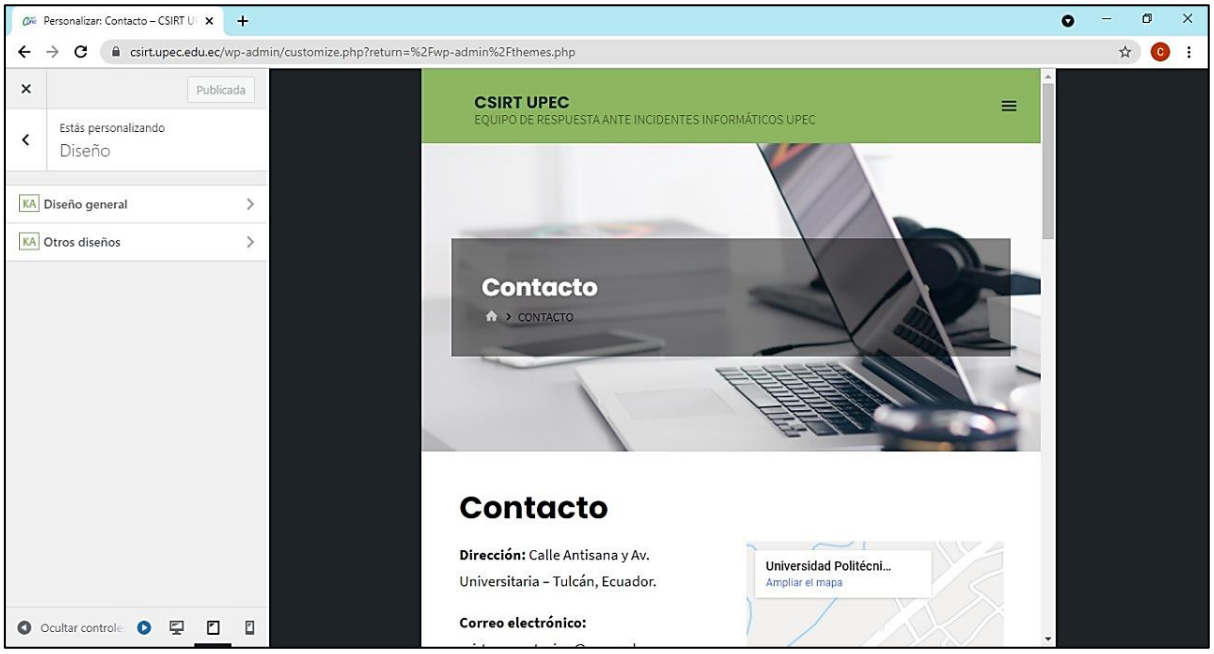


Figura 138. Personalizar diseño en WordPress

En la opción diseño general, se define el diseño principal de las páginas del sitio, como se observa en la figura 139, se da clic para seleccionar la opción de dos columnas y barra lateral en la derecha, además, se selecciona la opción de ancho en la alineación del tema para utilizar toda la pantalla, definimos el ancho del sitio en 1780 px (pixeles) y el ancho de la barra lateral izquierda en 380 px.

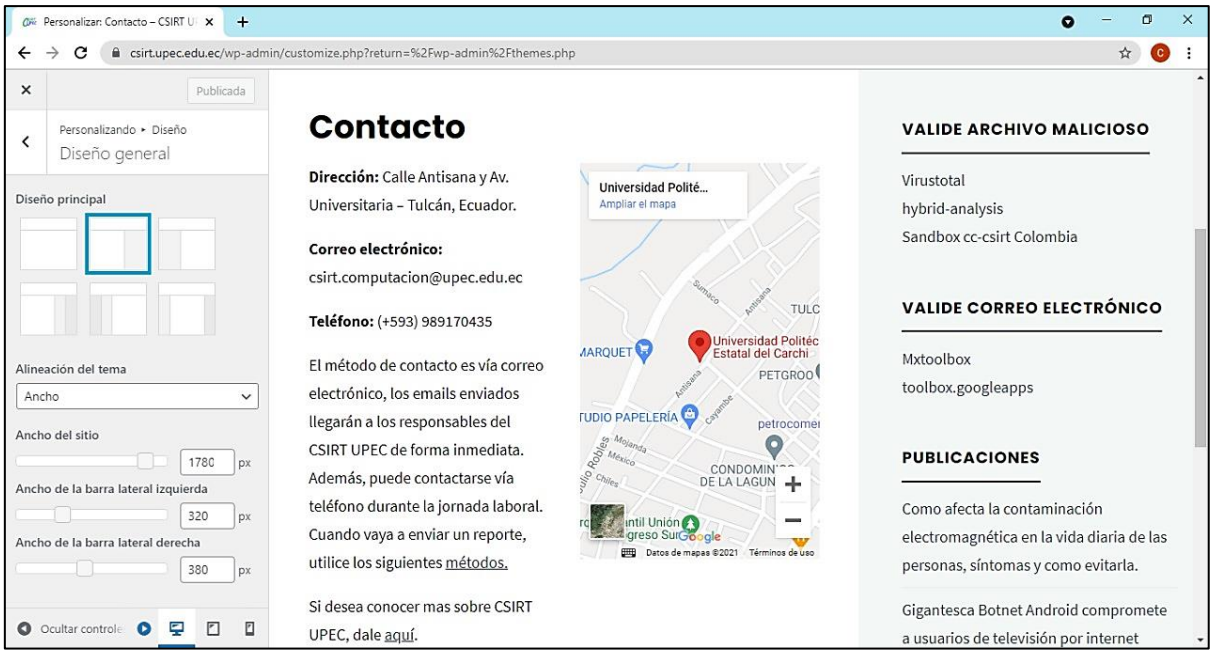


Figura 139. Establecer diseño principal, alineación y dimensiones en la estructura del sitio web

En la opción otros diseños, se da clic en diseño de dos columnas para establecer la estructura de las entradas que son publicadas, Además, se establece tres columnas y alineación por defecto para los widgets del pie de página como se muestra en la figura 140.



Figura 140. Definir diseño de las entradas y pie de página del sitio web

- **Cabecera**

  En el menú cabecera se establecen las propiedades del menú de navegación y el contenido de cabecera como se muestra en la figura 141. Las opciones de configuración son menú y contenido.

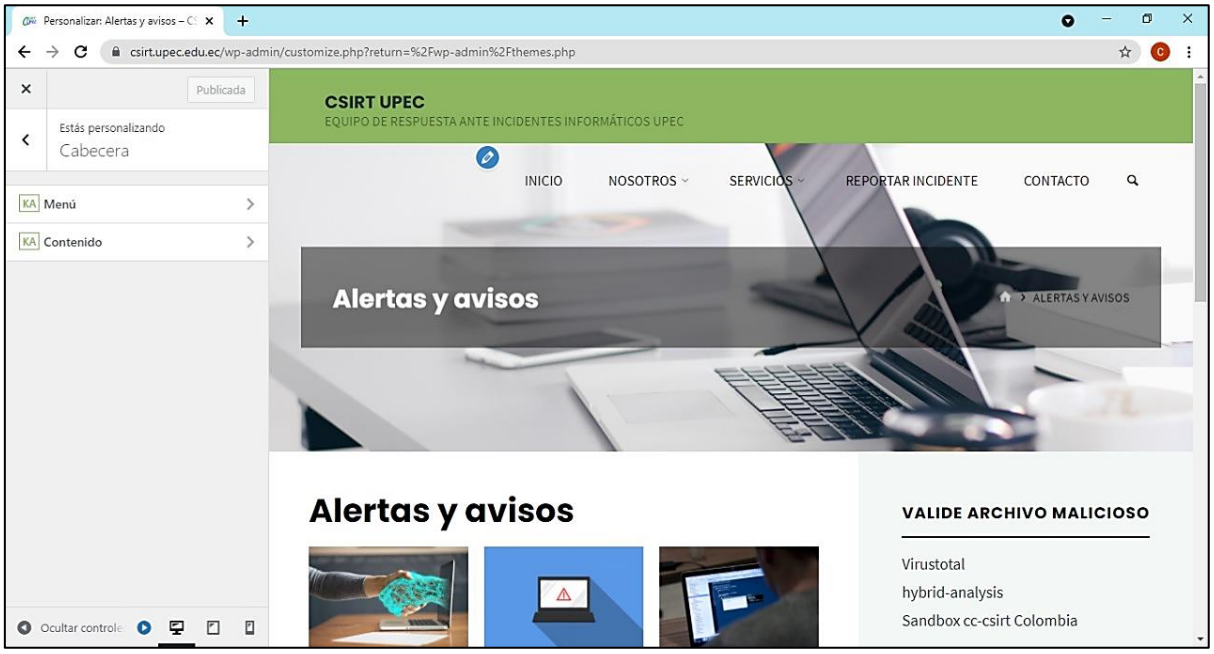


Figura 141. Personalizar cabecera en WordPress

En la opción menú, se activa la opción de menú fijo, se establece la altura del menú de cabecera en 85 px y se da clic en alineación a la derecha y en posición normal como se muestra en la figura 142.

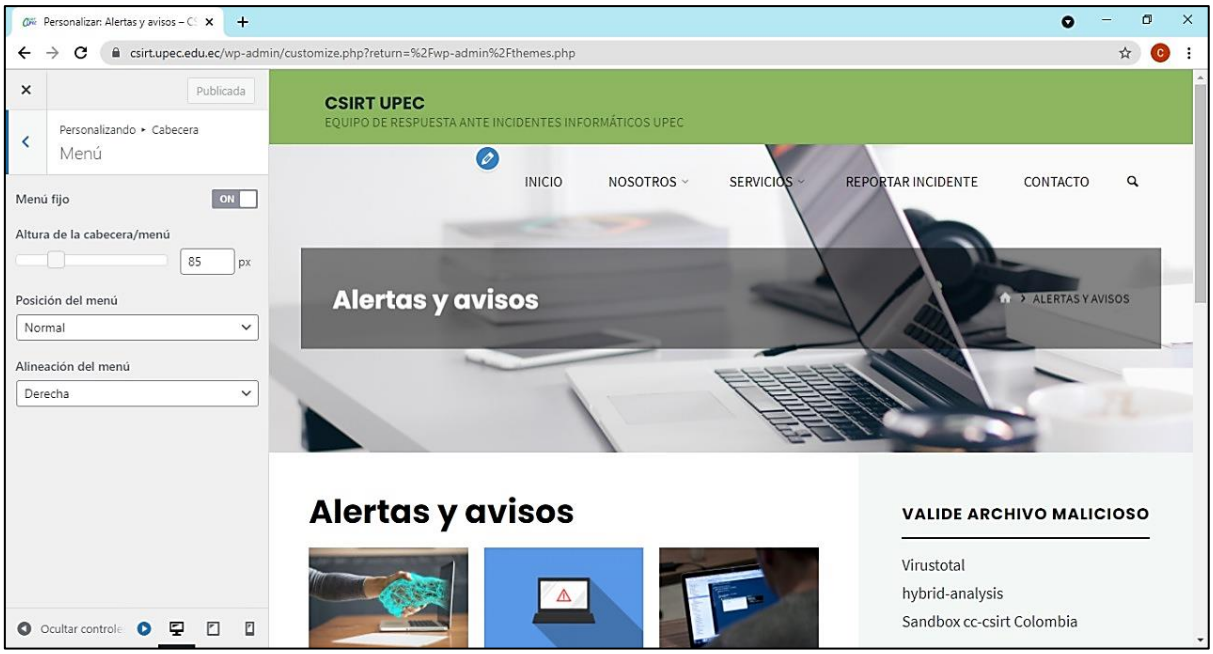


Figura 142. Definir altura, posición y alineación del menú para la cabecera del sitio web

Como se muestra en la figura 143, en contenido de la cabecera del sitio se selecciona la opción logotipo y título del sitio para añadir la identidad en la cabecera, se activa la casilla en mostrar la descripción corta para visualizarla debajo del título del sitio y se establece la altura de la imagen de cabecera en 350 px y comportamiento de la imagen en recortado.

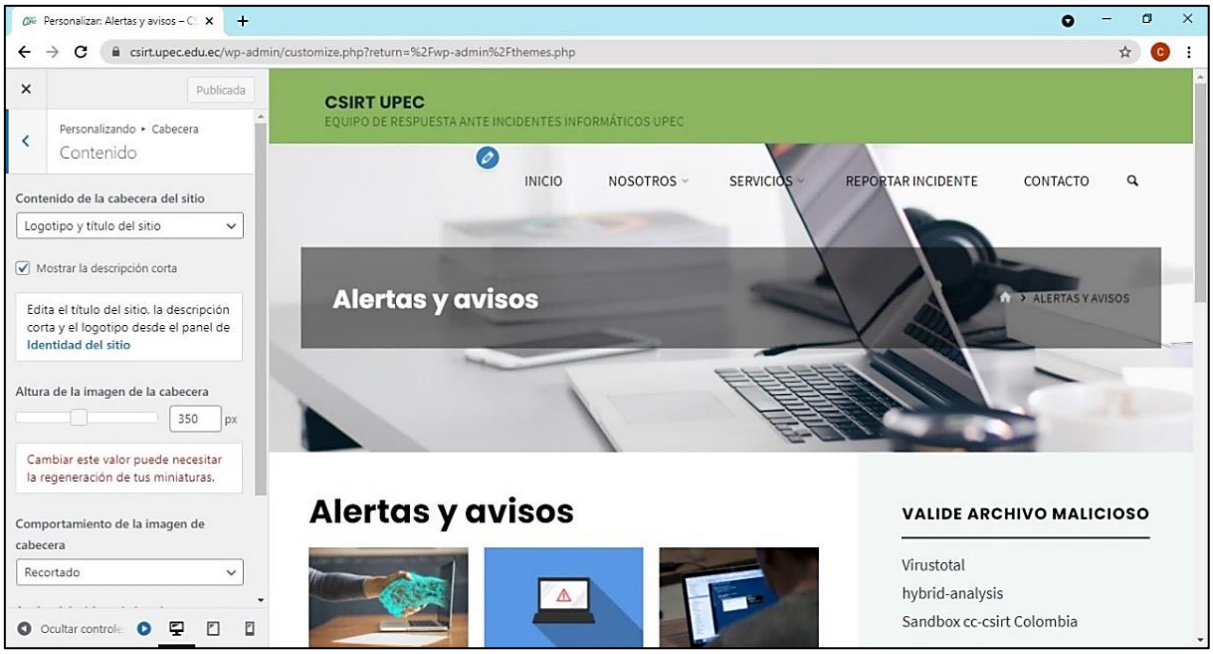


Figura 143. Establecer descripción, altura, comportamiento, ancho y alineación de la imagen de cabecera para el sitio web

- **General**

  En el menú general se configuran parámetros para multimedia, animación y de funcionalidad en el sitio. Como se muestra en la figura 144, las opciones de configuración son estructura, títulos de la cabecera, imágenes del contenido y caja de búsqueda.

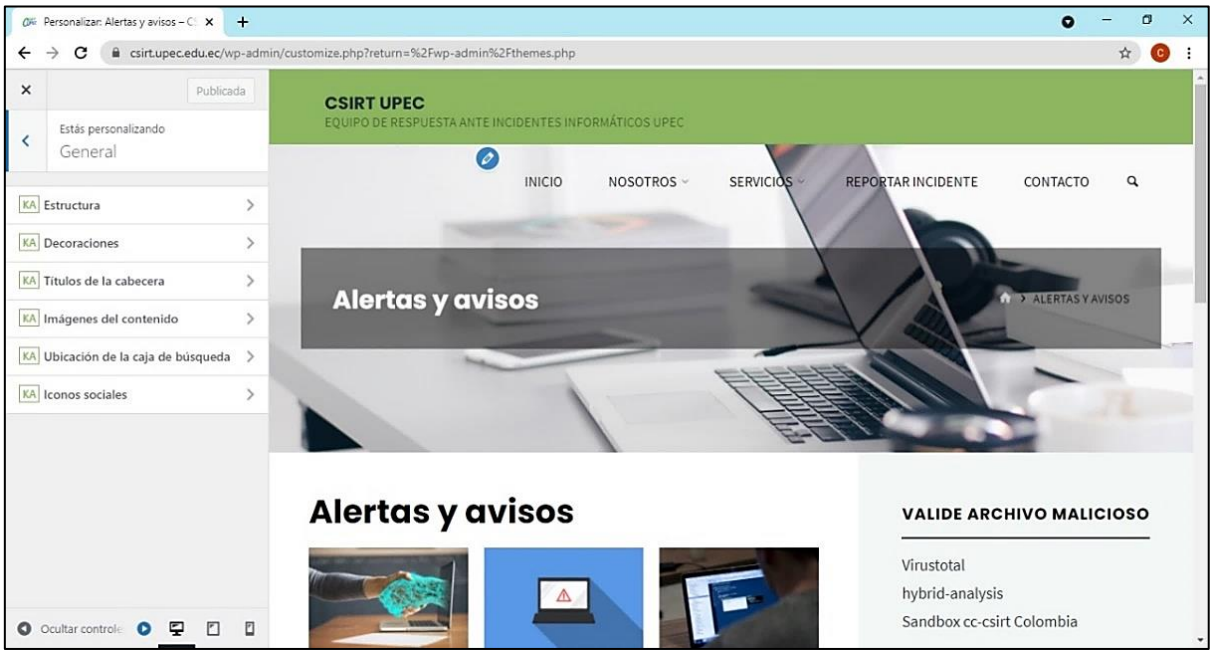


Figura 144. Personalización general en WordPress

En la opción estructura se selecciona la navegación en absoluto para habilitar el cambio entre entradas y se activa la visibilidad para los títulos de las páginas y categorías. Se habilita el botón volver arriba, se define su ubicación en el centro del pie de página, y se coloca los iconos sociales y copyright del sitio como se muestra en la figura 145. Se utiliza código HTML para añadir el copyright del sitio y sus iconos sociales.

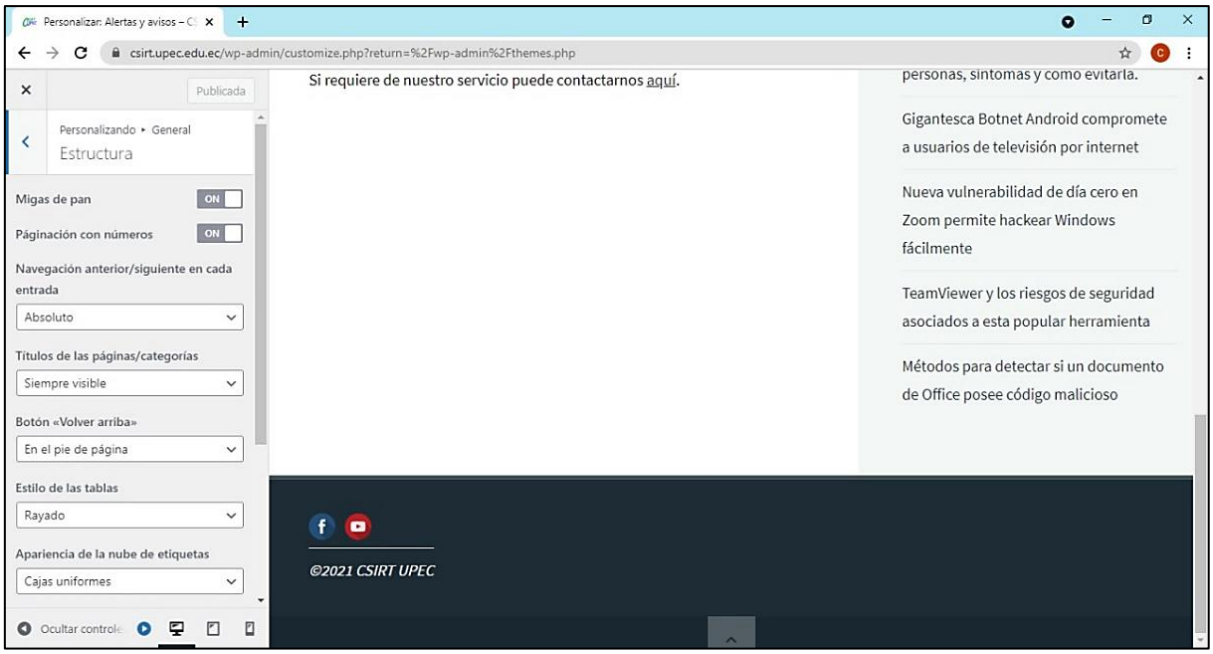


Figura 145. Activación de navegación, títulos de páginas y categorías y diseño del pie de página del sitio web

Como se observa en la figura 146, en la opción títulos de cabecera se activa los elementos, de los que se visualizará sus títulos en la imagen de cabecera al navegar por el sitio.

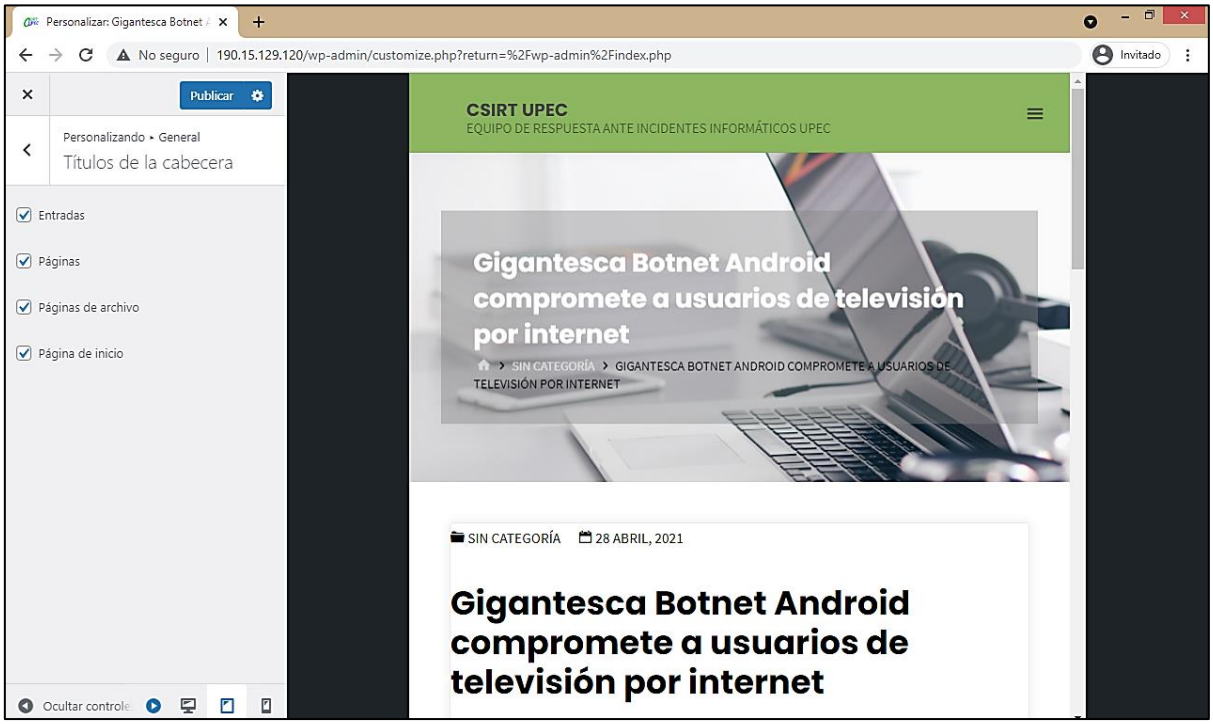


Figura 146. Marcar los títulos de cabecera para su visibilidad en la cabecera del sitio web

En la opción imágenes de contenido se elige el diseño para las imágenes destacadas en las entradas, como se observa en la figura 147.

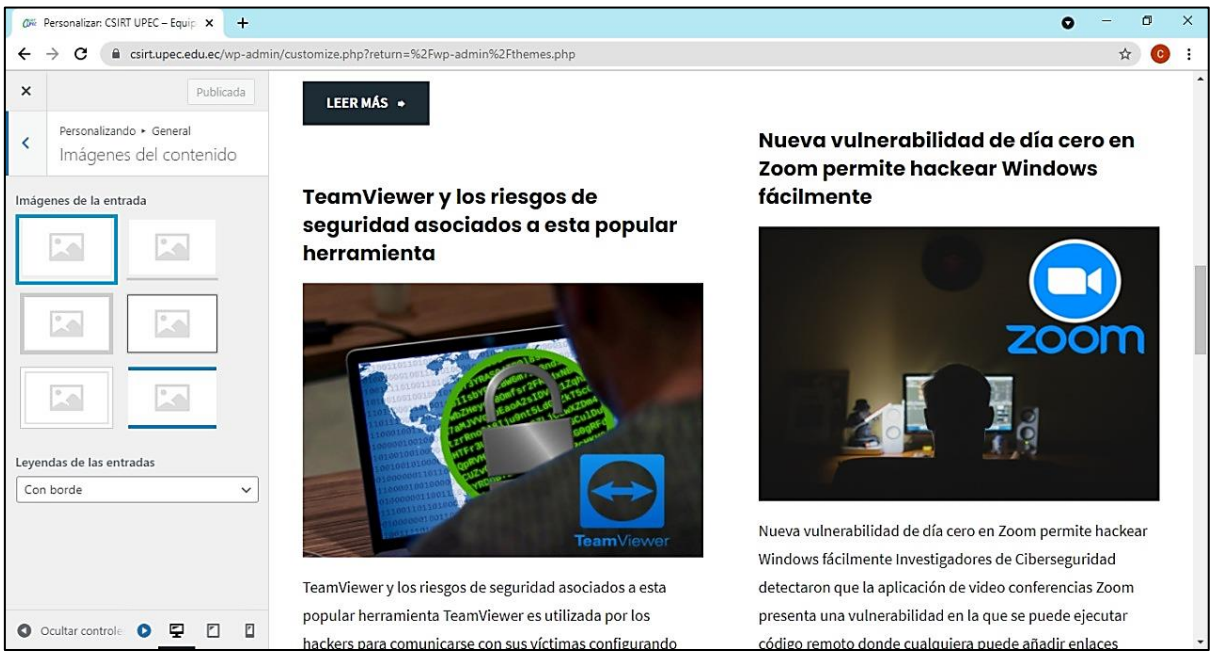


Figura 147. Establecer el diseño de las imágenes destacadas en las entradas del sitio web

En la opción ubicación de la caja de búsqueda, se activa la casilla de añadir búsqueda en el menú principal, el lugar adecuado para brindar su funcionalidad de buscar contenido en el sitio web como se muestra en la figura 148.

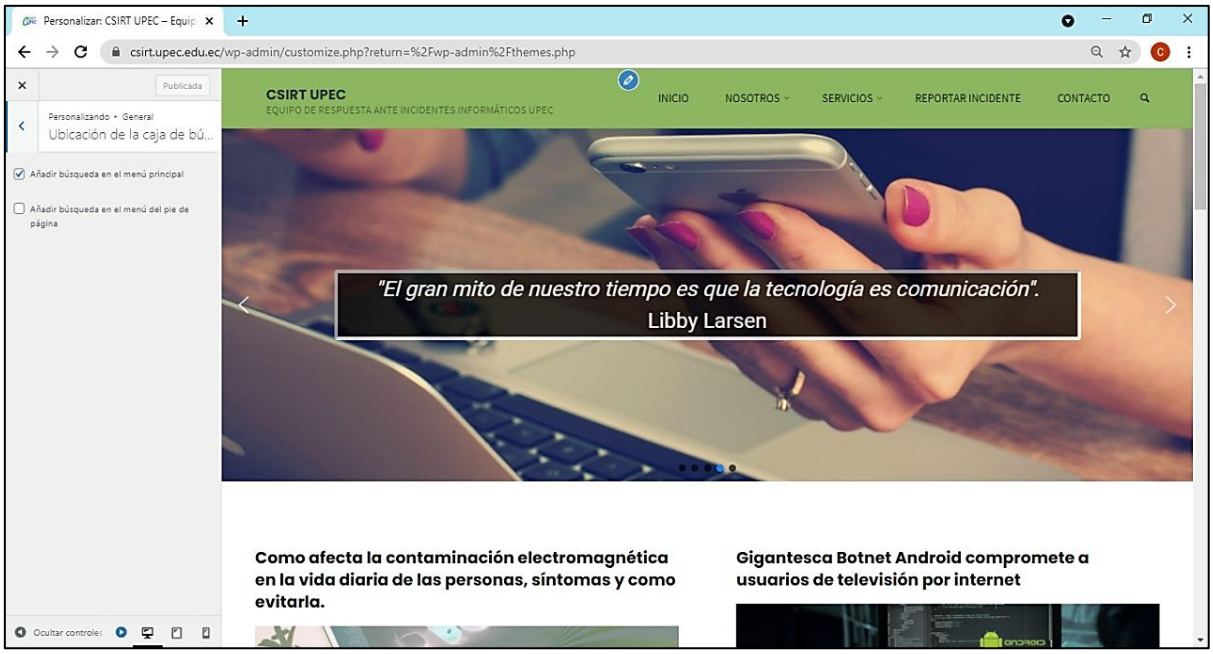


Figura 148. Activación de la caja de búsqueda en el sitio web

- **Colores**

  Como se observa en la figura 149, en el menú colores se establece los colores de los elementos que forman parte del sitio web, las opciones a configurar son contenido, cabecera, pie de página y página de destino.



Figura 149. Personalizar colores para el sitio web en WordPress

En la opción contenido se selecciona el color blanco para el fondo del sitio y contenido, plomo para la barra lateral izquierda y derecha, negro para el texto, encabezados del contenido, color de superposición y énfasis secundario y azul oscuro para énfasis principal como se muestra en la figura 150, además, se define un 47 % de opacidad en el color de superposición.



Figura 150. Establecer colores del contenido del sitio web

Como se observa en la figura 151, en la opción cabecera se selecciona el color verde claro para el fondo de cabecera, negro para el texto del menú y submenú y blanco para el fondo del submenú.

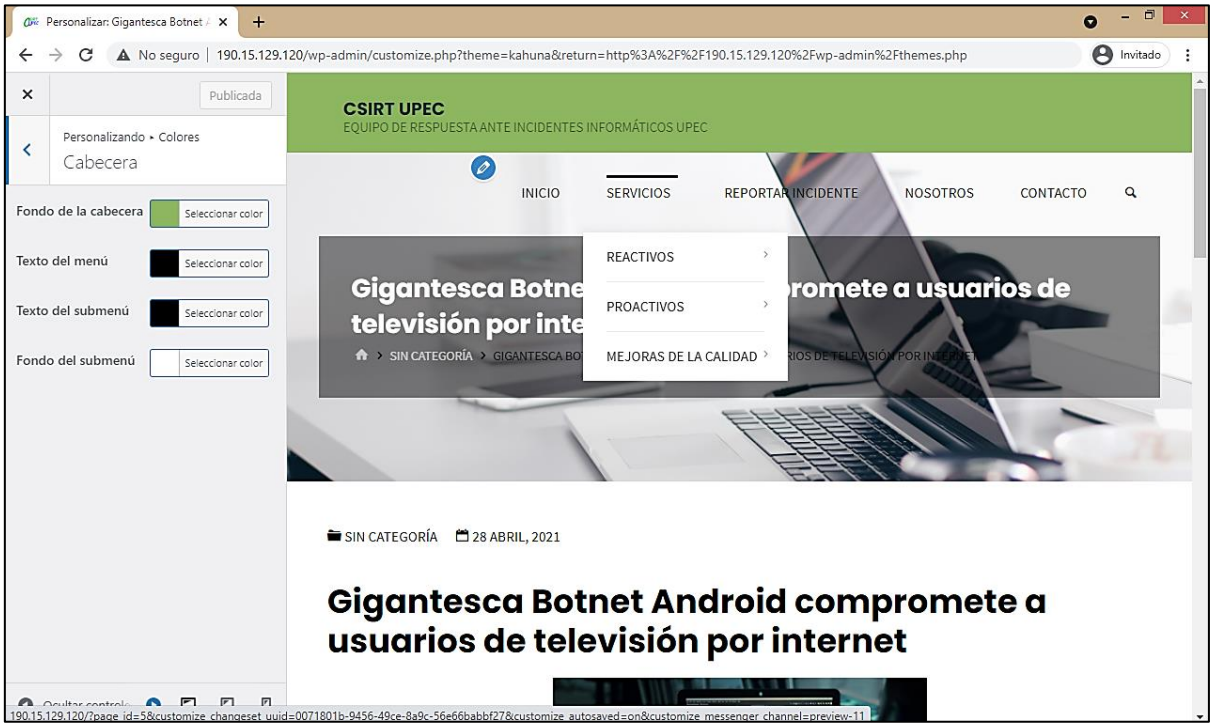


Figura 151. Establecer colores para la cabecera del sitio web

En la opción pie de página se selecciona el color azul oscuro para el fondo de pie de página y blanco para su texto como se muestra en la figura 152.

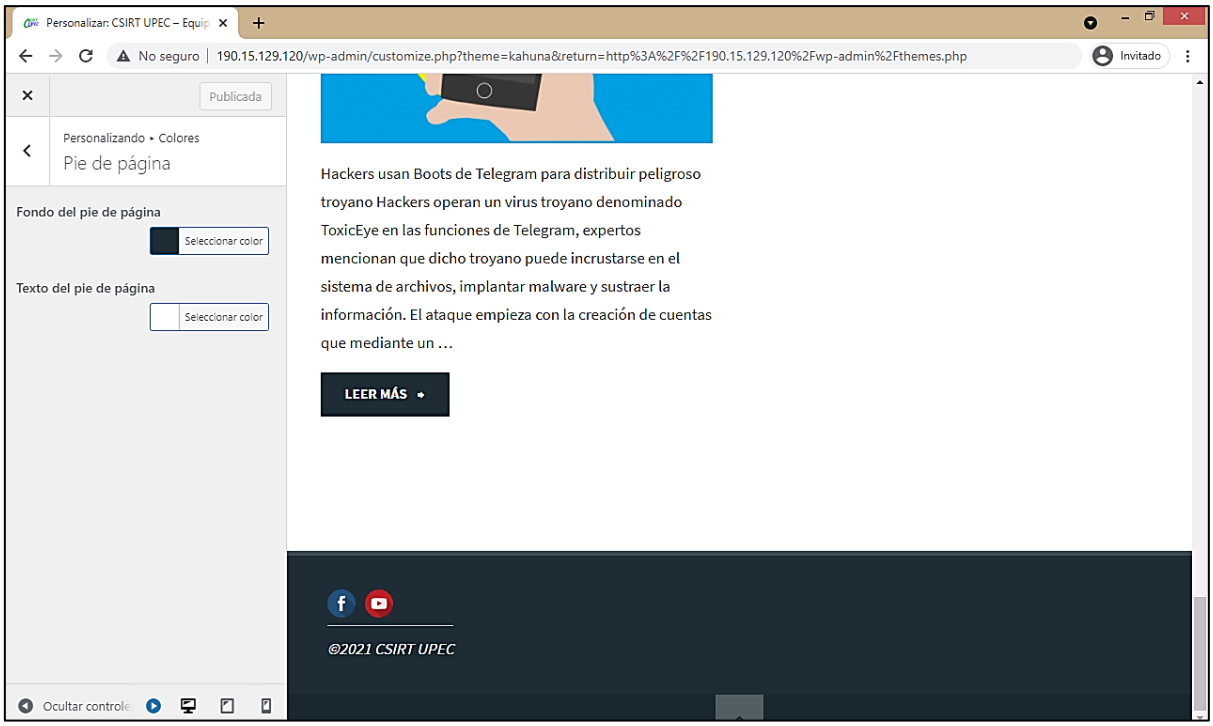


Figura 152. Establecer colores para el pie de página del sitio web

En la opción página de destino se selecciona el color plomo claro para bloques, cajas y áreas de texto y blanco para contenido destacado como se muestra en la figura 153.



Figura 153. Establecer colores para la página de destino del sitio web

- **Tipografía**

  Como se muestra en la figura 154, en el menú tipografía se establece las características del texto en fuente y tamaño, las opciones a configurar son formatos, fuente general, fuentes de cabecera, contenido y widgets.



Figura 154. Personalizar tipografía en WordPress

En la opción “fuente general” se selecciona la fuente Source Sans Pro para la fuente general con un tamaño de 18 px y en formato normal como se muestra en la figura 155.

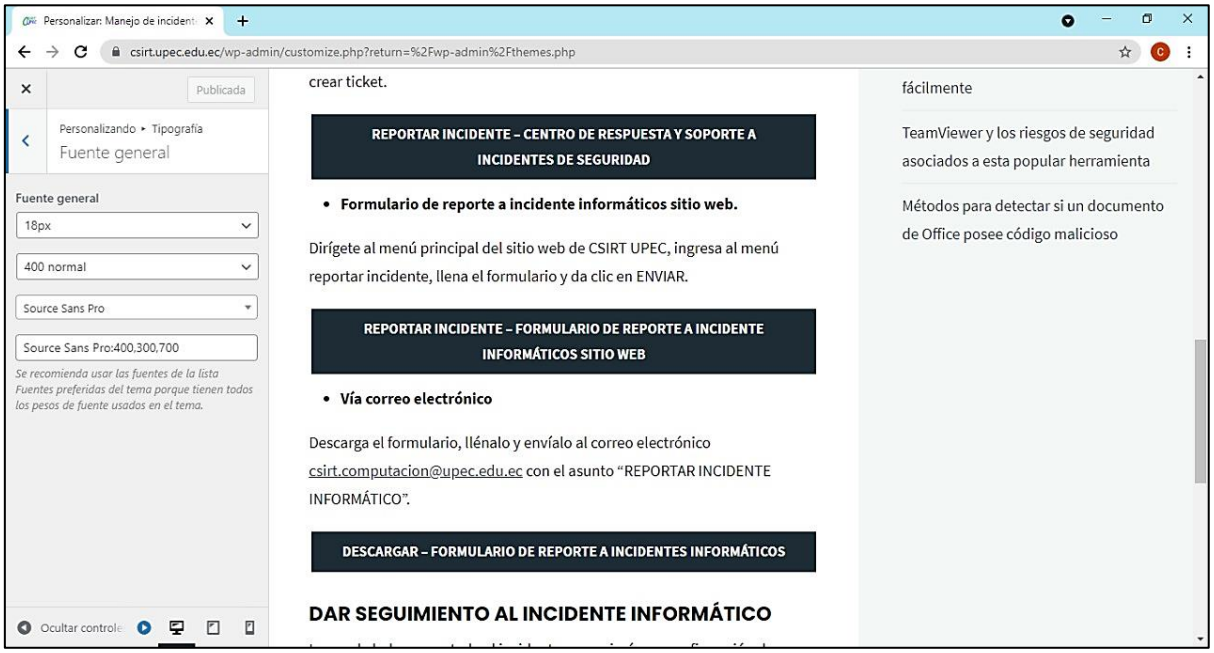


Figura 155. Definir la tipografía para la fuente general del sitio web

En la opción fuentes de la cabecera se selecciona la fuente Poppins al 110% en tamaño y 700 en formato negrita para el título del sitio; y para el menú principal se usa la fuente Source Sans Pro con un 90% de tamaño y 400 en formato normal como se observa en la figura 156.



Figura 156. Definir la tipografía para las fuentes de cabecera del sitio web

Como se muestra en la figura 157, en la opción fuentes del contenido se selecciona la fuente Poppins para los títulos de las entradas, 160% en tamaño y 700 en formato negrita, para los metadatos de la entrada se utiliza la fuente Source Sans Pro con un 90% en tamaño y 400 en formato normal; y para los encabezados se selecciona la fuente Poppins con 100% en tamaño y 700 en formato negrita.



Figura 157. Definir la tipografía para las fuentes del contenido del sitio web

Como se muestra en la figura 158, en la opción fuentes de los widgets se selecciona la fuente Poppins para los títulos, 100% en tamaño y 700 en formato negrita; y en el contenido de los widgets se utiliza la fuente Source Sans Pro con un 100% en tamaño y 400 en formato normal.

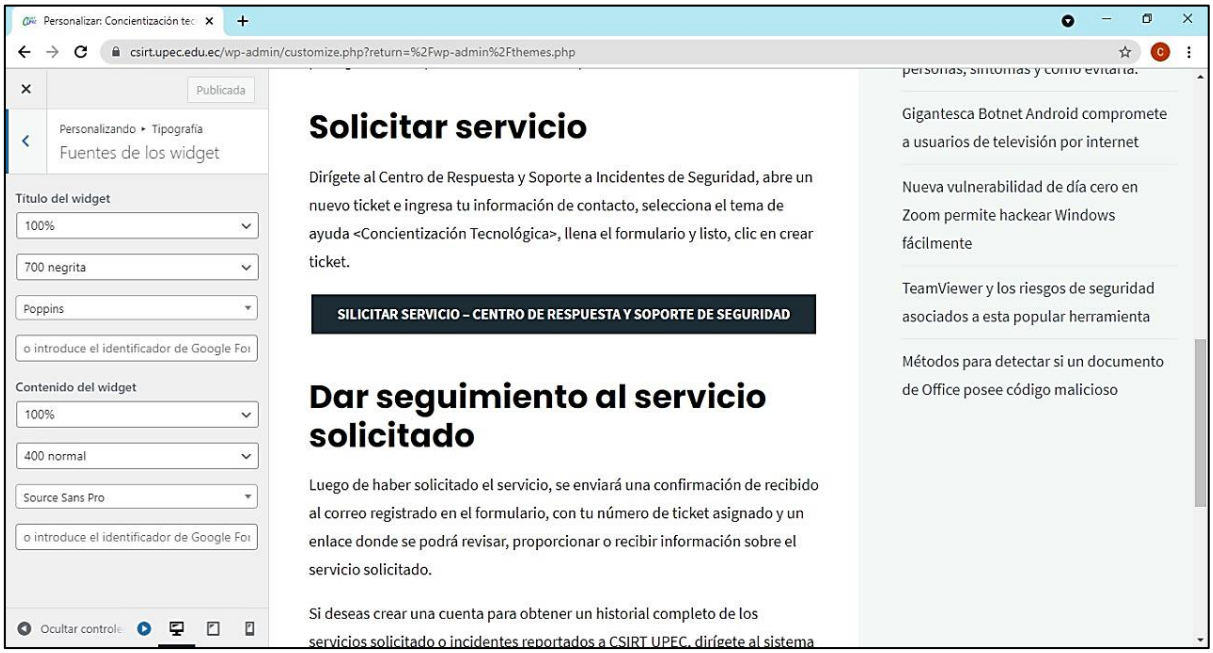


Figura 158. Definir la tipografía para las fuentes de los widgets del sitio web

En la opción formato se coloca 1.8 em en alto de línea, alineación de texto por defecto, 1 em para el espaciado de párrafos y 0 em en sangría de párrafos como se muestra en la

figura 159. Em es una unidad de medida que expresa su tamaño en puntos y es utilizada en la tipología tradicional.

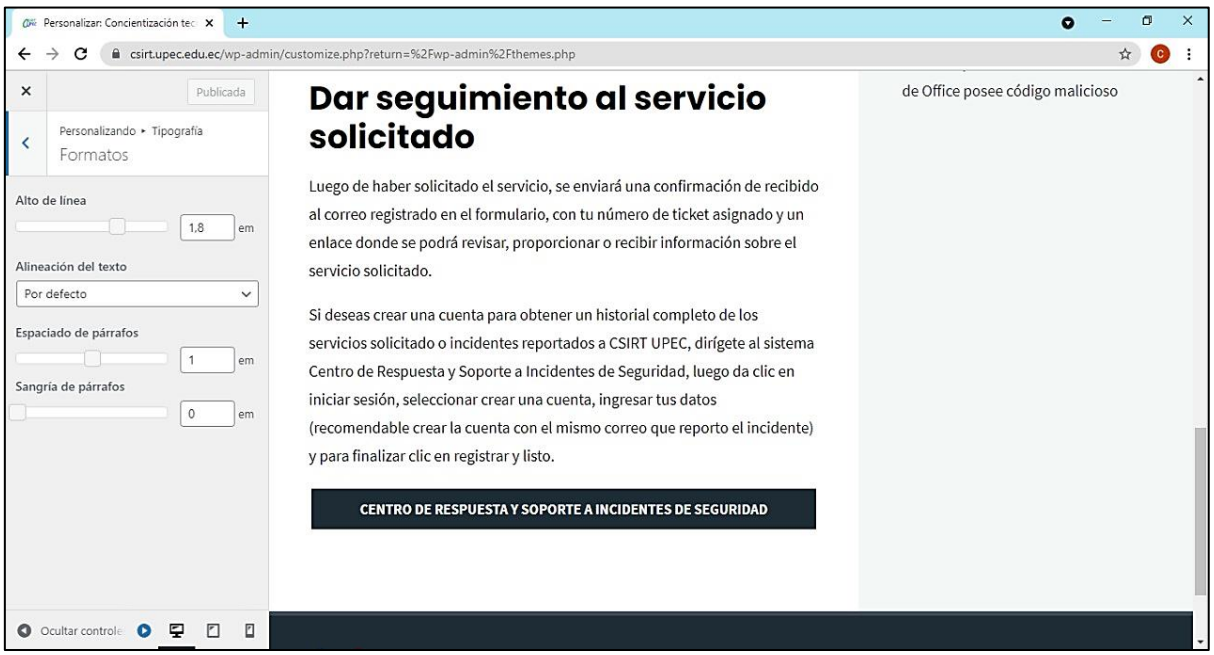


Figura 159. Definir los formatos en dimensiones para el sitio web

- **Información de las entradas**

  Como se observa en la figura 160, en el menú información de la entrada se configura y personaliza los elementos que conforman las entradas, las opciones de configuración son imagen destacada, información meta, extractos y comentarios.



Figura 160. Personalizar la información de la entrada en WordPress

En la opción imagen destacada, se activa el uso de imágenes destacadas y se establece su tamaño en 360 px, además se define el comportamiento en contenido para su escala en altas resoluciones y la posición centrada como se muestra en la figura 161.

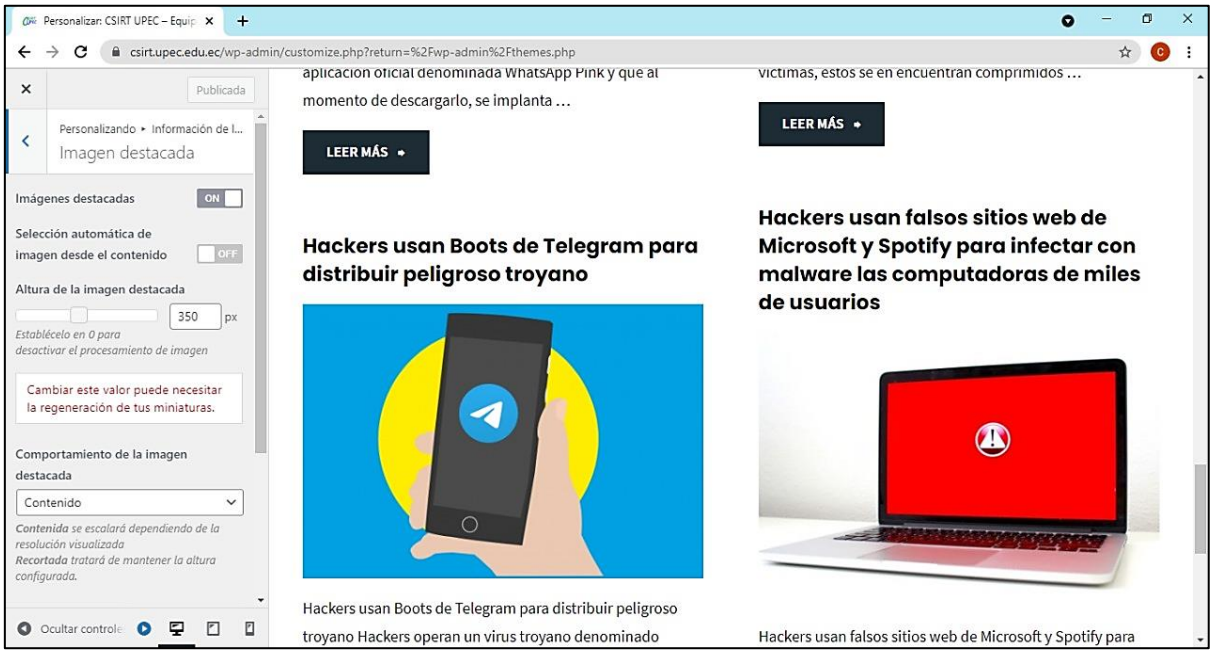


Figura 161. Definir el comportamiento de la imagen destacada para el sitio web

En la figura 162 se observa la opción información meta, donde se selecciona mostrar fecha y categoría como información que se muestra en las entradas. Información meta se compone de datos que definen un objeto en su contenido o concepto.

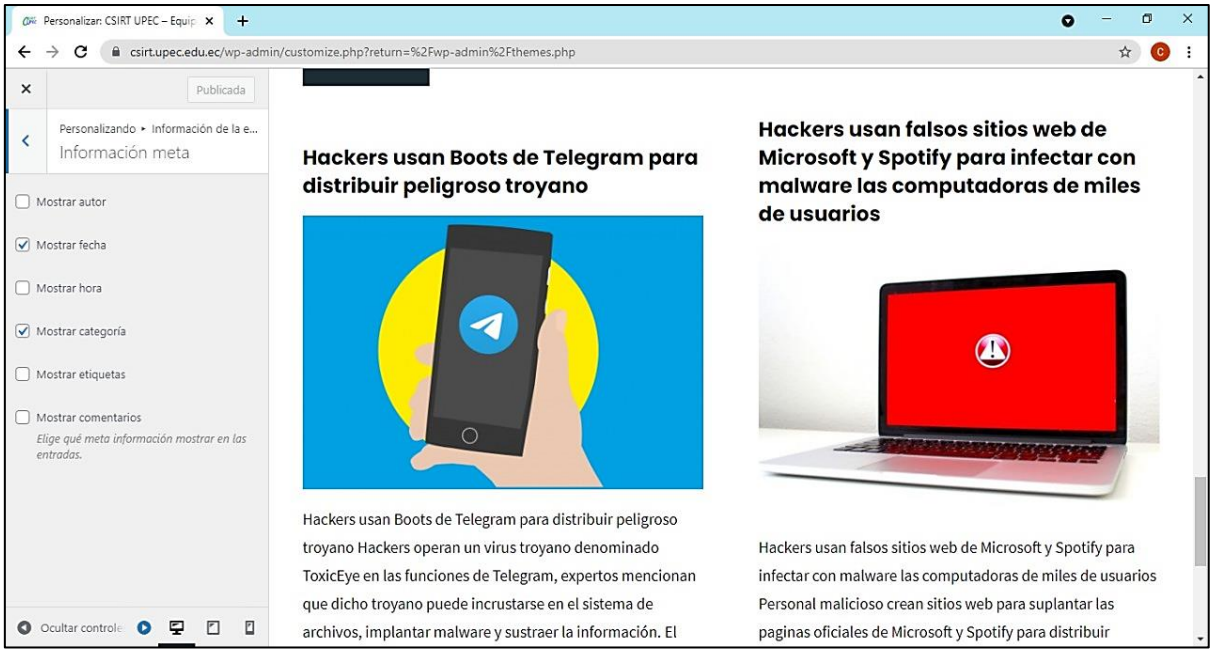


Figura 162. Definir la información meta para las entradas del sitio web

Como se observa en la figura 163, en la opción extractos se selecciona extracto para mostrar las entradas en la página de inicio, una longitud de 50 palabras, tres puntos que definen el sufijo del extracto y la etiqueta leer más para el botón que permite leer la entrada completa.

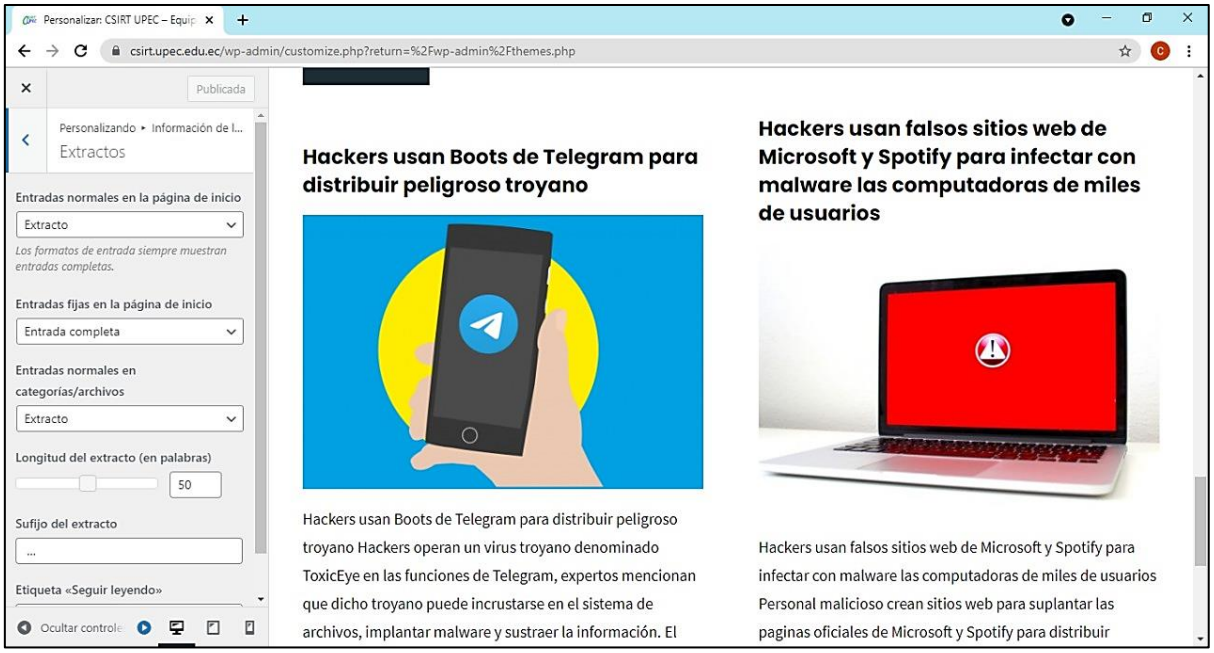


Figura 163. Activación de extracto para las entradas y establecer sus propiedades para el sitio web

Como se observa en la figura 164, en la opción comentarios se selecciona los comentarios que están cerrados para los lugares donde no se permite comentar, aplicar el formato relativo para la fecha, poner marcadores de posición para las etiquetas de los campos y establecer 250 px para el ancho del formulario de comentarios.

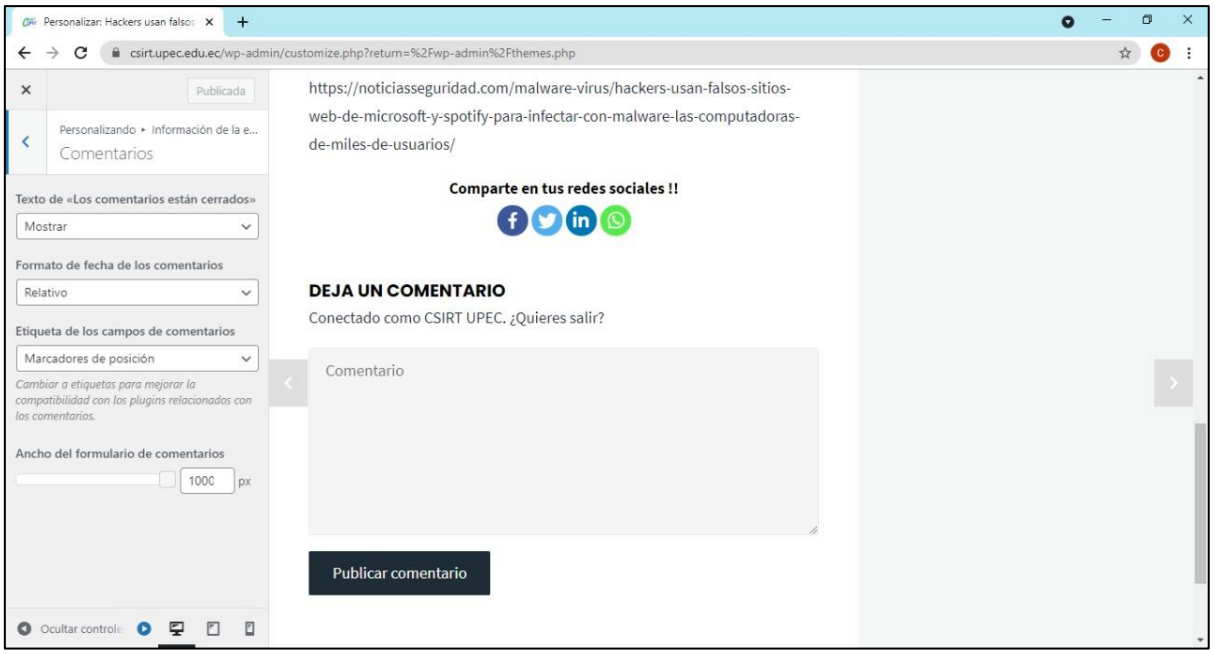


Figura 164. Definir las propiedades de los comentarios para las publicaciones del sitio web

Anexo 17 Creación y configuración vistas del sitio web

- **Página de inicio**

  Como se muestra en la figura 165, para crear la página de inicio se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título inicio, en los ajustes se establece la visibilidad como pública, plantilla del tema por defecto y clic en publicar.

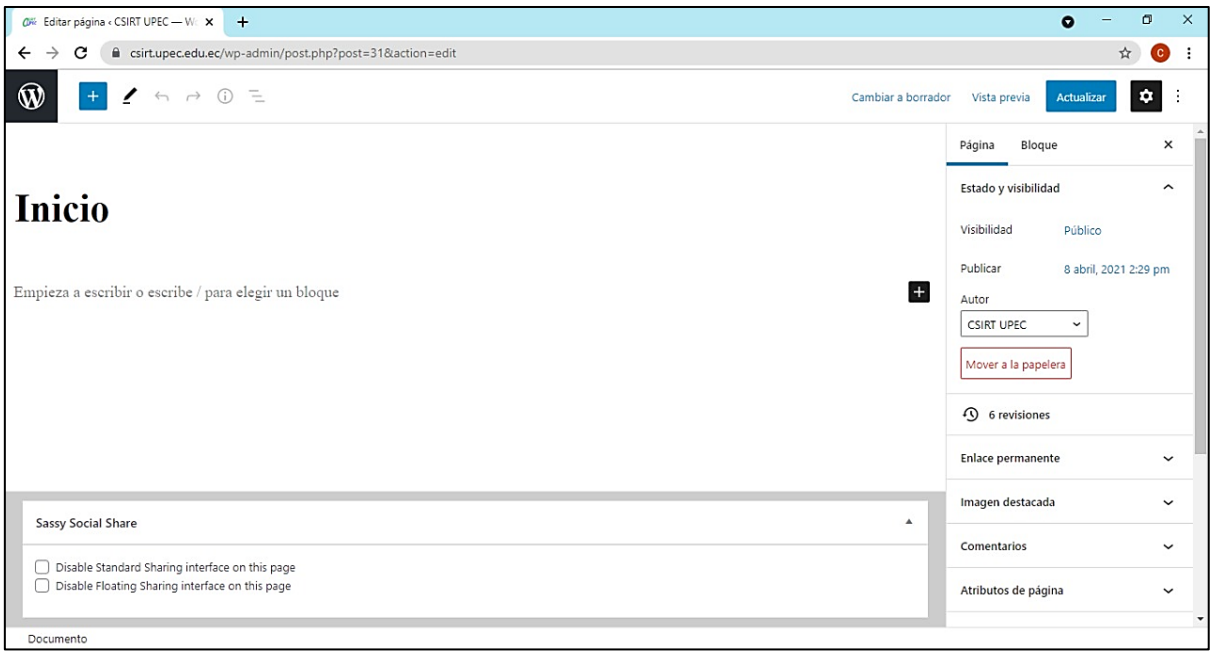


Figura 165. Crear la página de inicio para el sitio web

En el menú ajustes de portada de la personalización del tema, se define una página estática como portada y se selecciona la página creada con el nombre inicio como se muestra en la figura 166.



Figura 166. Establecer una página estática para la página de inicio del sitio web

Como se muestra en la figura 167, en el menú destino se activan los elementos que componen la página de inicio, las opciones a configurar son ajustes y carrusel.



Figura 167. Personalizar página de destino en WordPress

Como se muestra en la figura 168, en la opción página de destino se selecciona activado para permitir la personalización de la página de inicio de acuerdo a nuestros requerimientos.

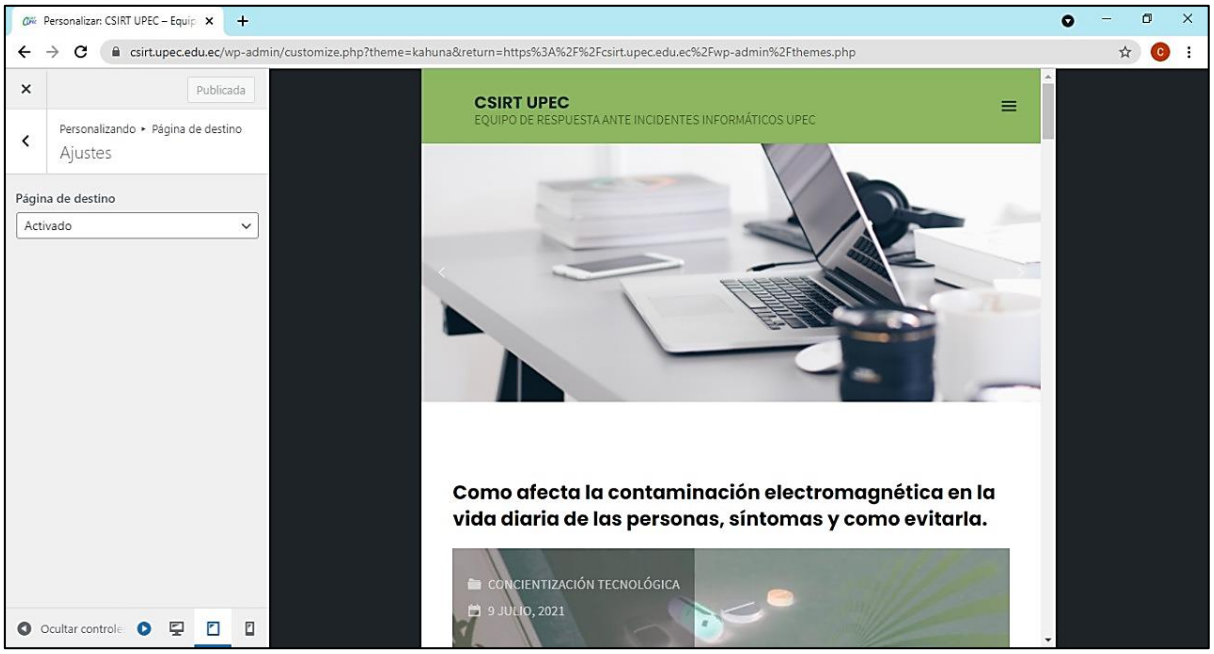


Figura 168. Activación de la página de destino personalizada para el sitio web

En la opción carrusel se selecciona la opción usar shortcode para activar el carrusel de imágenes que se visualizará en la cabecera del sitio web y se ingresa el shortcode proporcionado por el plugin instalado para su configuración. Shortcode es un fragmento de código para la inserción de contenido para el sitio web, como se observa en la figura 169.



Figura 169. Activación del carrusel con el uso de shortcode para el sitio web

En el menú de navegación WordPress, se da clic en el complemento Smart Slider y se elige la opción nuevo proyecto, en el tablero de configuración, se da clic en agregar diapositiva para añadir las imágenes del carrusel como se muestra en la figura 170.

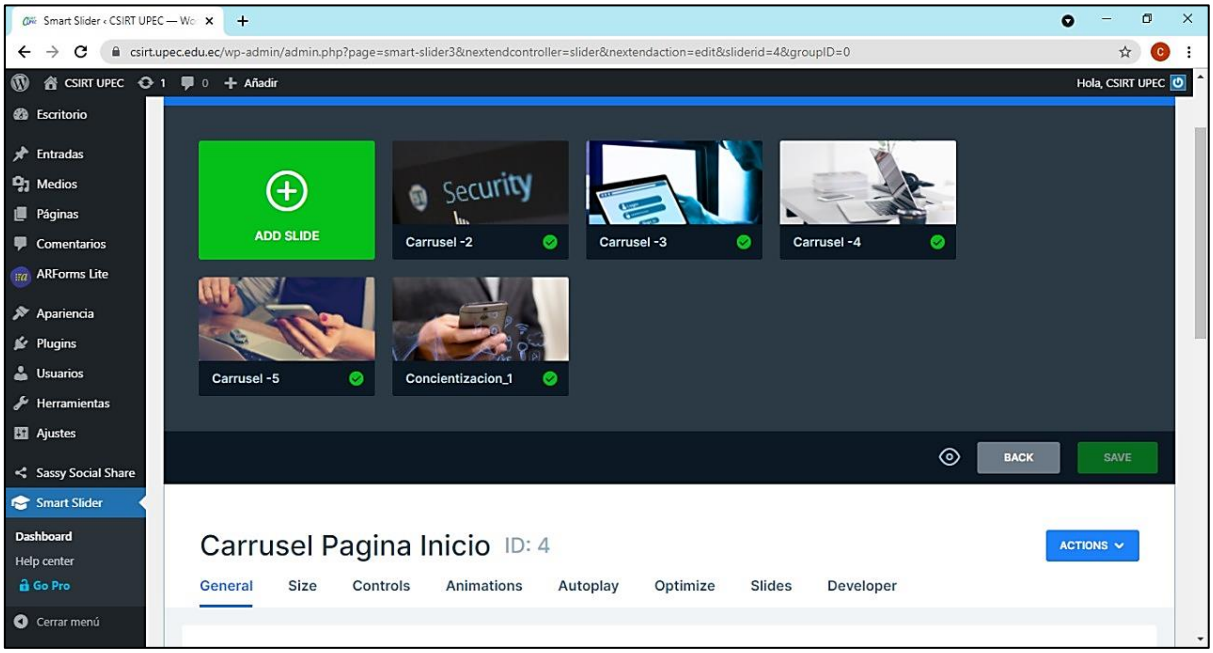


Figura 170. Agregar contenido multimedia para el carrusel ubicado en la página de inicio

En las opciones del carrusel se establece 1200 px para su ancho y con altura de 500 px, con un diseño de ancho completo, se activa las flechas para movilizarse por las

imágenes, su animación principal es horizontal y con una duración de cambio de 500 milisegundos (ms)

En la opción contenido destacado se selecciona la visualización de las entradas para el cuerpo de la página inicio como se muestra en la figura 171.

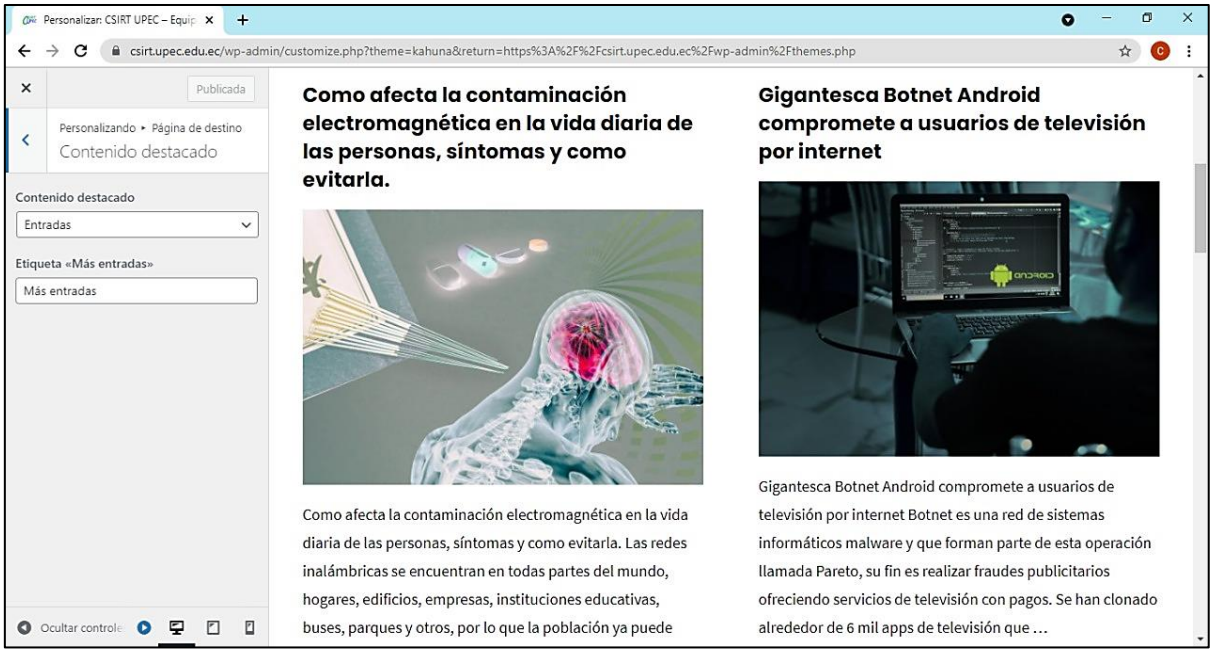


Figura 171. Activar entradas como contenido destacado para el cuerpo de la página de inicio del sitio web

Como se muestra en la figura 172, se tiene el resultado de la página de inicio, en la cabecera se encuentra el carrusel y en el cuerpo las entradas estructuradas en dos columnas.

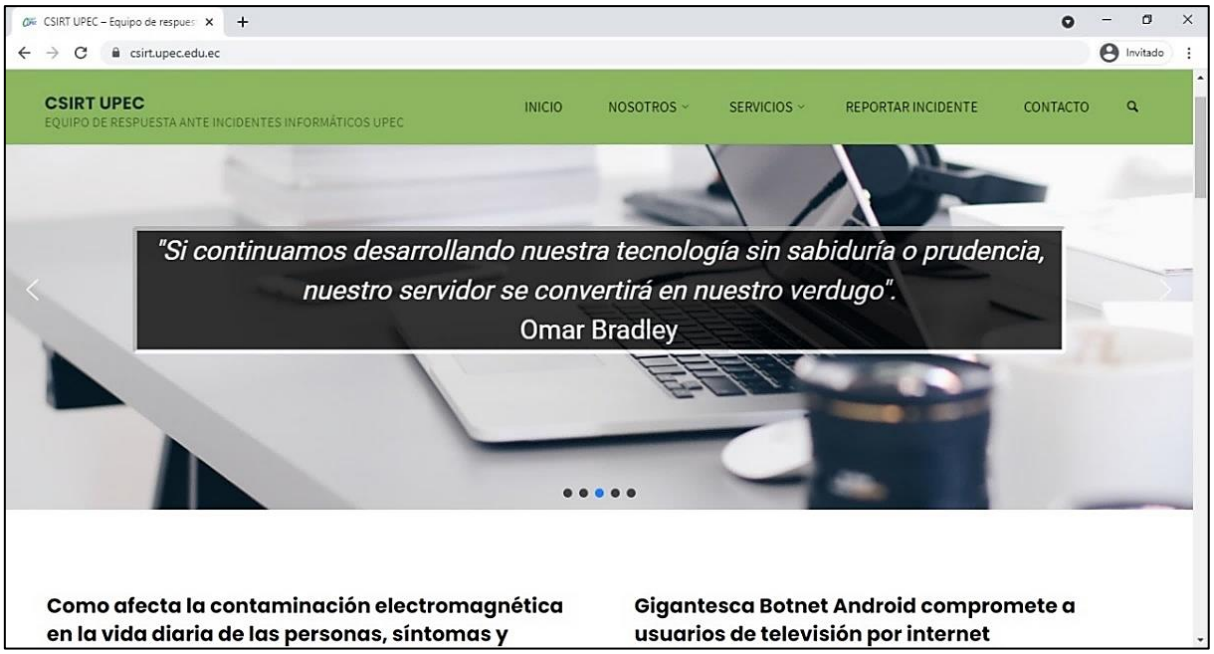


Figura 172. Vista previa de la página de inicio

- **Página de servicios**

  Como se muestra en la figura 173, para crear la página de servicios se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título servicios, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo servicios y en su configuración se selecciona el nivel de encabezado H2 , el bloque párrafo para colocar la descripción correspondiente a los servicios, el bloque lista para nombrar los servicios en viñetas y para añadir el enlace que direcciona a la página de contacto para solicitar información o el servicio, se selecciona la palabra aquí y en la configuración del bloque se selecciona el enlace, se coloca la dirección URL de la página de destino y se habilita la casilla abrir el enlace en una pestaña nueva.



Figura 173. Selección de bloques para la estructura de la página servicios del sitio web

Como se muestra en la figura 174, en el menú ajustes de página, se establece la visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.



Figura 174. Configuración de la página servicios para su publicación en el sitio web

Como se muestra en la figura 175, para visualizar el resultado de la ubicación del contenido y sus configuraciones se da clic en vista previa.



Figura 175. Vista previa de la página de servicios

- **Página de alertas y avisos**

  Como se muestra en la figura 176, para crear la página de alertas y avisos se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título alertas y avisos, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo alertas y avisos y en su configuración se selecciona el nivel de encabezado H2.

  Con el bloque de galería se añaden las imágenes que se relacionan con la temática del servicio, en su configuración se establece la visualización de las imágenes en tres columnas y se activa la opción recortar en un tamaño medio y bloque párrafo, donde se ingresa la descripción del servicio y se incorpora el enlace de la página de contacto para pedir información o solicitar el servicio; se selecciona la palabra aquí, clic en enlace, colocamos la URL de la página de destino y se activa la casilla abrir el enlace en una pestaña nueva.



Figura 176. Selección de bloques para la estructura de la página alertas y avisos del sitio web

Como se muestra en la figura 177, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

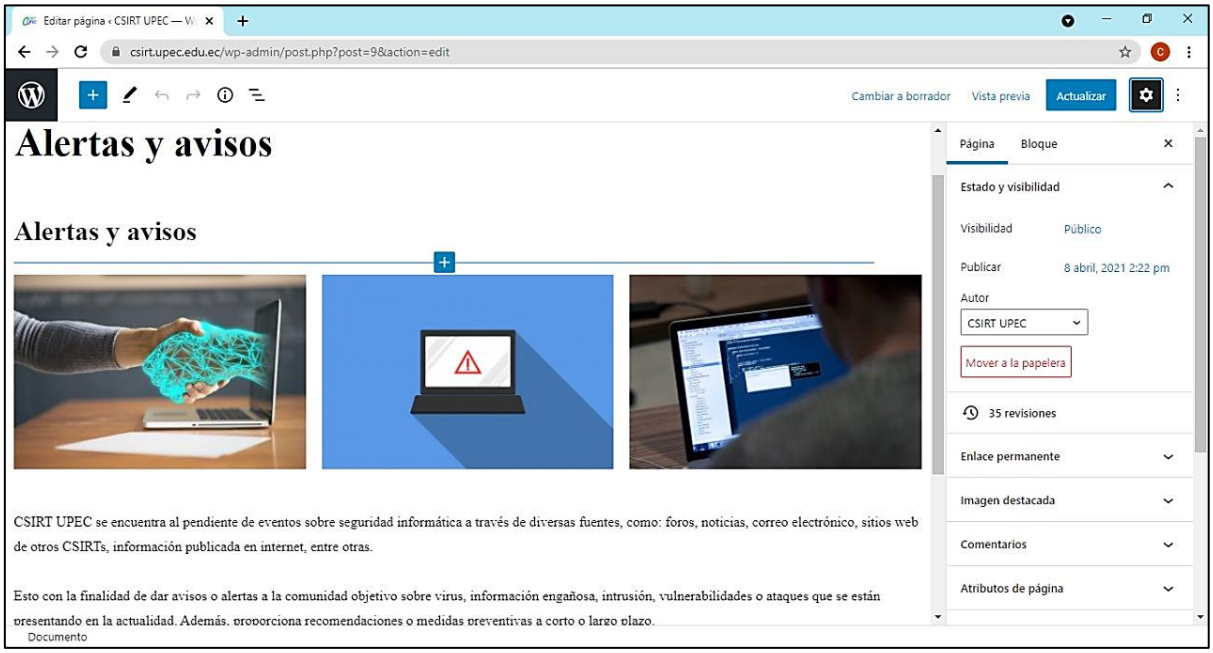


Figura 177. Configuración de la página alertas y avisos para su publicación en el sitio web

Se da clic en vista previa del editor de página de alertas y avisos para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 178.

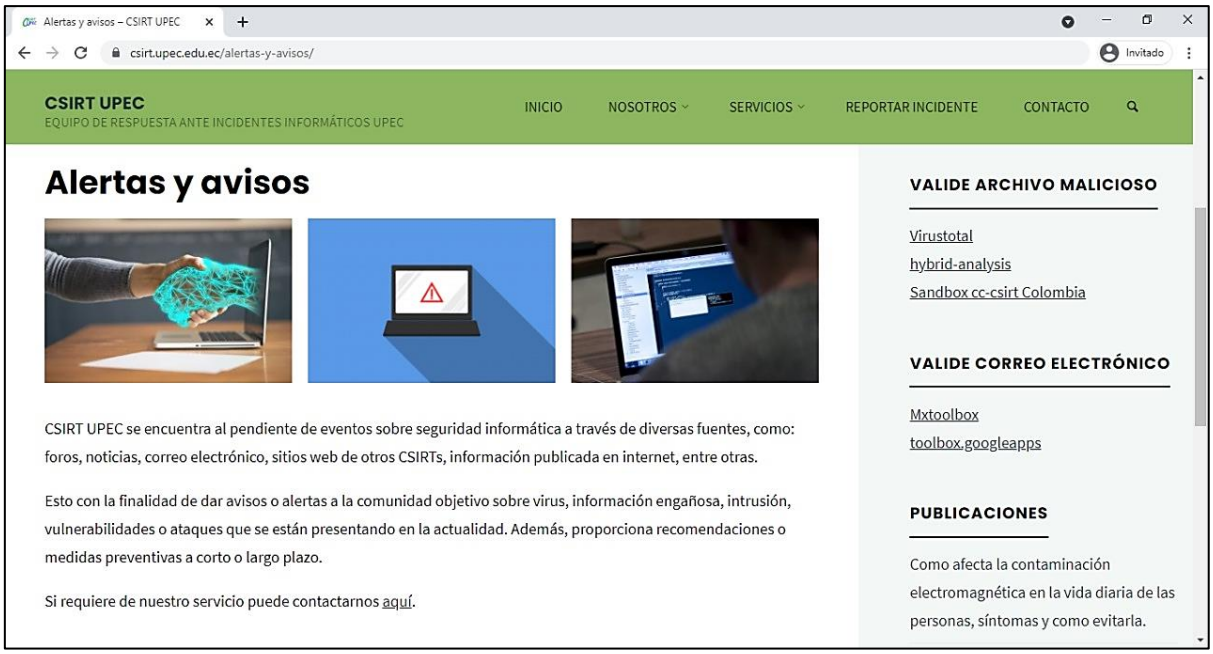


Figura 178. Vista previa de la página de alertas y avisos

- **Página de manejo de incidentes**

  Como se muestra en la figura 179, para crear la página manejo de incidentes se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título manejo de incidentes, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo manejo de incidentes y en su configuración se selecciona el nivel de encabezado H2.

  Con el bloque de galería se añaden las imágenes que se relacionan con la temática del servicio, en su configuración se establece la visualización de las imágenes en tres columnas y se activa la opción recortar en un tamaño medio y bloque párrafo, donde se ingresa la descripción del servicio y se incorpora el enlace de la página de contacto para pedir información o solicitar el servicio; se selecciona la palabra aquí, clic en enlace, colocamos la URL de la página de destino y se activa la casilla abrir el enlace en una pestaña nueva.



Figura 179. Selección de bloques para la estructura de la página manejo de incidentes del sitio web

Como se muestra en la figura 180, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

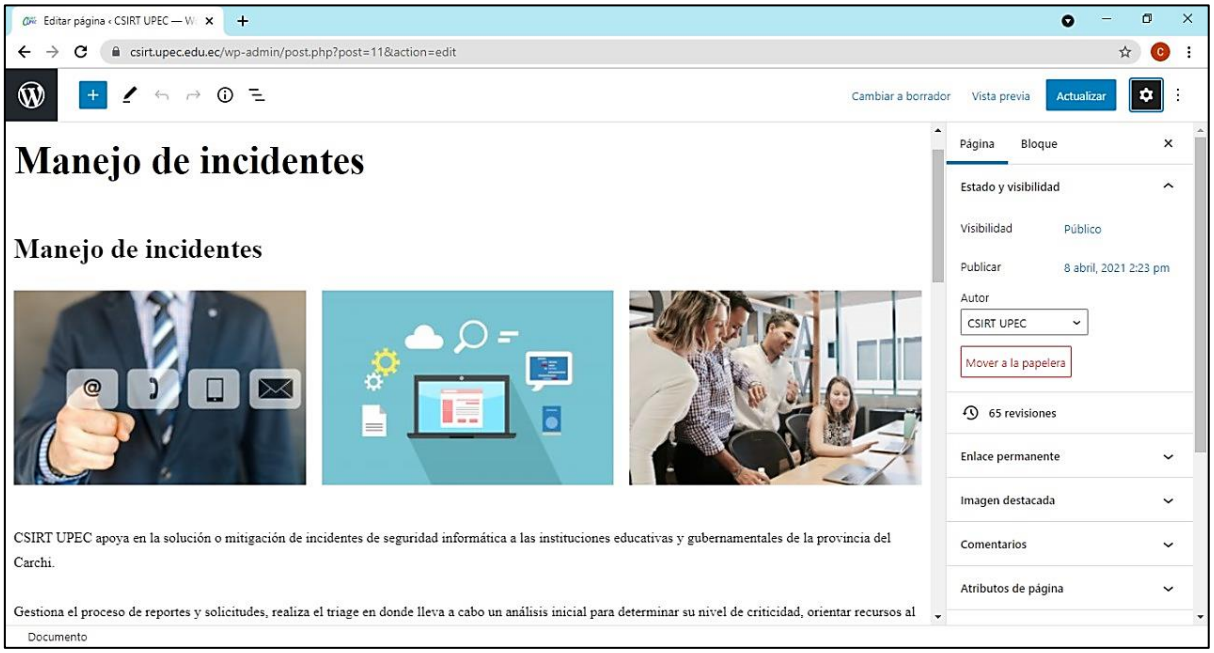


Figura 180. Configuración de la página manejo de incidentes para su publicación en el sitio web

Se da clic en vista previa del editor de página manejo de incidentes para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 181.



Figura 181. Vista previa de la página de manejo de incidentes

- **Página de anuncios**

  Como se muestra en la figura 182, para crear la página anuncios se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título anuncios, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo anuncios y en su configuración se selecciona el nivel de encabezado H2.

  Con el bloque de galería se añaden las imágenes que se relacionan con la temática del servicio, en su configuración se establece la visualización de las imágenes en tres columnas y se activa la opción recortar en un tamaño medio y bloque párrafo, donde se ingresa la descripción del servicio y se incorpora el enlace de la página de contacto para pedir información o solicitar el servicio; seleccionamos la palabra aquí, clic en enlace, colocamos la URL de la página de destino y se activa la casilla abrir el enlace en una pestaña nueva.

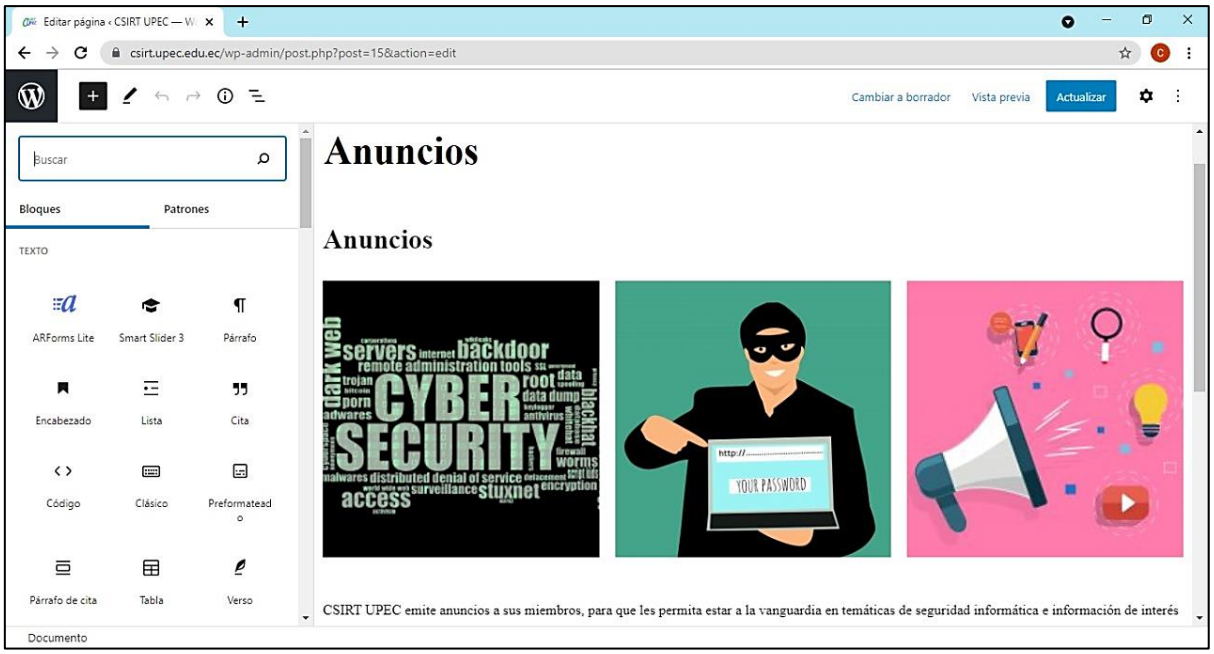


Figura 182. Selección de bloques para la estructura de la página anuncios del sitio web

Como se muestra en la figura 183, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

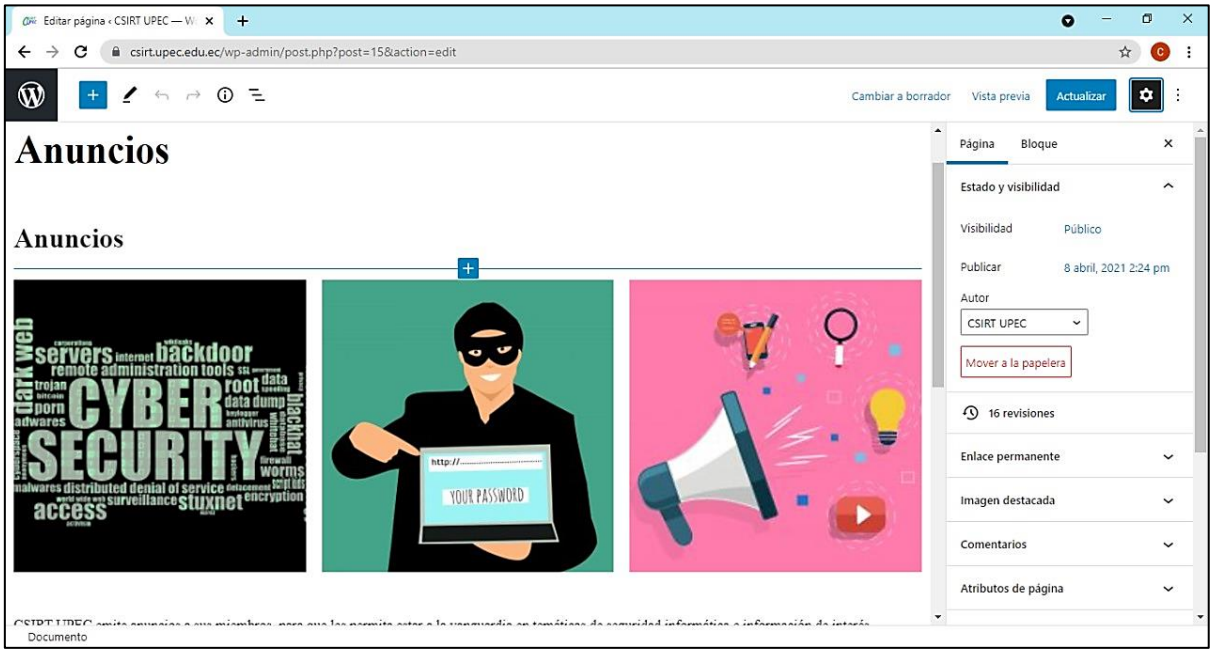


Figura 183. Configuración de la página anuncios para su publicación en el sitio web

Se da clic en vista previa del editor de la página anuncios para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 184.

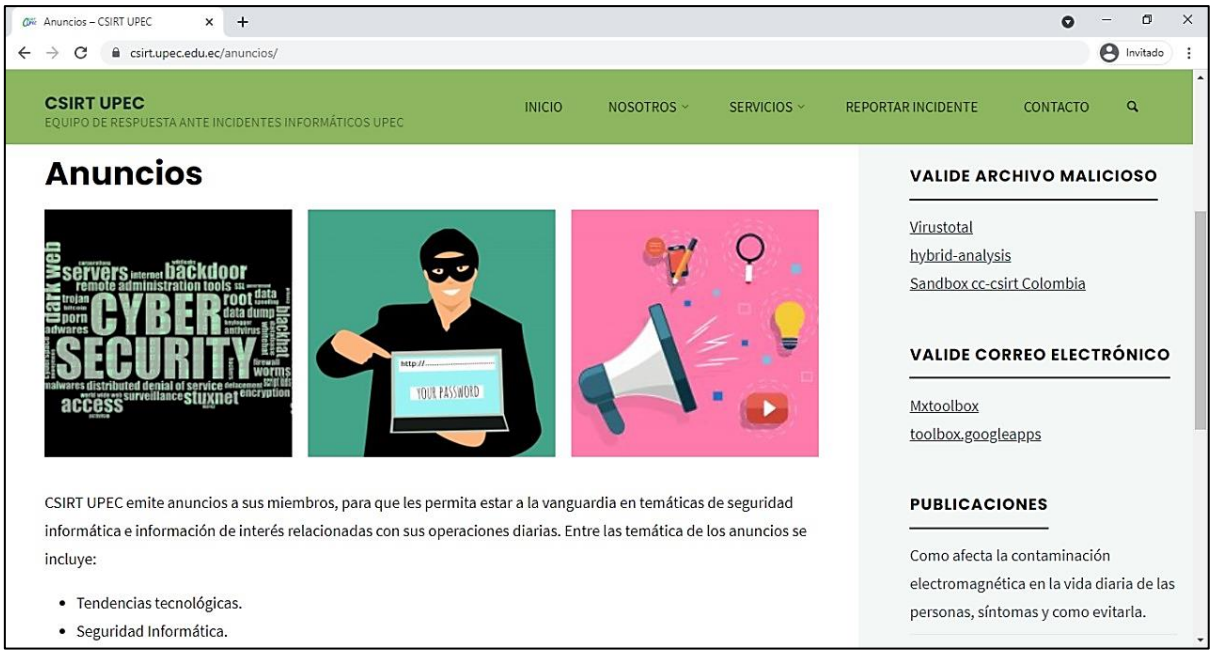


Figura 184. Vista previa de la página de anuncios

- **Página de concientización tecnológica**

  Como se muestra en la figura 185, para crear la página concientización tecnológica se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título concientización tecnológica, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo concientización tecnológica y en su configuración se selecciona el nivel de encabezado H2.

  Con el bloque de galería se añaden las imágenes que se relacionan con la temática del servicio, en su configuración se establece la visualización de las imágenes en tres columnas y se activa la opción recortar en un tamaño medio y bloque párrafo, donde se ingresa la descripción del servicio y se incorpora el enlace de la página de contacto para pedir información o solicitar el servicio; se selecciona la palabra aquí, clic en enlace, colocamos la URL de la página de destino y se activa la casilla abrir el enlace en una pestaña nueva.



Figura 185. Selección de bloques para la estructura de la página concientización tecnológica del sitio web

Como se muestra en la figura 186, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.



Figura 186. Configuración de la página concientización tecnológica para su publicación en el sitio web

Se da clic en vista previa del editor de página concientización tecnológica para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 187.



Figura 187. Vista previa de la página de concientización tecnológica

- **Página de reportar incidente**

  Como se muestra en la figura 188, para crear la página reportar incidente se da clic en el menú página y seleccionamos la opción añadir nueva, se muestra el editor de página donde se define el título reportar incidente, en la biblioteca de bloques se selecciona el bloque shortcode y pegamos el código corto de identificación del formulario “reportar incidente de seguridad informática” brindado por el plugin ARForms.



Figura 188. Incluir shortcode del formulario reportar incidente de seguridad informática en la página reportar incidente

Como se muestra en la figura 189, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

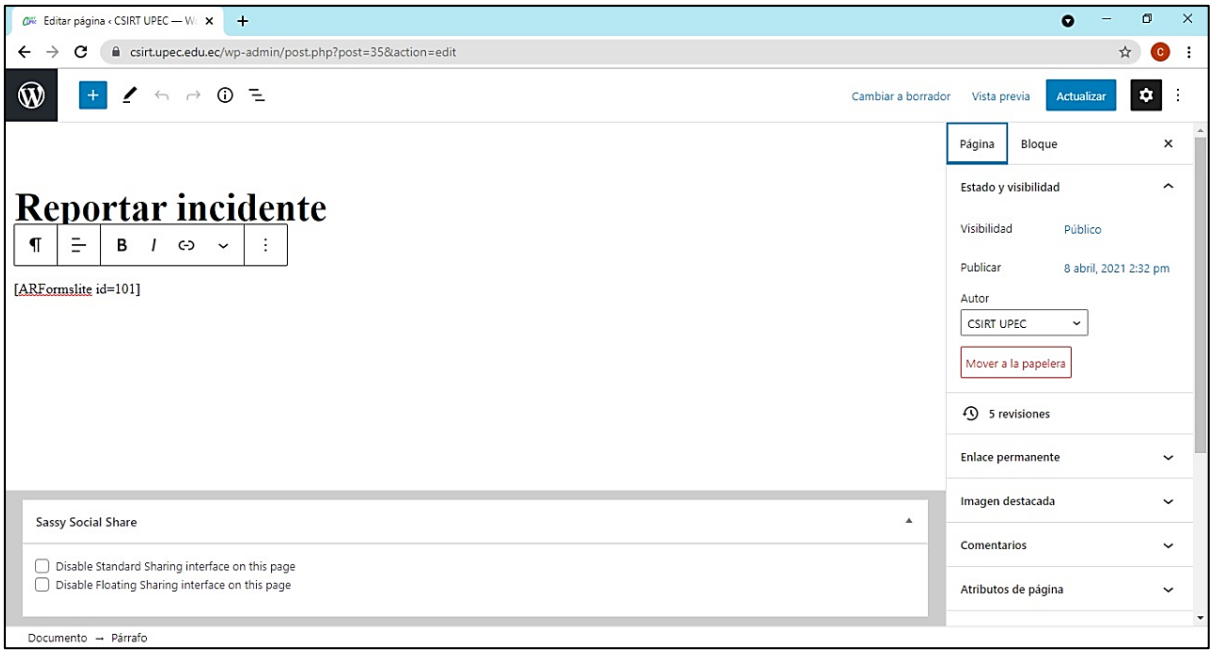


Figura 189. Configuración de la página reportar incidente para su publicación en el sitio web

Se da clic en vista previa del editor de página reportar incidente para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 190.

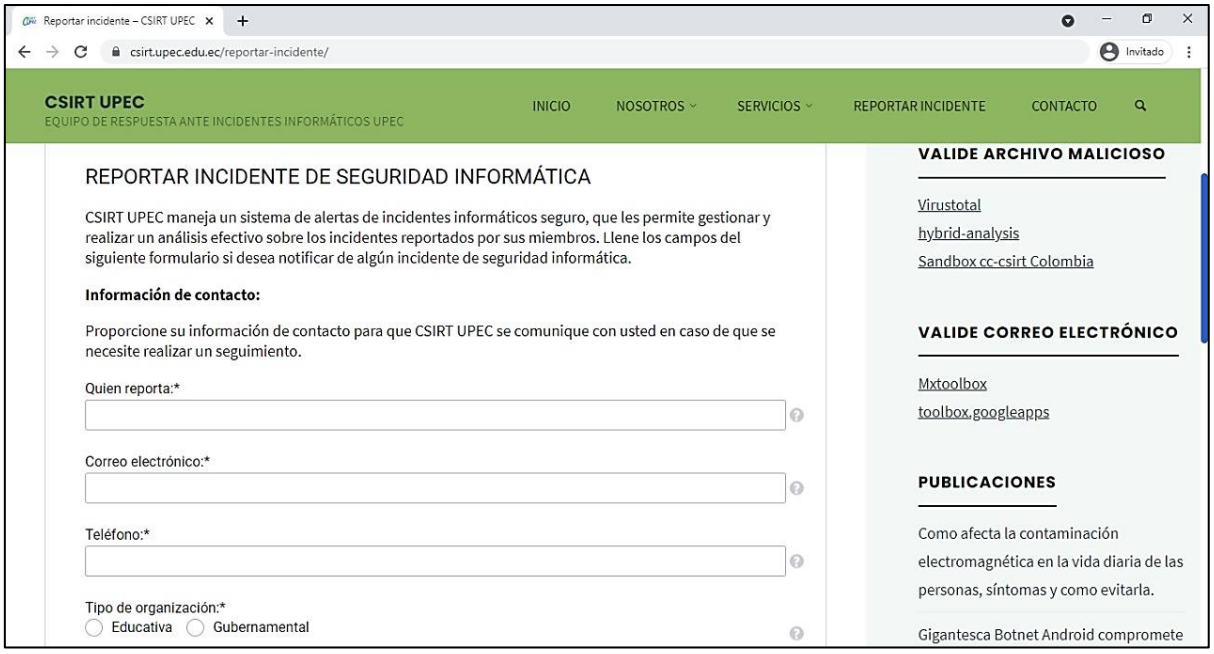


Figura 190. Vista previa de la página de reportar incidente

- **Página de política de privacidad**

  Como se muestra en la figura 191, para crear la página de política de seguridad se da clic en el menú página y seleccionamos la opción añadir nueva, se muestra el editor de página donde se define el título página de política de seguridad, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo política de seguridad y en su configuración se selecciona el nivel de encabezado H2 y el bloque párrafo donde se ingresa las descripciones de cada ítem.



Figura 191. Selección de bloques para la estructura de la página política de privacidad

Como se muestra en la figura 192, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

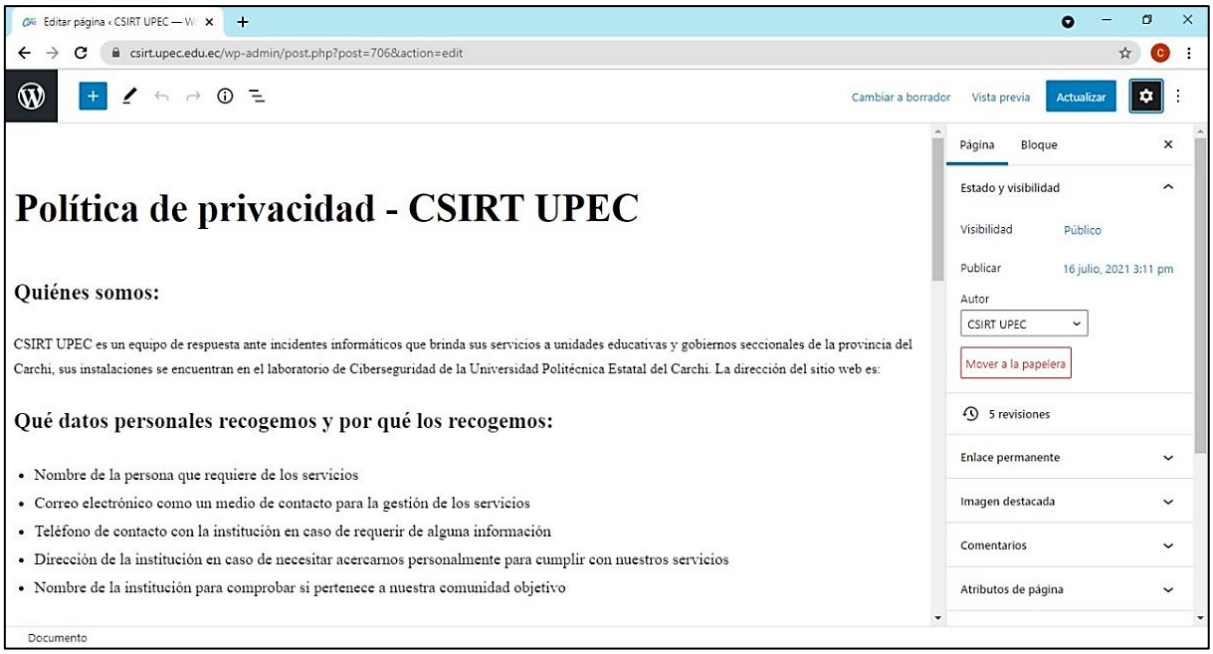


Figura 192. Configuración de la página política de privacidad - CSIRT UPEC para su publicación en el sitio web

Se da clic en vista previa del editor de página de política de privacidad CSIRT UPEC para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 193.



Figura 193. Vista previa de la página política de privacidad

- **Página de nosotros**

  Como se muestra en la figura 194, para crear la página nosotros se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se

define el título nosotros, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo nosotros y en su configuración se selecciona el nivel de encabezado H2.

Se selecciona el bloque columna y en su configuración incorporamos dos bloques internos, el bloque de imagen con alineación a la izquierda y activamos la opción recortar en un tamaño medio y seleccionamos el bloque párrafo donde se ingresa la descripción del servicio.



Figura 194. Selección de bloques para la estructura de la página nosotros del sitio web

Como se muestra en la figura 195, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.



Figura 195. Configuración de la página nosotros para su publicación en el sitio web

Se da clic en vista previa del editor de página nosotros para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 196.



Figura 196. Vista previa de la página nosotros

- **Página de contacto**

  Como se muestra en la figura 197, para crear la página de contacto se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se

define el título contacto, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo contacto y en su configuración se selecciona el nivel de encabezado H2.

Se selecciona el bloque columna y en su configuración se elige dos columnas, para el apartado izquierdo se elige el bloque párrafo donde se describe la información sobre las formas de contacto con CSIRT UPEC y en el apartado derecho se selecciona el bloque HTML personalizado, donde se ingresa el código proporcionado por Google Maps para incrustar mapas con una dirección en específico.



Figura 197. Selección de bloques para la estructura de la página contacto del sitio web

Como se muestra en la figura 198, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

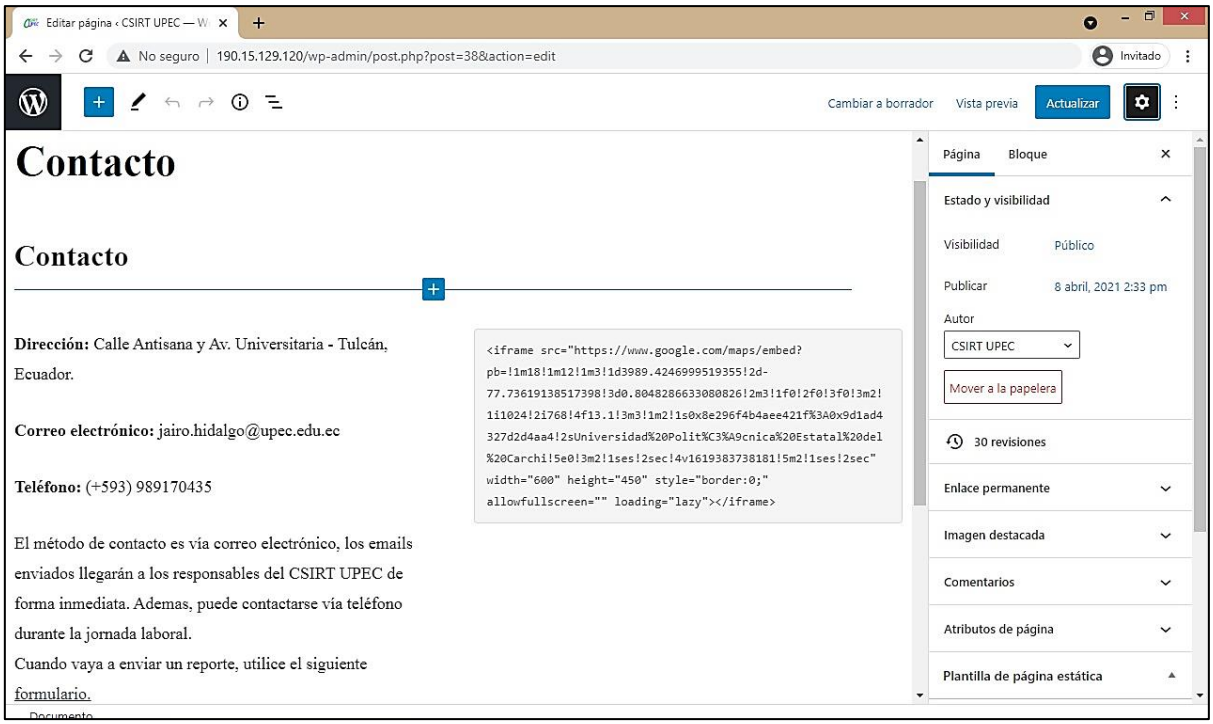


Figura 198. Configuración de la página contacto para su publicación en el sitio web

Se da clic en vista previa del editor de página de contacto para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 199.

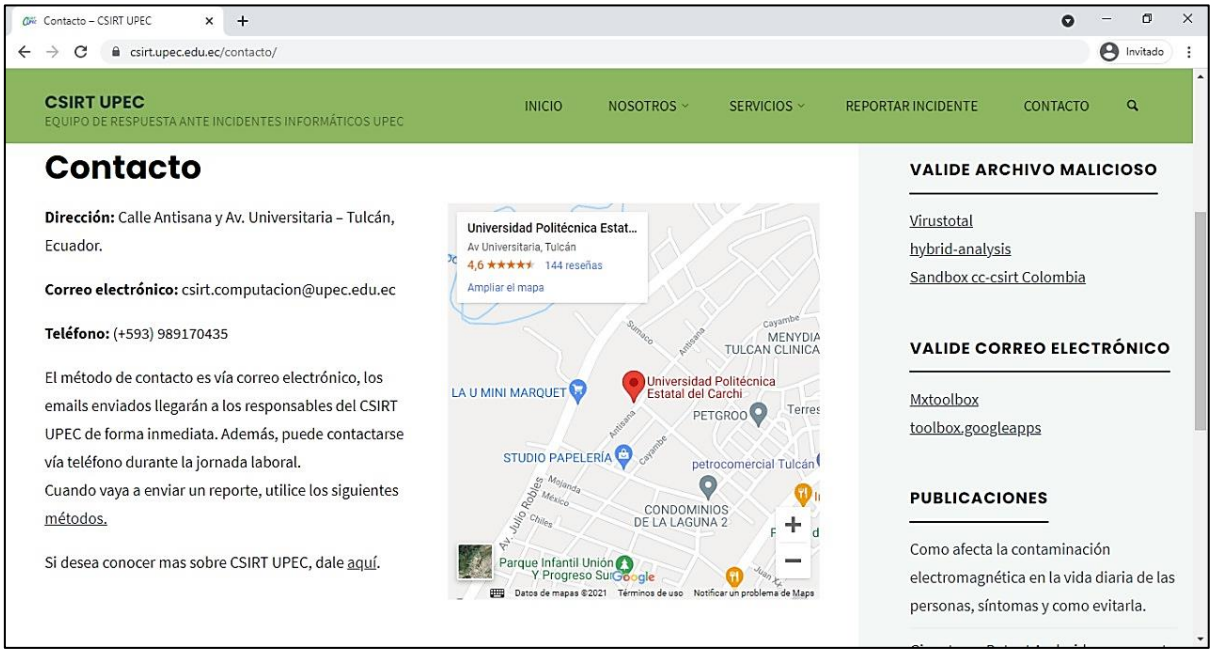


Figura 199. Vista previa de la página de contacto

Como se muestra en la figura 200, para crear la página norma RFC 2350 se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página

donde se define el título norma RFC 2350, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo norma RFC 2350 y en su configuración se selecciona el nivel de encabezado H2. Se selecciona el bloque párrafo para colocar las descripciones y el bloque tabla para colocar la información del equipo.



Figura 200. Selección de bloques para la estructura de la página norma RFC 2350 del sitio web

Como se muestra en la figura 201, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.

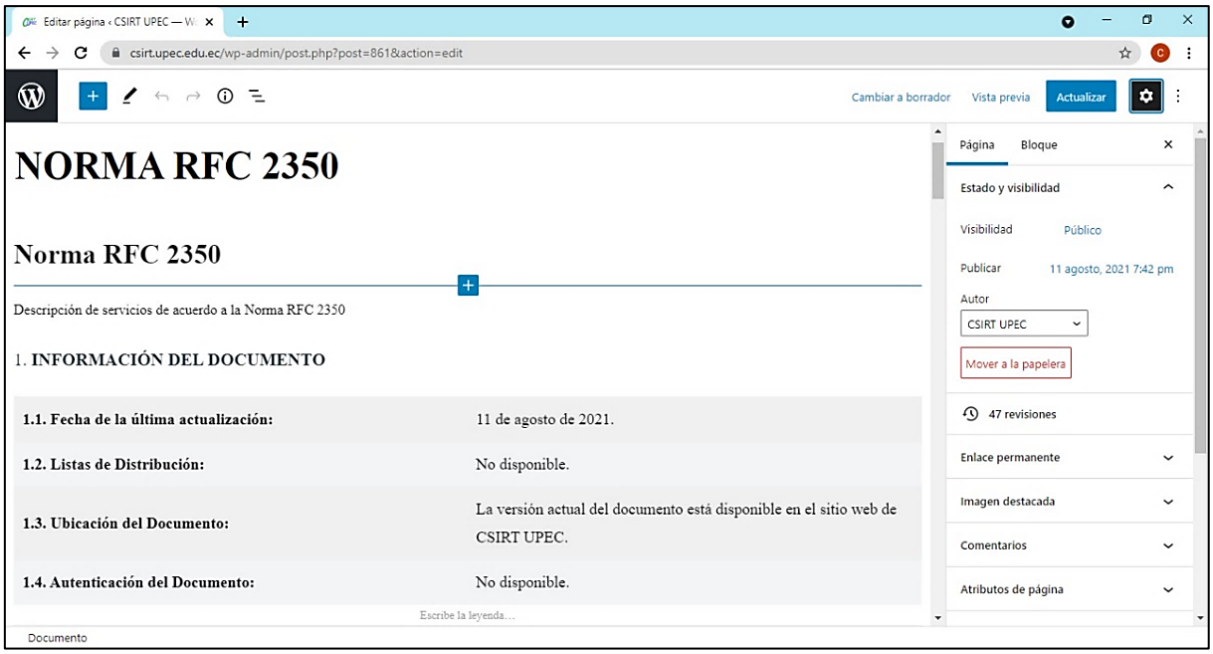


Figura 201. Configuración de la página norma RFC 2350 para su publicación en el sitio web

Se da clic en vista previa del editor de página norma RFC 2350 para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 202.



Figura 202. Vista previa de la página norma RFC 2350

Como se muestra en la figura 203, para crear la página manuales se da clic en el menú página y se selecciona la opción añadir nueva, se muestra el editor de página donde se define el título “manuales”, en la biblioteca de bloques se selecciona el bloque

encabezado para colocar el subtítulo manuales y en su configuración se selecciona el nivel de encabezado H2. Se selecciona el bloque párrafo para colocar las descripciones y el bloque lista para colocar la información de los integrantes del equipo que aprobó el manual.

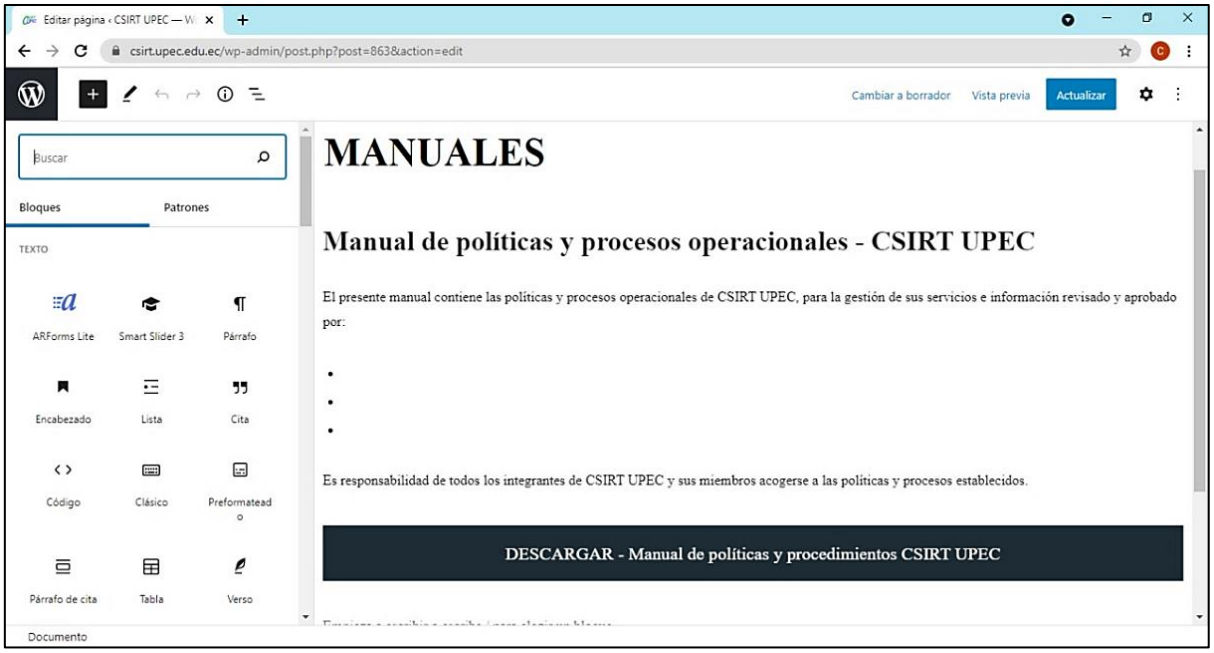


Figura 203. Selección de bloques para la estructura de la página manuales del sitio web

Como se muestra en la figura 204, en el menú ajustes de página, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor y clic en publicar.



Figura 204. Configuración de la página manuales para su publicación en el sitio web

Se da clic en vista previa del editor de página manuales para mostrar el formato del contenido y sus respectivas configuraciones como resultado que se muestra en la figura 205.



Figura 205. Vista previa de la página manuales

- **Administrador de páginas**

  Como se muestra en la figura 206, en el administrador de páginas se muestra todas las páginas creadas para el sitio web con su título, autor y fecha de publicación, además, se puede realizar búsquedas personalizadas, añadir nuevas páginas, editarlas y borrarlas.

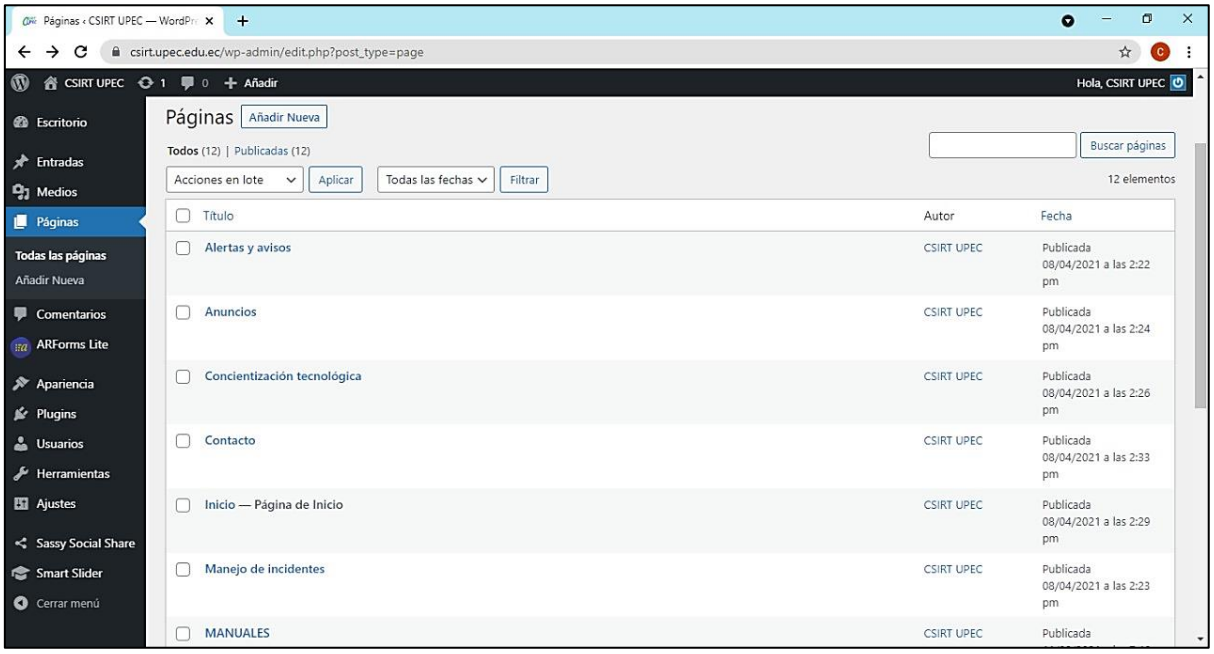


Figura 206. Lista de páginas creadas para el sitio web en el administrador de páginas

- **Entradas**

  Como se muestra en la figura 207, para crear una entrada se da clic en el menú entrada, se selecciona la opción añadir nueva, se muestra el editor de entradas donde se define su título, en la biblioteca de bloques se selecciona el bloque encabezado para colocar el subtítulo y en su configuración se selecciona el nivel de encabezado H2.

  Con el bloque imagen se añade el contenido multimedia, en su configuración se activa la opción recortar en un tamaño medio y bloque párrafo donde se ingresa la descripción del anuncio.



Figura 207. Crear entradas para el sitio web

Como se muestra en la figura 208, en el menú ajustes de entrada, se configura su visibilidad como pública, modo de publicación al instante, CSIRT UPEC como el autor, se establece las categorías a las que pertenece, una imagen destacada y sus etiquetas que hacen referencia a la temática de la entrada, se activa la casilla permitir comentarios y clic en publicar.



Figura 208. Configuración de las entradas para su publicación en el sitio web

En la figura 209 se muestra la vista previa en el editor de las entradas y como resultado del texto en el título, contenido y la imagen con las configuraciones aplicadas.

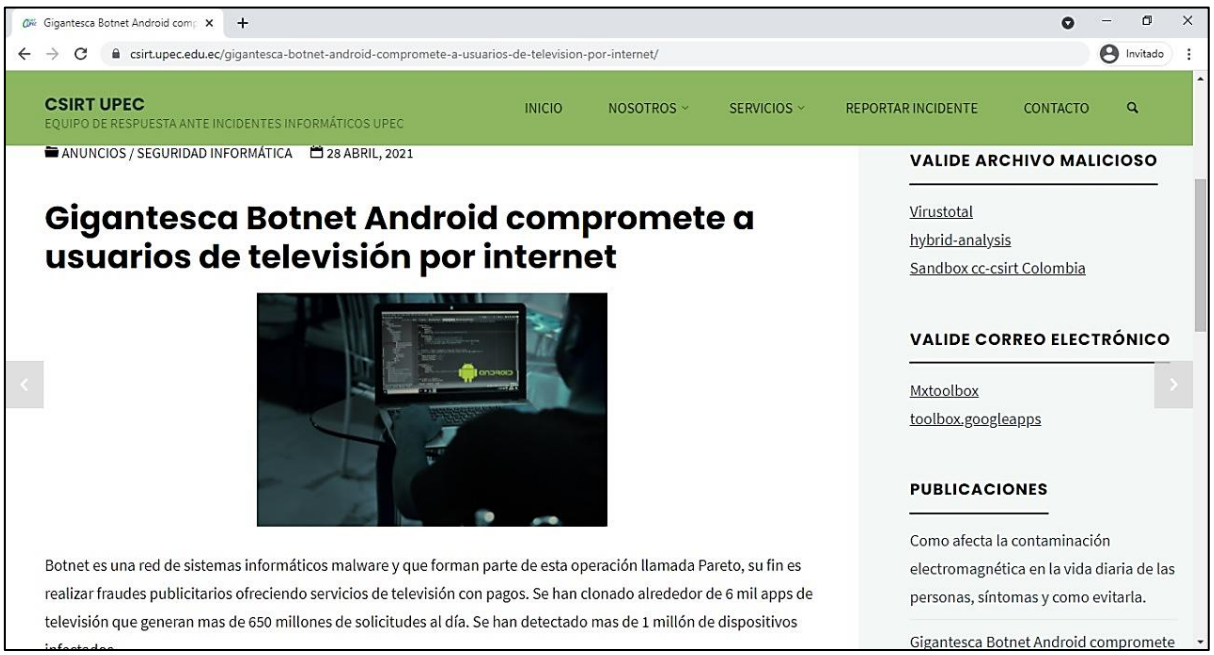


Figura 209. Vista Previa de las entradas publicadas en el sitio web

En el administrador de entradas se muestran todas las entradas realizadas, el título, autor, la o las categorías a las que pertenecen, etiquetas que permiten ser el resultado entre búsquedas similares y su fecha de publicación, se realiza búsquedas por filtros o nombres y se realizan las acciones de editar y eliminar, y en la parte superior se encuentra añadir nueva para crear una nueva entrada como se muestra en la figura 210.

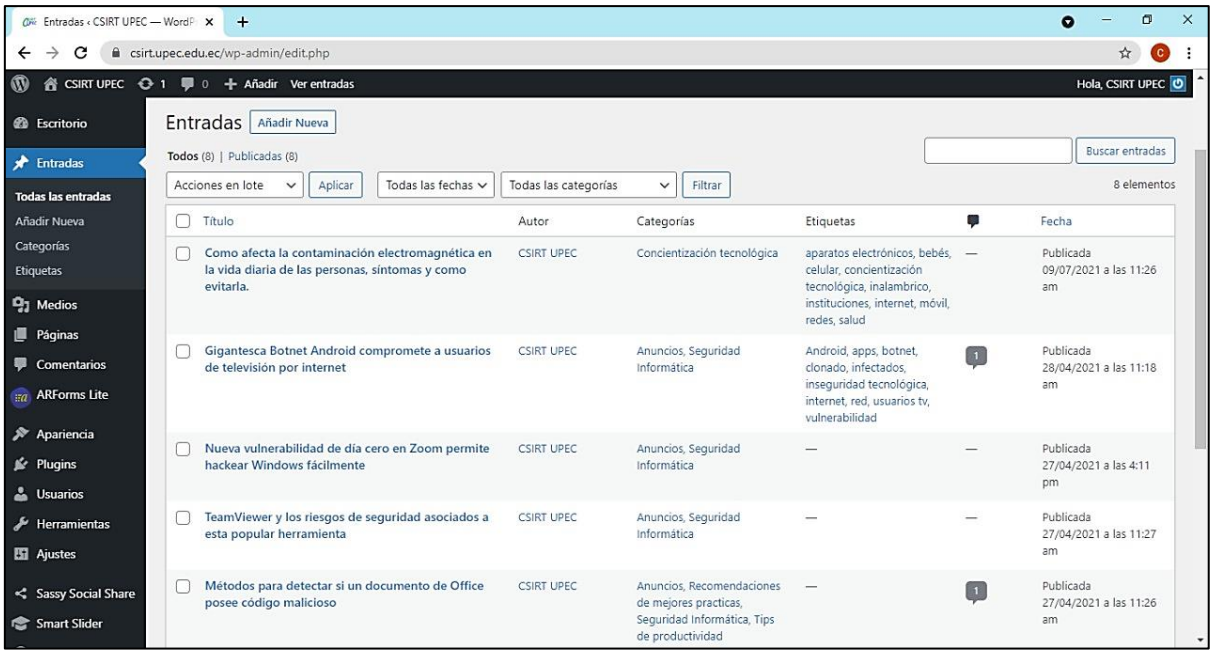


Figura 210. Lista de entradas y sus opciones de personalización

- **Administrador de comentarios**

  En el administrador de comentarios se muestra un listado de todos los comentarios existentes con el autor y correo electrónico respectivamente, la fecha y entrada en que se realizó el comentario, se realizan acciones de búsqueda al colocar palabras clave en la caja de búsqueda y por filtros, además, en la parte superior se muestra el número y estado en el que se encuentran los comentarios como se muestra en la figura 211. Los comentarios se los pueden editar, aprobar, responder, marcarlo como spam si el comentario resulta con características dudosas y enviarlos a la papelera de reciclaje o rechazarlos en caso de que presenten palabras groseras u ofensivas para el público.

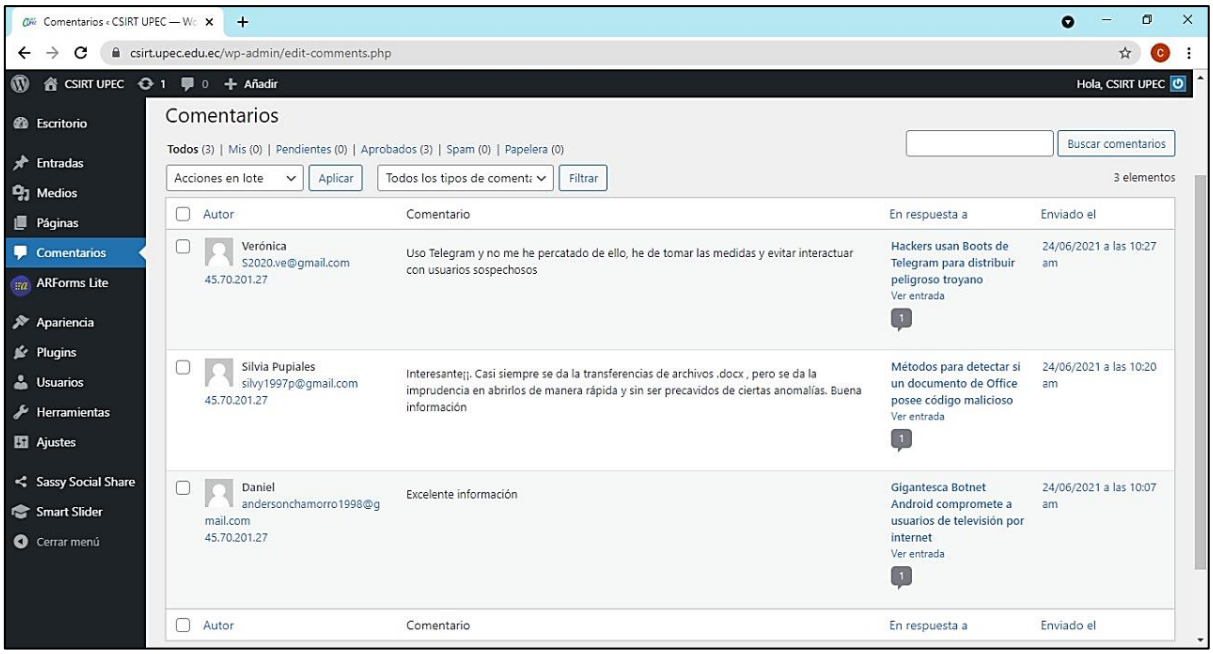


Figura 211. Administración de comentarios emitidos en las entradas

Anexo 18 Creación y configuración formularios del sitio web

Para crear los formularios se utiliza el complemento ARForms Lite en su versión gratuita.

- **Crear formulario para el reporte a incidentes informáticos**

  En el menú de navegación WordPress, se ubica el complemento ARForms Lite y se elige la opción agregar nuevo formulario como se muestra en la figura 212.

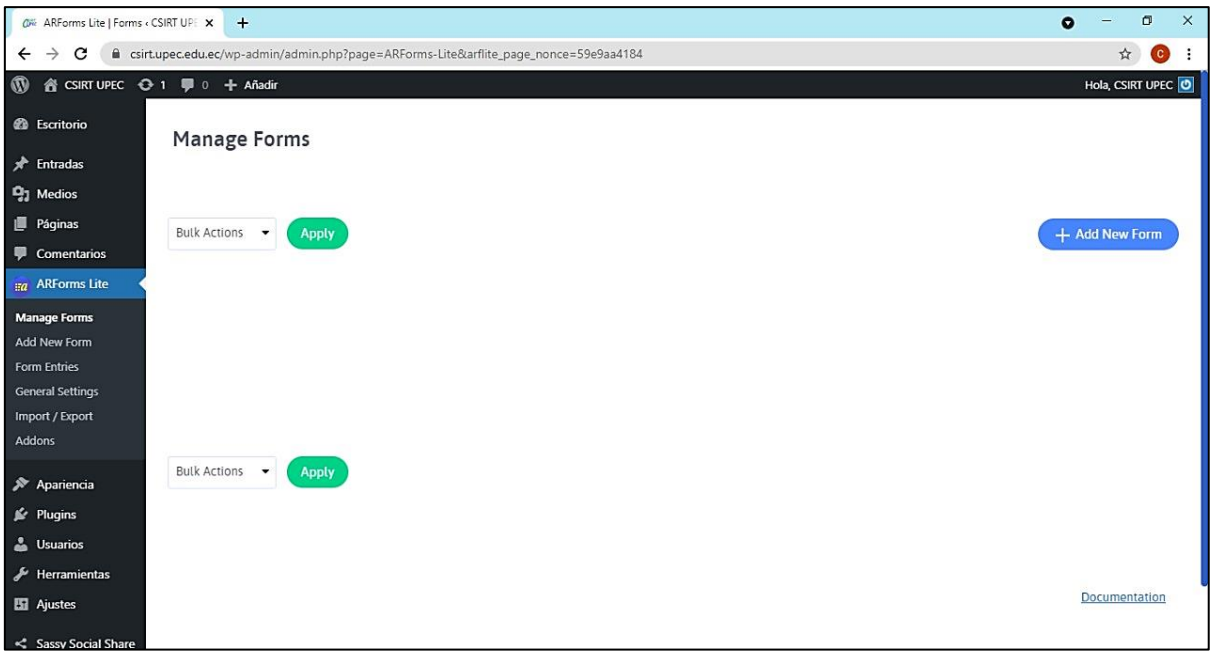


Figura 212. Crear nuevo formulario con ARForms Lite en WordPress

Como se muestra en la figura 213, en la ventana emergente nuevo formulario, se coloca el título, la descripción y se selecciona el estilo estándar para el formulario.

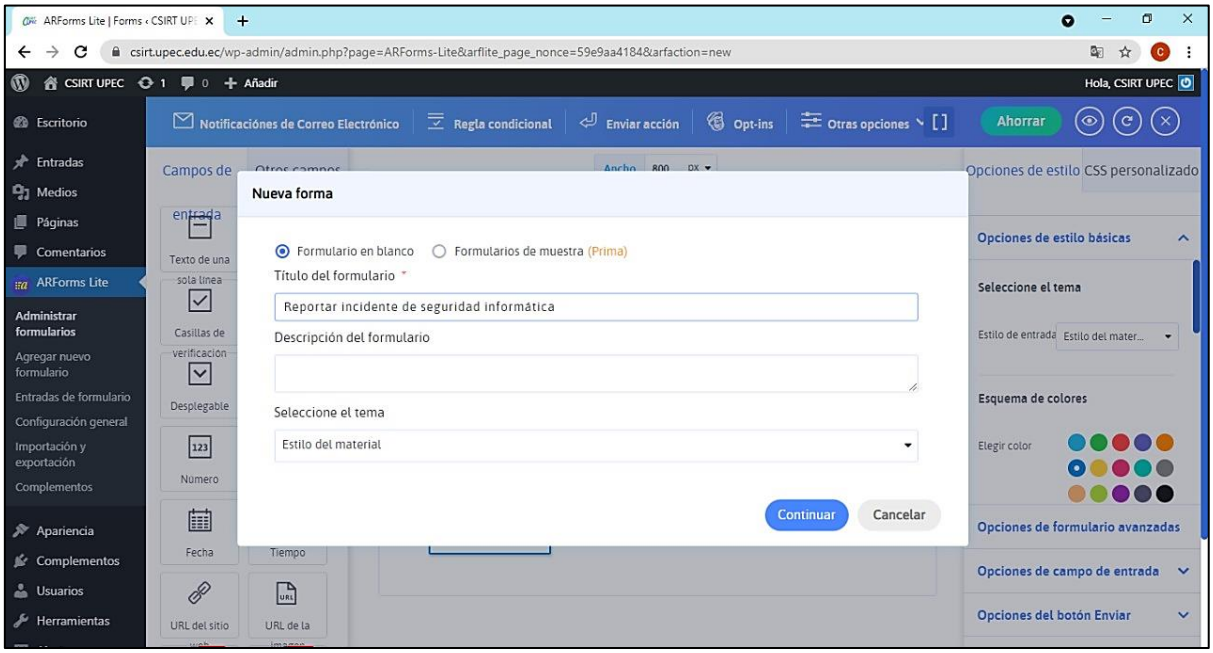


Figura 213. Configuración de identidad del formulario en WordPress

Como se muestra en la figura 214, en la barra lateral izquierda se elige los campos de entrada que dan estructura al formulario, teniendo en cuenta los tipos de datos que se requiere para recolectar la información.

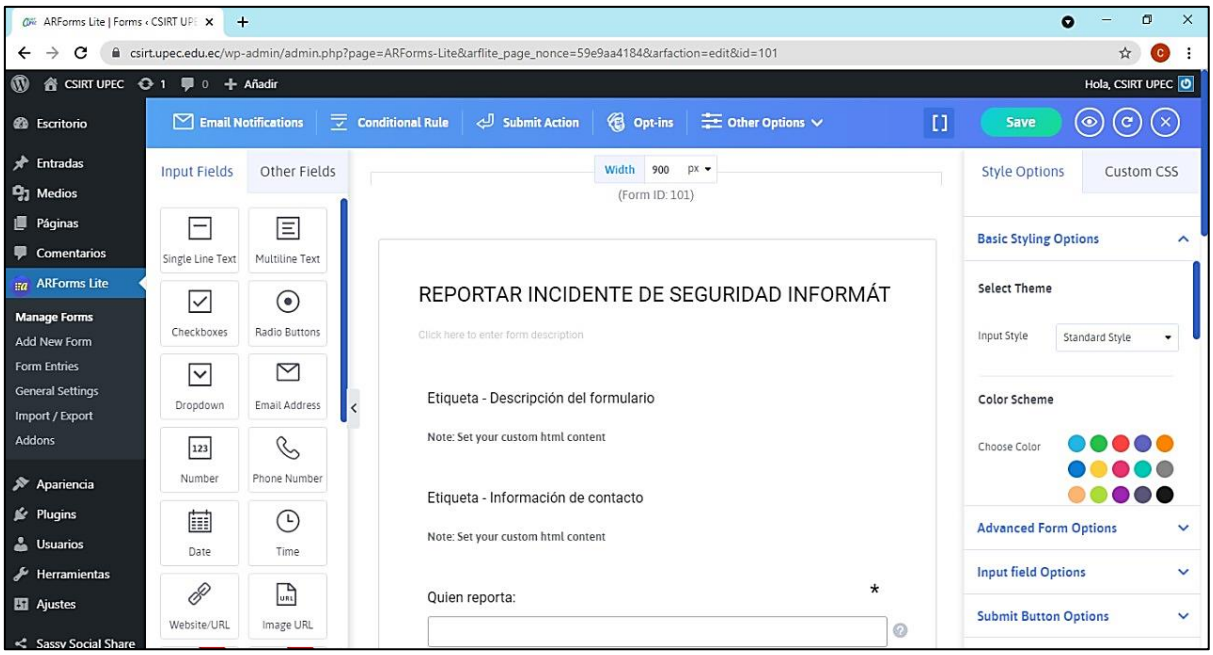


Figura 214. Selección de campos de entrada para la estructura del formulario

Como se muestra en la figura 215, para la etiqueta información de contacto se utiliza el campo de entrada HTML donde se coloca el nombre y una descripción corta de la sección. HTML es un lenguaje de hipertexto.

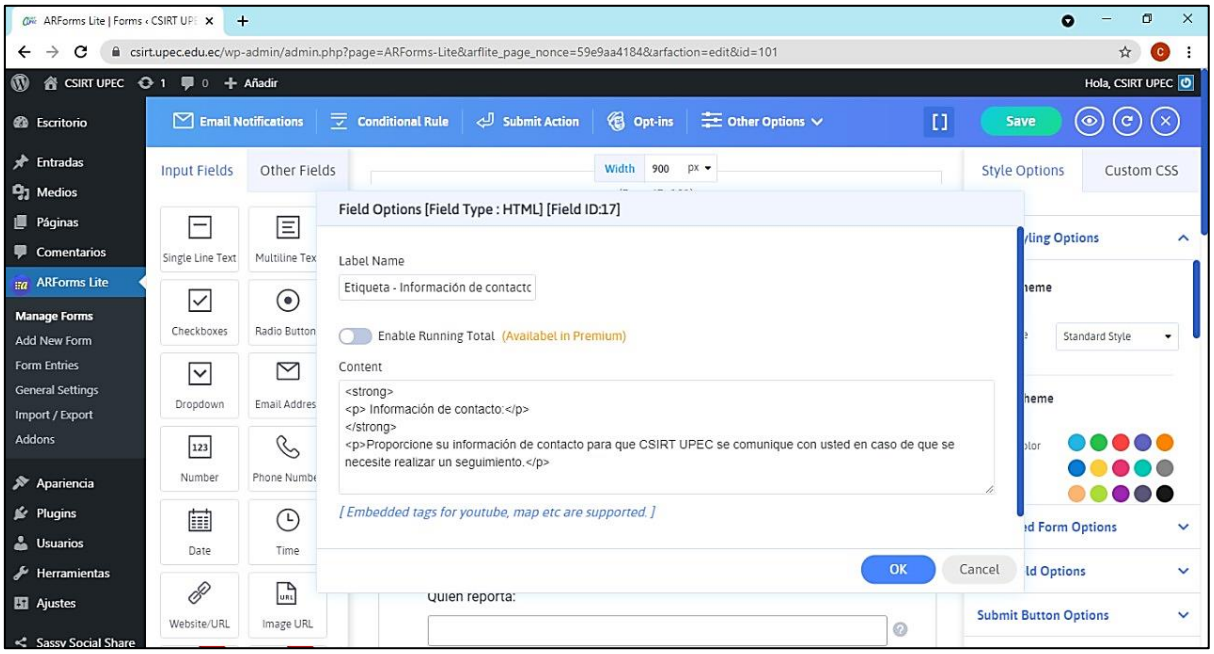


Figura 215. Configuración de la etiqueta para la sección información de contacto para el formulario de reporte a incidentes de seguridad informática

Para el campo quien reporta se selecciona el tipo de campo texto en una sola línea, en su configuración se implementa la validación de los datos estableciendo su ingreso como obligatorio y solo datos alfabetos, la longitud del campo con un ingreso mínimo de 5 y un máximo de 50 caracteres y se añaden los mensajes “el valor ingresado no es válido” cuando los valores ingresados son incorrectos, “este campo no puede estar vacío” al querer enviar el formulario con el campo vacío y “caracteres mínimos no válidos” cuando el mensaje no cumpla con la longitud mínima establecida como se muestra en la figura 216. Además, se coloca “ingresar nombres y apellidos de la persona que reporta el incidente” como mensaje de ayuda.

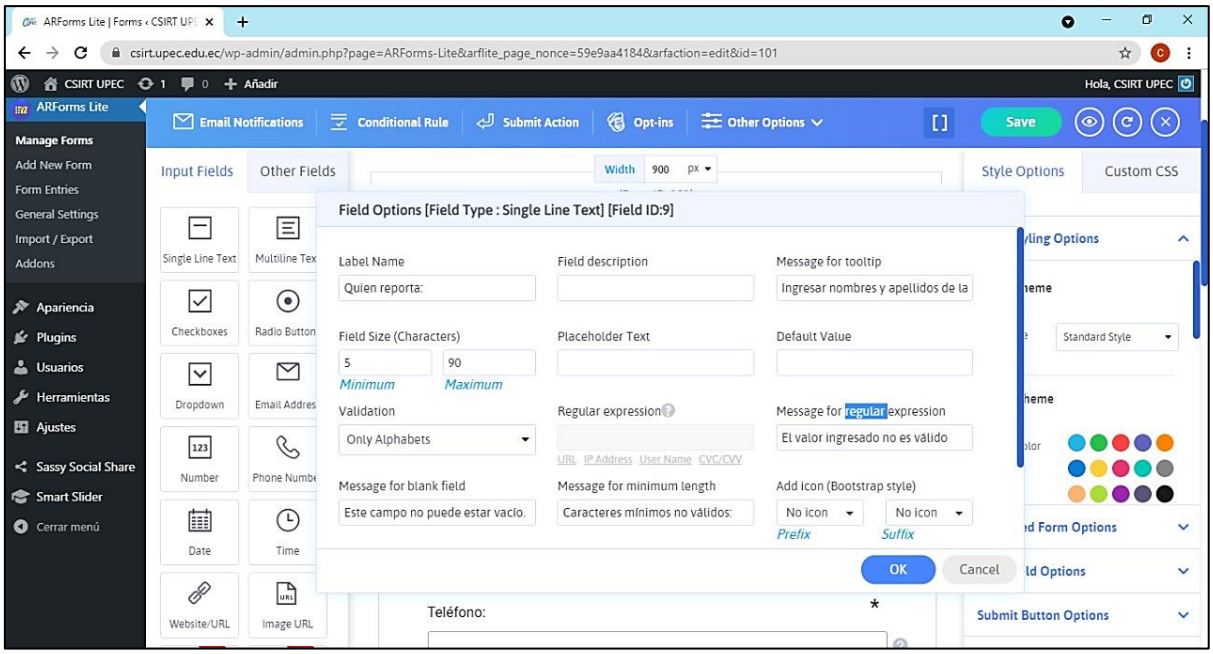


Figura 216. Configuración del campo quien reporta en el formulario de reporte a incidentes de seguridad informática

Para el campo correo electrónico se selecciona el tipo de campo correo, en su configuración se implementa la validación de los datos estableciendo su ingreso como obligatorio, la longitud del campo con un ingreso máximo de 30 caracteres y se añaden los mensajes “el correo electrónico es inválido” cuando los valores ingresados son incorrectos y “este campo no puede estar vacío” al querer enviar el formulario con el campo vacío como se muestra en la figura 217. Además, se coloca “ingresar correo electrónico de la organización o persona que reporta el incidente” como mensaje de ayuda.

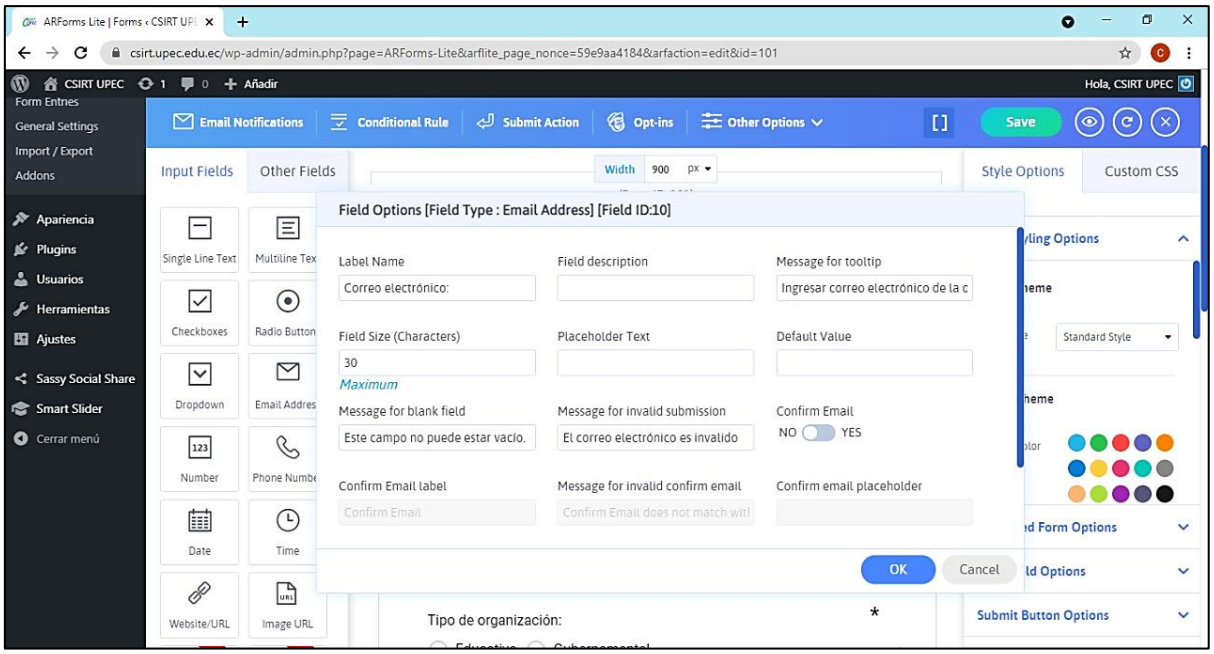


Figura 217. Configuración del campo correo electrónico para el formulario de reporte a incidentes de seguridad informática

Para el campo teléfono se selecciona el tipo de campo número de teléfono, en su configuración se implementa la validación de los datos estableciendo su ingreso como obligatorio, la longitud mínima de 6 y un máximo de 10 caracteres y se añaden los mensajes “número de teléfono inválido” cuando los valores ingresados son incorrectos y “este campo no puede estar vacío” al querer enviar el formulario con el campo vacío como se observa en la figura 218. Además, se coloca “ingresar el número de teléfono o celular de contacto de la organización o persona que reporta el incidente” como mensaje de ayuda

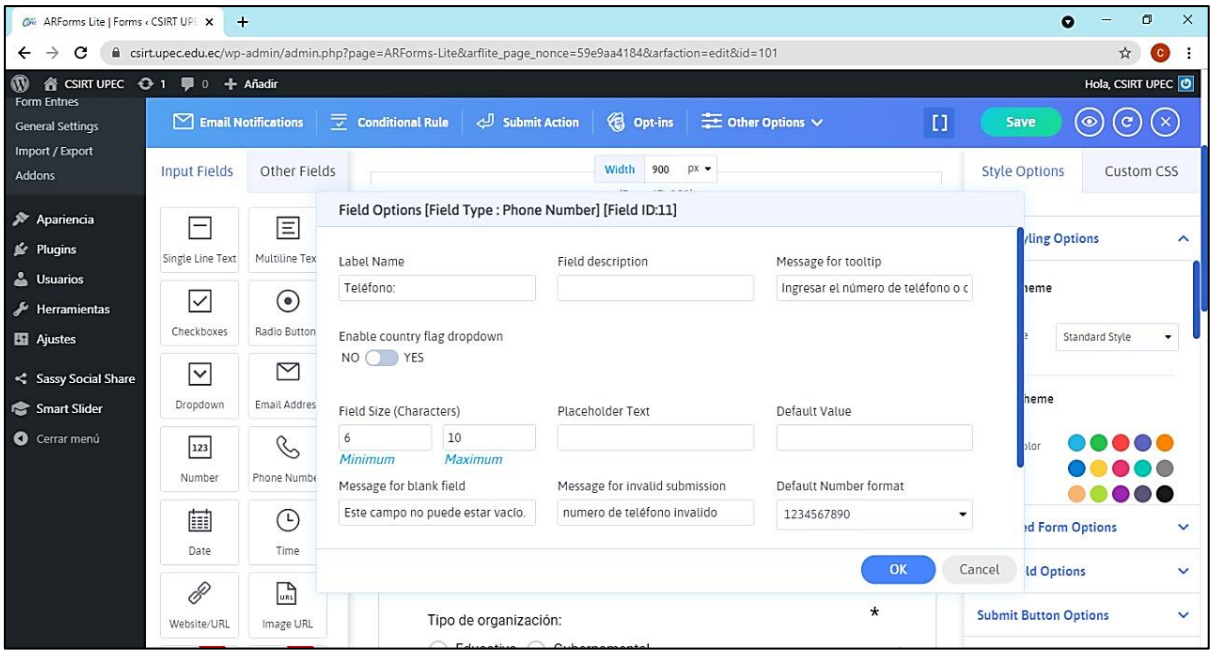


Figura 218. Configuración del campo teléfono para el formulario de reporte a incidentes de seguridad informática

Para el campo “tipo de organización” se establece el tipo de campo radio, se coloca las etiquetas de opción educativa y gubernamental; y en su configuración se implementa la validación de los datos “el campo no puede estar vacío” al querer enviar el formulario con el campo vacío, “seleccione el tipo de organización” como mensaje de ayuda, se establece la alineación en línea y el ingreso del campo obligatorio como se muestra en a figura 219.

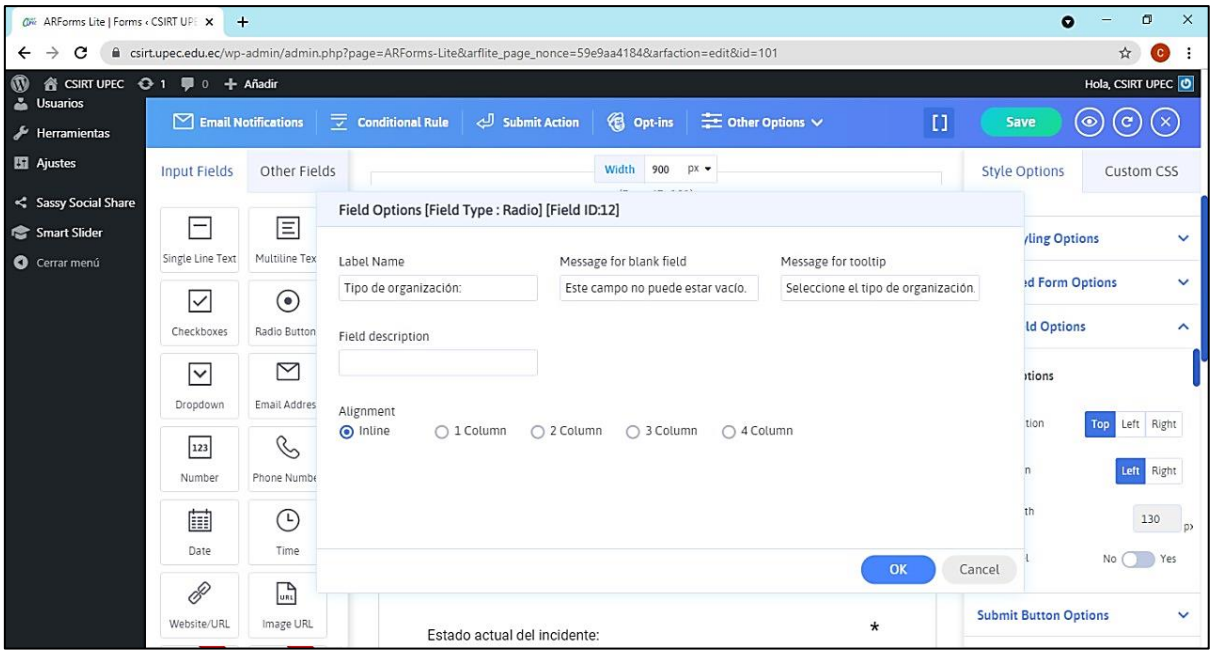


Figura 219. Configuración del campo tipo de organización para el formulario de reporte a incidentes de seguridad informática

Para el campo nombre de la organización se selecciona el tipo de campo texto en una sola línea, en su configuración se implementa la validación de los datos estableciendo su ingreso como obligatorio, la longitud del campo con un ingreso mínimo de 5 y un máximo de 80 caracteres y se añaden los mensajes “el valor ingresado no es válido” cuando los valores ingresados son incorrectos, “este campo no puede estar vacío” al querer enviar el formulario con el campo vacío y “caracteres mínimos no válidos” cuando el mensaje no cumpla con la longitud mínima establecida como se muestra en la figura 220. Además, se coloca “ingresar el nombre de la organización que reporta el incidente” como mensaje de ayuda.

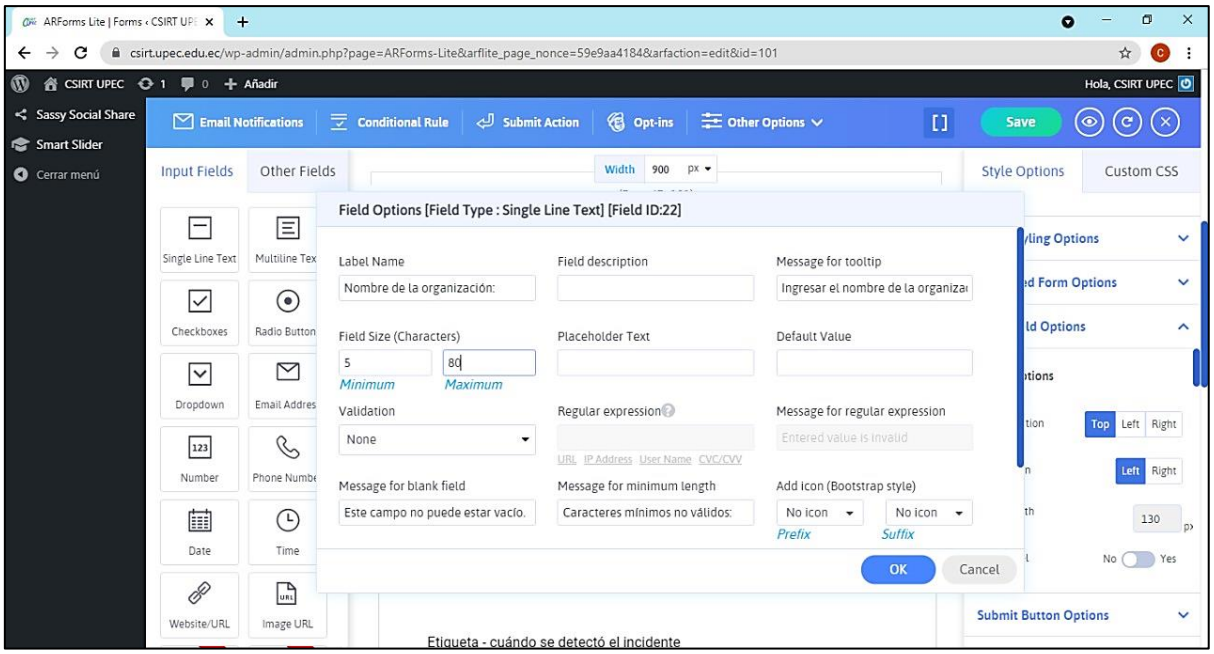


Figura 220. Configuración del campo nombre de la organización para el formulario de reporte a incidentes de seguridad informática

Para el campo estado actual del incidente se selecciona el tipo de campo radio, se coloca las etiquetas de opción ya pasó, en curso, amenaza y desconocido; y en su configuración se implementa la validación de los datos “el campo no puede estar vacío” al querer enviar el formulario con el campo vacío, “seleccionar el estado actual del incidente” como mensaje de ayuda, se establece la alineación en línea y el ingreso obligatorio como se muestra en a figura 221.

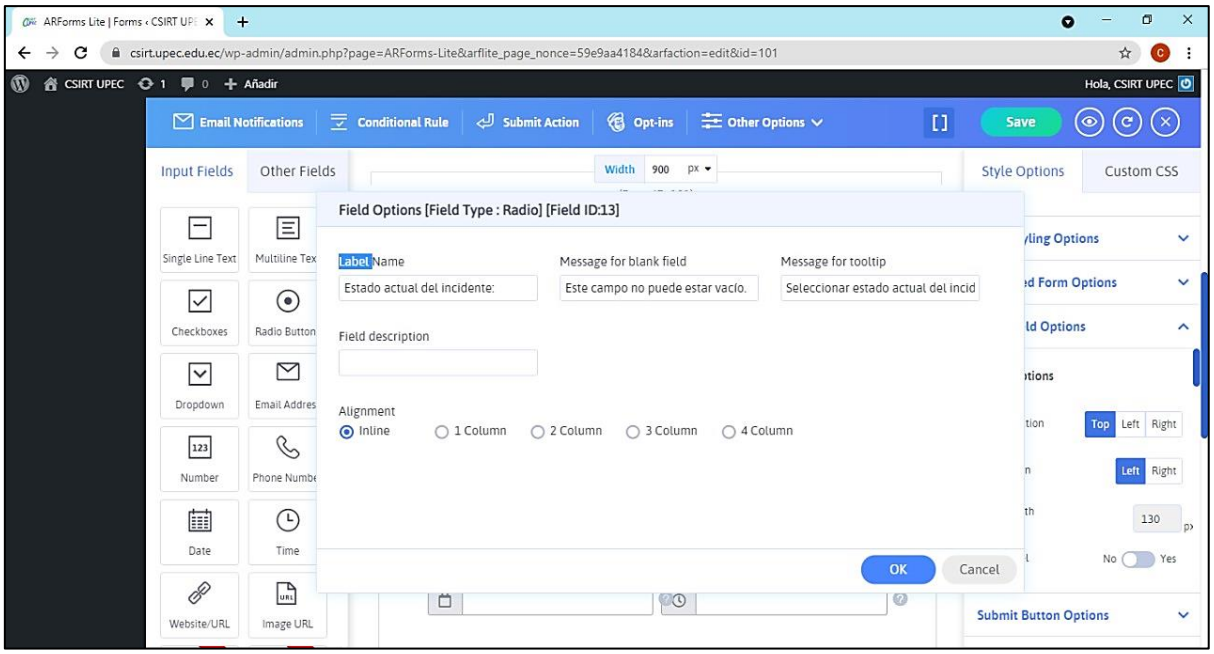


Figura 221. Configuración del campo estado actual del incidente para el formulario de reporte a incidentes de seguridad informática

Para el campo cuando se detectó el incidente se selecciona el tipo de campo fecha, en su configuración se implementa la validación de los datos “el campo no puede estar vacío” al querer enviar el formulario con el campo vacío, “seleccione la fecha aproximada en la que detectó el incidente” como mensaje de ayuda y se establece el obligatorio como se muestra en a figura 222.

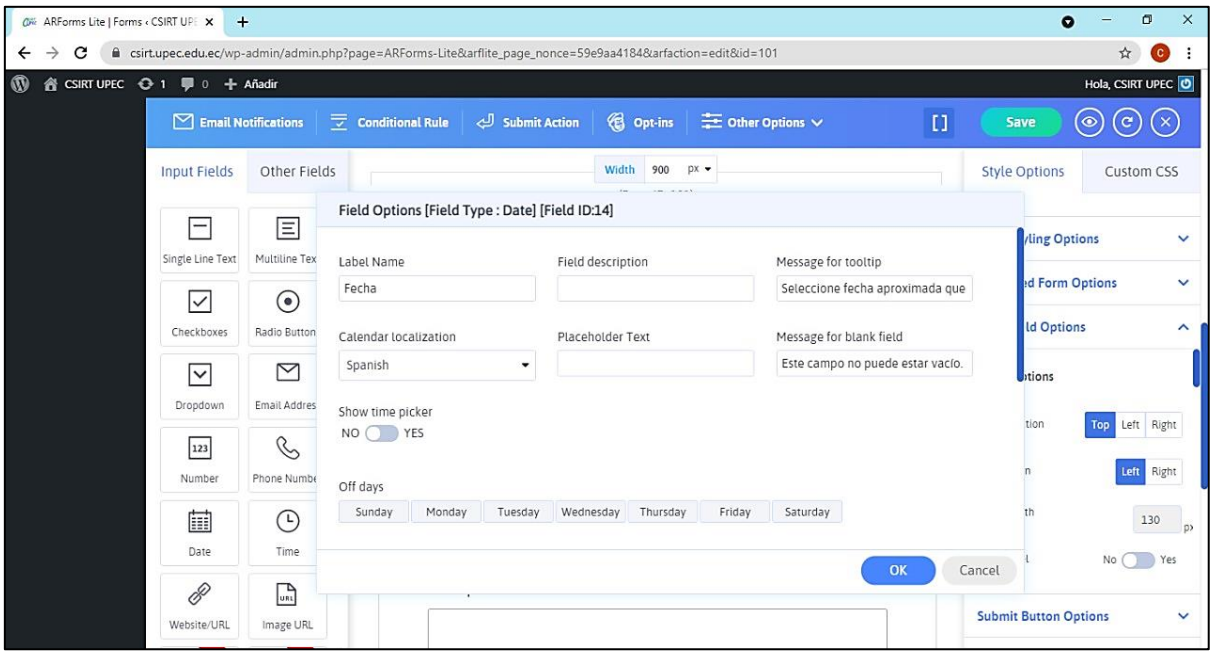


Figura 222. Configuración del campo cuando se detectó, fecha del incidente para el formulario de reporte a incidentes de seguridad informática

Para el campo cuando se detectó el incidente se selecciona el tipo de campo hora, en su configuración se implementa la validación de los datos “el campo no puede estar vacío” al querer enviar el formulario con el campo vacío, “seleccione la hora aproximada en la que detectó el incidente” como mensaje de ayuda y se establece el ingreso obligatorio como se muestra en a figura 223.

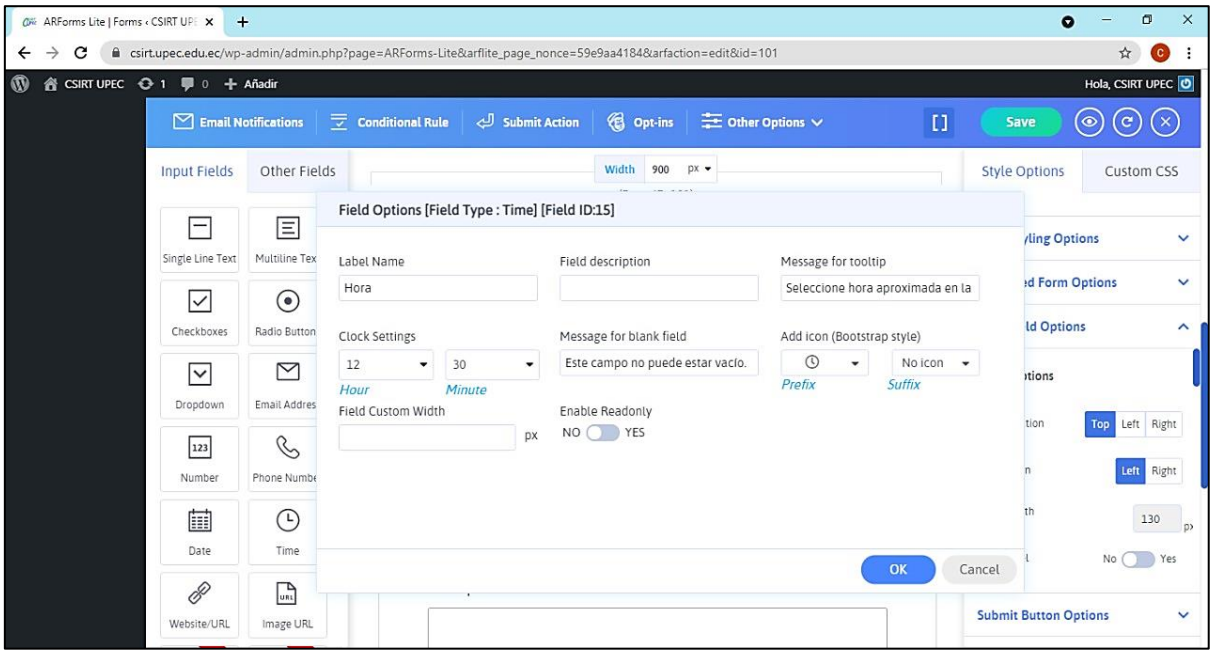


Figura 223. Configuración del campo cuando se detectó, hora del incidente para el formulario de reporte a incidentes de seguridad informática

Como se muestra en la figura 224, para la etiqueta detalles del incidente se utiliza el campo de entrada HTML, donde se coloca el nombre y una descripción corta de la sección.

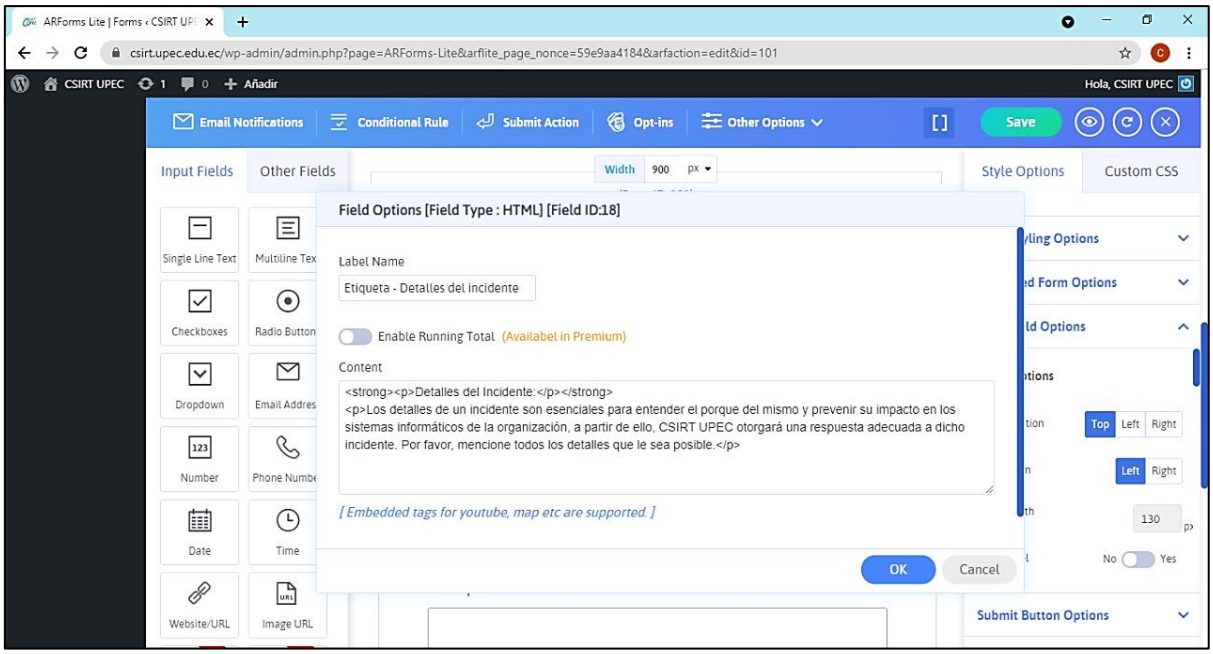


Figura 224. Configuración de la etiqueta para la sección detalles del incidente para el formulario de reporte a incidentes de seguridad informática

Para el campo descripción del incidente se selecciona el tipo de campo texto de varias líneas, en su configuración se implementa la validación de los datos estableciendo su ingreso como obligatorio, longitud mínima de 25 caracteres, se añade el mensaje “este campo no puede estar vacío” al querer enviar el formulario con el campo vacío y “caracteres mínimos no válidos” cuando el mensaje no cumpla con la longitud mínima establecida como se muestra en la figura 225. Además, se coloca “ingresar de forma muy detallada el incidente informático” como mensaje de ayuda.

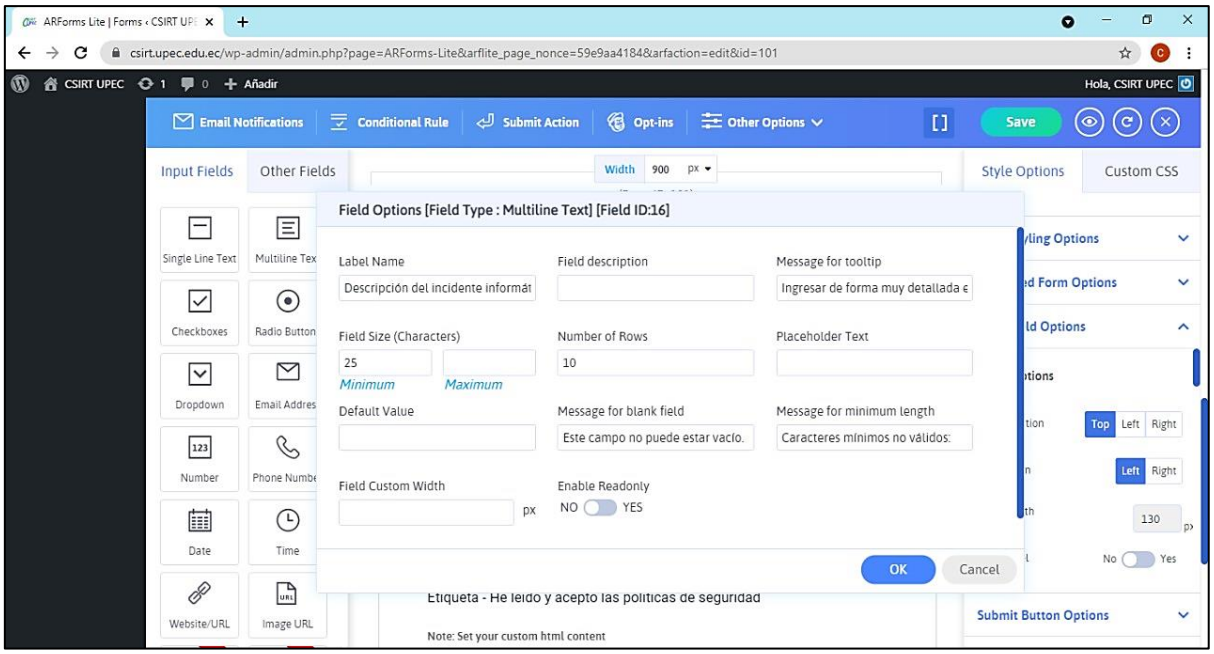


Figura 225. Configuración del campo descripción del incidente en el formulario de reporte a incidentes de seguridad informática

Para el campo he leído, comprendo y acepto las políticas de seguridad se selecciona el tipo de campo casilla de verificación, en su configuración se implementa la validación de los datos “el campo no puede estar vacío” al querer enviar el formulario con el campo vacío, “leer las políticas de seguridad de la información antes de aceptarlas” como mensaje de ayuda y el ingreso del campo es obligatorio como se muestra en a figura 226.

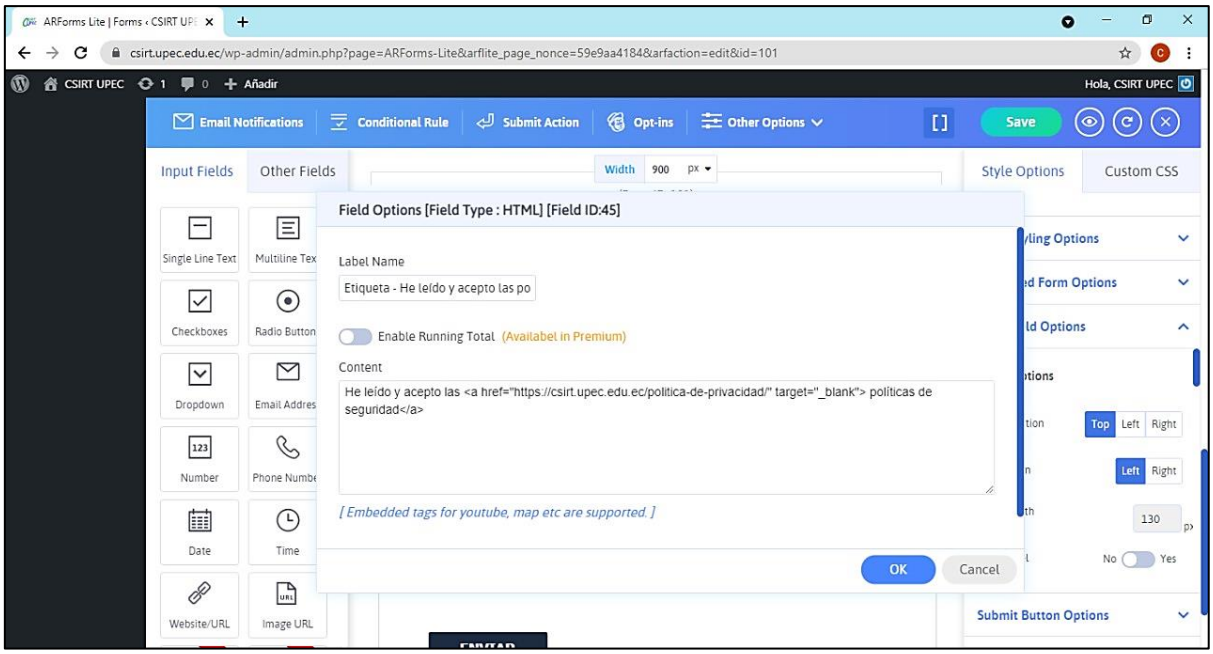


Figura 226. Configuración del campo de comprensión de políticas de seguridad para el formulario de reporte a incidentes de seguridad informática

- **Configurar formulario**

  Como se observa en la figura 227, en el menú opciones de estilo se define el diseño del formulario, las opciones a configurar son de estilo básicas, de formulario avanzadas, campo de entrada y botón enviar.

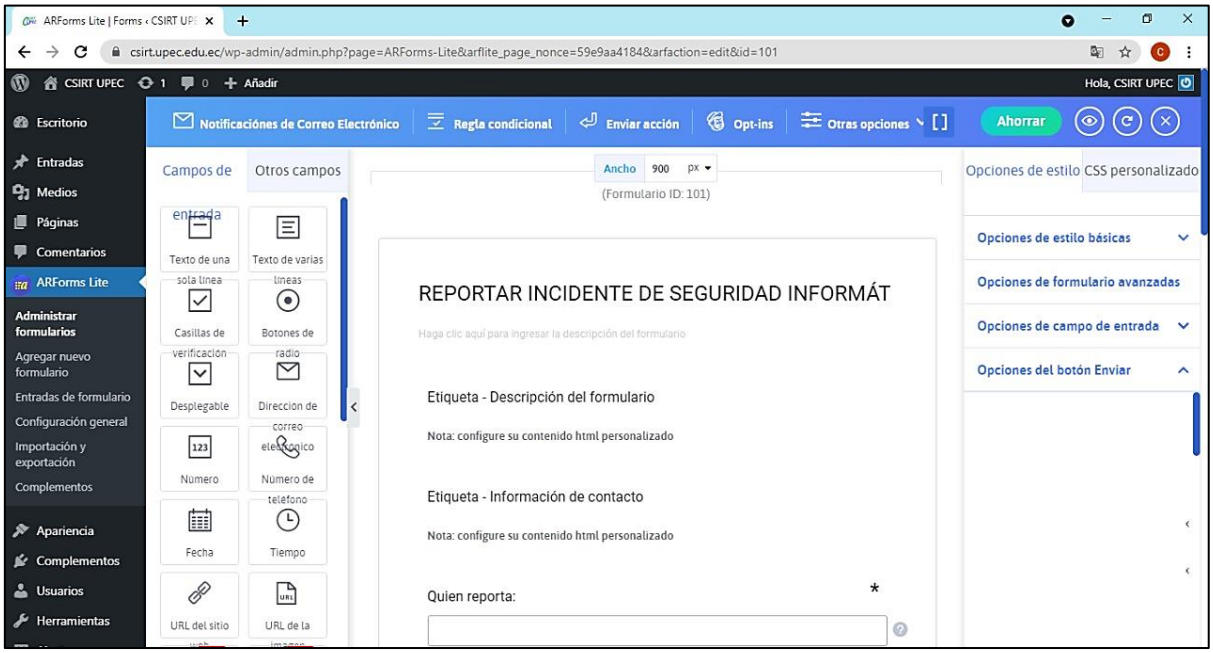


Figura 227. Personalizar las opciones de estilo para el formulario de reporte a incidentes de seguridad informática

En la opción estilo básico se selecciona estilo estándar para el tema, se establece el color blanco para el fondo del formulario, espacios de entrada, texto de las herramientas de campo y del botón, el color negro para el título del formulario, descripción, texto de etiqueta, fondo de las herramientas de campo y texto de mensaje de éxito y azul oscuro para el botón. Se utiliza la fuente Robot para el texto de todo el formulario, tamaño 3 en escala del 1 al 10 del texto, 900 px de ancho del formulario y formato moderno en posición de fondo para el mensaje de validación como se muestra en la figura 228.

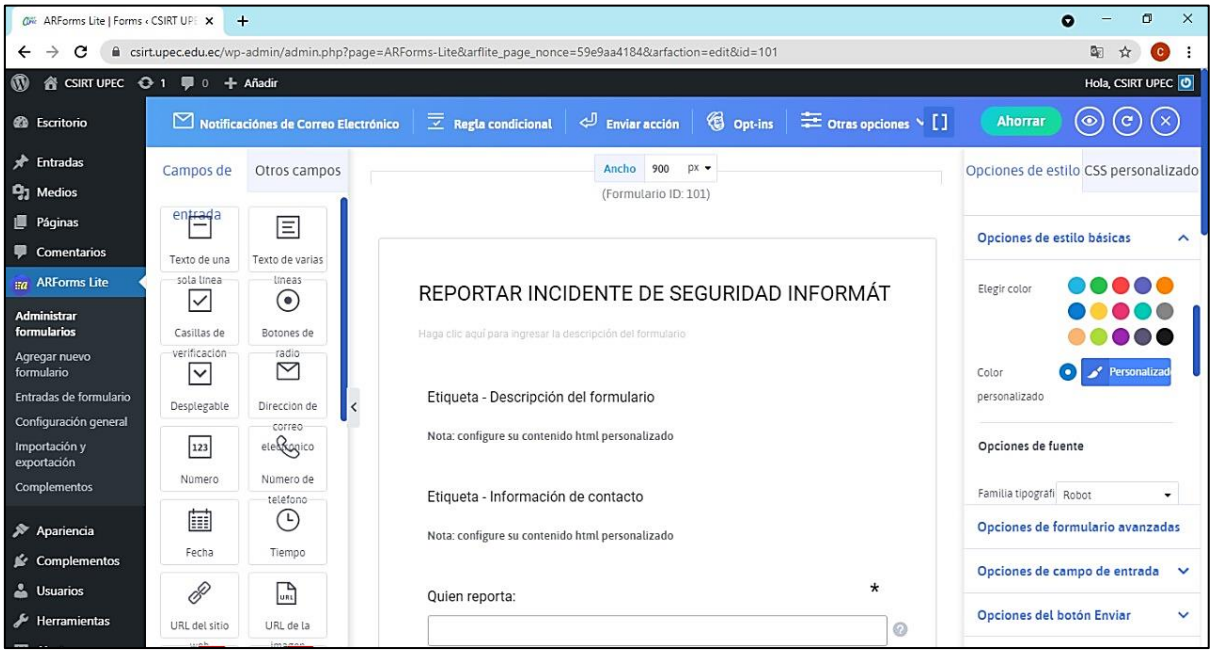


Figura 228. Configuración del estilo básico para el formulario de reporte a incidentes de seguridad informática

En la opción formulario avanzado se activa la visualización del título y descripción de la pantalla, se establece la alineación de los títulos del lado izquierdo con un margen de 20 px, además, se establece un margen de 1 px para los bordes del formulario como se muestra en la figura 229.

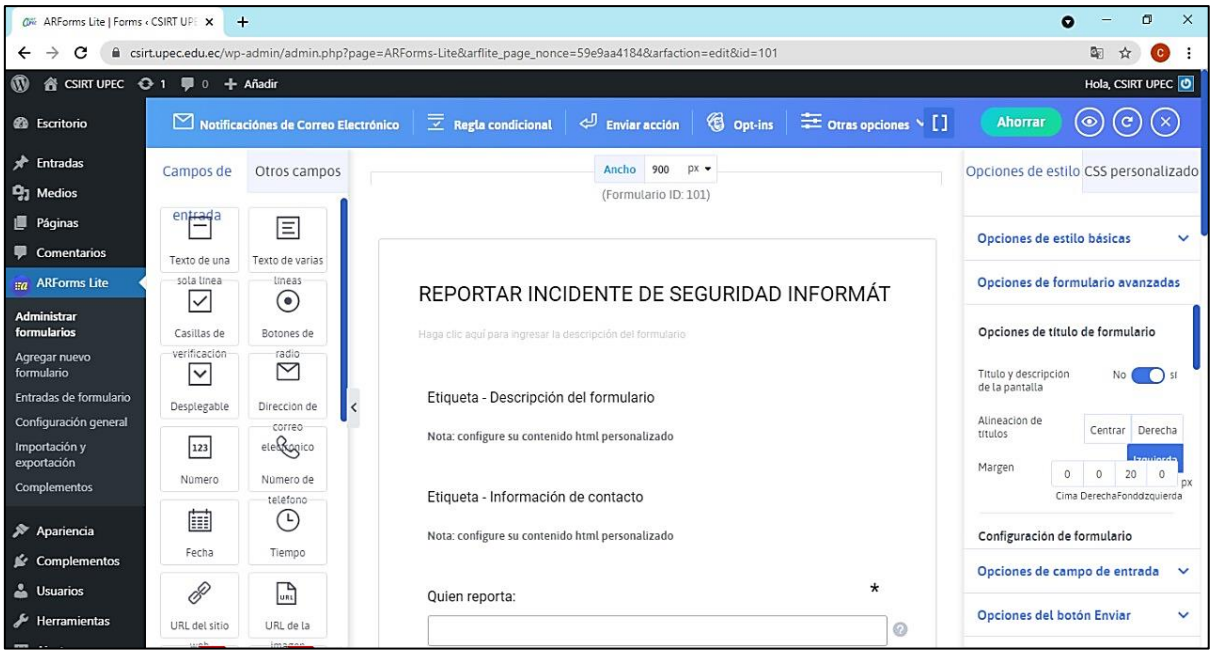


Figura 229. Configuración avanzada para el formulario de reporte a incidentes de seguridad informática

Como se muestra en la figura 230, en la opción “configuración de los campos de entrada” se establece 1 px para el tamaño del borde, estilo sólido, formato de fecha con AA/MM/DD y el estilo por defecto para las casillas de verificación y radio.

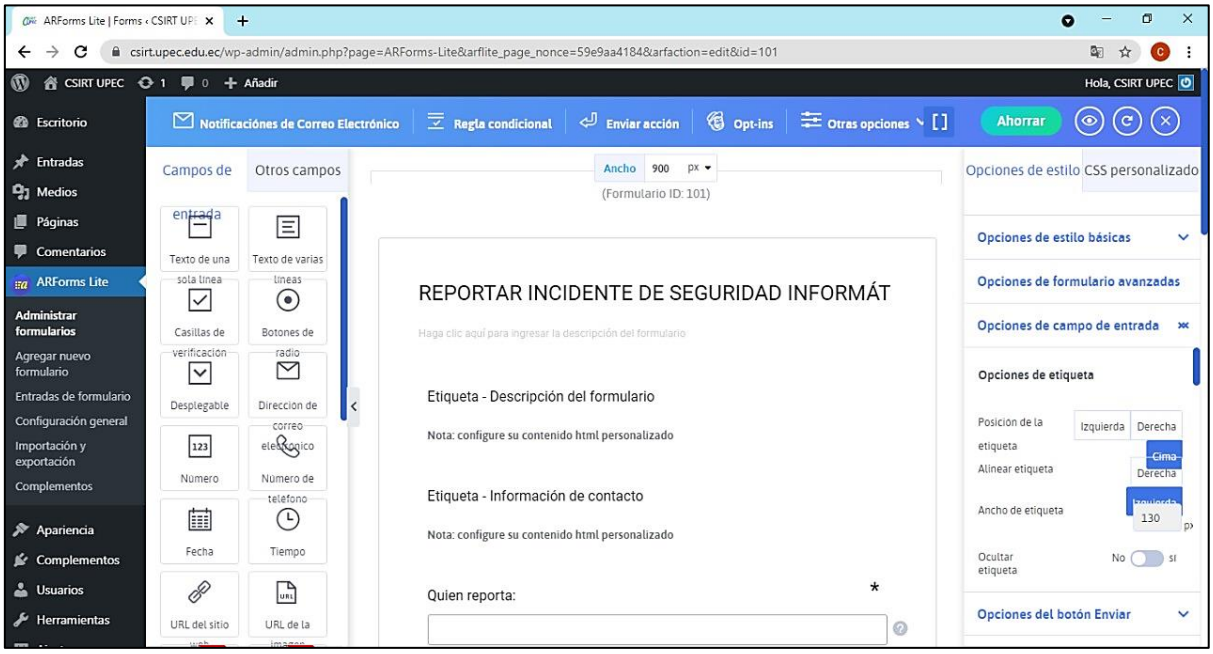


Figura 230. Configuración de los campos de entrada para el formulario de reporte a incidentes de seguridad informática

Como se muestra en la figura 231, en la opción configuración del botón enviar se establece la alineación del botón a la izquierda, con el texto enviar, estilo flat y la fuente Tahoma con tamaño 16 y estilo en negrita.

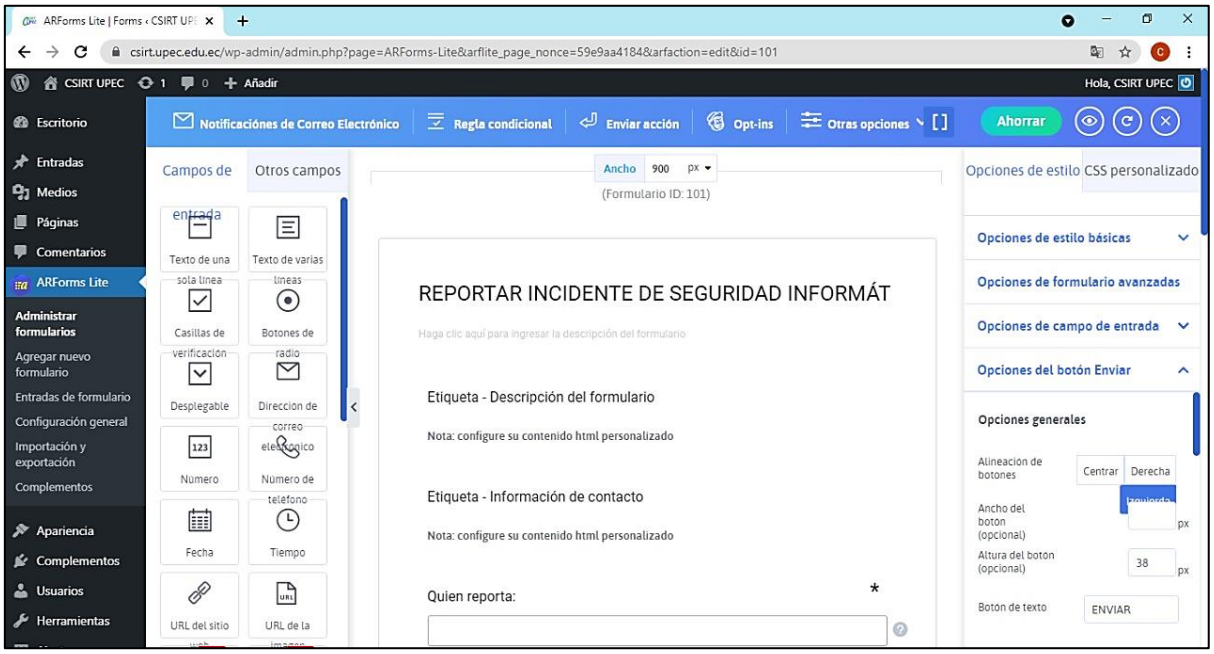


Figura 231. Configuración del botón enviar para el formulario de reporte a incidentes de seguridad informática

En la opción configuraciones de notificación por correo se activa la casilla de envío de respuesta automática a los usuarios después del envío del formulario como se muestra en la figura 232, para ello se toma en cuenta el campo correo electrónico recolectado por el formulario como destinatario, con el asunto del e-mail “correo de confirmación de reporte de incidente informático”, el correo del administrador como remitente y todos los campos recolectados por el formulario como el cuerpo del correo.

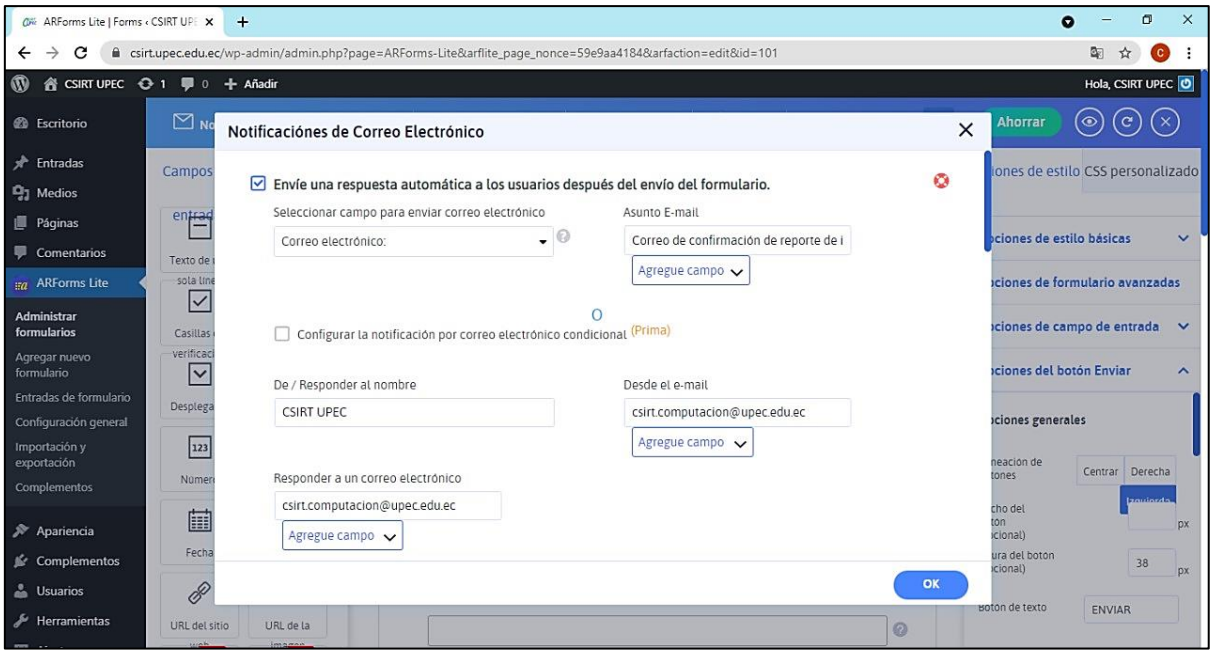


Figura 232. Configuración de notificación por correo automática después del envió del formulario de reporte a incidentes de seguridad informática

En el menú “enviar acción” se selecciona la opción mostrar contenido de otra página que permite redireccionarse a la página establecida “manejo de incidentes”, luego de enviar el formulario de reporte como se muestra en la figura 233.

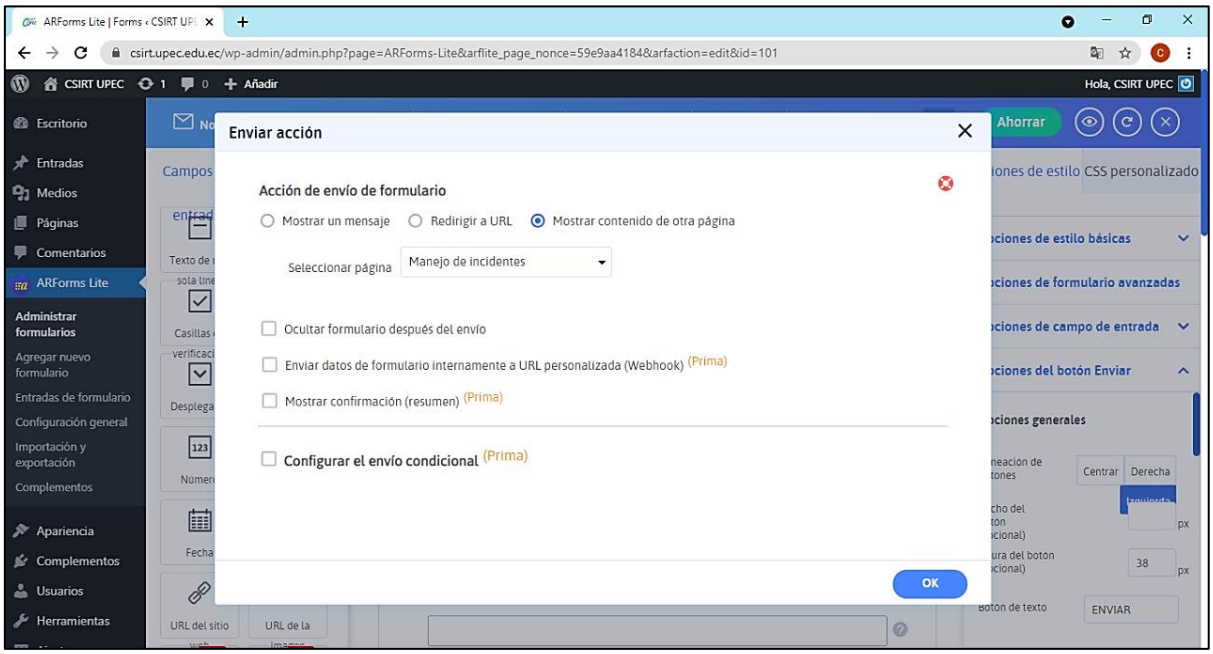


Figura 233. configuración de la acción de envío del formulario de reporte a incidentes de seguridad informática

- **Administración de formularios**

  En el menú de navegación WordPress, se ubica el complemento ARForms Lite y se elige la opción administrar formularios donde se visualiza su identificación, título, número de entradas, fecha de creación y el shortcode de los formularios existentes como se muestra en la figura 234, además, se puede editar, visualizar las entradas y exportarlas en formato CSV, duplicar el formulario, tener una vista previa del formulario, eliminar y agregar nuevos. CSV es un formato de documentos para representar los documentos en tablas, pasan a representar las columnas y filas por comas y saltos de líneas.

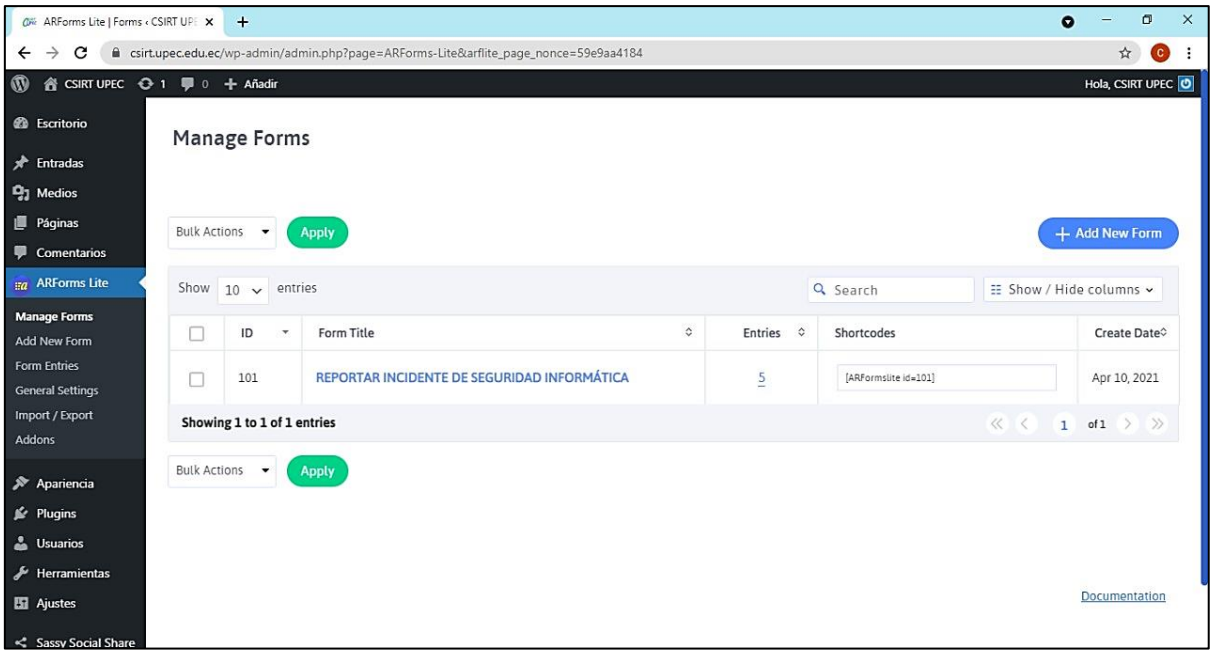


Figura 234. Administrador de formularios de ARForms Lite en WordPress

- **Visualización de las entradas del formulario**

  En el menú de navegación WordPress, se ubica el complemento ARForms Lite y se elige la opción entradas del formulario como se muestra en la figura 235, donde se puede seleccionar el formulario, visualizar sus entradas en forma de tabla como reporte, hacer un filtro por fecha, realizar búsquedas, mostrar y ocultar columnas y eliminar entradas.

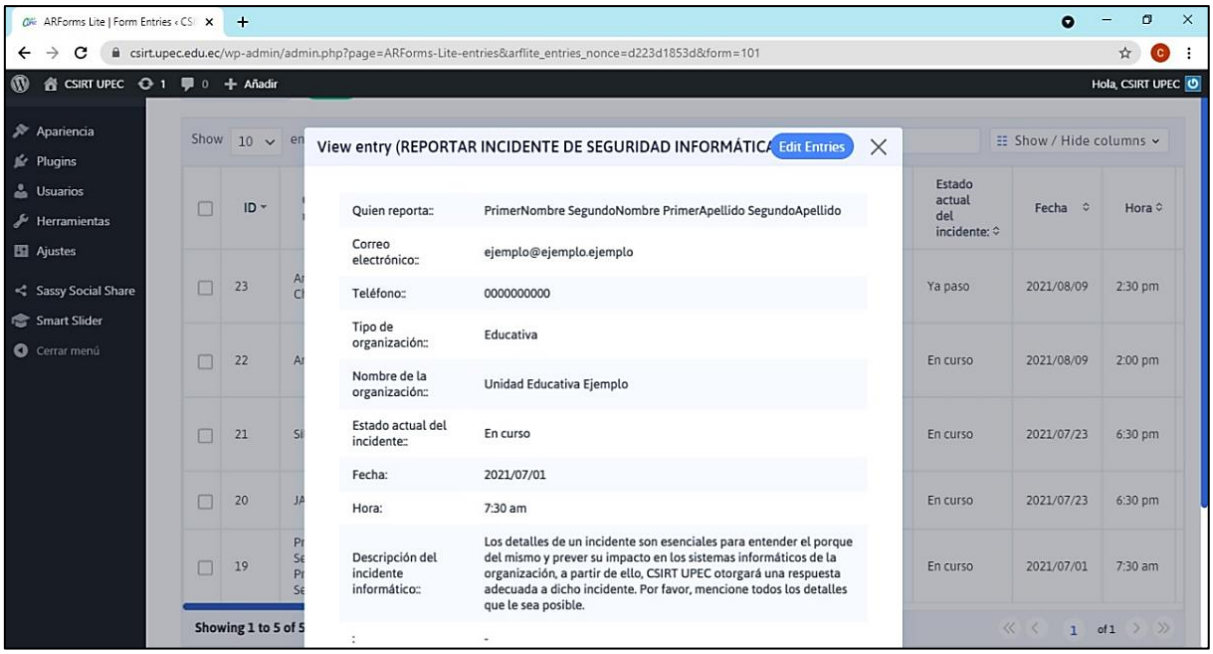


Figura 235. Entradas del formulario de ARForms Lite en WordPress

Anexo 19 Configuración servidor de registro y seguimiento de incidentes.

- **Configuración de ticket**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú configuración, se selecciona la opción ticket y apartado configuracion general, donde se define el formato de número de ticket en 6 caracteres numéricos, la secuencia del número en aleatorio, el estado predeterminado del ticket en abierto, la prioridad predeterminada en normal y clic en guardar cambios como se muestra en la figura 236.

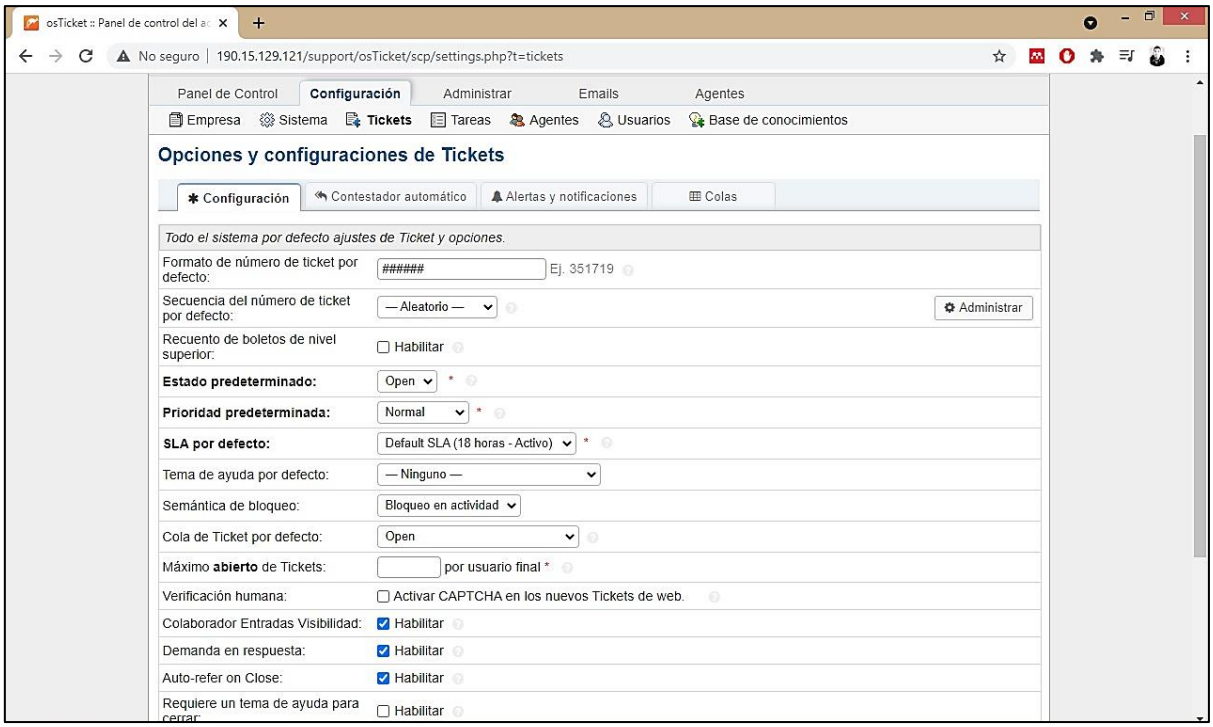


Figura 236. Configuración de los tickets en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

En el apartado alertas y notificaciones de ticket, se activa las casillas email de administrador y gerente del departamento para el aviso de nuevo ticket, se activa las casillas ultimo demandado y agente o equipo asignado para el aviso de nuevo mensaje, se activa la casilla moderador asignado para aviso de asignación de ticket, se activa la casilla agente o equipo asignado y gerente del departamento para alerta de ticket retrasado, se activan las casillas errores SQL e intentos excesivos de inicios de sesión fallidos para las alertas del sistema del departamento, para la alerta al trasferir un ticket y clic en guardar cambios como se muestra en la figura 237.

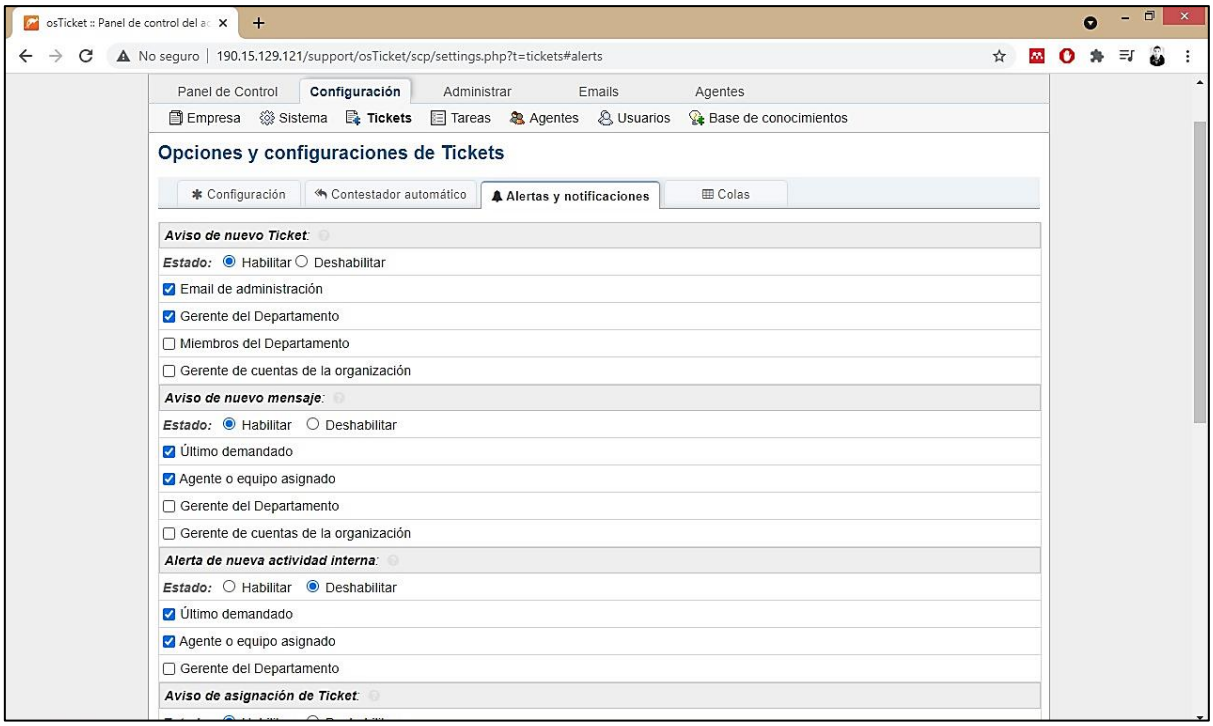


Figura 237. Configuración de avisos de tickets en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de temas de ayuda**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú administrar, se selecciona la opción temas de ayuda.

  Para generar el tema de ayuda CSIRT – Reportar Incidente, se da clic en crear un nuevo tema de ayuda donde se despliega un formulario para su registro, se define el nombre del tema CSIRT – Reportar Incidente, el estado como activo, de tipo público y tema de nivel alto. Se establece el departamento como Operaciones CSIRT, formato de numero de ticket como predeterminado, estado abierto, prioridad normal, página de agradecimiento como CSIRT UPEC – Página de agradecimiento y nombre del personal del departamento de operaciones quien recibe los tickets de manera automática. Para los detalles del ticket se selecciona el formulario personalizado CSIRT UPEC – Reportar incidente Informático y clic en guardar cambios como se muestra en la figura 238.

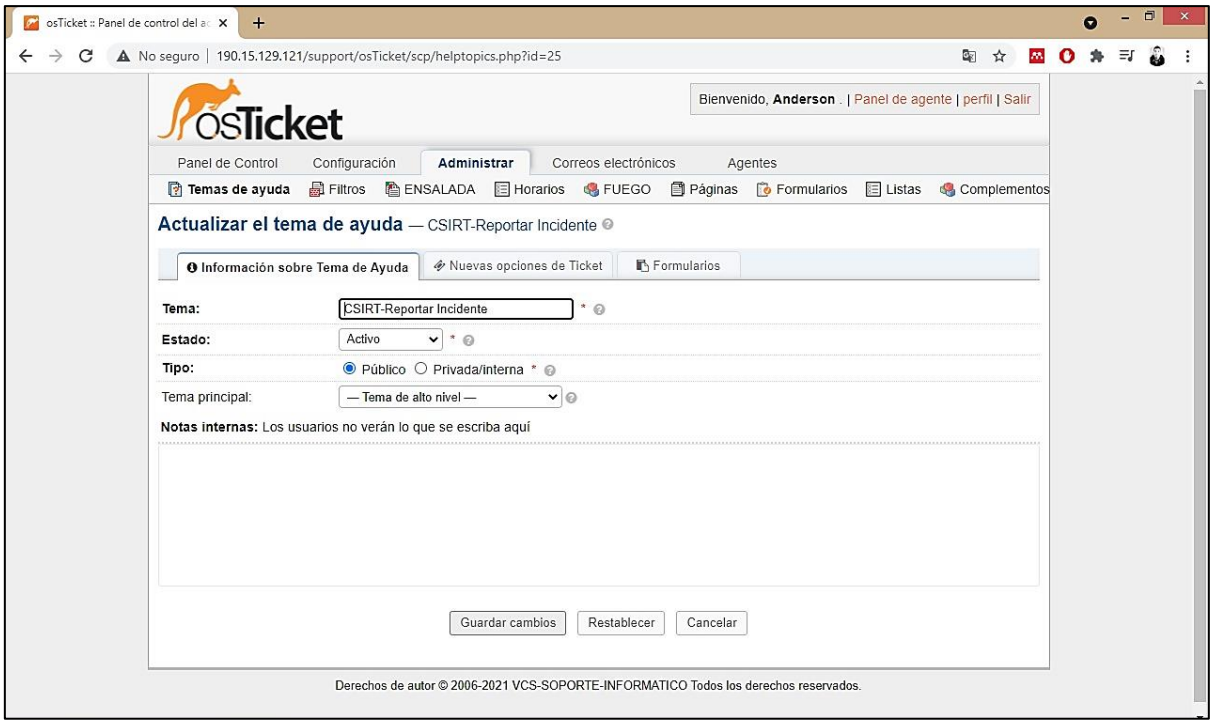


Figura 238. Configuración del tema de ayuda CSIRT – Reportar Incidente en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para generar el tema de ayuda CSIRT – Concienciación Tecnológica, se da clic en crear un nuevo tema de ayuda donde se despliega un formulario para su registro, se define el nombre del tema CSIRT – Concienciación Tecnológica, el estado como activo, de tipo público y tema de nivel alto. Se establece el departamento como Operaciones CSIRT, formato de número de ticket como predeterminado, estado abierto, prioridad normal, página de agradecimiento como CSIRT UPEC – Página de agradecimiento, nombre del personal del departamento de operaciones quien recibe los tickets de manera automática. Para los detalles del ticket se selecciona el formulario personalizado CSIRT UPEC – Concienciación Tecnológica y clic en guardar cambios como se muestra en la figura 239.

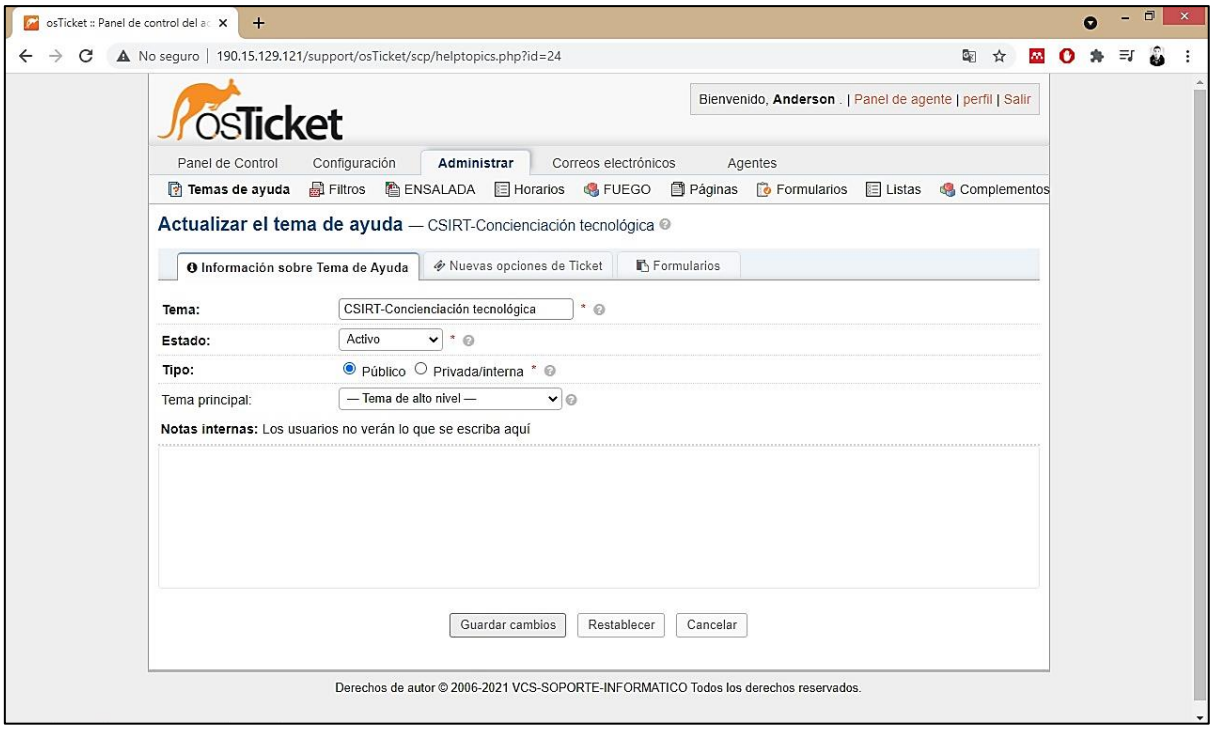


Figura 239. Configuración del tema de ayuda CSIRT – Concienciación Tecnológica en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los temas de ayuda creados, se selecciona la opción temas de ayuda, donde se muestra una tabla con el nombre del tema, estado, tipo, prioridad, departamento, fecha de creación y última actualización como se muestra en la figura 240.

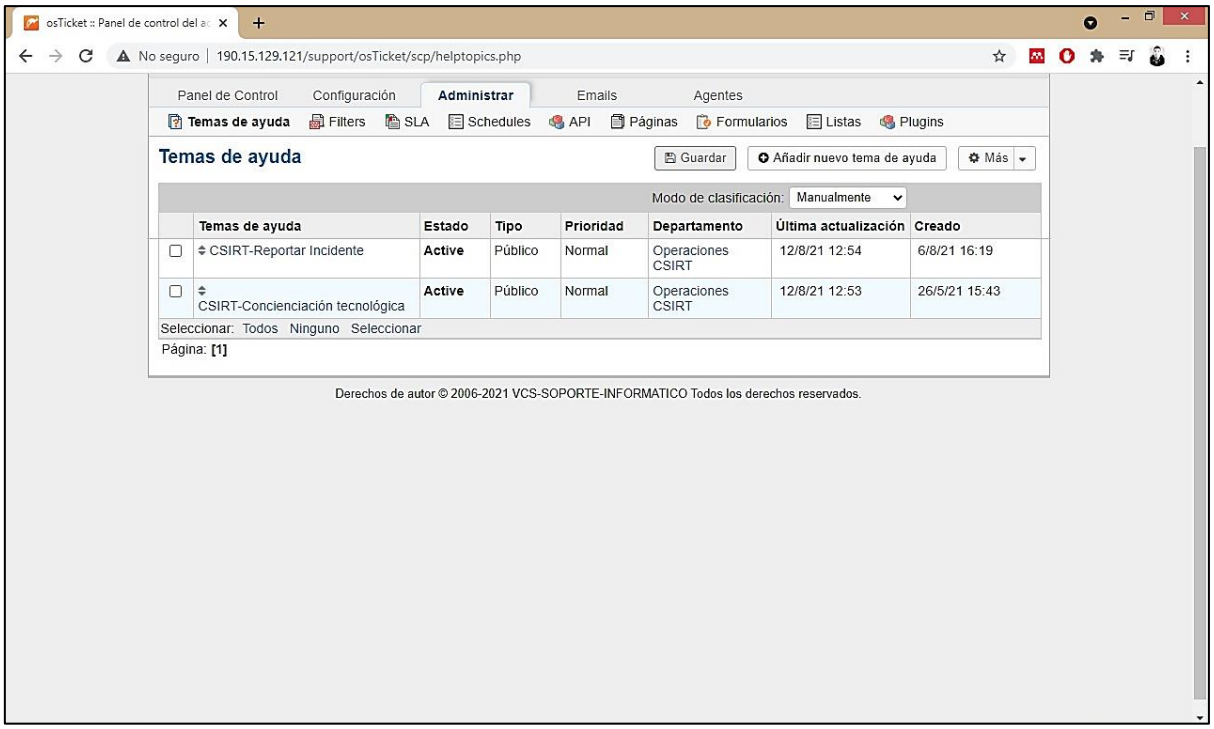


Figura 240. Página de los temas de ayuda registrados en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de páginas**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú administrar y se selecciona la opción páginas. Para crear la página ventana principal, se da clic en añadir nueva página donde se despliega un formulario para su registro, se define el nombre de la página ventana principal, tipo página de inicio, estado activo y en contenido de página se añade la información respectiva como se muestra en la figura 241.

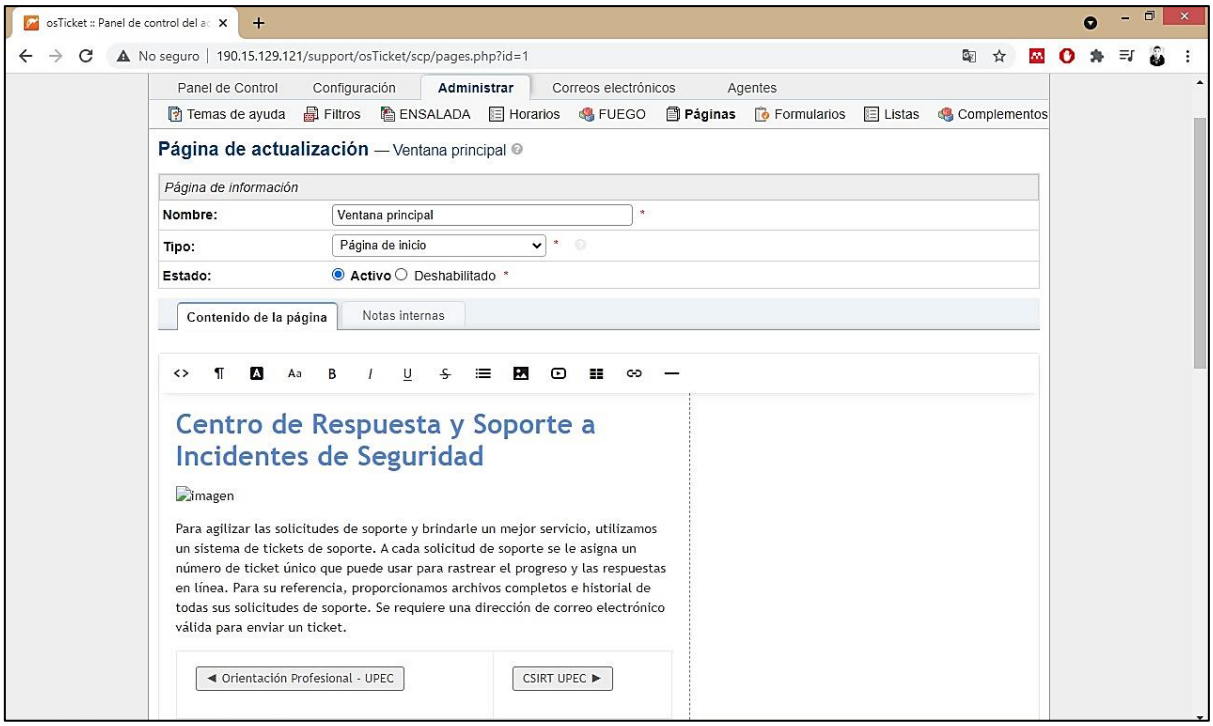


Figura 241. Crear la página ventana principal en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para crear la página CSIRT UPEC – Página de agradecimiento, se da clic en añadir nueva página donde se despliega un formulario para su registro, se define el nombre de la página CSIRT UPEC – Página de agradecimiento, tipo página de agradecimiento, estado activo y en contenido de página se añade la información respectiva como se muestra en la figura 242.

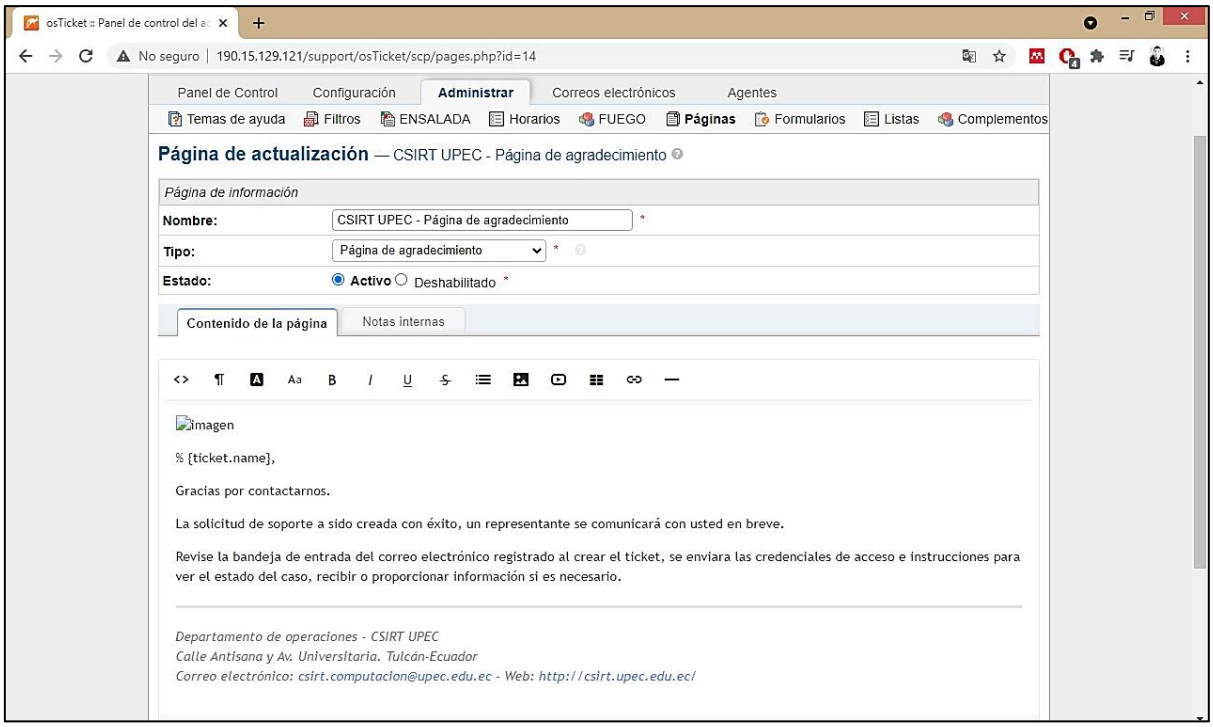


Figura 242. Crear la página CSIRT UPEC - Página de agradecimiento en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para crear la página fuera de servicio, se da clic en añadir nueva página donde se despliega un formulario para su registro, se define el nombre de la página fuera de servicio, tipo página offline, estado activo y en contenido de página se añade la información respectiva como se muestra en la figura 243.

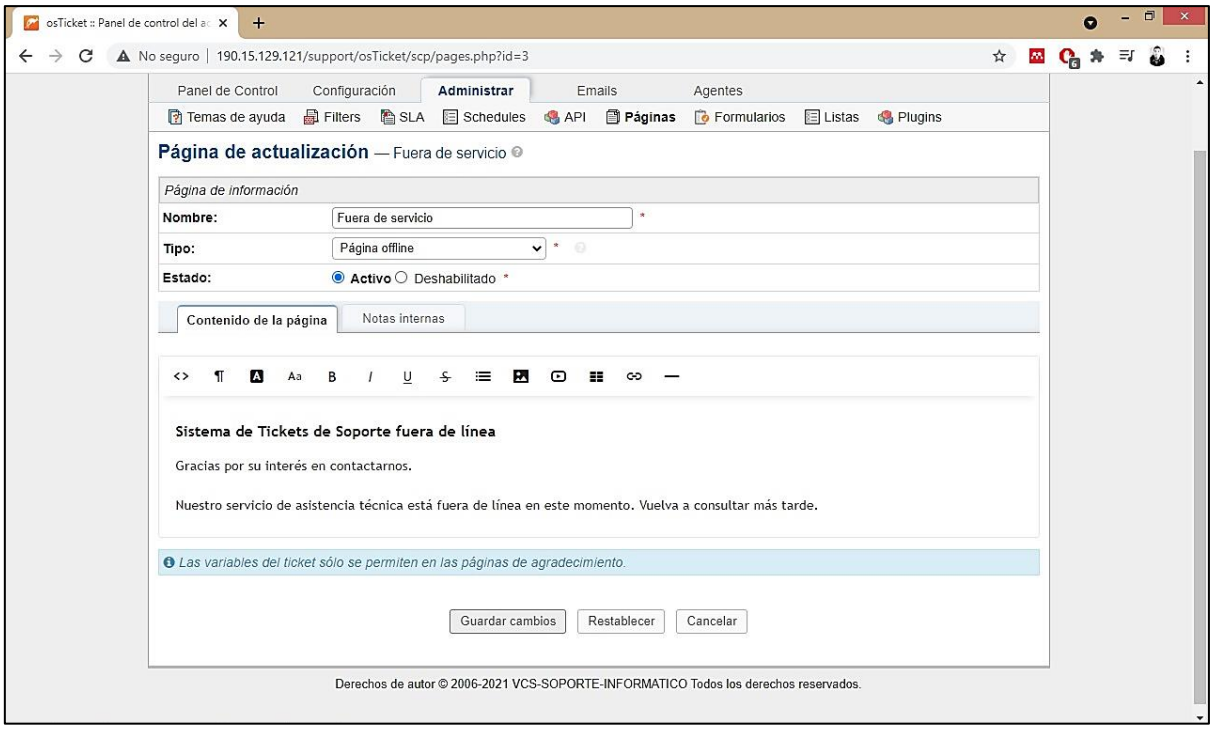


Figura 243. Crear la página fuera de servicio en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar las páginas creadas, se selecciona la opción páginas, donde se muestra una tabla con nombre de la página, tipo, estado, fecha de creación y última actualización como se muestra en la figura 244.

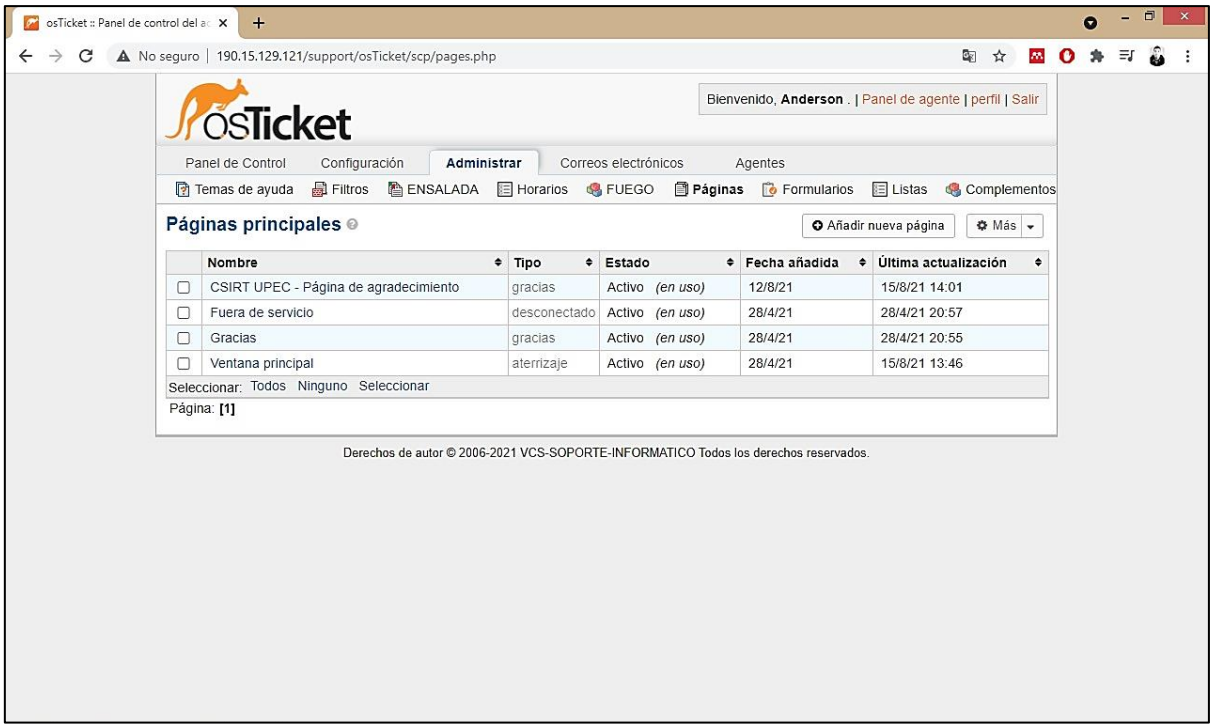


Figura 244. Administración de páginas creadas en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de formularios**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú administrar, se selecciona la opción formularios.

  Para crear el formulario CSIRT UPEC- Concienciación tecnológica, se da clic en añadir nuevo formulario personalizado donde se despliega un formulario para su registro, se define el nombre del formulario CSIRT UPEC- Concienciación tecnológica y las instrucciones. En los campos del formulario se establece la etiqueta tipo de organización de tipo opciones (educativa y gubernamental), visibilidad requerida y la variable tipoorgn, la etiqueta nombre de la organización de tipo respuesta corta, visibilidad requerida y variable nombreorgn, la etiqueta detalles de la concientización de tipo salto de sección y variable detallesconc, la etiqueta temática requerida de tipo respuesta larga, visibilidad requerida y variable tematicaconc, la etiqueta forma de concientización de tipo opciones (online y presencial), visibilidad requerida y variable formaconc y en la etiqueta fecha aproximada del acercamiento de tipo fecha y hora, visibilidad requerida y variable fechaconc, clic en guardar cambios como se muestra en la figura 245.

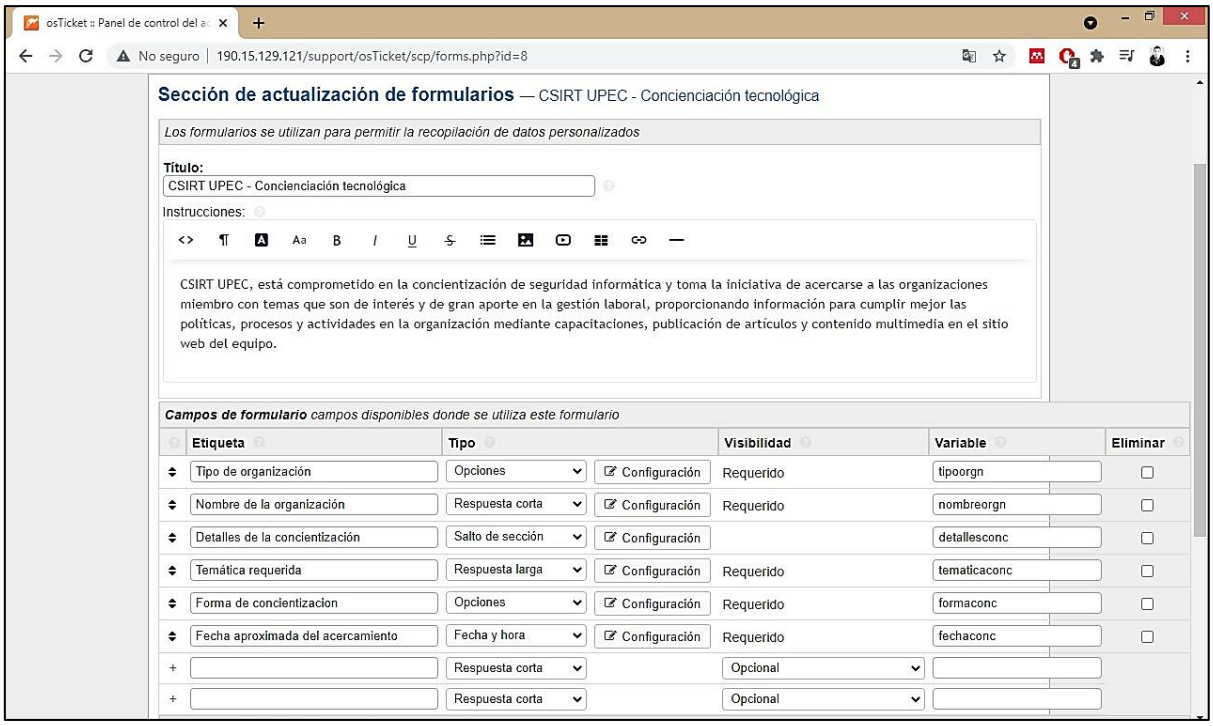


Figura 245. Configuración del formulario CSIRT UPEC - Concienciación tecnológica en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para crear el formulario CSIRT UPEC- Reportar incidente informático, se da clic en añadir nuevo formulario personalizado donde se despliega un formulario para su registro, se define el nombre del formulario CSIRT UPEC- Reportar incidente informático y las instrucciones. En los campos del formulario se establece la etiqueta tipo de organización tipo opciones (educativa y gubernamental), visibilidad requerida y variable tipoorg, la etiqueta nombre de la organización de tipo respuesta corta, visibilidad requerida y variable nombreorg, la etiqueta estado actual del incidente de tipo opciones (ya pasó, en curso, amenaza y desconocido), visibilidad requerida y variable estadoinci, la etiqueta cuando se detectó el incidente de tipo fecha y hora, visibilidad requerida y variable fechainci, la etiqueta detalles del incidente de tipo salto de sección y variable detallesinci, la etiqueta descripción del incidente informático de tipo respuesta larga, visibilidad requerida y variable descripcioninci y la etiqueta he leído y acepto las políticas de seguridad tipo casilla de verificación, visibilidad requerida y variable politicainci, clic en guardar cambios como se muestra en la figura 246.

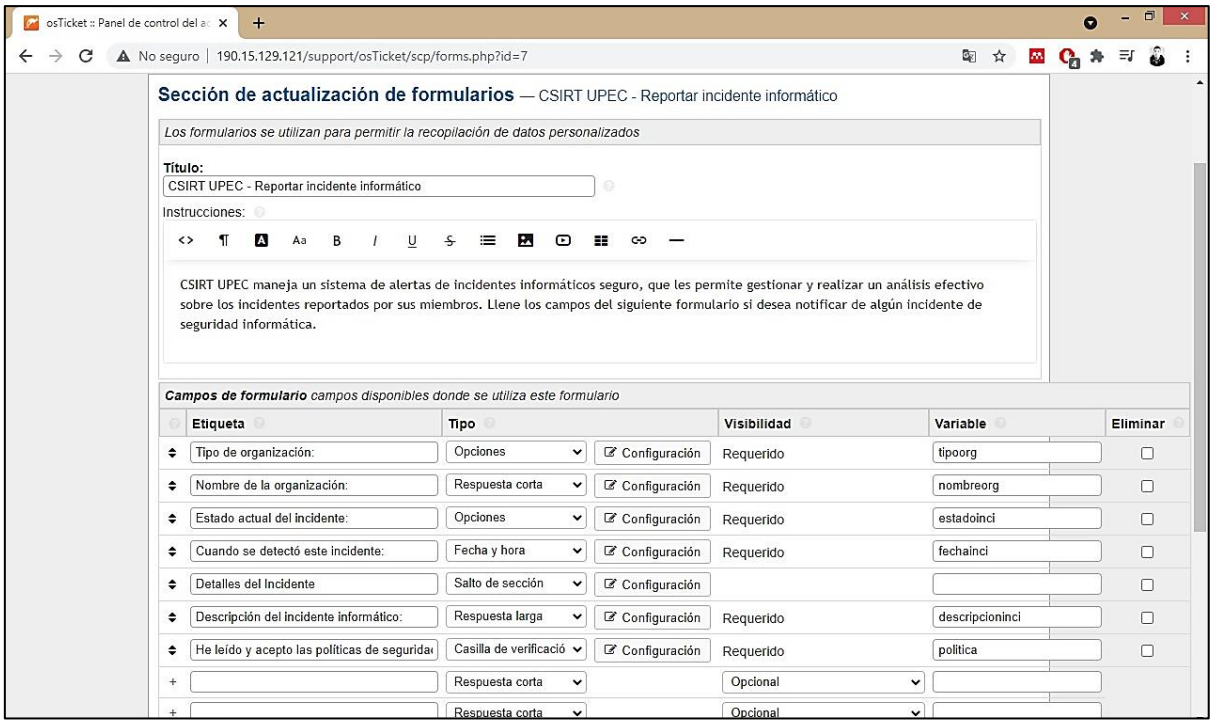


Figura 246. Configuración del formulario CSIRT UPEC - Reportar incidente informático en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los formularios creados, se selecciona la opción formularios, donde se muestra una tabla con nombre de los formularios existentes y fecha de última actualización como se muestra en la figura 247.

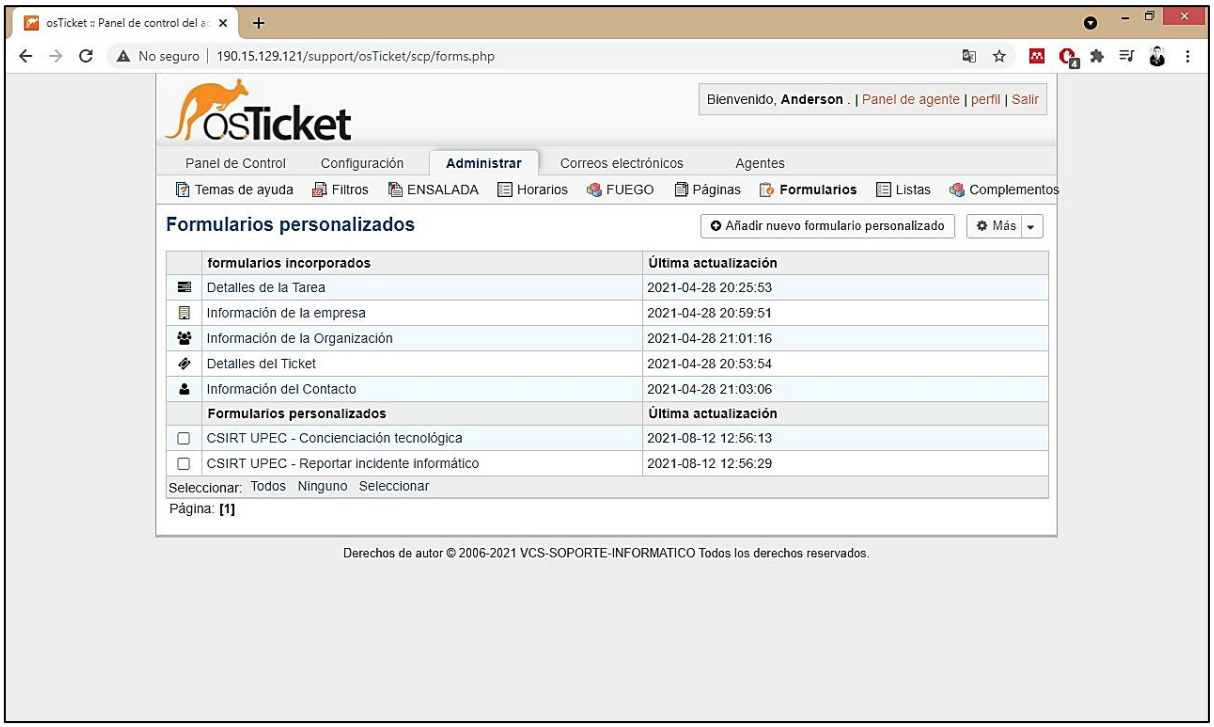


Figura 247. Página de administración de formularios personalizados en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de correo electrónico**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú emails y se selecciona la opción emails.

  Para añadir un nuevo email, se da clic en añadir nuevo email donde se despliega un formulario para su registro, en información y ajustes de email se define el correo electrónico csirt.computacion@upec.edu.ec y nombre del correo CSIRT UPEC, en nueva configuración de ticket se establece el departamento operaciones CSIRT, prioridad normal y temas de ayuda como sistema predeterminado, en información de acceso se ingresa el nombre de usuario csirt.computacion@upec.edu.ec y contraseña, y en enviar emails mediante SMTP se define estado habilitado, nombre de host smtp.office365.com, numero de puerto 587, autenticación requerida activa, nombre de usuario csirt.computacion@upec.edu.ec y contraseña, clic en guardar cambios como se muestra en la figura 248.

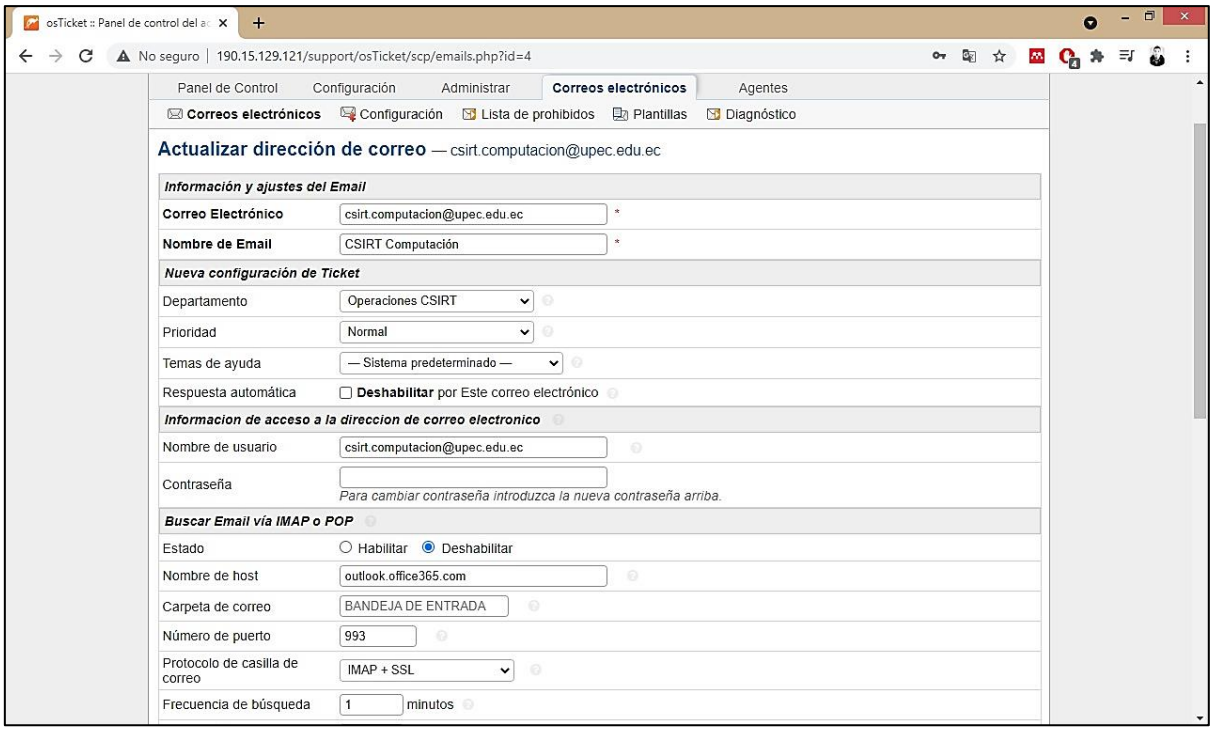


Figura 248. Configuración de correo electrónico de CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los correos electrónicos añadidos al sistema, se selecciona la opción emails, donde se muestra una tabla con nombre de email, prioridad, departamento, fecha creación y última actualización como se muestra en la figura 249.

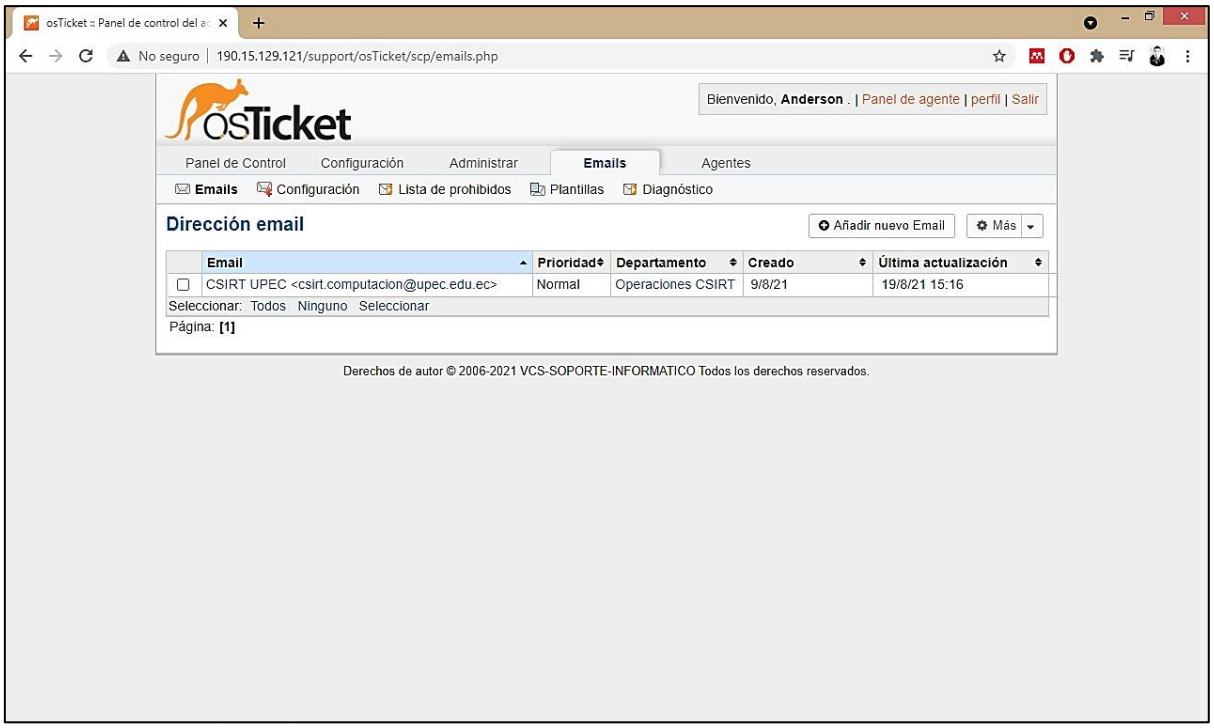


Figura 249. Página de administración de correos electrónicos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configurar plantillas de respuesta automáticas**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú emails y se selecciona la opción plantillas.

  Para añadir un conjunto de plantillas de correo electrónico, se da clic en añadir nuevo conjunto de plantillas, se define el nombre del conjunto respuestas CSIRT, estado permitido e idioma español. Para editar las plantillas se da clic en el título y se coloca el nombre del asunto en el cuerpo del correo, las variables que contienen información de los tickets, organizaciones y demás, y en el pie del correo se coloca el logo de CSIRT UPEC e información de contacto como se muestra en la figura 250, clic en guardar cambios.

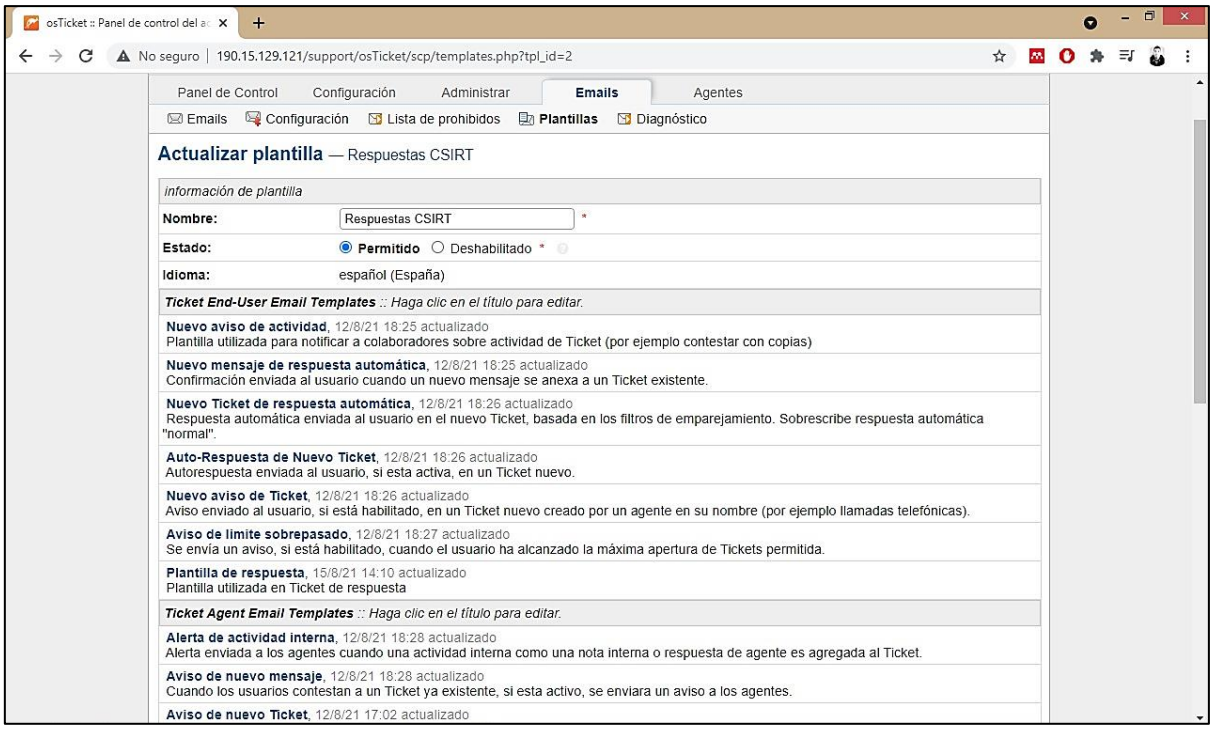


Figura 250. Configuración de plantillas de correo electrónico automáticas en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar las plantillas de correo electrónico, se da clic en la opción plantillas, donde se muestra una tabla con el nombre del conjunto de plantillas, su estado, si está en uso, fecha creación y última actualización como se muestra en la figura 251.

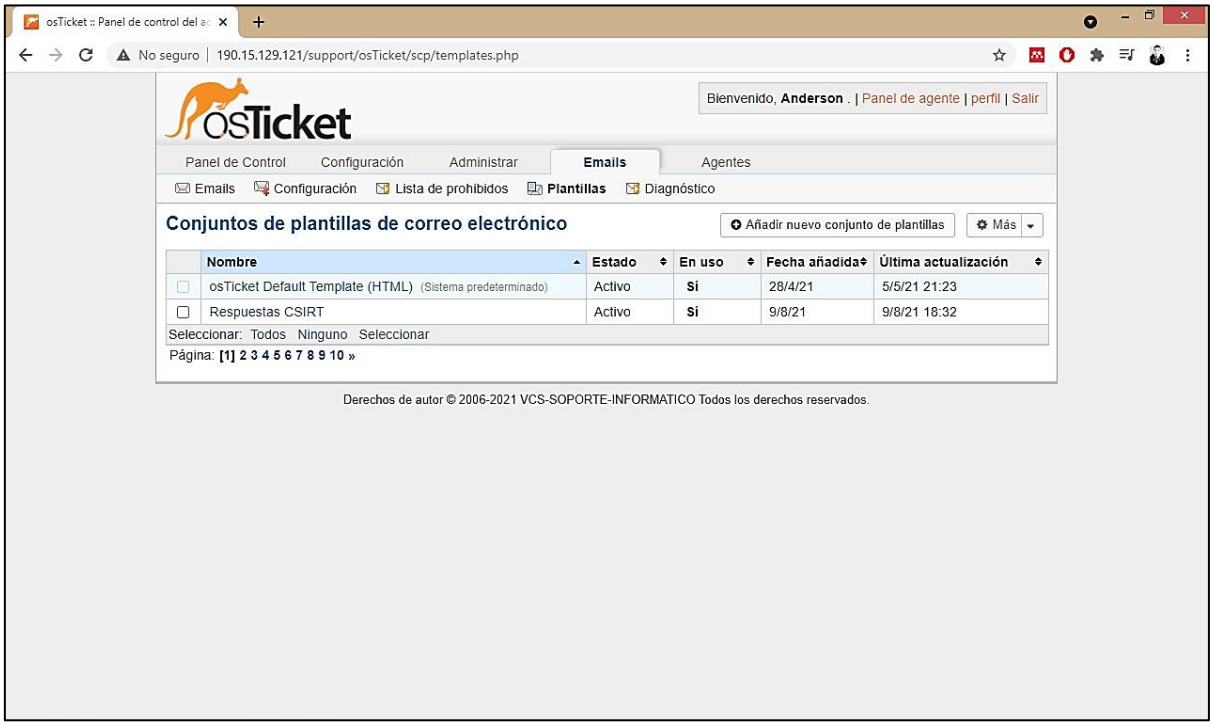


Figura 251. Página de administración de plantillas automáticas de correo electrónico CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de agentes**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú agentes y se selecciona la opción agente.

  Para añadir un nuevo agente, se da clic en añadir nuevo agente donde se despliega un formulario de registro, se define los nombres, correo electrónico, teléfono, nombre de usuario, rol que desempeña, departamento primario y los permisos como se muestra en la figura 252.

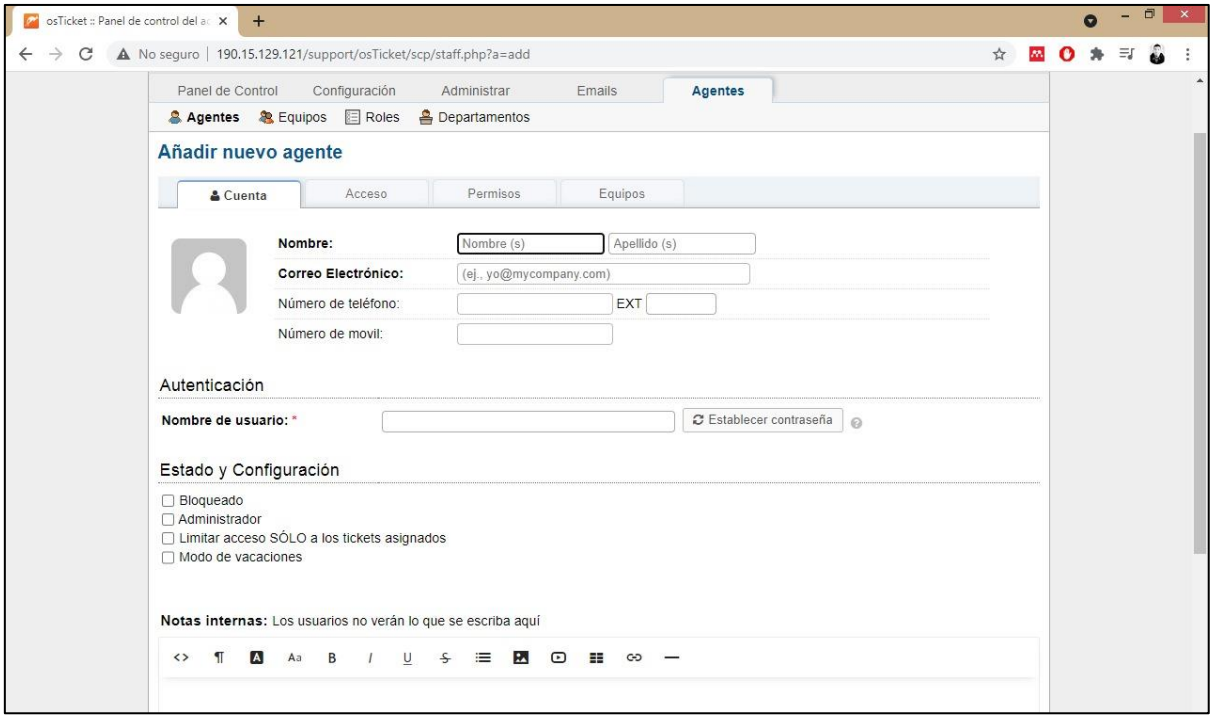


Figura 252. Configuración de agentes CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los agentes de CSIRT UPEC, se da clic en la opción agentes, donde se muestra una tabla con el nombre del agente, nombre de usuario, estado, departamento, fecha de creado y su ultimo inicio de sesión como se muestra en la figura 253.

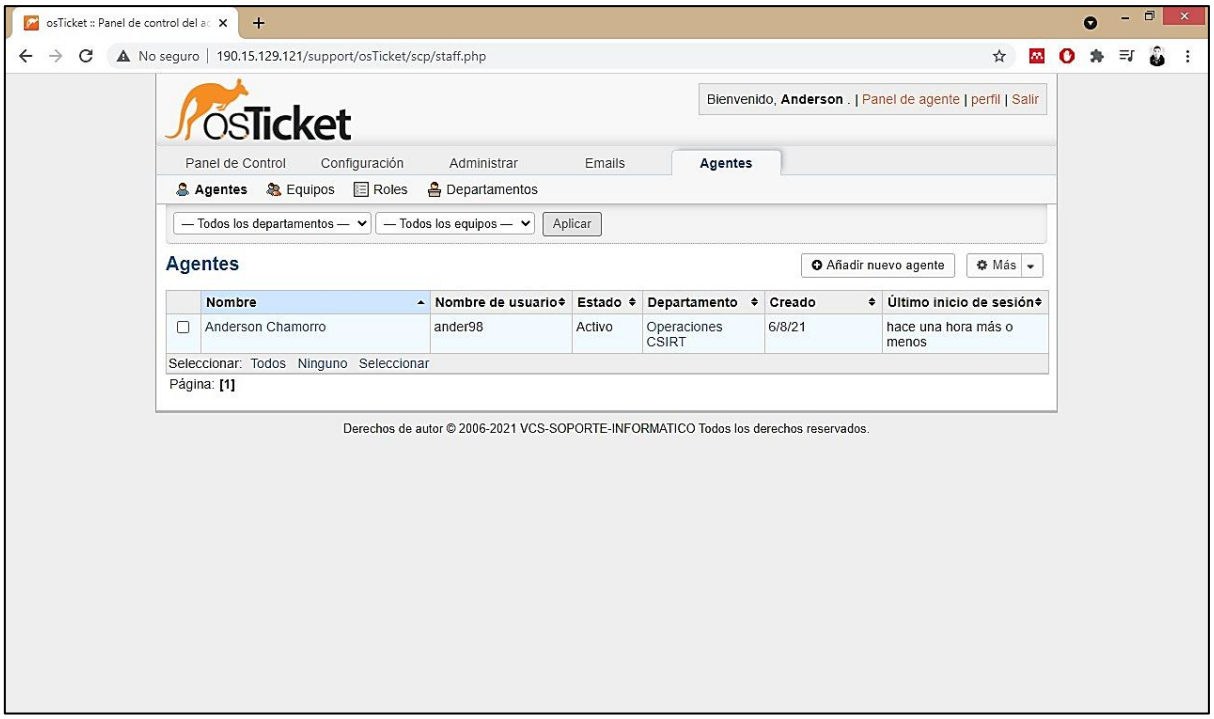


Figura 253. Página de administración de agentes CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de departamentos**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú agentes y se selecciona la opción departamentos.

  Para añadir un nuevo departamento, se da clic en añadir un nuevo departamento donde se despliega un formulario de registro, se define como departamento principal, nombre operaciones CSIRT, estado activo, tipo público, nombre del administrador, asignar tickets por miembros del departamento, email saliente CSIRT UPEC <csirt.computacion@upec.edu.ec>, conjunto de plantillas respuestas CSIRT, email de respuesta automática CSIRT UPEC <csirt.computacion@upec.edu.ec> y alertas y notificaciones solo a miembros del departamento como se muestra en la figura 254, clic en guardar cambios.

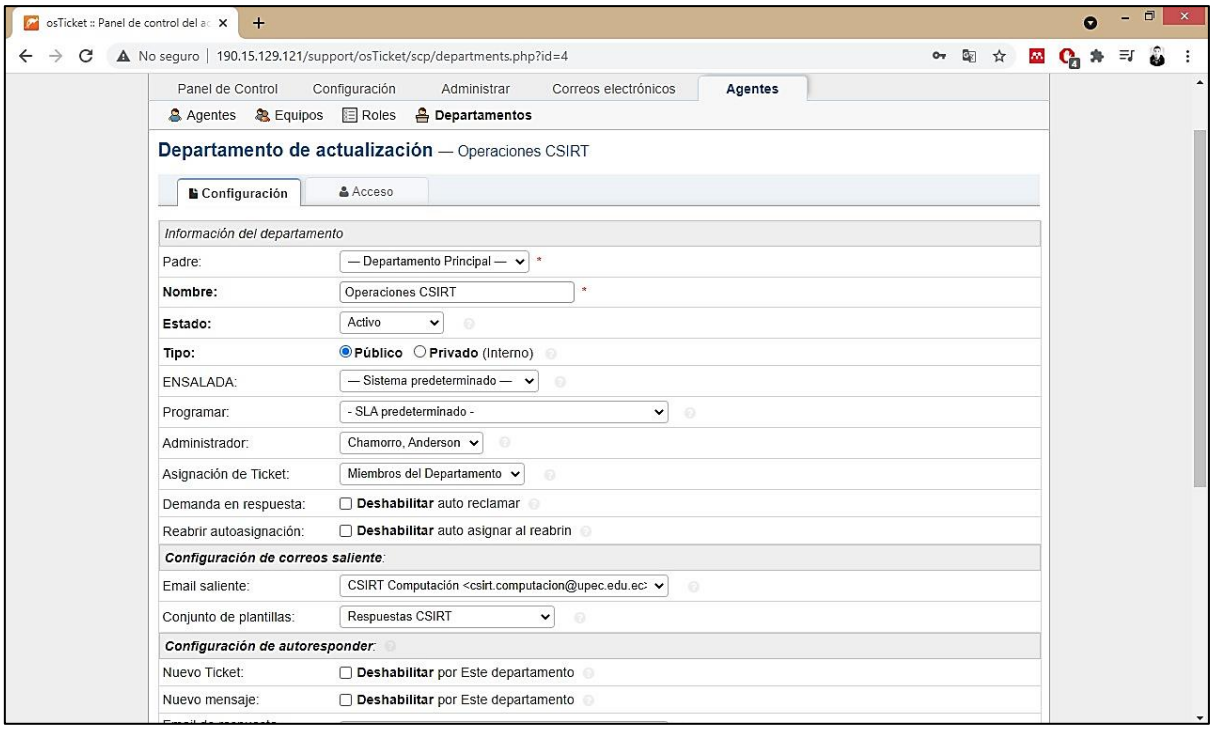


Figura 254. Configuración de departamentos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los departamentos de CSIRT UPEC, se da clic en la opción departamentos donde se muestra una tabla con el nombre del departamento, estado, tipo, número de agentes que conforman el departamento, correo electrónico, nombre del administrador y fecha creada como se muestra en la figura 255.

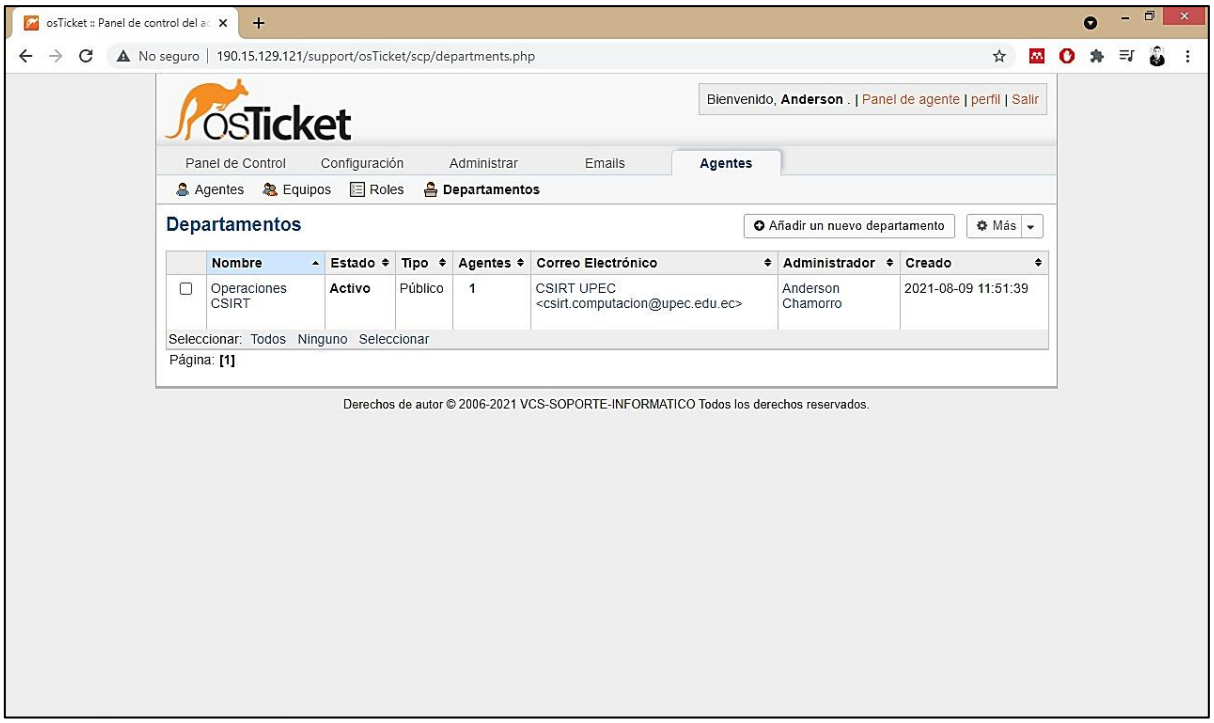


Figura 255. Página de administración de departamentos CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de usuarios**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú usuarios y seleccionar la opción directorio de usuarios.

  Para añadir un nuevo usuario, se da clic en añadir usuario donde se despliega un formulario de registro, se define correo electrónico, nombres, número de teléfono y clic en añadir usuario como se muestra en la figura 256.

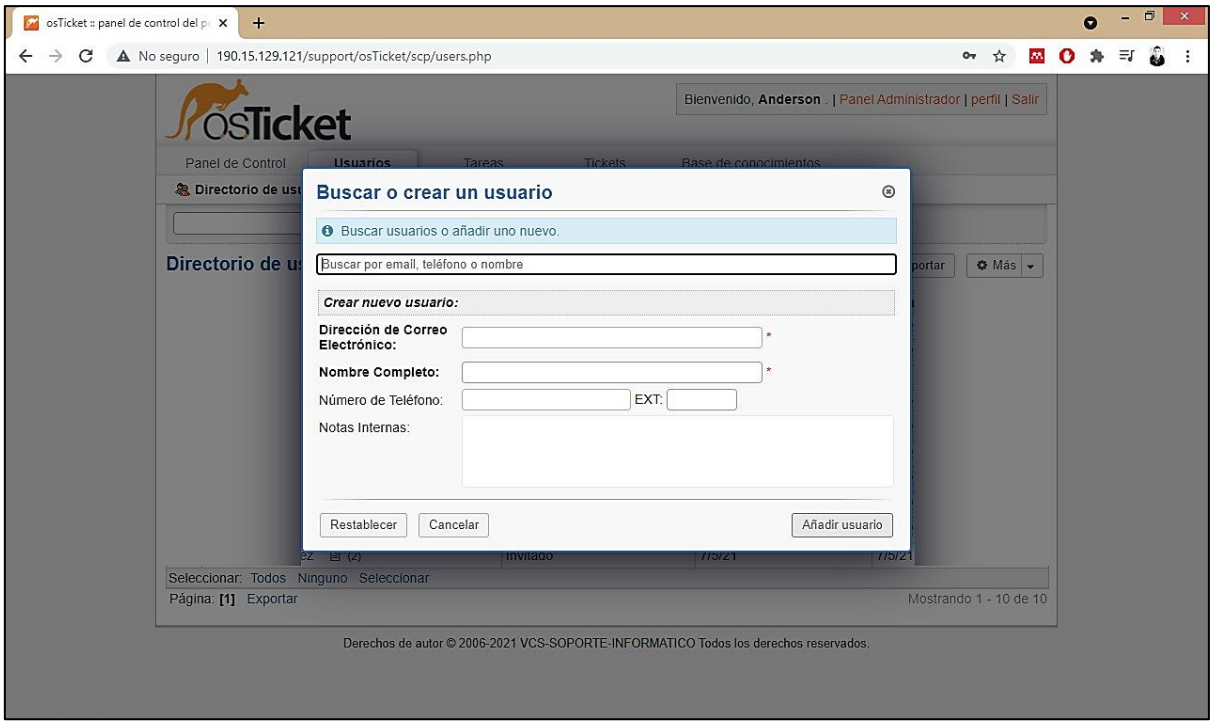


Figura 256. Configuración de un nuevo usuario CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar los usuarios de CSIRT UPEC, se da clic en la opción usuarios donde se muestra una tabla con el nombre del usuario, estado, y fecha de creado y actualizado como se muestra en la figura 257.

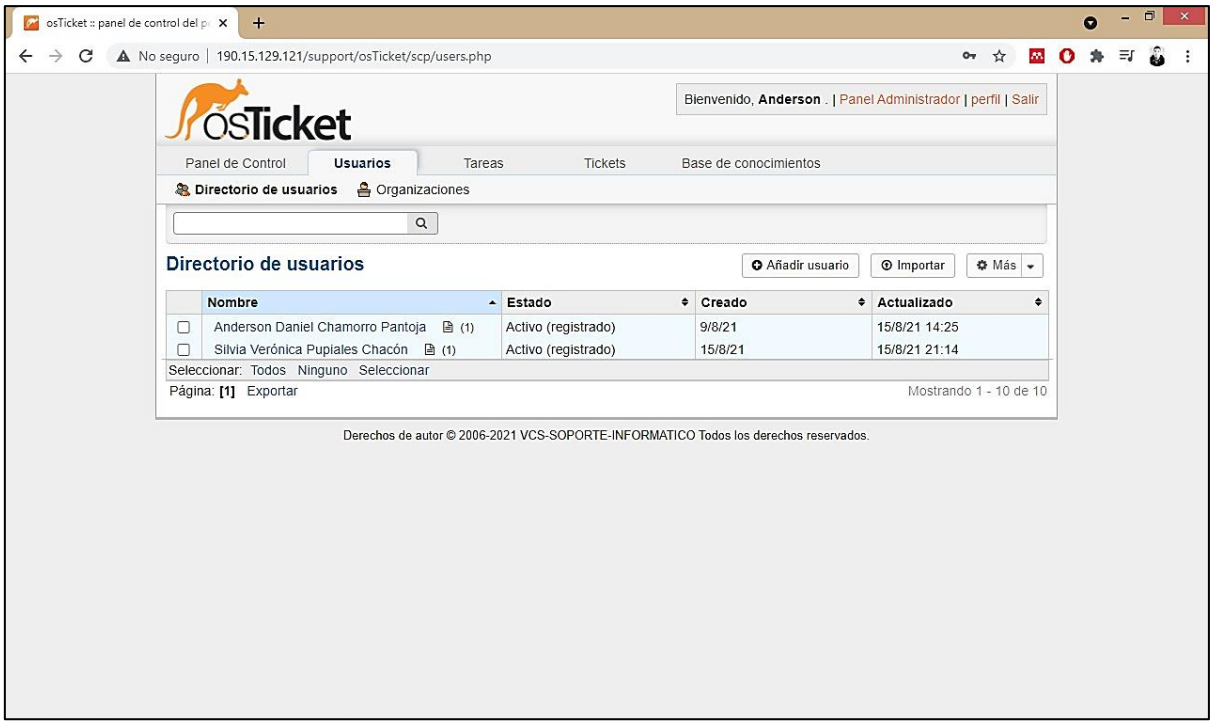


Figura 257. Página de administración de usuarios CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

- **Configuración de organizaciones**

  Se ingresa al panel de administrador del sistema Centro de Respuesta y Soporte a Incidentes de Seguridad, clic en el menú usuarios y se selecciona la opción organizaciones.

  Para añadir la organización Gobiernos Seccionales Provincia Carchi, se da clic en agregar organización donde se despliega un formulario de registro, se define el nombre Gobiernos Seccionales Provincia Carchi, dirección provincia Carchi y las notas internas como se muestra en la figura 258, clic agregar organización.

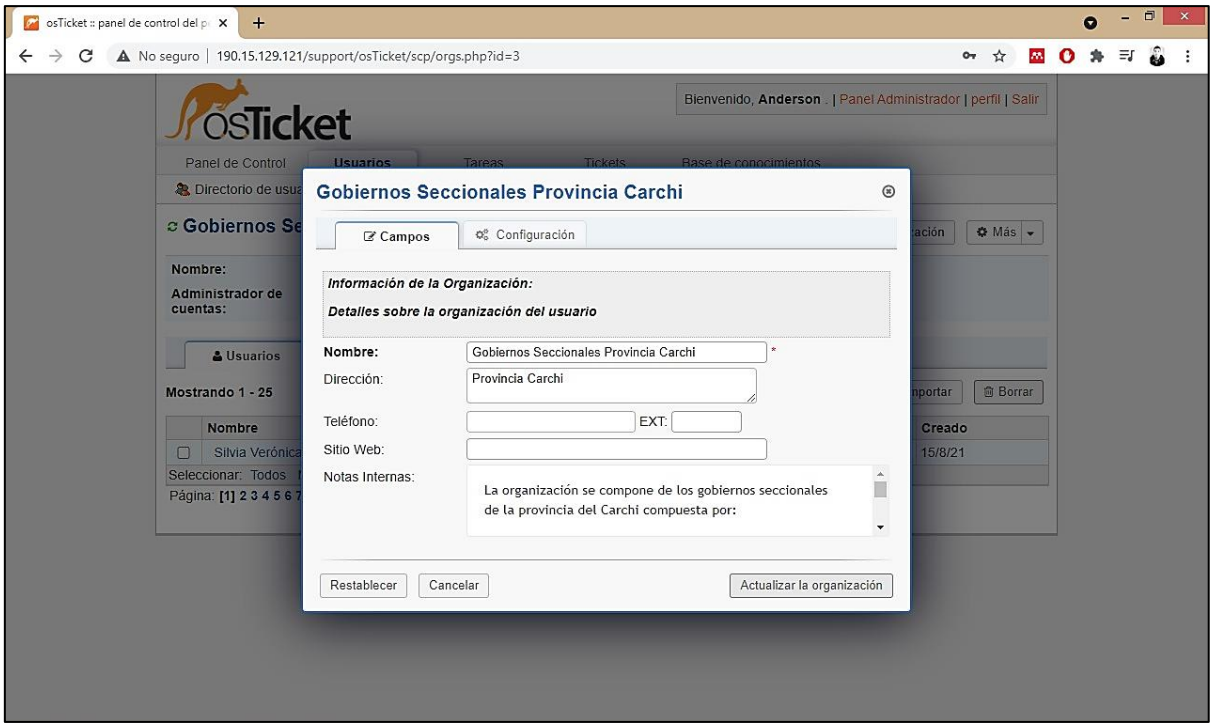


Figura 258. Configuración de la organización Gobiernos Seccionales Provincia Carchi en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para añadir la organización Unidades Educativas Provincia Carchi, se da clic en agregar organización donde se despliega un formulario de registro, se define el nombre Unidades Educativas Provincia Carchi, dirección provincia Carchi y las notas internas como se muestra en la figura 259, clic en agregar organización.

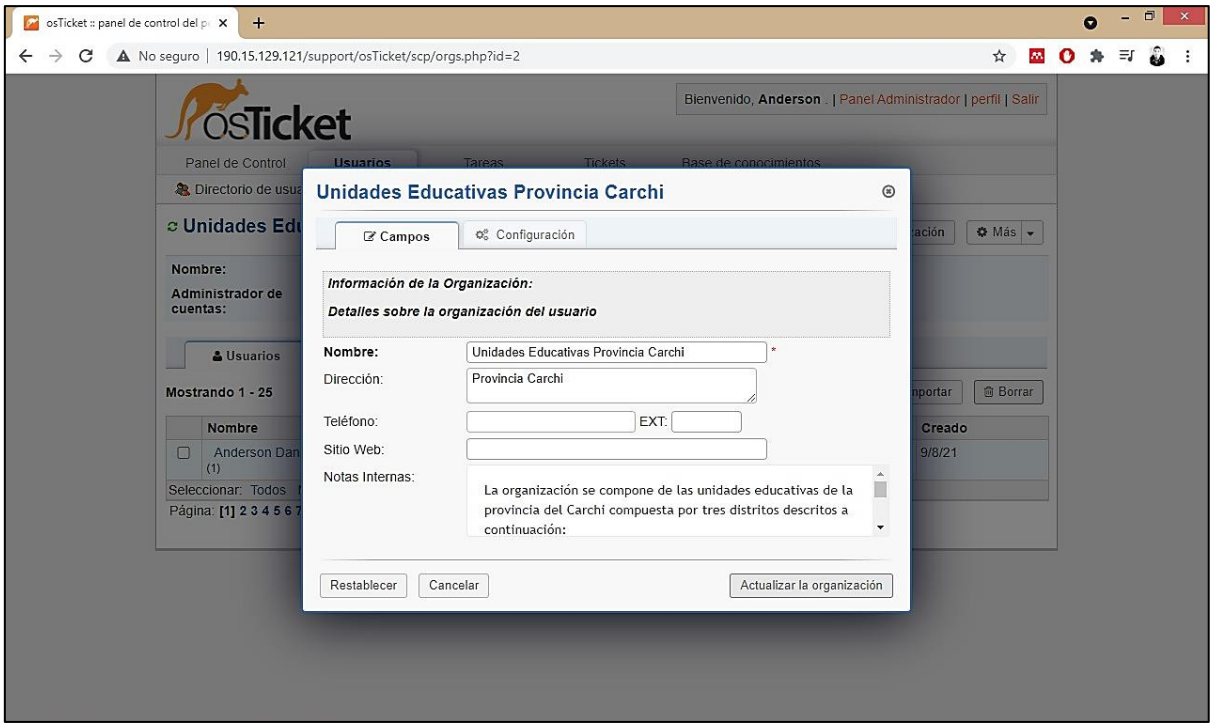


Figura 259. Configuración de la organización Unidades Educativas Provincia Carchi en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Para administrar las organizaciones de CSIRT UPEC, se da clic en la opción organizaciones donde se muestra una tabla con el nombre de la organización, número de usuarios que pertenecen a la organización fecha de creado y última actualización como se muestra en la figura 260.

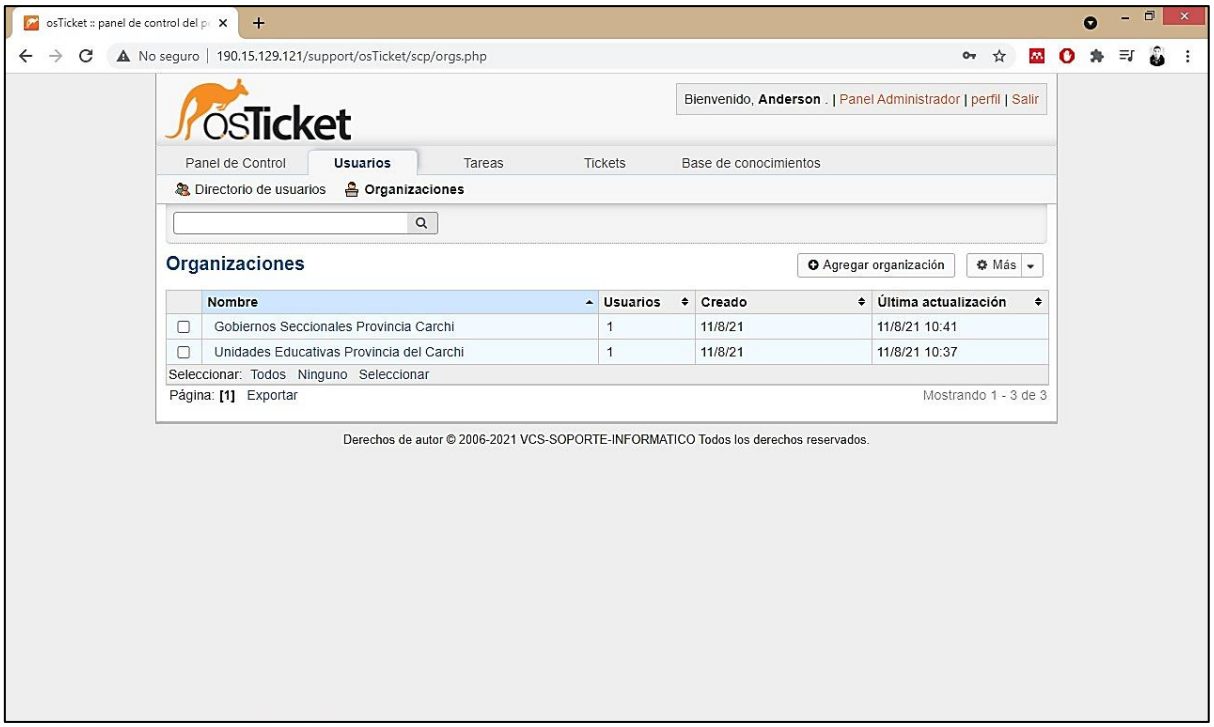


Figura 260. Página de administración de organizaciones CSIRT UPEC en el sistema Centro de Respuesta y Soporte a Incidentes de Seguridad

Anexo 20 Instalación y configuración de Nessus Essentials en Kali Linux.

Se ingresa a la página oficial de la herramienta de escaneo de vulnerabilidades Nessus "https://www.tenable.com/downloads/nessus?loginAttempted=true", clic en descargar la versión compatible con el servidor (Nessus-8.15.1-debian6_amd64.deb) y elegir la opción guardar archivo como se muestra en la figura 261.



Figura 261. Descarga del paquete Nessus de la página oficial

Una vez terminada la descarga, se ingresa a la terminal de Kali Linux y al directorio de descarga con el comando cd Descargas, se verifica que el paquete Nessus se encuentre en el directorio con el comando “ls” y se descomprime el paquete con el comando “dpkg -i Nessus-8.15.1-debian6_ amd64.deb” como se muestra en la figura 262.

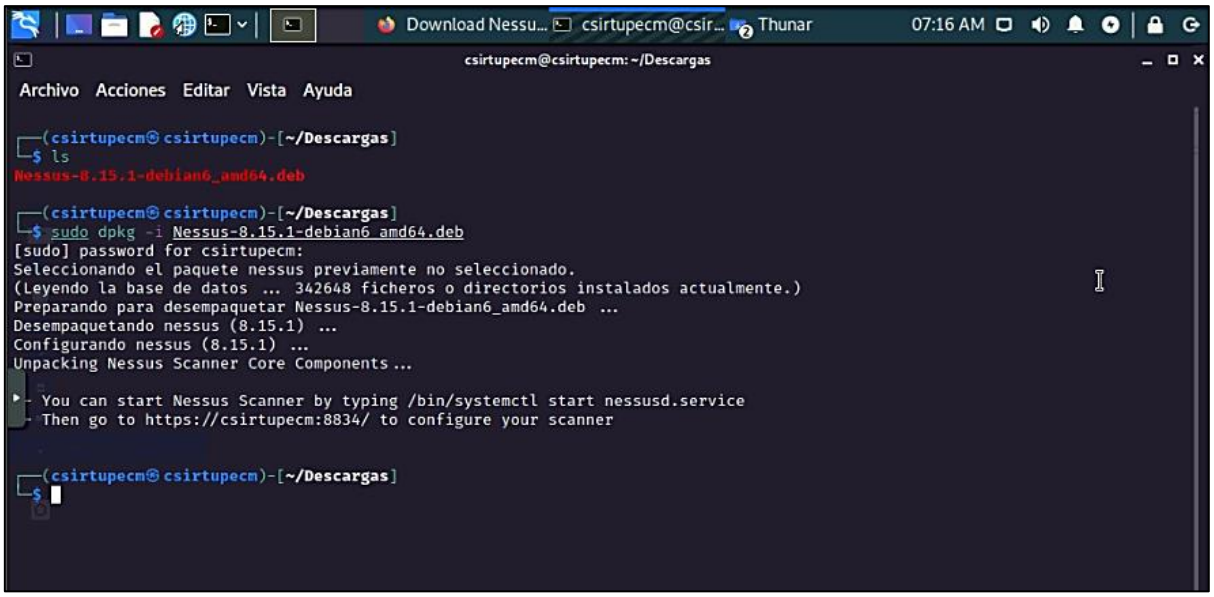


Figura 262. Verificar y descomprimir el paquete de instalación Nessus con la terminal de Kali Linux

Se inicia el servicio Nessus con el comando “systemctl start nessusd”, para activar el iniciado automático luego de reiniciar el servidor se ingresa el comando “systemctl enable nessusd” y se verifica el estado del servicio con el comando “systemctl status nessusd” como se muestra en la figura 263.

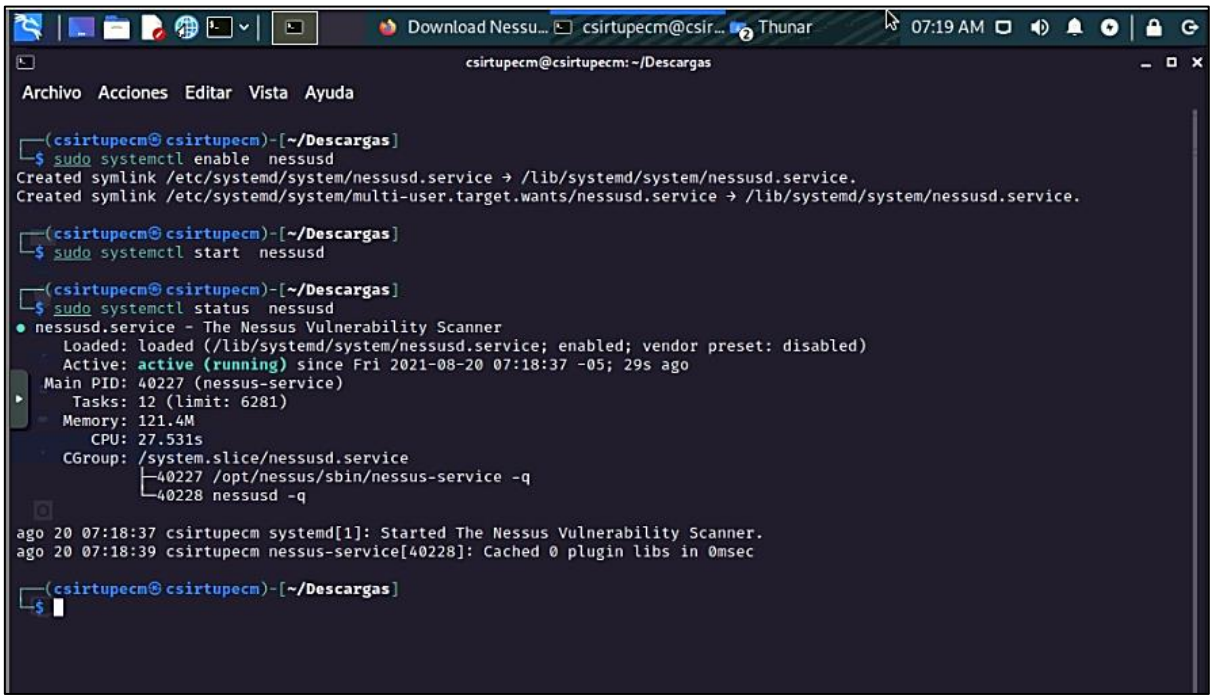


Figura 263. Activar el arranque automático y verificar el estado de la herramienta Nessus.

Se ingresa a la interfaz web con la URL https://127.0.0.1:8834 para terminar el proceso de instalación, se selecciona la versión a instalar Nessus Essentials y clic en continuar como se muestra en la figura 264.

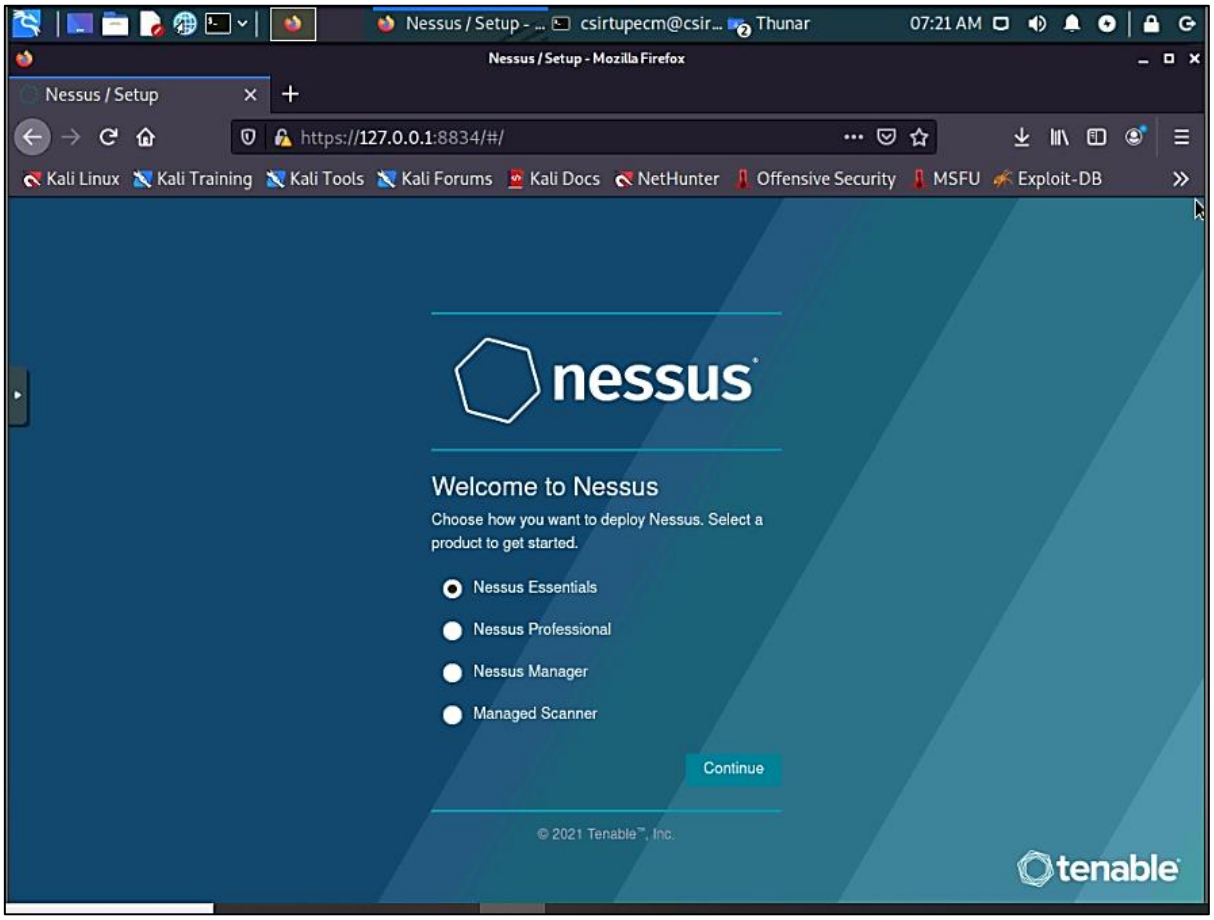


Figura 264. Selección de la versión de la herramienta Nessus a instalar

Se llena el formulario de registro para obtener el código de activación de acuerdo a la versión de Nessus seleccionada, se registra el nombre CSIRT, apellido UPEC, dirección de correo electrónico csirt.upec@gmail.com y clic en email como se muestra en la figura 265.

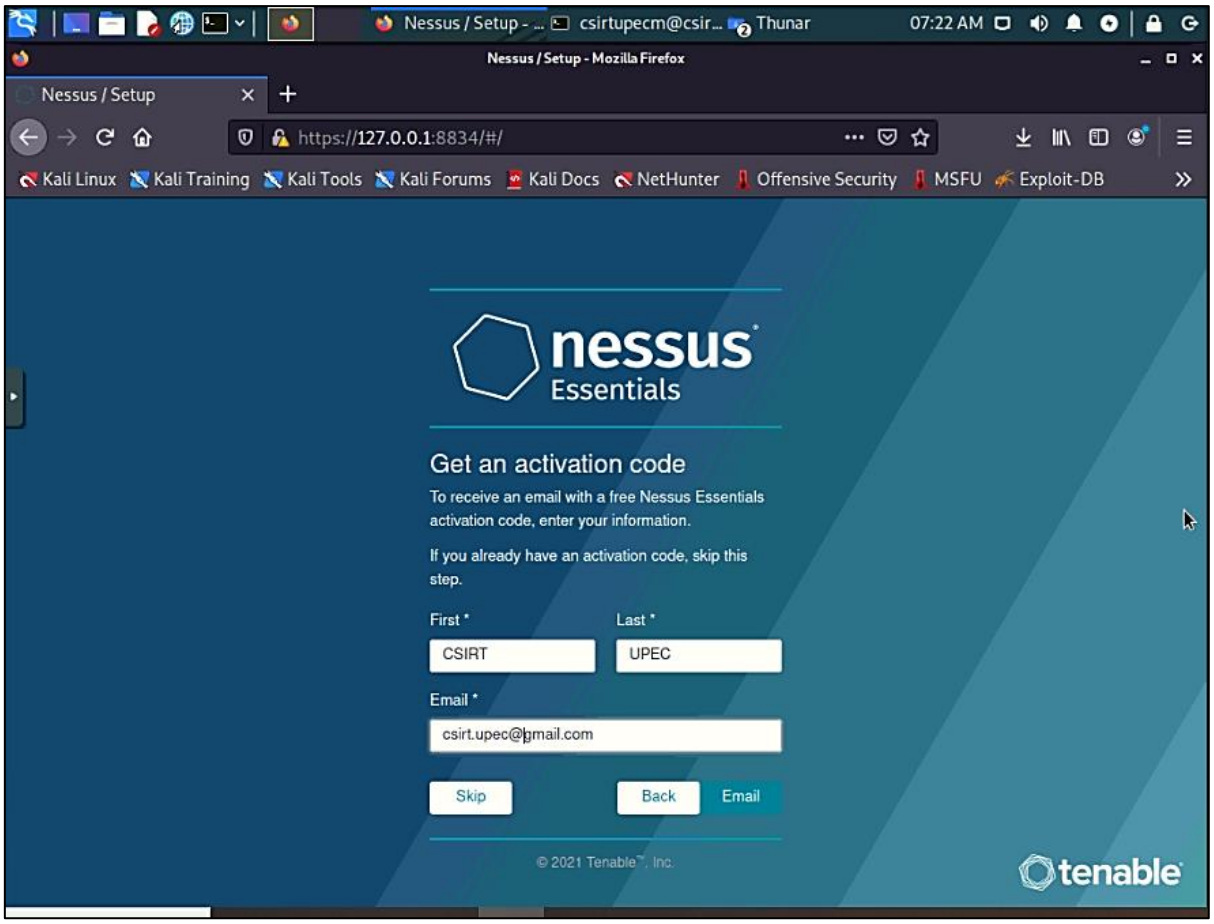


Figura 265. Registro para obtener el código de verificación de la herramienta Nessus

Se revisa el mensaje en la bandeja de entrada del correo registrado para la obtención del código de verificación como se muestra en la figura 266.



Figura 266. Correo electrónico con el código de activación para la herramienta Nessus

Se ingresa el código de activación de Nessus Essentials que se obtuvo mediante el correo electrónico y clic en continuar como se observa en la figura 267.

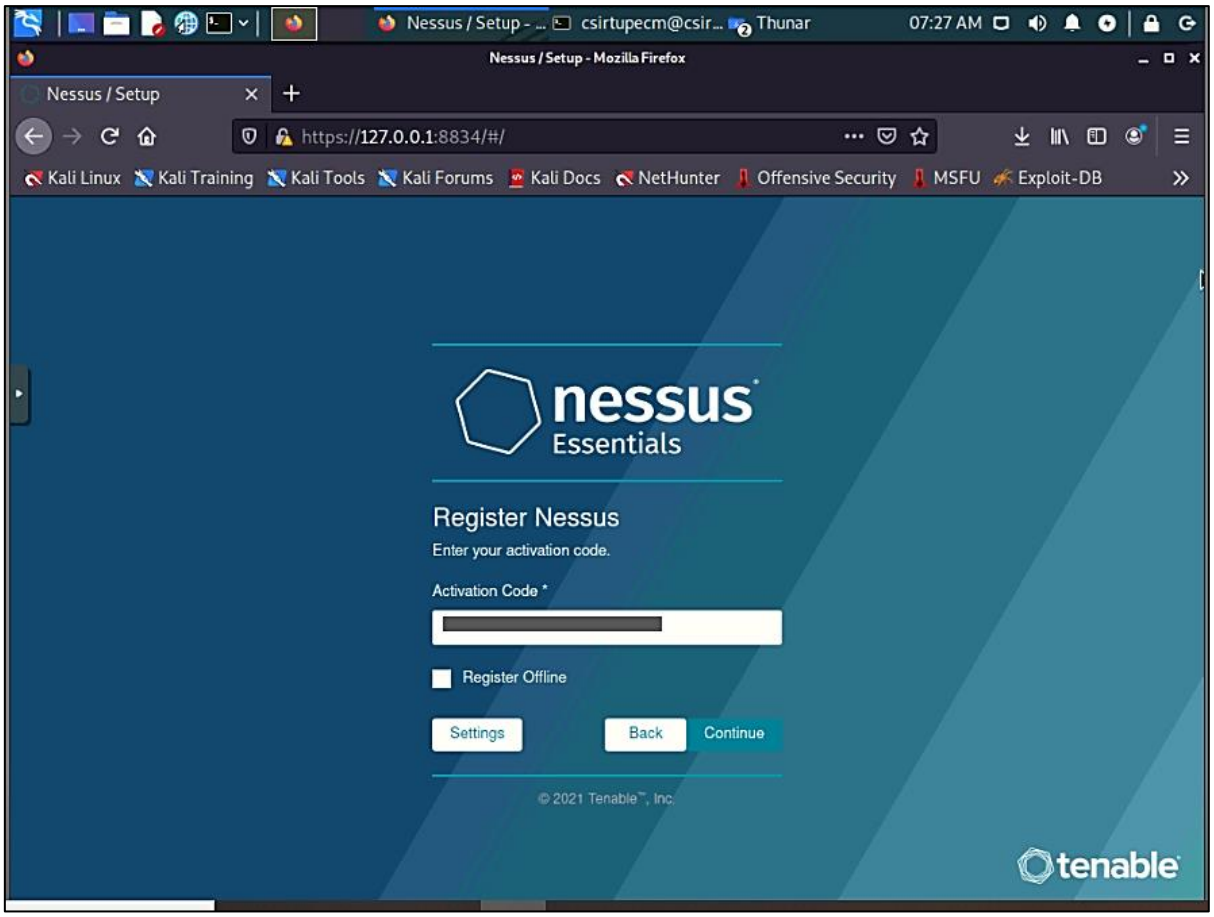


Figura 267. Ingreso del código de verificación de la herramienta Nessus

Se crea una cuenta de usuario csirtup y una contraseña para la administración de Nessus, clic en continuar como se muestra en la figura 268.

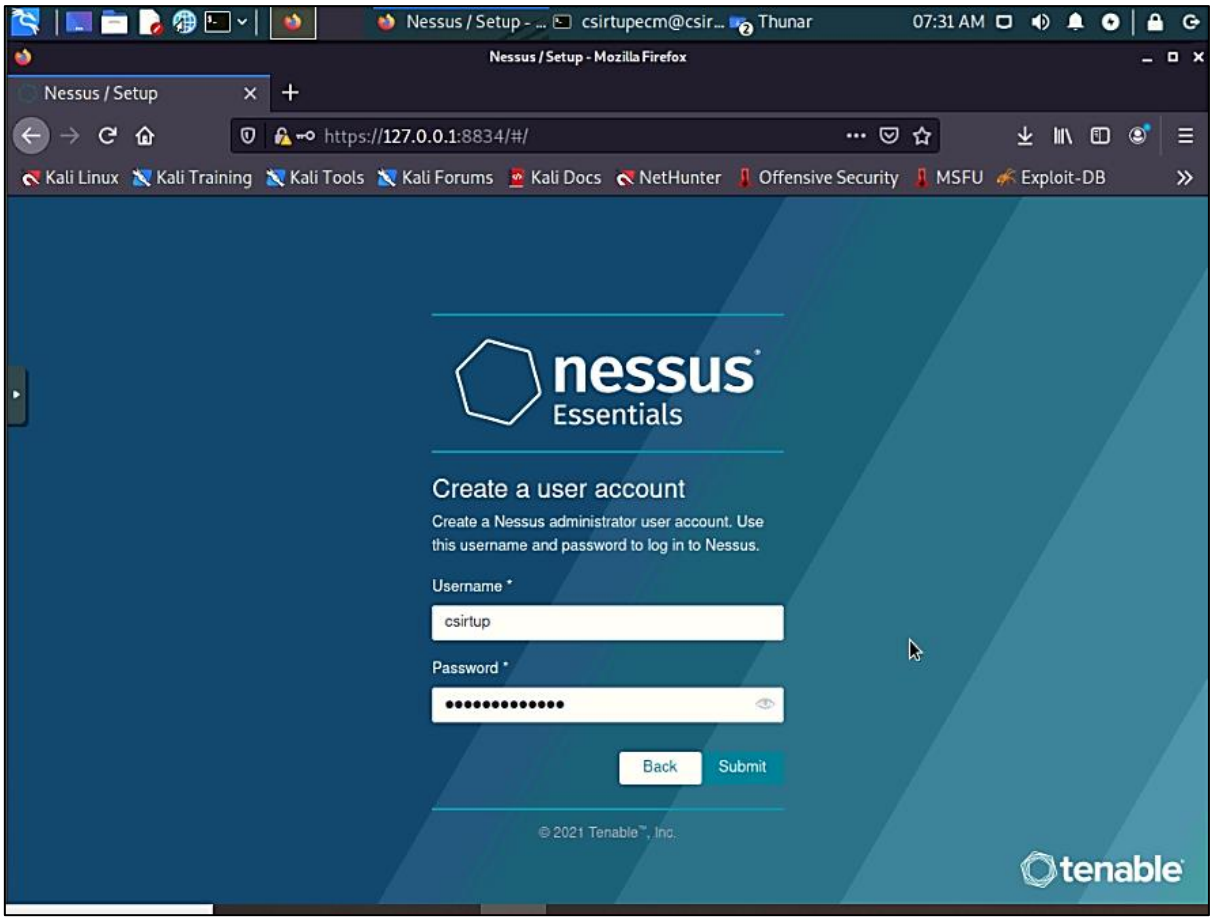


Figura 268. Registro de cuenta de usuario para la administración de la herramienta Nessus

Como se observa en la figura 269, se inicia la descarga instalación de los complementos necesarios para el funcionamiento de Nessus.

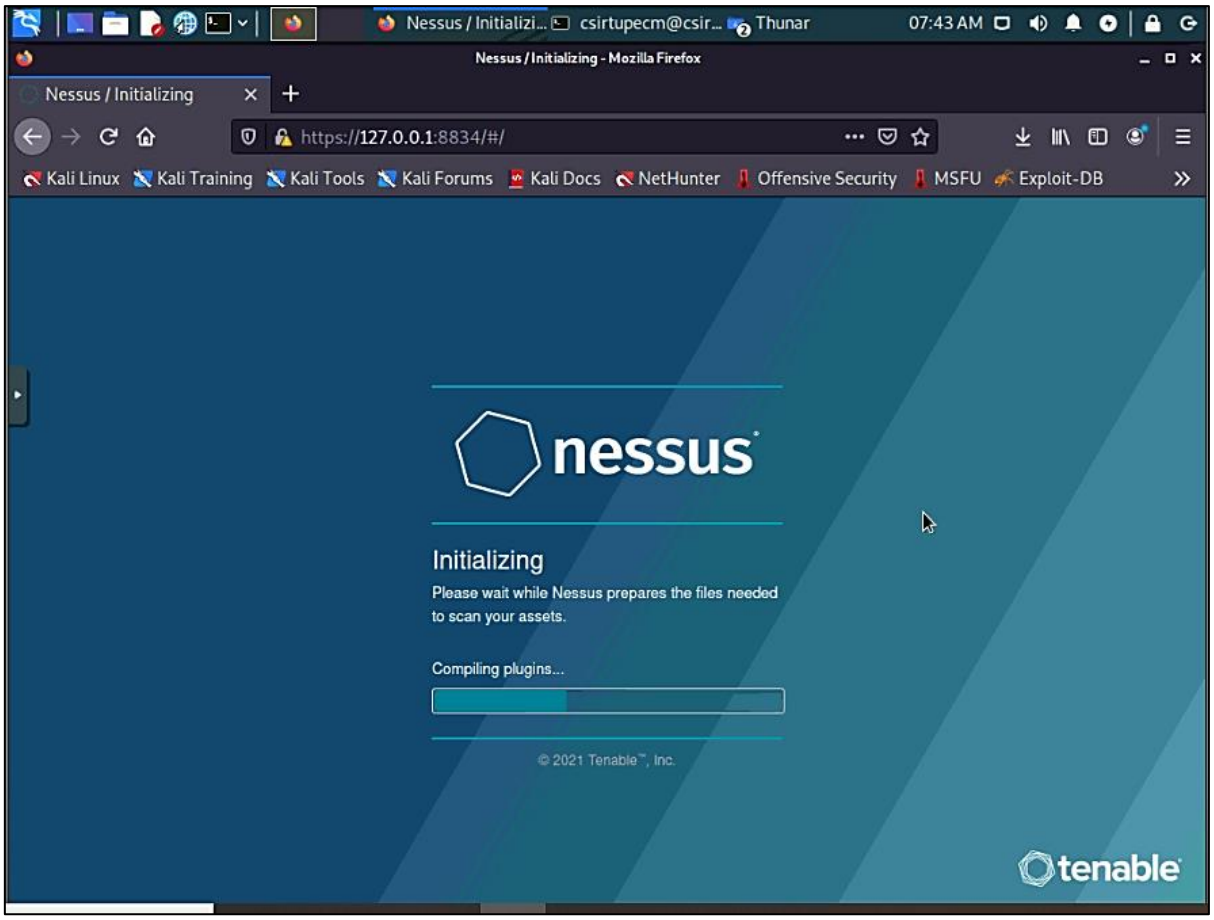


Figura 269. Instalación de complementos de la herramienta Nessus

Culminada la instalación de la herramienta Nessus Essentials, se muestra su área de trabajo con las opciones necesarias para la gestión de vulnerabilidades como se muestra en la figura 270.

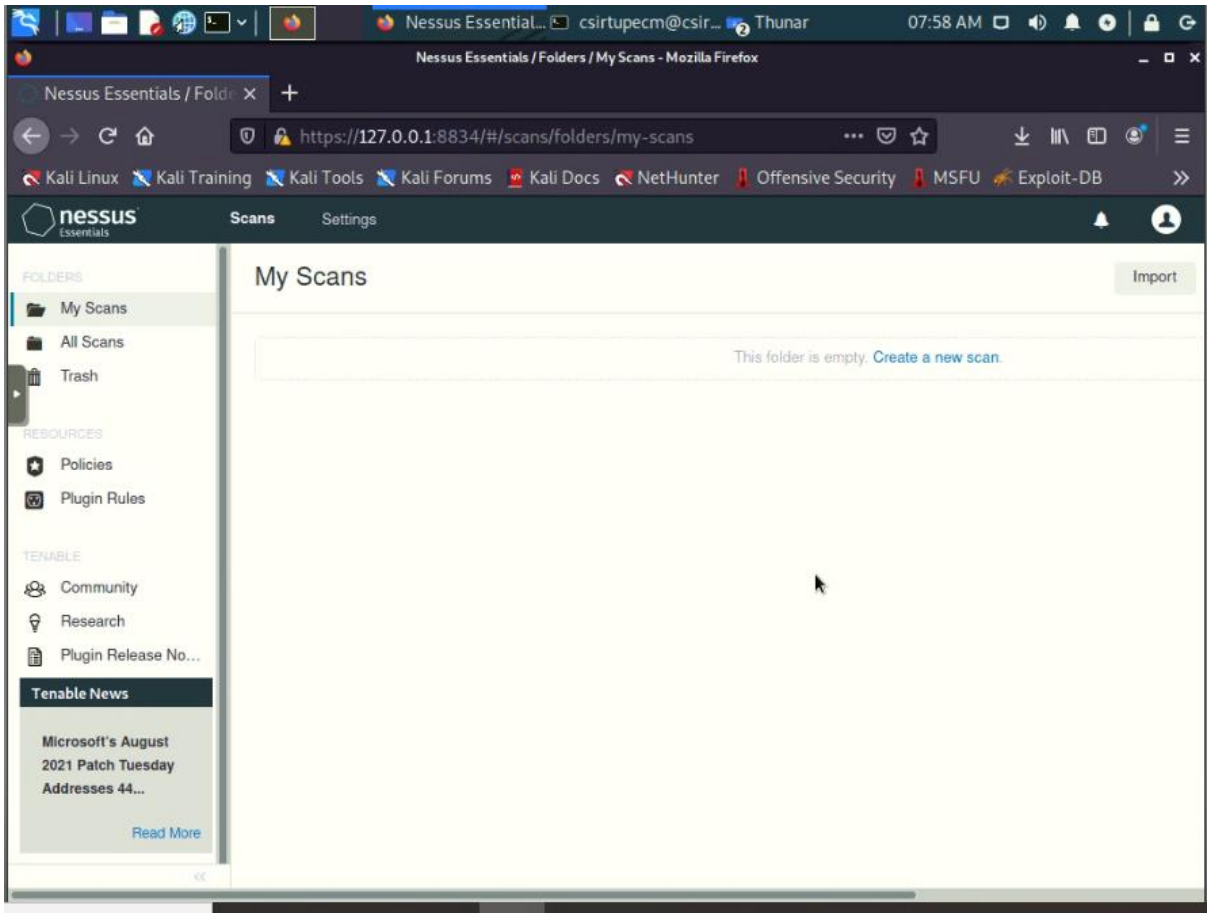


Figura 270. Área de trabajo de la herramienta Nessus

Anexo 21 Formato solicitud de destrucción de información.

SOLICITUD DE DESTRUCCIÓN DE INFORMACIÓN

Datos del solicitante

Nombres del solicitante:	
Departamento:	
Correo electrónico:	
Teléfono:	
Fecha de solicitud:	

Datos de la información a eliminar

N°	Título del documento	Descripción	Ruta de archivo

Observaciones:

Aprobación:	Si	No

_____

NOMBRE
LÍDER DEPARTAMENTO ----------

_____

NOMBRE
DIRECTOR(A) DE CSIRT UPEC

Figura 271. Formato solicitud de destrucción de información

Anexo 22 Formato informe final de destrucción de información.

INFORME FINAL DE DESTRUCCIÓN DE INFORMACIÓN

Datos generales

Nombres del personal a cargo:	
Departamento:	
Correo electrónico:	
Teléfono:	
Fecha de destrucción:	

Registro de destrucción

N°	Título del documento	Tipo de eliminación	Observaciones

Anexos
Nombre anexo N° 1
Nombre anexo N° 2
Nombre anexo N° 3
Nombre anexo N° …

_____

NOMBRE
LÍDER DEPARTAMENTO DE TECNOLOGÍA

_____

NOMBRE
DIRECTOR(A) DE CSIRT UPEC

Figura 272. Formato informe final de destrucción de información

Anexo 23 Formato compromiso de confidencialidad.

COMPROMISO DE CONFIDENCIALIDAD

En la ciudad de _____, a los ____ días del mes de _____ del año _____, el Sr./Sra._____ con CI/pasaporte _____, en su calidad de _____ del Equipo de Respuesta a Incidentes Informáticos CSIRT UPEC, declara que:

PRIMERO: Objetivo. - Por la prestación de servicios laborales, el trabajador puede acceder a documentos en físico y digital, equipos y software utilizado en la gestión de servicios del equipo. Está obligado a no divulgar la información que es considerada como confidencial, no puede exponerla a terceros porque podría causar perjuicios a las instituciones y generar una mala reputación de CSIRT UPEC.

SEGUNDO: Obligaciones de confidencialidad. - Se exige la confidencialidad de toda documentación de: informes, contratos, servicios, charlas, capacitaciones, reuniones, diálogos donde se intercambia información sumamente delicada y cualquier otro medio por el que el equipo maneje la información.
Acatar las medidas correctamente para el manejo de la información recibida de manera física o digital.

TERCERO: Finalización laboral. - Por cualquier motivo por el que se dé la terminación laboral, entregar todo tipo de documentación manejada como confidencial y la información mentalizada debe ser un secreto por respeto a la confidencialidad de CSIRT UPEC.

CUARTO: Sanciones. - CSIRT UPEC puede tomar acciones legales en el caso de incumplir el acuerdo de confidencialidad presentado en este documento, determinará los reglamentos y medidas necesarias que le corresponda para aplicar la sanción conveniente.

Demostrando la conformidad con el acuerdo en el lugar y fecha establecidos en la parte superior, se puntúa sus datos de identificación para constancia de la misma.

_____
Firma

C.I.

Figura 273. Formato compromiso de confidencialidad

Anexo 24 Formato reporte de incidentes informáticos.

REPORTE DE INCIDENTE DE SEGURIDAD INFORMÁTICA

CSIRT UPEC maneja un sistema de alertas de incidentes informáticos seguro, que les permite gestionar y realizar un análisis efectivo sobre los incidentes reportados por sus miembros. Llene los campos del siguiente formulario si desea notificar de algún incidente de seguridad informática.

Información de contacto:

Proporcione su información de contacto para que CSIRT UPEC se comunique con usted en caso de que se necesite realizar un seguimiento.

Quien reporta:		
Correo electrónico:		
Teléfono:		
Tipo de organización	Educativa:	
	Gubernamental:	
Nombre de la organización:		

Detalles del incidente:

Los detalles de un incidente son esenciales para entender el porqué del mismo y prever su impacto en los sistemas informáticos de la organización, a partir de ello, CSIRT UPEC otorgará una respuesta adecuada a dicho incidente. Por favor, mencione todos los detalles que le sea posible.

Cuando se detectó el incidente	Fecha:		
	Hora:		
Estado actual del incidente	Ya pasó:		
	En curso:		
	Amenaza:		
	Desconocido:		
Descripción del incidente:			

Figura 274. Formato reporte de incidentes informáticos

Anexo 25 Formato de valoración de incidentes.

VALORACIÓN DEL INCIDENTE

Información de valoración del incidente:

Fecha y hora de valoración:	
Nombre de quien valora:	
Observaciones de la valoración:	

Información general del incidente:

Fecha y hora de reporte:	
Código de ticket:	
Descripción del incidente:	

Consultar el reporte de incidentes emitido por la institución afectada para completar la descripción del incidente.

Priorización del incidente

Nivel de criticidad	Riesgo alto:	
	Riesgo medio:	
	Riesgo bajo:	
Incidente informático	Clasificación:	
	Tipo:	
Tiempo aproximado para ser atendido:		

Consultar la matriz de priorización de incidentes para completar la siguiente información.

Asignación de recursos

Recursos humanos		
Nombre	Cargo	Correo electrónico

Recursos tecnológicos		
Recurso	Detalle	Cantidad

NOMBRE
LÍDER DEPARTAMENTO DE OPERACIONES

NOMBRE
DIRECTOR(A) DE CSIRT UPEC

Figura 275. Formato de valoración de incidentes

Anexo 26 Formato de notificación por correo sobre la confirmación del formulario para reportar incidentes.

NOTIFICACIÓN – RECEPCIÓN DEL FORMULARIO DE REPORTE A INCIDENTES INFORMÁTICOS

Mensaje nuevo

Destinatario	nombre@dominio.dominio
Asunto	CSIRT-Reportar Incidente [#ticket]

Saludos cordiales. -

Su solicitud ha sido recibida y será revisada por nuestro personal de operaciones. Para conocer y proporcionar información adicional acerca de la solicitud del servicio, ingrese al Centro de Respuesta y Soporte a Incidentes dando clic al siguiente enlace:

Dirección URL: Conocer el estado de mi ticket

Número de ticket: ######

Soporte - CSIRT UPEC
Calle Antisana y Av. Universitaria. Tulcán-Ecuador
Correo electrónico: csirt.computacion@upec.edu.ec - Web: https://csirt.upec.edu.ec/

Figura 276. Formato de notificación por correo sobre la confirmación del formulario para reportar incidentes

Anexo 27 Formato de informe de resultados en la gestión del incidente.

INFORME DE RESULTADOS EN LA GESTIÓN DEL INCIDENTE

Código de ticket:	

Estado del incidente

Estado del incidente:	
Fecha y hora de finalización:	

Información de la institución atendida

Nombre de quien reporta:		
Tipo de organización	Educativa:	
	Gubernamental:	

Nombre de la organización:	
Teléfono:	
Correo electrónico:	

Información del incidente

Situación inicial:
Hallazgos encontrados:
Recomendaciones de solución:
Resultados obtenidos:

Observaciones / recomendaciones

_____

NOMBRE
LÍDER DEPARTMENTO DE OPERACIONES

_____

NOMBRE
DIRECTOR(A) DE CSIRT UPEC

Figura 277. Formato de informe de resultados en la gestión del incidente

Anexo 28 Formato para la identificación de confiabilidad de la fuente.

PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE CONFIABILIDAD DE LA FUENTE

Marcar el casillero con una "X" de acuerdo a las características que presenta la fuente de información, las respuestas le permitirán dar un criterio para determinar su veracidad en el contenido que provee.

Lista de comprobación general

Respuesta de verificación	**Si**	**No**
¿La fuente es conocida o registrada?		
¿Se reconoce al autor de la información?		
¿La forma de comunicación fue la adecuada?		
¿La información llega por medios regulares?		
¿La información contiene datos extraños o sin sentido?		
Observaciones:		

Si la información parece dudosa se debe volver a verificarla con otras fuentes de información.

Correo electrónico - Fuentes

Respuesta de verificación	**Si**	**No**
¿La dirección es conocida por el equipo?		
¿Es correcta la firma GPG (Firma digital de cifrado)?		
¿El correo que recibió está alojado en la bandeja de spam?		
Observaciones:		

Si se presentan inconvenientes o dudas con la verificación del mensaje, compruebe los datos del remitente; y si se presentan inconvenientes con la verificación del remitente, utilice las herramientas MxToolbox o Messageheader para verificar el correo electrónico.

WWW - Fuentes

Respuesta de verificación	**Si**	**No**
¿El sitio web de donde se expone la información cuenta con sus certificados de seguridad https?		
¿Se utilizan términos (tecnológicos) correctos en el contenido de la información?		
¿Existen vínculos que direccionan a páginas o descargas sospechosas?		
Observaciones:		

Si presenta dudas con el sitio web, utilice los comandos lookup o dig para comprobar su dominio y traceroute para verificar la ruta de envió de paquetes.

Teléfono

Respuesta de verificación	**Si**	**No**
¿Escuchó o preguntó el nombre de la persona de la que recibió la llamada?		
¿Se identificó el objetivo de la llamada?		
¿Identificó los datos expuestos durante la transmisión del mensaje?		
¿La duración de la llamada fue suficiente para entender la transmisión de la información que el emisor quiso dar a conocer?		
Observaciones:		

Si presenta dudas acerca de la fuente que emitió o de la información recibida, contáctese nuevamente con el autor de la llamada.

Figura 278. Formato para la identificación de confiabilidad de la fuente

Anexo 29 Formato para la distribución de alertas y avisos.

DISTRIBUCIÓN DE ALERTAS Y AVISOS

Título del aviso:	
Sistemas afectados:	
- - -	
Sistema operativo relacionado y versión:	
- - -	
Riesgo (Alto-Medio-Bajo):	

Descripción general de la vulnerabilidad:
Consecuencias:
Solución:
Apéndice:
- - -

_____	_____
NOMBRE	**NOMBRE**
LÍDER DEPARTAMENTO DE OPERACIONES	**DIRECTOR(A) DE CSIRT UPEC**

Figura 279. Formato para la distribución de alertas y avisos

Anexo 30 Formato de solicitud para concientización tecnológica.

SOLICITUD – CONCIENTIZACIÓN TECNOLÓGICA

Información de contacto:

Proporcione su información de contacto para que CSIRT UPEC se comunique con usted.

Quien Solicita:		
Correo electrónico:		
Teléfono:		
Tipo de organización	Educativa:	
	Gubernamental:	
Nombre de la organización:		

Detalles:

Temática requerida:			
Forma de concientización	Online	Zoom	
		Facebook live	
		Microsoft Teams	
		Otros Especificar cual:	
	Presencial		
Fecha aproximada del acercamiento	Fecha:		
	Hora:		

La fecha para el acercamiento la debe establecer con un mínimo de 5 días laborables.

Figura 280. Formato de solicitud para concientización tecnológica

Anexo 31 Métricas e indicadores para medir los procesos alertas - avisos, publicación de anuncios y gestión de riesgos

Tabla 49. Métrica gestión de solicitudes del servicio alertas y avisos

CSF	KPI	Fórmula	Fuente de datos	Meta	Frecuencia
Brindar el servicio de forma eficiente.	Porcentaje de calificación como información útil	$\frac{\text{N° de votos con calificación util}}{\text{Total de votos en el mes}} \times 100$	Encuesta de satisfacción	N/A	Mensual
	Porcentaje de calificación como información no útil	$\frac{\text{N° de votos con calificación no util}}{\text{Total de votos en el mes}} \times 100$	Encuesta de satisfacción	N/A	Mensual

Tabla 50. Métrica gestión de solicitudes del servicio anuncios

CSF	KPI	Fuente de datos	Meta	Frecuencia
Brindar el servicio de forma eficiente.	Número de votos por entrada.	Sistema web	N/A	Mensual
	Promedio de puntuación	Sistema web	N/A	Mensual
	Tiempo de visualización de entrada antes de la puntuación	Sistema web	N/A	Mensual

Tabla 51. Métrica nivel de gestión de riesgo

CSF	KPI	FORMULA	Fuente de datos	Meta	Frecuencia
Identificar riesgos de forma eficiente	Porcentaje de incremento de riesgos informáticos reportados al CSIRT	$\frac{\text{N° de riesgos identificados mes actual} - \text{N° de riesgos identificados mes anterior}}{\text{N° de riesgos identificados mes anterior}} \times 100$	Sistema de ticket	N/A	Mensual