

**NEUMANN BUSINESS SCHOOL**  
ESCUELA DE POSTGRADO

**MAESTRÍA EN  
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**



**“PROPUESTA DE MEJORA APLICANDO DIRECCIÓN DE  
PROYECTOS BAJO ENFOQUE PMI EN EL DESARROLLO DE  
ACTUALIZACIONES DE SEGURIDAD PARA LA RED  
ASISTENCIAL TACNA ESSALUD”**

**TRABAJO DE INVESTIGACIÓN  
PARA OPTAR EL GRADO A NOMBRE DE LA NACIÓN DE:**

**MAESTRO EN  
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

**AUTOR:**  
LARRY EDWIN ANIBAL RIEGA RIEGA

**DOCENTE GUÍA:**  
ERNESTO ALESSANDRO LEO ROSSI

**TACNA – PERÚ  
2020**

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) auto (es)”

Pág.

## ÍNDICE

RESUMEN EJECUTIVO .....	21
INTRODUCCIÓN.....	23
CAPÍTULO I.....	26
Antecedentes Del Estudio.....	26
1.1 Título del Tema .....	26
1.2. Planteamiento del Problema .....	26
1.3. Formulación del Problema.....	30
1.4. Objetivos.....	30
1.5. Justificación.....	31
1.6. Metodología.....	38
1.7. Definiciones Operacionales.....	39
1.8. Definiciones.....	43
1.9. Alcances y Limitaciones.....	48
CAPÍTULO II.....	56
Marco Teórico .....	56
2.1. Conceptualización de Actualizaciones de Seguridad .....	56
2.2 Importancia de la variable tópico .....	80
2.3 Análisis Comparativo .....	82
2.5. Análisis Crítico.....	93

CAPÍTULO III .....	94
Marco Referencial.....	94
3.1. Reseña histórica.....	94
3.2 Filosofía Organizacional.....	94
3.3 Diseño Organizacional .....	96
3.4 Productos y/o servicios.....	101
3.5 Diagnóstico Organizacional.....	103
CAPÍTULO IV .....	110
Desarrollo del Tema.....	110
4.1. Diagnóstico.....	110
4.2. Diseño de la Mejora.....	191
4.3. Mecanismos de Control .....	333
CAPÍTULO V .....	336
Sugerencias.....	336

## INDICE DE GRÁFICOS

Gráfico 1. Collections y Site en EsSalud .....	27
Gráfico 2. Relación de Servidores Distribution Point en EsSalud.....	28
Gráfico 3. Grupos de Trabajo Red Asistencial Tacna EsSalud .....	30
Gráfico 4. Malware de mayor detección a nivel nacional.....	32
Gráfico 5. TOP 10 Malware detectado .....	34
Gráfico 6. TOP 10 Departamentos con SO obsoletos.....	35
Gráfico 7. Cantidad de Equipos con CXmal/Wanna-A.....	35
Gráfico 8. Fecha de Soporte Extendido Sistemas Operativos .....	36
Gráfico 9. Optimizaciones Recomendadas Innovare e-Business S.A.C .....	37
Gráfico 10. Vulnerabilidades Críticas y Actividades de Ataque.....	66
Gráfico 11. Biblioteca de terceros y vulnerabilidades de IoT .....	67
Gráfico 12. Comportamiento de Parches antes y despues de Wanacry .....	69
Gráfico 13: Tendencias de Parches de dispositivos IoT.....	70
Gráfico 14. Vulnerabilidades de baja gravedad detectadas con mayor frecuencia 2016-2017.....	71
Gráfico 15. Vulnerabilidades en los Navegadores 2015 2016 2017. ....	72
Gráfico 16. Número total de vulnerabilidades 2015 2016 2017.....	72
Gráfico 17. Vulnerabilidades Zero-day 2015 2016 2017 .....	73
Gráfico 18. Ataques de Malware más destructivos.....	74
Gráfico 19. Tipo de Incidentes Malware 2017 .....	75
Gráfico 20. Infecciones de malware por país 2017.....	76
Gráfico 21. Porcentaje de empresas que no tienen ningún control de seguridad .....	76

Gráfico 22. Cuadrante Mágico para Plataformas de Protección de Endpoint 2018.....	85
Gráfico 23. Cuadrante Mágico para Plataformas de Protección de Endpoint 2019.....	85
Gráfico 24. Cantidad de Redes por Ubicación Geográfica .....	113
Gráfico 25. Total de Sedes y Redes – PROVINCIAS .....	115
Gráfico 26. Organigrama de GCTIC .....	116
Gráfico 27. Diagrama de Arquitectura de Red ESSALUD .....	120
Gráfico 28. Equipos Desktop a nivel nacional.....	123
Gráfico 29. Equipos Desktop Redes Lima .....	123
Gráfico 30. Equipos Desktop Redes Provincias .....	124
Gráfico 31. Total de Switches – Lima .....	126
Gráfico 32. Total de Switches – Provincias .....	127
Gráfico 33. Total de Switches a Nivel Nacional por Antigüedad .....	127
Gráfico 34. Total de Switches por antigüedad – LIMA .....	128
Gráfico 35. Total de Switches por antigüedad – PROVINCIAS.....	129
Gráfico 36. Total de Switches por Marca – LIMA .....	129
Gráfico 37. Total de Switches por Marca – PROVINCIAS.....	130
Gráfico 38. Malla de Firewall Perimetral.....	134
Gráfico 39. Topología de Internet hasta 2017 .....	159
Gráfico 40. Lista de Control de Acceso sexURL Servidor Osiris EsSalud.....	161
Gráfico 41. Squid.conf Servidor Osiris EsSalud .....	162
Gráfico 42. Literal 7.2 Directiva de Gerencia General N.º 021-GG-ESSALUD-2013.....	162
Gráfico 43. Capacidad de Procesamiento Servidor Osiris EsSalud.....	163
Gráfico 44. Tamaño de Actualizaciones Desplegadas con SCCM (LIMA) .....	173
Gráfico 45. Diagrama de Red Sede Central .....	175

Gráfico 46. Device Collections EsSalud .....	179
Gráfico 47. Despliegue de Actualizaciones a través de SCCM.....	180
Gráfico 48. Bloqueo Windows Update .....	182
Gráfico 49. Versión Linux Centos .....	195
Gráfico 50. Ruta de descarga servidor \\172.20.0.166\Parches\ISO\Centos.....	196
Gráfico 51. Ruta a través de SMB desde cualquier estación cliente. ....	196
Gráfico 52. Selección del datastore respectivo .....	197
Gráfico 53. Seleccionamos la distribución de Linux.....	197
Gráfico 54. Verificación del Datastore destino .....	198
Gráfico 55. Create New Virtual Machine .....	199
Gráfico 56. Nombre de Máquina Virtual .....	200
Gráfico 57. Selección Datastore de Máquina Virtual.....	201
Gráfico 58. Selección Tipo de Sistema Operativo de la Máquina Virtual.....	202
Gráfico 59. Configuración conexión de Red de la Máquina Virtual.....	203
Gráfico 60. Configuración del espacio en disco de la Máquina Virtual.....	204
Gráfico 61. Resumen de Configuración de la Máquina Virtual.....	205
Gráfico 62. Cantidad de memoria de la Máquina Virtual .....	206
Gráfico 63. Cantidad de sockets y cores de la Máquina Virtual .....	207
Gráfico 64. Máquina Virtual Creada.....	208
Gráfico 65. Configuración final de la Máquina Virtual .....	209
Gráfico 66. Consola de la Máquina Virtual .....	209
Gráfico 67. Encendido de la Máquina Virtual .....	210
Gráfico 68. Pantalla de Bienvenida de Linux Centos .....	210
Gráfico 69. Instalación de Linux Centos v6.9 32 Bits: Omitir verificación de media.....	211

Gráfico 70. Instalación de Linux Centos v6.9 32 Bits: Next .....	212
Gráfico 71. Instalación de Linux Centos v6.9 32 Bits: Idioma de Instalación .....	213
Gráfico 72. Instalación de Linux Centos v6.9 32 Bits: Tipo de teclado.....	213
Gráfico 73. Instalación de Linux Centos v6.9 32 Bits: Tipo de Almacenamiento.....	214
Gráfico 74. Instalación de Linux Centos v6.9 32 Bits: Aviso antes de eliminar partición.....	215
Gráfico 75. Instalación de Linux Centos v6.9 32 Bits: Configuración Soporte Red .....	215
Gráfico 76. Instalación de Linux Centos v6.9 32 Bits: Configuración localidad.....	216
Gráfico 77. Instalación de Linux Centos v6.9 32 Bits: Configuración de root.....	216
Gráfico 78. Instalación de Linux Centos v6.9 32 Bits: Configuración tipo de instalación.....	217
Gráfico 79. Instalación de Linux Centos v6.9 32 Bits: Selección de SDA.....	217
Gráfico 80. Instalación de Linux Centos v6.9 32 Bits: Tipo de partición.....	218
Gráfico 81. Instalación de Linux Centos v6.9 32 Bits: Punto de montaje /.....	218
Gráfico 82. Instalación de Linux Centos v6.9 32 Bits: Punto de montaje /boot. ....	219
Gráfico 83. Instalación de Linux Centos v6.9 32 Bits: Punto de montaje /home. ....	219
Gráfico 84. Instalación de Linux Centos v6.9 32 Bits: SWAP .....	220
Gráfico 85. Instalación de Linux Centos v6.9 32 Bits: Punto de montaje /respaldo.....	220
Gráfico 86. Instalación de Linux Centos v6.9 32 Bits: Puntos de montajes definidos .....	221
Gráfico 87. Instalación de Linux Centos v6.9 32 Bits: Formato Tabla de Partición .....	221
Gráfico 88. Instalación de Linux Centos v6.9 32 Bits : Aviso de escritura.....	222
Gráfico 89. Instalación de Linux Centos v6.9 32 Bits : Creación de volúmenes.....	222
Gráfico 90. Instalación de Linux Centos v6.9 32 Bits : Instalación de boot loader.....	222
Gráfico 91. Instalación de Linux Centos v6.9 32 Bits : Instalación de paquetes .....	223
Gráfico 92. Instalación de Linux Centos v6.9 32 Bits : Fin de Instalación de paquetes .....	224
Gráfico 93. Instalación de Linux Centos v6.9 32 Bits : Pantalla de login.....	224



Gráfico 94. Instalación de Linux Centos v6.9 32 Bits.....	225
Gráfico 95. Ingreso por SSH para configurar repositorio y File Server.....	225
Gráfico 96. Consulta de registro de la llave .....	226
Gráfico 97. Ingreso remoto al servidor Linux Centos v6.9 32 Bits. ....	226
Gráfico 98. Configuración de nombre de host al servidor Linux Centos v6.9 32 Bits.....	227
Gráfico 99. Modificación de nombre de host al servidor Linux Centos v6.9 32 Bits.....	227
Gráfico 100. Asignación de nombre de host al servidor Linux Centos v6.9 32 Bits. ....	228
Gráfico 101. Usando comando hostname para asignación de nombre de host. ....	229
Gráfico 102. Usando comando hostname para asignación de nombre de host.....	229
Gráfico 103. Verificación de versión de Linux Instalada.....	230
Gráfico 104. Desactivación de Firewall de Linux.....	230
Gráfico 105. Desactivación de Firewall de Linux.....	231
Gráfico 106. Paralización del servicio de Firewall de Linux.....	231
Gráfico 107. Cambio de zona horaria.....	232
Gráfico 108. Edición del archivo config y desabilitamos el SELINUX.....	232
Gráfico 109. Creación de los directorios de la solución antimalware.....	233
Gráfico 110. Generación del usuario y creación de la contraseña .....	233
Gráfico 111. Asignamos de los permisos correspondientes .....	234
Gráfico 112. Edición del archivo /etc/yum.conf .....	234
Gráfico 113. Edición del archivo /etc/yum.repos.d/nginx.repo .....	235
Gráfico 114. Instalación de epel-release .....	235
Gráfico 115. Instalación de dependencias epel-release.....	236
Gráfico 116. Finalización instalación de dependencias epel-release.....	236
Gráfico 117. Instalación de nginx .....	237

Gráfico 118. Instalación de nginx finalizada.....	238
Gráfico 119. Creación de los directorios para NGINX.....	239
Gráfico 120. Desinstalación de Apache .....	240
Gráfico 121. Configuración del inicio automático de Ngnix.....	241
Gráfico 122. Instalación de RSYNC.....	242
Gráfico 123. Inicio de Instalación de RSYNC.....	243
Gráfico 124. Creación y Configuración de los scripts de actualización .....	244
Gráfico 125. Asignar permisos de ejecución al script .....	245
Gráfico 126. Sincronizar archivos de configuración de nginx .....	245
Gráfico 127. Modificación de archivo nginx. ....	246
Gráfico 128. Configurar nginx con los ip's autorizados a descargar las actualizaciones. ....	247
Gráfico 129. Reiniciar Servicio nginx. ....	247
Gráfico 130.. Definir en el script la frecuencia de actualización .....	248
Gráfico 131. Verificación del tamaño de disco, antes de la descarga de firmas inicial. ....	248
Gráfico 132. Ejecutamos la descarga inicial .....	249
Gráfico 133. Descarga inicial finalizada. ....	250
Gráfico 134. Instalación de SAMBA (SMB). ....	250
Gráfico 135. Descarga de paquetes de instalación de SAMBA . ....	251
Gráfico 136. Instalación de SAMBA (SMB) finalizada.....	252
Gráfico 137. Configuración de Inicio automático de SAMBA (SMB) .....	253
Gráfico 138.. Editamos el servicio automático de SAMBA (SMB) .....	254
Gráfico 139. Configuración de SAMBA (SMB) .....	255
Gráfico 140. Reinicio de servicio de SAMBA (SMB) .....	256
Gráfico 141. Accediendo a File Server desde cualquier IP de EsSalud (SMB) . ....	257

Gráfico 142. Verificación de contenido de File Server desde cualquier IP de EsSalud (SMB) . . . .	258
Gráfico 143. Test de validación de SMB . . . . .	259
Gráfico 144. Verificación de parámetros de SMB . . . . .	260
Gráfico 145. Repositorio de Firmas y Parches CAPI Ilabaya . . . . .	261
Gráfico 146. Direcciones Ip matriculadas Repositorio CAPI Ilabaya . . . . .	262
Gráfico 147. Repositorio de Firmas y Parches CAPI ITE . . . . .	263
Gráfico 148. Rangos de direcciones Ip matriculadas Repositorio CAPI ITE . . . . .	263
Gráfico 149. Accediendo por SMB a servidor 172.30.229.14 . . . . .	264
Gráfico 150. Repositorio de Firmas y Parches CAPI Tarata . . . . .	265
Gráfico 151. Rangos de direcciones Ip matriculadas Repositorio CAPI Tarata . . . . .	265
Gráfico 152. Accediendo por SMB a servidor 172.30.222.14 . . . . .	266
Gráfico 153. Repositorio de Firmas y Parches CAPII Luis Palza Lévano . . . . .	266
Gráfico 154. Direcciones Ip matriculadas Repositorio CAPII Luis Palza Lévano . . . . .	267
Gráfico 155. Accediendo por SMB a servidor 172.30.220.14 . . . . .	267
Gráfico 156. Repositorio de Firmas y Parches CAPII Óscar Fernández Dávila . . . . .	268
Gráfico 157. Ips matriculadas repositorio CAPII Óscar Fernández Dávila . . . . .	268
Gráfico 158. Accediendo por SMB al repositorio antimalware local . . . . .	269
Gráfico 159. Repositorio de Firmas y Parches CAPIII Metropolitano . . . . .	270
Gráfico 160. Direcciones Ip matriculadas Repositorio CAPIII Metropolitano . . . . .	270
Gráfico 161. Accediendo por SMB al repositorio antimalware local . . . . .	271
Gráfico 162. Repositorio de Firmas y Parches HIII Daniel Alcides Carrión . . . . .	271
Gráfico 163. Direcciones Ip matriculadas Repositorio HIII Daniel Alcides Carrión . . . . .	272
Gráfico 164. Accediendo por SMB al repositorio antimalware local . . . . .	272
Gráfico 165. Repositorio de Firmas y Parches PM Locumba . . . . .	273

Gráfico 166. Rangos de Ips matriculadas Repositorio CAPI Locumba .....	273
Gráfico 167. Accediendo por SMB al repositorio antimalware local .....	274
Gráfico 168. Verificación para aceptar conexiones .....	279
Gráfico 169. Ruta Archivos Configuración OpenSSH Global .....	280
Gráfico 170. Visualización de archivo ssh_host_key.pub.....	281
Gráfico 171. Fingerprint del archivo ssh_host_key.pub .....	282
Gráfico 172. Ruta Archivos Configuración OpenSSH específica .....	283
Gráfico 173. Generando pares de claves rsa públicas / privadas .....	285
Gráfico 174. Generación de claves de autenticación para SSH .....	286
Gráfico 175. Copia de clave pública a servidor remoto 172.26.35.207.....	286
Gráfico 176. Verificación de clave pública a servidor remoto 172.26.35.207 .....	287
Gráfico 177. Inclusión de clave pública al archivo authorized_keys en 172.26.35.207 .....	288
Gráfico 178.Verificación de archivo authorized_keys en 172.26.35.207 .....	288
Gráfico 179. Copia de llave pública al servidor destino 172.30.225.14.....	289
Gráfico 180. Copia del archivo id_rsa.pub a 172.30.225.14 finalizada. ....	289
Gráfico 181. Ingreso a servidor 172.30.225.14 .....	290
Gráfico 182, Modificación del archivo id_rsa.pub por authorized_keys en 172.30.225.14. ....	291
Gráfico 183. Ingreso por SSH a CAPI Ilabaya sin solicitar contraseña.....	291
Gráfico 184. Copia del archivo id_rsa.pub a 172.30.229.14 .....	292
Gráfico 185. Proceso de copia finalizado en 172.30.229.14.....	293
Gráfico 186. Ingreso a repositorio de CAPI ITE .....	293
Gráfico 187. Ingresamos al repositorio destino 172.30.229.14. ....	294
Gráfico 188. Renombramos el archivo id_rsa.pub por authorized_keys.....	294
Gráfico 189. Copia de archivo id_rsa_pub a CAP I Tarata.....	295

Gráfico 190. Ingreso de contraseña a servidor 172.30.222.14 .....	295
Gráfico 191. Copia del archivo id_rsa.pub al servidor 172.30.222.14.....	296
Gráfico 192. Ingreso de contraseña a servidor 172.30.222.14 .....	297
Gráfico 193. Renombramos id_rsa.pub por authorized_keys en 172.30.222.14 .....	297
Gráfico 194. Ingreso a CAP I Tarata sin solicitar contraseña .....	298
Gráfico 195. Ingreso a 172.20.0.166 para copia de id_rsa.pub a 172.30.220.14.....	298
Gráfico 196. Solicitud de contraseña en 172.30.220.14.....	299
Gráfico 197. Ingreso de la contraseña servidor 172.30.220.14.....	300
Gráfico 198. Renombramos id_rsa.pub por authorized_keys en 172.30.220.14 .....	300
Gráfico 199. Ingreso remoto a al repositorio destino 172.30.220.14. ....	301
Gráfico 200. Copia del archivo id_rsa.pub al servidor destino 172.30.223.14 .....	302
Gráfico 201. Verificación de contraseña servidor destino 172.30.223.14 .....	302
Gráfico 202. Transferencia de archivo id_rsa.pub a 172.30.223.14 .....	303
Gráfico 203. Ingreso al servidor 172.30.223.14 .....	304
Gráfico 204. Renombramos id_rsa.pub por authorized_keys en 172.30.223.14.....	304
Gráfico 205. Modificación del archivo id_rsa.pub por authorized_keys en 172.30.223.14 .....	305
Gráfico 206. Copia de id_rsa.pub al servidor destino 172.30.221.10 .....	305
Gráfico 207. Posterior al ingreso de la contraseña se concreta la transferencia .....	306
Gráfico 208. Ingresamos al repositorio destino 172.30.221.10 .....	307
Gráfico 209. Renombramos el archivo id_rsa.pub por authorized_keys .....	307
Gráfico 210. Transferencia Automática a través de un script .....	308
Gráfico 211. Scrip trasmite-HIII_DanielAlcidesCarrion.sh .....	309
Gráfico 212. Alojamiento de Instalador de Wsus Off Line en 172.20.0.166.....	310
Gráfico 213. Ejecución de UpdateGenerator .....	311

Gráfico 214. Selección de Alternativas Windows .....	311
Gráfico 215. Selección de Alternativas Office .....	312
Gráfico 216. Selección de Alternativas Legacy Windows.....	313
Gráfico 217. Descarga de paquetes seleccionados .....	313
Gráfico 218. Modelo de Equipo de EsSalud .....	314
Gráfico 219. Información de la Plataforma de Windows .....	316
Gráfico 220. Dirección IP equipo.....	316
Gráfico 221. Versión del Sistema Operativo DOS .....	317
Gráfico 222. Versión del Sistema Operativo Windiows .....	317
Gráfico 223. Configuración encendido.....	318
Gráfico 224. Selección Dia y Hora de encendido.....	318
Gráfico 225. Encendido programado confirmado .....	319
Gráfico 226. Configuración de Encendido programado. ....	320
Gráfico 227. Programador de Tareas .....	320
Gráfico 228. Descripción de la tarea.....	321
Gráfico 229. Configuración Semanal .....	322
Gráfico 230. Definición de dia de la semana .....	322
Gráfico 231. Definimos la acción.....	323
Gráfico 232. Para Windows Seven generamos la colección definida. ....	324
Gráfico 233. Para Windows 10 generamos la colección definida.....	324
Gráfico 234. Programa o script a iniciar .....	325
Gráfico 235. Finalización de tarea .....	326
Gráfico 236. Verificación de tarea .....	327
Gráfico 237. Configuración pestaña General.....	327

Gráfico 238. Ingresamos la configuración de la cuenta del administrador de la pc.....	328
Gráfico 239. Situación de Parches antes de Procedimiento.....	333
Gráfico 240. Situación de Parches después de Procedimiento .....	334

## INDICE DE TABLAS

Tabla 1. Definiciones Operacionales .....	39
Tabla 2. Carpetas compartidas Directorio Activo .....	50
Tabla 3. Cuadrantes Mágicos de Gartner.....	83
Tabla 4. Despliegue de Actualizaciones de Seguridad con Soluciones de Software.....	91
Tabla 5. Objetivos Estratégicos Institucionales.....	95
Tabla 6 Integrantes del Consejo Directivo .....	98
Tabla 7 Análisis FODA .....	105
Tabla 8. Topología de Comunicaciones EsSalud.....	119
Tabla 9 NTP ISO/IEC 17799-2007. Tecnología de la Información .....	132
Tabla 10 Documento Regulatorio. Ficha del Documento Regulatorio N° 246-2007-PCM.....	135
Tabla 11. Ficha del Documento Regulatorio N° 004-2016-PCM .....	141
Tabla 12 Matriz Situacional de Vulnerabilidades de Comunicaciones.....	144
Tabla 13. Matriz de Riesgos de Comunicaciones .....	154
Tabla 14. Matriz de Riesgos de Operaciones .....	156
Tabla 15. Procedimiento reactivo ante la incidencia.....	158
Tabla 16. Fabricantes Antivirus con Mayor reconocimiento de la Industria 2018 – 2019.....	165
Tabla 17. Sistemas de Puntuación Fabricantes con mayor reconocimiento .....	165
Tabla 18. Características Detección Malware.....	166
Tabla 19. Sistemas de Puntuación Detección de Malware .....	166
Tabla 20. Características Respuestas a Incidentes.....	167
Tabla 21. Sistemas de Puntuación Características Respuestas a Incidentes .....	167



Tabla 22. Despliegue de Actualizacion de Firmas Antivirus .....	168
Tabla 23. Sistemas de Puntuación Despliegue de Actualización de firmas Antivirus .....	168
Tabla 24. Gestión de Parches y Vulnerabilidades .....	169
Tabla 25. Sistema de Puntuación Gestión de Parches y Vulnerabilidades .....	169
Tabla 26. Cotizaciones y Despliegue.....	170
Tabla 27. Sistema de Puntuación Cotizaciones y Despliegue .....	170
Tabla 28. Resumen Funcionalidades Producto .....	171
Tabla 29. Actualizaciones Desplegadas con SCCM (LIMA) y BW EsSalud Tacna .....	172
Tabla 30. Sedes con Enlace Satelital Red Asistencial Tacna EsSalud.....	173
Tabla 31. Funcionalidades Sophos XG Firewall (Modo Virtual) .....	183
Tabla 32. Funcionalidades GFI Languard .....	184
Tabla 33. Precio GFI Languard.....	187
Tabla 34. Análisis Tipos de Despliegue de Actualizaciones de Seguridad .....	188

## INDICE DE ANEXOS

ANEXO A. CAP III Metropolitano. Control de Parches.....	345
ANEXO B. HIII Daniel Alcides Carrión. PM Locumba. Control de Parches .....	347
ANEXO C. Ancho De Banda (BW) Red EsSalud Tacna .....	369
ANEXO D. Diagrama De Red Final EsSalud .....	370
ANEXO E. Cotización LanGuard .....	371
ANEXO F. Informe Aranda .....	372
ANEXO G. Cantidad de Equipos Red EsSalud Tacna .....	373
ANEXO H. Precio Filtro Web .....	374
ANEXO I. Plan de Trabajo Enrolamiento al Directorio Activo de EsSalud.....	375
ANEXO J. Cotización Licencias para Directorio Activo .....	376
ANEXO K. Tabla de % Uso BW Red Tacna para Actualizaciones .....	377
ANEXO L. Sedes Red Asistencial Tacna - EsSalud .....	378
ANEXO M. Alertas de Ransomware Red Asistencial Tacna – EsSalud Periodo Actual.....	379
ANEXO N. Parches peligrosidad CRÍTICA por instalar Red Asistencial Tacna – EsSalud .....	380
ANEXO O. Parches peligrosidad ALTA por instalar Red Asistencial Tacna – EsSalud .....	389
ANEXO P. Parches peligrosidad MEDIA por instalar Red Asistencial Tacna – EsSalud .....	393
ANEXO Q. Parches peligrosidad BAJA por instalar Red Asistencial Tacna – EsSalud .....	394
ANEXO R. Cuadro de Actividades Sede Central Lima EsSalud .....	395
ANEXO S. Cuadro de Actividades HIII Daniel Alcides Carrión – EsSalud Tacna .....	396
ANEXO T. Cuadro de Actividades C.A.P. II Luis Palza Levano – EsSalud Tacna .....	397
ANEXO U. Cuadro de Actividades CAPIII Metropolitano EsSalud Tacna .....	398

ANEXO V. Cuadro de Actividades C.A.P. I Tarata EsSalud Tacna .....	399
ANEXO W. Cuadro de Actividades C.A.P. II Ilabaya EsSalud Tacna .....	400
ANEXO X. Cuadro de Actividades C.A.P. I Locumba EsSalud Tacna .....	401
ANEXO Y. Cuadro de Actividades C.A.P. I ITE EsSalud Tacna .....	402
ANEXO Z. Cuadro de Actividades C.A.P.II Oscar Fernández Dávila EsSalud Tacna .....	403
ANEXO AA. Presupuesto .....	404
ANEXO BB. Cronograma .....	405
ANEXO CC. Indicadores de Éxito .....	406



## **RESUMEN EJECUTIVO**

La presente investigación, tiene como fin, plantear algunas alternativas de mejora automatizadas a muy bajo costo, sin el uso de Internet y de manera transparente para el usuario final, con el objetivo de contar con una estrategia para establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información en la Red Asistencial Tacna EsSalud , estableciendo un procedimiento para el tratamiento adecuado de los riesgos de seguridad de la información, tratando de minimizar al máximo la afectación de los servicios de salud y establecer medidas de de prevención, respuesta, recuperación y rehabilitación que garanticen la continuidad de las operaciones en la mencionada Red Asistencial.

En suma, se trata de un estudio del tipo de investigación cuantitativa y de alcance explicativo. El diseño de la investigación es no experimental longitudinal de tendencia, la técnica fue la observación y la muestra fue 441 equipos de cómputo funcionando bajo plataforma Windows de la Red Asistencial Tacna EsSalud.

Los informes del control de parches de Sophos (Anexo C), indican que existen en todas las sedes de la Red Asistencial Tacna EsSalud, direcciones Ip con vulnerabilidades críticas, altas, medias y bajas en el sistema operativo, sin solucionar, producto de la falta del despliegue de actualizaciones y parches de seguridad en los equipos de cómputo hacia la mencionada red, desde el Data Center principal en Sede Central en Lima, ya que toda la infraestructura de TI en EsSalud a nivel nacional es gestionada de manera centralizada desde dicho departamento .

Entre los principales hallazgos, podemos mencionar que la Red Asistencial Tacna EsSalud, aún tiene equipos con plataforma Windows XP (17) , lo que constituye una grave fuente de vulnerabilidad dentro del parque informático de la Red Asistencial Tacna EsSalud.

Se obtienen como principales conclusiones, la necesidad de implementar un sistema automatizado multiplataforma de despliegue e instalación de actualizaciones y parches de seguridad sin costo para EsSalud, con una mínima intervención del personal de TI, sin el uso de Internet y evitando cualquier tipo de afectación a los servicios que la entidad brinda a los asegurados.

## INTRODUCCIÓN

Las vulnerabilidades electrónicas son uno de los aspectos más críticos dentro de la seguridad de la información. En el periodo 1999-2003 crecieron en un 807% según el CERT, mientras los incidentes en el mismo periodo crecieron en un 1,295% según la misma fuente. Por otro lado, desde el 2001 al 2004, el tiempo de aparición de los mecanismos de explotación de las vulnerabilidades se ha reducido en un 50% año a año.

La primera aproximación hacia el control de las vulnerabilidades se basó en la detección de las mismas y en una priorización de su severidad. En la medida que la complejidad de la red crece, este modelo colapsa por su incapacidad de responder de manera rápida a preguntas tales como : ¿cuál es mi nivel de riesgo actual? ¿Qué mitigo primero? ¿cuánto tiempo tengo para mitigar? ¿cómo ha evolucionado mi riesgo? ¿Qué riesgo debo aceptar?.

Hoy la industria coincide en enfocarse en la Gestión de Vulnerabilidades, buscando responder a las preguntas anteriores con el fin de optimizar el uso de recursos, cumplir con requerimientos legales, normativos y cumplir con los objetivos de negocio.

Es necesario alinear las nuevas tecnologías de seguridad para soportar las necesidades corporativas, esto ayuda con el cumplimiento de los objetivos del negocio, es precisamente ello lo que no está sucediendo en la mayoría de las empresas, porque los mecanismos tradicionales de control reactivos actuales no soportan un crecimiento de negocio inesperado, tampoco hay un adecuado mantenimiento e integración de los sistemas obsoletos heredados. Actualmente, los controles gestionados con tablas de bases de datos, que no son dinámicos como la amenaza moderna, son insuficientes para hacerse cargo de esta realidad, sin capacidad de generar firmas para la velocidad de surgimiento de nuevas

variantes o para detectar su ingreso en código web, presentan lamentablemente una brecha significativa.

La seguridad de información tiene muchas facetas diferentes siendo la meta principal proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización, cualquier incidente que afecte a uno de estos componentes puede poner en riesgo rápidamente a toda una organización, exponiéndola a conflictos legales y daño en su imagen corporativa. La tendencia en estos momentos es usar Sandboxing, lo que permite aproximarse a controles más efectivos con la utilización de máquinas virtuales, el uso de seguridad positiva a nivel de los dispositivos y la detección de tráfico de servidores de comando y control.

En empresas con esquema de seguridad tradicional, es necesario cambiar la arquitectura centralizada de protección del perímetro, debido a que no pueden bloquear las amenazas de malware moderno-provenientes de la nube, para ello es necesario proceder de manera homogénea, coordinada y cooperativa. Es necesario implementar procedimientos complementarios a la estructura actual, que permitan delegar la administración de los dispositivos de seguridad de la gestión preventiva y reactiva de incidentes a un equipo de personas con experiencia en combatir el malware basado en comportamiento. Este tipo de actividades va a garantizar la respuesta de amenazas globales mediante su detección temprana en la red con una mitigación coordinada entre los motores de inteligencia global propietarios; la gestión de vulnerabilidades y el análisis de las reglas del firewall también vienen acompañados de este escenario granular.

La mayoría de las instituciones no está en la capacidad de prevenir, ni de responder adecuadamente a estas amenazas de malware moderno, porque no tiene una visión de conjunto de cómo estos abusos o amenazas potenciales puede dañar la identidad digital de la empresa al negocio, su impacto es transversal a toda la organización. No es posible anticiparse a riesgos de seguridad, debido a que no



cuentan con una solución predictiva e inteligente, que permita predecir de forma continua las amenazas de malware moderno y anticiparse a los riesgos empresariales, no existe una evaluación proactiva de seguridad con ataques del mundo real.

Se debe de simular las potenciales rutas de ataque, revelando exposiciones presentes en la arquitectura actual, es necesario cambiar el modelo y la forma de pensar para hacer frente a múltiples amenazas que no están basadas en firmas, con el modelo de red actual no se puede garantizar una cobertura del total del vector de amenazas de malware.

Es muy difícil investigar la naturaleza de un evento de malware, debido a la ausencia de herramientas para el análisis forense, lo que se realiza en la mayoría de las veces es restaurar al equipo a su estado original de fábrica, no hay una base de datos de conocimientos. Las Tecnologías de correlación (SIEM) y recolección de logs (Loggers) se encargan de este tipo de tareas y recopilan información sobre la amenaza, facilitando de este modo la actividad forense y un futuro requerimiento de auditoría.