DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL DEPARTAMENTO DE INFORMATICA DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO

LOILEIMAN ENRIQUE QUINTERO PARRA

Trabajo de tesis de grado, para optar al título de Especialista en Seguridad Informática

Director:
Martin Camilo Cancelado Ruiz
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIAS – ECBTI
BOGOTA D.C. - COLOMBIA
2015

CONTENIDO

pág.

INTRODUCCION.....26

1. GENERALIDADES DEL PROYECTO.....28

1.1 DESCRIPCION DEL PROBLEMA.....28

1.2 FORMULACION DEL PROBLEMA.....31

1.3 JUSTIFICACION.....31

2. FORMULACION DE OBJETIVOS.....33

2.1 OBJETIVO GENERAL.....33

2.2 OBJETIVOS ESPECIFICOS.....33

3. MARCO REFERENCIAL.....34

3.1 MARCO TEORICO.....34

3.1.1 ¿Qué se entiende por Seguridad Informática?.....34

3.1.2 Factores de los que depende la Seguridad Informática.....34

3.1.3 Objetivos de la Seguridad Informática.....35

3.1.4 ¿Qué es un Sistema de Gestión de Seguridad de la Información (SGSI).....35

3.1.5 ¿Para qué sirve un SGSI?.....36

3.1.6 ¿Cuáles son los beneficios de un SGSI?.....36

3.1.7 Ciclo de Deming – Mejora Continua.....37

3.1.8 Normas y estándares para el diseño e implementación de un SGSI.....43

3.1.9 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).....43

3.2 MARCO CONTEXTUAL.....44

3.2.1 Misión.....44

3.2.2 Visión.....44

3.2.3 Valores.....45

3.2.4 Dirección y administración.....45

3.2.5 Estructura Superintendencia de Notariado y Registro.....45

3.2.6 Oficina de Tecnologías de la Información.....46

3.3 MARCO LEGAL.....47

3.4 MARCO METODOLOGICO.....51

3.4.1 Tipo de investigación.....51

3.4.2 Población.....51

4. FASES.....52

4.1 FASE I – LEVANTAMINETO DE INFORMACION.....52

4.1.1 Descripción Superintendencia de Notariado y Registro (SNR)……..52

4.1.1.1 Objetivos.....52

4.1.1.2 Dirección y administración.....52

4.1.1.3 Integración del consejo directivo.....52

4.1.1.4 Funciones de la Superintendencia de Notariado y Registro (SNR).....52

4.1.1.5 Procesos generales de la Superintendencia de Notariado y Registro (SNR).....54

4.1.2 Descripción Departamento de Informática (Oficina de Tecnologías de la Información).....61

4.1.2.1 Funciones del Departamento de Informática (Oficina de Tecnologías de la Información).....61

4.1.2.2 Procesos internos del Departamento de Informática (Oficina de Tecnologías de la Información).....63

4.1.3 Estudio situación actual de seguridad…….....81

4.1.3.1 Recaudo de información relacionada con la seguridad de la información en la Superintendencia de Notariado y Registro (SNR) 81

4.1.3.2 Levantamiento de información de activos.....81

4.1.3.3 Análisis de riesgos.....82

4.1.3.4 Resumen valoración situación actual.....188

4.2 FASE II – CONSTRUCCION DE DISEÑO.....191

4.2.1 Argumentación necesidad de Sistema de Gestión de Seguridad de la Información (SGSI).....191

4.2.2 Construcción de diseño SGSI.....193

4.2.2.1 Plan de tratamiento de riesgos.....193

4.2.2.2 Declaración de aplicabilidad SOA.....221

4.2.2.3 Políticas de seguridad.....241

5. CONCLUSIONES.....254

BIBLIOGRAFIA.....256

ANEXOS.....258

LISTA DE ANEXOS

pág.

Anexo A. Circular No. 77 de 2008 (Políticas de Seguridad en los Sistemas de Información).....258

Anexo B. Circular No. 230 de 2009.....278

Anexo C. Comunicado 003 de 2010.....279

LISTA DE FIGURAS

pág.

Figura 1. Ciclo de Deming.....38

Figura 2. Organigrama.....46

Figura 3. Procesos SNR.....54

Figura 4. Representación de activos.....83

Figura 5. Representación de pertenencia a clases de los activos de activos esenciales.....86

Figura 6. Representación de pertenencia a clases de los activos de servicios internos.....86

Figura 7. Representación de pertenencia a clases de los activos de equipamiento - aplicaciones.....87

Figura 8. Representación de pertenencia a clases de los activos de equipamiento - equipos.....88

Figura 9. Representación de pertenencia a clases de los activos de equipamiento - comunicaciones.....88

Figura 10. Representación de pertenencia a clases de los activos de equipamiento - elementos auxiliares.....88

Figura 11. Representación de pertenencia a clases de los activos de equipamiento - soporte de información.....89

Figura 12. Representación de pertenencia a clases de los activos de servicios subcontratados.....89

Figura 13. Representación de pertenencia a clases de los activos de instalaciones.....89

Figura 14. Representación de pertenencia a clases de los activos de personal.....89

Figura 15. Representación general dependencias.....90

Figura 16. Representación de dependencias de los activos de activos esenciales.....90

Figura 17. Representación de dependencias de los activos de servicios internos.....91

Figura 18. Representación de dependencias de sistema de información notarial.....91

Figura 19. Representación de dependencias sistema de personal y nomina.....92

Figura 20. Representación de dependencias IRIS documental.....92

Figura 21. Representación de dependencias sistema de procesos judiciales.....92

Figura 22. Representación de dependencias hoja de vida de notarios.....93

Figura 23. Representación de dependencias sistema de control interno disciplinario.....93

Figura 24. Representación de dependencias sistema de control interno disciplinario notarias.....93

Figura 25. Representación de dependencias sistema integrado web.....94

Figura 26. Representación de dependencias registro - catastro.....94

Figura 27. Representación de dependencias botón de pago.....94

Figura 28. Representación de dependencias ventanilla única de registro.....95

Figura 29. Representación de dependencias netbackup.....95

Figura 30. Representación de dependencias oracle virtual machine.....95

Figura 31. Representación de dependencias endpointsecurity.....95

Figura 32. Representación de dependencias exadata.....96

Figura 33. Representación de dependencias exalogic.....96

Figura 34. Representación de dependencias servidores.....96

Figura 35. Representación de dependencias computadores.....97

Figura 36. Representación de dependencias portátiles.....97

Figura 37. Representación de dependencias impresoras.....97

Figura 38. Representación de dependencias switch.....97

Figura 39. Representación de dependencias firewall.....98

Figura 40. Representación de dependencias red LAN.....98

Figura 41. Representación de dependencias Internet.....98

Figura 42. Representación de dependencias aire acondicionado.....98

Figura 43. Representación de dependencias arreglo de discos.....99

Figura 44. Representación de dependencias librería de cintas.....99

Figura 45. Representación general de valoración de activos.....100

Figura 46. Representación valoración de los activos de activos esenciales.....101

Figura 47. Representación valoración de los activos de servicios internos.....101

Figura 48. Representación valoración de los activos de equipamiento - aplicaciones.....102

Figura 49. Representación valoración de los activos de equipamiento - equipos.....102

Figura 50. Representación valoración de los activos de equipamiento - comunicaciones.....103

Figura 51. Representación valoración de los activos de equipamiento - elementos auxiliares.....103

Figura 52. Representación valoración de los activos de equipamiento - soporte de información.....104

Figura 53. Representación valoración de los activos de servicios subcontratados.....104

Figura 54. Representación valoración de los activos de instalaciones.....105

Figura 55. Representación valoración de los activos de personal.....105

Figura 56. Representación de amenazas sobre los activos de activos esenciales.....106

Figura 57. Representación de amenazas sobre activo servicios internos - directorio activo.....106

Figura 58. Representación de amenazas sobre activo servicios internos - DNS.....107

Figura 59. Representación de amenazas sobre activo servicios internos - DHCP.....107

Figura 60. Representación de amenazas sobre activo servicios internos - BIOMETRICO.....107

Figura 61. Representación de amenazas sobre activo aplicaciones - sistema de información notarial.....108

Figura 62. Representación de amenazas sobre activo aplicaciones - sistema de personal y nomina.....108

Figura 63. Representación de amenazas sobre activo aplicaciones - IRIS documental.....109

Figura 64. Representación de amenazas sobre activo aplicaciones - sistema de procesos judiciales.....109

Figura 65. Representación de amenazas sobre activo aplicaciones - hoja de vida de notarios.....110

Figura 66. Representación de amenazas sobre activo aplicaciones - sistema de control interno disciplinario.....110

Figura 67. Representación de amenazas sobre activo aplicaciones - sistema de control interno disciplinario notarias.....111

Figura 68. Representación de amenazas sobre activo aplicaciones - sistema integrado web.....111

Figura 69. Representación de amenazas sobre activo aplicaciones - interrelación registro - catastro.....111

Figura 70. Representación de amenazas sobre activo aplicaciones - botón de pago.....112

Figura 71. Representación de amenazas sobre activo aplicaciones - ventanilla única de registro.....112

Figura 72. Representación de amenazas sobre activo aplicaciones - netbackup.....112
Figura 73. Representación de amenazas sobre activo aplicaciones - oracle virtual machine.....113

Figura 74. Representación de amenazas sobre activo aplicaciones - endpointsecurity.....113

Figura 75. Representación de amenazas sobre activo equipos - exadata.....113

Figura 76. Representación de amenazas sobre activo equipos - exalogic.....114

Figura 77. Representación de amenazas sobre activo equipos - servidores.....114

Figura 78. Representación de amenazas sobre activo equipos - computadores.....115

Figura 79. Representación de amenazas sobre activo equipos - portátiles.....115

Figura 80. Representación de amenazas sobre activo equipos - impresoras.....116

Figura 81. Representación de amenazas sobre activo equipos - switch..116

Figura 82. Representación de amenazas sobre activo equipos - firewall.117

Figura 83. Representación de amenazas sobre activo comunicaciones - red LAN.....117

Figura 84. Representación de amenazas sobre activo comunicaciones - Internet.....118

Figura 85. Representación de amenazas sobre activo elementos auxiliares - ups.....118

Figura 86. Representación de amenazas sobre activo elementos auxiliares - fuentes de alimentación.....118

Figura 87. Representación de amenazas sobre activo elementos auxiliares - aire acondicionado.....119

Figura 88. Representación de amenazas sobre activo soporte de información - arreglo de discos.....119

Figura 89. Representación de amenazas sobre activo soporte de información - librería de cintas.....120

Figura 90. Representación de amenazas sobre activo soporte de información - DVD.....120

Figura 91. Representación de amenazas sobre activo servicios subcontratados - correo electrónico.....121

Figura 92. Representación de amenazas sobre activo servicios subcontratados - portal.....121

Figura 93. Representación de amenazas sobre activo servicios subcontratados - hosting y administración.....121

Figura 94. Representación de amenazas sobre activo instalaciones - centro de datos.....122

Figura 95. Representación de amenazas sobre activo personal - administradores de sistemas.....122

Figura 96. Representación de amenazas sobre activo personal - administradores de comunicaciones.....122

Figura 97. Representación de amenazas sobre activo personal - administradores de bases de datos.....123

Figura 98. Representación probabilidad ocurrencia amenazas y degradación sobre activo activos esenciales - formato administración cuentas de usuarios.....124

Figura 99. Representación probabilidad ocurrencia de amenazas y degradación sobre activo activos esenciales-registros de recurso.....124

Figura 100. Representación probabilidad ocurrencia de amenazas y degradación sobre activo activos esenciales - autenticación de usuarios.....124

Figura 101. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos - directorio activo.....125

Figura 102. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos - DNS.....125

Figura 103. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos- DHCP.....125

Figura 104. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos - BIOMETRICO.....126

Figura 105. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema de información notarial.....126

Figura 106. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema de personal y nomina.....127

Figura 107. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - IRIS documental.....127

Figura 108. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema de procesos judiciales.....128

Figura 109. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - hoja de vida de notarios.....128

Figura 110. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema de control interno disciplinario.....129

Figura 111. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema de control interno disciplinario notarias.....129

Figura 112. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - sistema integrado web.....130

Figura 113. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - interrelación registro-catastro.....130

Figura 114. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - botón de pago.....130

Figura 115. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - ventanilla única de registro.....131

Figura 116. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - netbackup.....131

Figura 117. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - oracle virtual machine.....131

Figura 118. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones - endpointsecurity.....132

Figura 119. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - exadata.....132

Figura 120. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - exalogic.....133

Figura 121. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - servidores.....133

Figura 122. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - computadores.....134

Figura 123. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - portátiles.....134

Figura 124. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - impresoras.....135

Figura 125. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - switch.....135

Figura 126. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos - firewall.....136

Figura 127. Representación probabilidad ocurrencia de amenazas y degradación sobre activo comunicaciones - red LAN.....136

Figura 128. Representación probabilidad ocurrencia de amenazas y degradación sobre activo comunicaciones - Internet.....137

Figura 129. Representación probabilidad ocurrencia de amenazas y degradación sobre activo elementos auxiliares - ups.....137

Figura 130. Representación probabilidad de ocurrencia de amenazas y degradación sobre activo elementos auxiliares - fuentes de alimentación.....137

Figura 131. Representación probabilidad de ocurrencia de amenazas y degradación sobre activo elementos auxiliares - aire acondicionado.....138

Figura 132. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información - arreglo de discos.....138

Figura 133. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información - librería de cintas.....139

Figura 134. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información - DVD.....139

Figura 135. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados - correo electrónico.....140

Figura 136. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados - portal.....140

Figura 137. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados - hosting y administración.....140

Figura 138. Representación probabilidad ocurrencia de amenazas y degradación sobre activo instalaciones - centro de datos.....141

Figura 139. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal - administradores de sistemas.....141

Figura 140. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal - administradores de comunicaciones.....141

Figura 141. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal - administradores de bases de datos.....142

Figura 142. Código de colores niveles de criticidad 144

Figura 143. Representación general de impacto.....145

Figura 144. Representación de impacto sobre activo servicios internos - Directorio activo.....145

Figura 145. Representación de impacto sobre activo servicios internos - Servicio de nombres de dominio (DNS).....146

Figura 146. Representación de impacto sobre activo servicios internos - DHCP.....146

Figura 147. Representación de impacto sobre activo servicios internos - BIOMETRICO.....146

Figura 148. Representación de impacto sobre activo aplicaciones - sistema de información notarial (SIN).....147

Figura 149. Representación de impacto sobre activo aplicaciones - sistema de personal y nomina.....147

Figura 150. Representación de impacto sobre activo aplicaciones - IRIS documental.....148

Figura 151. Representación de impacto sobre activo aplicaciones - sistema de procesos judiciales.....148

Figura 152. Representación de impacto sobre activo aplicaciones - hoja de vida de notarios.....148

Figura 153. Representación de impacto sobre activo aplicaciones - sistema de control interno disciplinario.....149

Figura 154. Representación de impacto sobre activo aplicaciones - sistema de control interno disciplinario notarias.....149

Figura 155. Representación de impacto sobre activo aplicaciones - sistema integrado web.....150

Figura 156. Representación de impacto sobre activo aplicaciones - interrelación registro-catastro.....150

Figura 157. Representación de impacto sobre activo aplicaciones - botón de pago.....150

Figura 158. Representación de impacto sobre activo aplicaciones - ventanilla única de registro VUR).....151

Figura 159. Representación de impacto sobre activo aplicaciones - netbackup.....151

Figura 160. Representación de impacto sobre activo aplicaciones - oracle virtual machine (OVM).....151

Figura 161. Representación de impacto sobre activo aplicaciones - endpointsecurity.....152

Figura 162. Representación de impacto sobre activo equipos - exadata.152

Figura 163. Representación de impacto sobre activo equipos - exalogic.152

Figura 164. Representación de impacto sobre activo equipos - servidores.....153

Figura 165. Representación de impacto sobre activo equipos - computadores.....153

Figura 166. Representación de impacto sobre activo equipos - portátiles.153

Figura 167. Representación de impacto sobre activo equipos - impresoras.....154

Figura 168. Representación de impacto sobre activo equipos - switch....154

Figura 169. Representación de impacto sobre activo equipos - firewall...154

Figura 170. Representación de impacto sobre activo comunicaciones - red LAN.....155

Figura 171. Representación de impacto sobre activo comunicaciones - internet.....155

Figura 172. Representación de impacto sobre activo elementos auxiliares - sistema de alimentación ininterrumpida (UPS).....155

Figura 173. Representación de impacto sobre activo elementos auxiliares - fuentes de alimentación.....156

Figura 174. Representación de impacto sobre activo elementos auxiliares - aire acondicionado.....156

Figura 175. Representación de impacto sobre activo soporte de información - arreglo de discos.....157

Figura 176. Representación de impacto sobre activo soporte de información - librería de cintas.....157

Figura 177. Representación de impacto sobre activo soporte de información - unidad DVD.....158

Figura 178. Representación de impacto sobre activo servicios subcontratados - correo electrónico.....158

Figura 179. Representación de impacto sobre activo servicios subcontratados - portal.....158

Figura 180. Representación de impacto sobre activo servicios subcontratados - hosting y administración.....159

Figura 181. Representación de impacto sobre activo instalaciones - centro de datos.....159

Figura 182. Representación de impacto sobre activo personal - administradores de sistemas.....159

Figura 183. Representación de impacto sobre activo personal - administradores de comunicaciones.....160

Figura 184. Representación de impacto sobre activo personal - administradores de bases de datos.....160

Figura 185. Representación de riesgos sobre activos.....161

Figura 186. Representación de riesgos sobre activo servicios internos - Servicio de nombres de dominio (DNS).....161

Figura 187. Representación de riesgos sobre activo servicios internos - DHCP.....162

Figura 188. Representación de riesgos sobre activo servicios internos - BIOMETRICO.....162

Figura 189. Representación de riesgos sobre activo aplicaciones - Sistema de información notarial (SIN).....162

Figura 190. Representación de riesgos sobre activo aplicaciones - Sistema de personal y nomina.....163

Figura 191. Representación de riesgos sobre activo aplicaciones - IRIS documental.....163

Figura 192. Representación de riesgos sobre activo aplicaciones - Sistema de procesos judiciales.....163

Figura 193. Representación de riesgos sobre activo aplicaciones - Hoja de vida de notarios.....164

Figura 194. Representación de riesgos sobre activo aplicaciones - Sistema de control interno disciplinario.....164

Figura 195. Representación de riesgos sobre activo aplicaciones - Sistema de control interno disciplinario notarias.....164

Figura 196. Representación de riesgos sobre activo aplicaciones - Sistema integrado web.....165

Figura 197. Representación de riesgos sobre activo aplicaciones - Interrelación registro-catastro.....165

Figura 198. Representación de riesgos sobre activo aplicaciones - Botón de pago.....165

Figura 199. Representación de riesgos sobre activo aplicaciones - Ventanilla única de registro (VUR).....166

Figura 200. Representación de riesgos sobre activo aplicaciones - Netbackup.....166

Figura 201. Representación de riesgos sobre activo aplicaciones - Oracle virtual machine.....166

Figura 202. Representación de riesgos sobre activo aplicaciones - Endpointsecurity.....167

Figura 203. Representación de riesgos sobre activo aplicaciones.....167

Figura 204. Representación de riesgos sobre activo equipos - Exadata..167

Figura 205. Representación de riesgos sobre activo equipos - Exalogic.168

Figura 206. Representación de riesgos sobre activo equipos - Servidores.....168

Figura 207. Representación de riesgos sobre activo equipos - Computadores.....168

Figura 208. Representación de riesgos sobre activo equipos - Portátiles.169

Figura 209. Representación de riesgos sobre activo equipos - Impresoras.....169

Figura 210. Representación de riesgos sobre activo equipos - Switch....169

Figura 211. Representación de riesgos sobre activo equipos - Firewall..170

Figura 212. Representación de riesgos sobre activos equipos.....170

Figura 213. Representación de riesgos sobre activo comunicaciones - Red LAN.....170

Figura 214. Representación de riesgos sobre activo comunicaciones - Internet.....171

Figura 215. Representación de riesgos sobre activos comunicaciones..171

Figura 216. Representación de riesgos sobre activo elementos auxiliares - Sistema de alimentación ininterrumpida (UPS).....171

Figura 217. Representación de riesgos sobre activo elementos auxiliares - Fuentes de alimentación.....172

Figura 218. Representación de riesgos sobre activo elementos auxiliares - Aire acondicionado.....172

Figura 219. Representación de riesgos sobre activo soporte de información - arreglo de discos.....172

Figura 220. Representación de riesgos sobre activo soporte de información - Librería de cintas.....173

Figura 221. Representación de riesgos sobre activo soporte de información- Unidad DVD.....173

Figura 222. Representación de riesgos sobre activos soporte de información.....173

Figura 223. Representación de riesgos sobre activo servicios subcontratados - Correo electrónico.....174

Figura 224. Representación de riesgos sobre activo servicios subcontratados - Portal.....174

Figura 225. Representación de riesgos sobre activo servicios subcontratados - Hosting y administración.....174

Figura 226. Representación de riesgos sobre activos servicios subcontratados.....174

Figura 227. Representación de riesgos sobre activo instalaciones - Centro de datos.....175

Figura 228. Representación de riesgos sobre activos instalaciones.....175

Figura 229. Representación de riesgos sobre activo personal - Administradores de sistemas.....175

Figura 230. Representación de riesgos sobre activo personal - Administradores de comunicaciones.....175

Figura 231. Representación de riesgos sobre activo personal - Administradores de bases de dato.....176

Figura 232. Representación de riesgos sobre activos personal.....176

Figura 233. Representación impacto sobre activos.....177

Figura 234. Representación riesgos sobre activos.....181

Figura 235. Esquema calificación de riesgos.....194

LISTA DE CUADROS

pág.

Cuadro 1. Ciclo básico de la gestión del proceso Gestión Tecnológica....64

Cuadro 2. Ciclo básico de la gestión del proceso gestión incorporación de tecnología.....66

Cuadro 3. Riesgos y controles implícitos del proceso.....67

Cuadro 4. Ciclo básico de la gestión del proceso gestión de recursos de tecnología.....71

Cuadro 5. Riesgos y controles implícitos del proceso.....73

Cuadro 6. Plan de tratamiento de riesgos.....194

Cuadro 7. Declaración de aplicabilidad SOA.....221

RESUMEN

En nuestros tiempos el uso de la tecnología se ha convertido en una necesidad fundamental y es parte imprescindible de nuestro diario acontecer, en esta era digital la información se ha constituido en el elemento esencial.

Para muchas organizaciones en el mundo la información se constituye en la esencia fundamental de su existencia y se ha constituido imperativamente en el activo más importante dentro de su patrimonio.

Algunas organizaciones son muy conscientes de la necesidad de diseñar e implementar las medidas necesarias para salvaguardar la integridad, confidencialidad y disponibilidad de la información, los tres pilares fundamentales de la seguridad de la información.

La seguridad de la información implica la consideración de múltiples alternativas de seguridad que en conjunto y de manera integral sean capaces de asegurar la información contra las distintas amenazas que se ciernen sobre ella. Las formas y tipos de ataques a la seguridad de la información evolucionan dinámicamente y de forma permanente, las herramientas y facilidades para la ejecución de ataques cibernéticos desafortunadamente se encuentran a la mano de cualquier individuo que sin la necesidad de disponer de amplios conocimientos tecnológicos pueden ser capaces de generar y emitir ataques en contra de la integridad y seguridad de la información.

Los propósitos de los delincuentes cibernéticos son cada vez más destructivos y sus ambiciones totalmente desmedidas. Por desgracia estos ciberdelincuentes en la mayoría de los casos encuentran los escenarios propicios y favorables para la planeación y ejecución de ataques en contra de la seguridad de la información con resultados positivos para ellos. Todo en razón a que muchas organizaciones no son conscientes de la importancia de la seguridad alrededor del tema de la información.

De forma voluntaria o involuntaria son las organizaciones las responsables de que los ataques cibernéticos ejecutados por los ciberdelincuentes tengan éxito, por no considerar, revisar y evaluar de forma permanente y sin tregua los lineamientos de seguridad que permitan proteger estrictamente la información y toda la infraestructura tecnológica dispuesta para su administración y uso.

Basados en el hecho innegable de que la información está expuesta a múltiples amenazas que pueden comprometer seriamente la integridad, confidencialidad y disponibilidad de la información en cualquier organización independientemente de su naturaleza privada o pública y su razón social. El presente trabajo de grado denominado "Diseño de un sistema de gestión de seguridad de la información

(SGSI) para el departamento de informática de la Superintendencia de Notariado y Registro", Busca proponer el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), a través del cual se proponen las medidas de seguridad necesarias para la salvaguarda de la información en la Superintendencia de Notariado y Registro, basados fundamentalmente en la evaluación estricta de la seguridad de la información actualmente en la entidad.

Para el diseño del Sistema de Gestión de Seguridad de la Información, que se propone para la Superintendencia de Notariado y Registro se consideraran fundamente los conceptos y planteamientos de los estándares internacionales de la ISO, específicamente las normas ISO/IEC 27001 e ISO/IEC 27002. Así como la aplicación de la metodología MAGERIT para la ejecución de la tarea de análisis de riesgo respectivo, metodología diseñada por el gobierno español para la ejecución de análisis de riesgo.

El propósito final del presente trabajo de grado será una propuesta de diseño de un Sistema de un Sistema de Gestión de Seguridad de la Información que proporcione las respuestas necesarias a los problemas de seguridad que se evidencian al interior del departamento de informática de la entidad.

INTRODUCCION

El siglo XX fue una época de enorme inspiración donde mentes de todo el mundo hicieron aportes intelectuales de enorme valor a partir de lo cual se gestaron descubrimientos e innovaciones de gran importancia para la humanidad.

A partir de la revolución industrial los métodos tradicionales de producción sucumbirían ante las nacientes innovaciones de tipo tecnológico que afectarían en adelante y para siempre los modelos de producción hasta entonces conocidos.
Pero sería solo hasta la segunda mitad del siglo XX y luego de los terribles episodios de la segunda guerra mundial que empezarían a darse pasos interesantes en el desarrollo de un campo de conocimiento hasta ese momento muy incipiente pero que en el mediano plazo influiría de manera directa en la vida de todo ser humano. La informática.

Los adelantos tecnológicos que fueron generándose cada vez con mayor periodicidad permitieron el desarrollo de diferentes campos del conocimiento, entre ellos el desarrollo de la informática lo que permitió en primer lugar la tecnificación de procesos industriales eliminando para siempre procesos y procedimientos manuales poco eficientes y productivos.

Los procesos y procedimientos de las compañías fueron ajustados de acuerdo a las facilidades que aportaba el uso y aplicación de la informática.

Los adelantos tecnológicos en el campo de la informática fueron tan progresivos y continuos que el uso de la tecnología informática dejaría de ser de uso exclusivo de las grandes compañías y llego el buen momento en que cualquier compañía grande o pequeña, así como cualquier persona pudieran acceder a la tecnología informática, fenómeno al que se le denomino "masificación de la tecnología".

Hoy en día todas las organizaciones en el mundo independiente de su actividad. Hacen uso de la tecnología informática para la administración de su información, catalogada hoy en día por los entendidos como el mayor activo de cualquier organización.

Al ser catalogada la información como el activo más importante de cualquier organización, obliga imperativamente a su estricta protección y seguridad. Por desgracia la masificación de la tecnología y la facilidad en su acceso que en su momento se tradujo en una valiosa oportunidad de progreso de entidades e individuos. Hoy se aprecian efectos negativos en ello en la medida en que individuos han encontrado en el uso indebido de la tecnología la forma de acceder ilegalmente a la información y poner en riesgo la integridad, confidencialidad y disponibilidad de la misma.

Existen innumerables amenazas latentes sobre la información y su conservación e integridad exigen la consideración e implementación de todos los mecanismos y las medidas de seguridad posibles, que eviten o por lo menos disminuyan los riesgos latentes sobre la información y los recursos tecnológicos a través de los cuales se administra tal información.

1. GENERALIDADES DEL PROYECTO

1.1 DESCRIPCION DEL PROBLEMA

Las superintendencias son organismos técnicos a través de los cuales el Presidente de la República por delegación ejerce inspección y vigilancia de las entidades asignadas a cada superintendencia, adscritas a los ministerios, tienen personería jurídica, autonomía administrativa y patrimonio propio.

La Superintendencia de Notariado y Registro garantiza la guarda de la fe pública en Colombia mediante la prestación del servicio público registral y la orientación, inspección, vigilancia y control del servicio público notarial.

Entre sus funciones se encuentran:

- Adelantar las gestiones necesarias para la eficaz y transparente prestación del servicio público notarial y registral.
- Impartir las instrucciones de carácter general, dictar las resoluciones y demás actos que requiera la eficiente prestación de los servicios públicos de notariado y de registro de instrumentos públicos, las cuales serán de obligatorio cumplimiento.
- Instruir a los notarios y registradores de instrumentos públicos, sobre la aplicación de las normas que regulan su actividad.
- Fijar los estándares de calidad requeridos para la prestación de los servicios de notariado y de registro de instrumentos públicos.
- Administrar y organizar el registro de instrumentos públicos de conformidad con la ley, sin perjuicio de la facultad del Gobierno Nacional para la creación o supresión de círculos y de oficinas del registro de instrumentos públicos.
- Ejercer la inspección, vigilancia y control de las notarías y las oficinas de registro de instrumentos públicos, en los términos establecidos en las normas vigentes, mediante visitas generales, especiales, de seguimiento, por procedimientos virtuales o por cualquier otra modalidad.
- Realizar visitas periódicas de vigilancia, inspección y control a los entes vigilados.
- Investigar y sancionar las faltas disciplinarias de los notarios y registradores de instrumentos públicos, en el desarrollo de sus funciones, sin perjuicio del poder preferente que podrá ejercer la Procuraduría General de la Nación.
- Establecer sistemas administrativos y operativos para lograr la eficiente atención de los servicios de notariado y de registro de instrumentos públicos procurando su racionalización y modernización.

- Adelantar las gestiones necesarias para asignar a las oficinas de registro de instrumentos públicos el presupuesto necesario para garantizar una adecuada y eficiente prestación del servicio público.

En el desarrollo de sus funciones la Superintendencia de Notariado y Registro ha realizado inversiones significativas en tecnología de punta que ha venido implementando a través de su departamento de Informática con el fin de administrar su información de la manera más eficientemente posible. Sin embargo la implementación de seguridad es un concepto todavía muy crudo al interior de la entidad incluido el departamento de Informática que presenta serias falencias de seguridad y en donde no se observan mecanismos de control consistentes y fiables que permita garantizar un uso seguro de la información y una administración correcta, responsable y segura de los recursos tecnológicos a través de los cuales se administra la información, El departamento de Informática debería ser punto de referencia obligado para los demás departamentos mediante iniciativas de seguridad que pudieran replicarse a cada uno de los departamentos existentes.

A pesar de que al interior del departamento de Informática cada día se viene adquiriendo cierta concientización de la necesidad de implementar mecanismos de seguridad que le permitan administrar de forma segura la información, los esfuerzos para conseguirlo han sido poco consistentes y desafortunadamente se han convertido en esfuerzos aislados.

Al interior del departamento de Informática se pueden evidenciar entre otros los siguientes síntomas que también padecen otros departamentos y que reflejan una ausencia de normas y mecanismos de control que permitan asegurar la información y el acceso a la misma:

- Lentitud en el desempeño de los computadores.
- Formateo frecuente de las estaciones de trabajo a causa de contaminación de virus.
- Lentitud de red LAN.
- Proliferación de virus.
- Saturación de Discos Duros con información personal y de entretenimiento.
- Uso de correos privados al interior de la entidad, a pesar de la asignación de cuentas de correo institucional.
- Acceso de personas no autorizadas a zonas declaradas como restringidas.
- Facilidad en el acceso a la red LAN por parte de visitantes.
- Traslado de computadores entre áreas sin control alguno.
- Utilización generalizada de medios de almacenamiento extraíbles sin control alguno.

- Escaso control por parte de funcionarios y contratistas en el manejo de sus cuentas de usuarios.
- Entrada y salida de documentos del departamento y de las instalaciones físicas de la entidad, con información oficial.
- Entrada y salida de portátiles sin verificación de su contenido.
- Desmesura en el número de usuarios habilitados para navegación en Internet.
- Ausencia de un plan de mantenimiento preventivo a los computadores.
- Ausencia de reportes que informen sobre retiros de funcionarios y contratistas.
- Dificultad en la administración de roles, ante ausencia de información relacionada con el retiro de funcionarios y contratistas.
- No existe control alguno sobre qué tipo de información de la entidad se puede enviar por el correo institucional.

Entre las posibles causas que se pueden enumerar, que hacen que se generen los anteriores síntomas y que darían respuesta a las debilidades que se presentan en el manejo y acceso a la información podrían citarse las siguientes:

- No existen procedimientos definidos que determinen la correcta utilización de memorias USB y en general de medios de almacenamiento extraíbles.
- No existe normatividad alguna que especifique la correcta utilización de los Discos Duros.
- No existen mecanismos de control que establezcan formalmente la no utilización de cuentas de correo electrónico privado al interior de la entidad y en caso de excepciones los controles que deben seguirse.
- No existe un marco normativo en el que se estipule el correcto uso de Internet.
- No existe un marco normativo que defina y establezca que son las zonas restringidas, ni mecanismos de control que permitan aplicar el respectivo control.
- No existe un marco normativo que defina como y en qué condiciones podrán acceder a la red LAN, personal de origen externo.
- No existe un marco normativo que establezca las condiciones bajo las cuales los computadores serán movidos entre áreas. Previniendo perdida, destrucción, copia y borrado de información.
- No existe un marco normativo en el que se establezcan las directrices sobre la administración de las cuentas de usuarios y las obligaciones que asumen los funcionarios y contratistas en el manejo de las mismas.
- No existe un marco normativo en el que se establezcan los requisitos a cumplir para la utilización de portátiles al interior del departamento de Informática y la entidad en general por parte de visitantes y funcionarios o contratistas que ingresen portátiles de su propiedad.

- Se carece de procedimientos en el que se definan las condiciones a cumplir para que sea aprobado a un funcionario o contratista acceso a Internet.

Sin la implementación de mecanismos y soportes de seguridad especialmente en el departamento de Informática como punto central de la información la naturaleza misma de la Superintendencia de Notariado y Registro como guarda de la Fe pública podría estar en riesgo.

La principal amenaza para la seguridad de la información se encuentra al interior del departamento de Informática, en donde debido a la falta de un marco de procedimientos, métodos y controles claramente definidos y de obligatorio y drástico cumplimiento se podría estar dando una peligrosa fuga de información o en su defecto sus recursos de tecnología pueden estar expuestos a riesgos varios y desastrosos.

1.2 FORMULACION DEL PROBLEMA

¿Mediante que mecanismo se puede preservar la seguridad integral de la información y establecer controles eficientes de acceso a la misma al interior del departamento de Informática de la Superintendencia de Notariado y Registro?

1.3 JUSTIFICACION

A través de un Sistema de Gestión de Seguridad de la Información (SGSI), el departamento de Informática de la Superintendencia de Notariado y Registro podrá contar con un marco de reglas y procedimientos que regularan la utilización de los recursos de tecnología y del acceso a la información, imprimiendo un sello de seguridad sobre la información.

Mediante el Sistema de Gestión de Seguridad de la Información (SGSI), Se establecerán una serie de políticas de obligatorio y estricto cumplimiento, políticas que regularan todo lo relacionado con el manejo, uso y administración de la información.

El SGSI, será el punto central alrededor del cual giraran todos los temas complementarios de seguridad, en el futuro todas las decisiones que se tomen y afecten el estado de la seguridad y en general las plataformas y recursos tecnológicos en general con que cuenta el departamento de Informática de la Superintendencia de Notariado y Registro, serán evaluadas tomando como referencia el SGSI.

El SGSI, le permitirá al departamento de Informática de la Superintendencia de Notariado y Registro contar con un marco de referencia y regulación que le permitirá administrar la información de forma segura y eficiente. Reduciendo los niveles de riesgo a valores mínimos y ubicados dentro de márgenes controlables y administrables. Asegurando de esta forma la disponibilidad, confidencialidad e integridad de la información.

Al prestar servicios varios a la ciudadanía, es obligación de la Superintendencia de Notariado y Registro y especialmente de su departamento de Informática contar con todos los mecanismos necesarios que le permitan proteger y salvaguardar la información, para de esta forma proporcionar de manera segura y eficiente cada uno de los servicios que se ofrecen hoy en día a la ciudadanía.

Dada la sensibilidad de la información que se maneja en la Superintendencia de Notariado y Registro, un Sistema de Gestión de Seguridad de la Información (SGSI), Le proporcionara al departamento de Informática un valioso instrumento para ejercer de forma estricta y rigurosa un control sobre la información y los recursos tecnológicos que se utilizan para su administración mediante la aplicación de buenas prácticas según estándares internacionales. Podría ser un punto de partida fundamental a la hora de tomar decisiones que tengan que ver con la implementación de proyectos de diversa índole y que puedan poner en riesgo la seguridad de la información.

2. FORMULACION DE OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de la seguridad de la información (SGSI) para el departamento de Informática de la Superintendencia de Notariado y Registro mediante la aplicación de las normas ISO/IEC 27001 e ISO/IEC 27002 para establecer controles de acceso a la información y preservar la seguridad de la información.

2.2 OBJETIVOS ESPECIFICOS

- Determinar los niveles de vulnerabilidades en la red de datos de la Superintendencia de Notariado y Registro mediante un análisis de riesgos en esta entidad.
- Determinar la manera más eficiente de salvaguardar los recursos informáticos de robos, pérdidas y daños intencionados o no que puedan afectar la disponibilidad de los recursos tecnológicos e información. Basados en la aplicación de las normas ISO/IEC 27001 e ISO/IEC 27002.
- Determinar las políticas y controles necesarios para asegurar el buen uso de los recursos de tecnología y sistemas de información por parte de los funcionarios y contratistas del departamento de Informática.

3. MARCO REFERENCIAL

3.1 MARCO TEORICO

3.1.1 ¿Qué se entiende por seguridad informática?. La seguridad informática se puede definir como cualquier medida que lleve implícita la intención de impedir la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan llevar implícitos daños sobre la información, comprometer su estado de confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Según la norma ISO/IEC 17799 la Seguridad de la Información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

Según la norma ISO 7498 la Seguridad Informática se define como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

3.1.2 Factores de los que depende la seguridad informática. La seguridad informática depende de factores muy diversos entre los que podríamos citar los siguientes:

- La sensibilización de los directivos y responsables de la organización, que deberán ser conscientes de la necesidad de destinar recursos a esta función.
- La concientización, formación y asunción de responsabilidades por parte de los usuarios de los sistemas.
- La correcta instalación, configuración y mantenimiento de los equipos.
- Contemplar las amenazas tanto del exterior como de las amenazas procedentes del interior de la organización.
- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización. Evitar el diseño de políticas y procedimientos genéricos.
- El soporte continuo y permanente de los fabricantes de hardware y software, a través de la publicación periódica de los parches y actualizaciones de seguridad de sus productos que permitan corregir fallos y problemas de seguridad.

Hoy en día uno de los principios de las buenas prácticas de la gestión empresarial es el de la seguridad de la información, siendo responsabilidad irrenunciable e intransferible de la dirección general disponer los recursos y medios necesarios

para la implantación de un adecuado sistema de gestión de la seguridad de la información en la organización.

3.1.3 Objetivos de la seguridad informática. Entre los principales objetivos de la seguridad informática se pueden definir los siguientes:

- Identificar, Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la correcta y adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar al mínimo las pérdidas que puedan generarse y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para cumplir con los objetivos anteriormente planteados, cualquier organización deberá ser consciente de actuar sobre los siguientes cuatro planos de acción:

- Técnico: Considerar tanto a nivel físico como a nivel lógico.
- Legal: En algunos países se exige la implementación de medidas de seguridad para ciertos sectores de la economía mediante disposiciones de Ley.
- Humano: Mediante la permanente orientación, formación y capacitación de todo el personal de la compañía incluido el personal directivo de la compañía.
- Organizativo: Mediante el diseño, definición e implantación de políticas de seguridad, normas, procedimientos, planes y buenas prácticas.

La Seguridad Informática debe ser entendida por cualquier organización como un proceso. Se trata de un ciclo iterativo, en el que se incluyen una serie de actividades como la valoración de riesgos, tareas de prevención, detección y mecanismos de respuesta ante incidentes de seguridad.

3.1.4 ¿Qué es un Sistema de Gestión de Seguridad de la Información (SGSI)?. Un Sistema de Gestión de Seguridad de la Información se define como aquella parte constitutiva del sistema general de gestión que comprende la política, la estructura organizativa, los recursos, los procedimientos y los procesos fundamentales para implantar la gestión de la seguridad de la información en una organización.

Para gestionar de manera eficiente la seguridad de la información es de vital importancia considerar una serie de tareas y procedimientos que permitan garantizar los niveles óptimos de seguridad que exige la organización, teniendo

siempre presente que no se puede lograr un nivel de seguridad del 100% ya que los riesgos no se pueden eliminar en su totalidad.

Las políticas orientadas a la Gestión de Seguridad de la Información están compuestas por el conjunto de normas reguladoras, reglas, procedimientos y buenas prácticas que determinan el modo en que todos los activos y recursos de la organización considerando la información misma son gestionados, protegidos y distribuidos.

Para implementar un Sistema de Gestión de Seguridad de la Información, toda organización debe considerar los siguientes aspectos:

1). Formalizar la gestión de la seguridad de la información.
2). Analizar y gestionar los riesgos.
3). Establecer procesos de gestión de la seguridad siguiendo la metodología PDCA:
* Plan: Selección y definición de medidas y procedimientos.
* Do: Implantación de medidas y procedimientos de mejora.
* Check: Comprobación y verificación de las medidas que se han Implantado.
* Act: Actuación para corregir todas las deficiencias detectadas en el Sistema.
4). Certificación de la gestión de la seguridad.

3.1.5 ¿Para qué sirve un SGSI?. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y actualiza constantemente.

3.1.6 ¿Cuáles son los beneficios de un SGSI?

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Definir objetivos y metas.
- Integrar la gestión de la seguridad de la información con el resto de sistemas de gestión existentes en la entidad.
- Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en su SGSI.
- Cumplimiento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, etc.
- Mejora continua de la gestión de la seguridad.

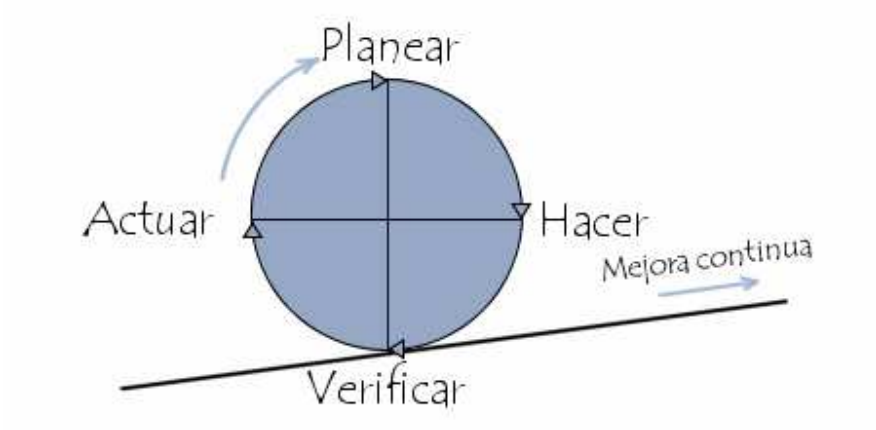
- Incremento de confianza de clientes y socios. Los clientes tienen acceso a la información a través de medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Garantía de continuidad de negocio.
- Posicionamiento positivo de imagen de empresa a nivel internacional y como elemento diferenciador ante la competencia.
- Confianza y reglas claras tanto para empleados como para contratistas de la organización.
- Reducción de costos y mejoramiento continúo de procesos y procedimientos.
- Incremento de la seguridad basada en la gestión de procesos y no en la compra sistemática de productos y tecnologías.

3.1.7 Ciclo Deming – Mejora Continua. Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

El Ciclo de Deming así llamado por su creador Edwards Deming, también es conocido como Ciclo de Mejora Continua. Esta metodología menciona cuatro pasos fundamentales que deben seguirse para lograr la mejora continua, esos cuatro pasos deben llevarse a cabo de forma sistemática.

La aplicación del Ciclo de Deming aporta como beneficio fundamental a cualquier empresa la mejora de productos, servicios y competitividad mediante la mejora permanente de la calidad, disminución y reducción de costos, optimización de los niveles de productividad, reducción a valores mínimos de los precios. Beneficios que se traducen en un incremento de la rentabilidad de cualquier compañía y una mayor presencia en el mercado.

Figura 1. Ciclo de Deming



Fuente http://es.ccm.net/contents/606-calidad

El Ciclo Deming se compone de cuatro etapas que son cíclicas, lo que se traduce en que una vez culminada la última etapa se debe volver nuevamente a la primera etapa y volver a iniciar el ciclo. La aplicación es cíclica ya que de esta manera es posible diseñar y aplicar las mejoras que sean necesarias.

Las cuatro etapas que componen el Ciclo de Deming o Ciclo de Mejora Continua son:

Planear (Plan):

- Definir alcance del SGSI.
- Definir política de seguridad.
- Metodología de evaluación de riesgos.
- Inventario de activos.
- Identificar amenazas y vulnerabilidades.
- Identificar impactos.
- Análisis y evaluación de riesgos.
- Selección de controles y SOA.

Hacer (Do):

- Definir plan de tratamiento de riesgos.
- Implantar plan de tratamiento de riesgos.
- Implementar los controles.
- Formación y concienciación.
- Operar el SGSI.

Verificar (Check):

- Revisar el SGSI.
- Medicar eficacia de los controles.
- Revisar riesgos residuales.
- Realizar auditorías internas del SGSI.
- Realizar acciones y eventos.

Actuar (Act):

- Implantar mejoras.
- Acciones correctivas.
- Acciones preventivas.
- Comprobar eficacia de las acciones.

Descripción detallada de las etapas del Ciclo de Deming

PLAN= Establecer con planificación

Definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) en términos del negocio, la organización, la localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es de vital importancia definir los límites del SGSI ya que no es necesario, no es obligatorio que un SGSI deba cubrir todas las áreas de la organización, incluso lo recomendable es comenzar por un alcance limitado. En esta etapa se recomienda tener en cuenta las siguientes consideraciones:

- Disponer de mapa de procesos de negocio.
- Identificar las terceras partes (proveedores, clientes, etc.), que influyan sobre la seguridad de la información de acuerdo al alcance establecido.
- Crear mapas de redes y sistemas.
- Definir las ubicaciones físicas.
- Disponer de organigrama de la organización.

Entre otras consideraciones.

En el proceso de construcción de un SGSI se debe definir el enfoque de evaluación de riesgos mediante una metodología de evaluación del riesgo que sea apropiada para el SGSI y los requerimientos propios del negocio. En razón a que es imposible eliminar el riesgo en su totalidad se hace necesario definir una estrategia de aceptación del riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Existen numerosas metodologías estandarizadas para la evaluación de riesgos, las organizaciones podrán optar por cualquiera de ellas, aplicar una combinación de varias o diseñar una propia ajustada a las características propias de la organización.

Identificación de los riesgos

Para la identificación de los riesgos deberán tenerse en cuenta las siguientes consideraciones:

- Identificar todos aquellos activos de información que tienen algún valor para la organización y que están dentro del alcance definido para el SGSI e identificar también a sus responsables directos, a los que se denomina propietarios.
- Identificar cada una de las amenazas que se ciernen sobre los activos identificados.
- Identificar las vulnerabilidades que puedan hacer posible la materialización de las amenazas.
- Identificar el impacto que podría generarse a partir de la perdida de confidencialidad, integridad y disponibilidad para los activos identificados.

Análisis y evaluación de riesgos

Para el análisis y evaluación de riesgos deberán tenerse en cuenta las siguientes consideraciones:

- Evaluar el impacto que representa para el negocio la ocurrencia de fallos de seguridad que atenten contra la integridad, confidencialidad o disponibilidad de los activos identificados.
- Evaluar estrictamente la probabilidad de ocurrencia de cada fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
- Estimación estricta de los niveles de riesgo.
- Determinar, de acuerdo a los criterios de aceptación de riesgo previamente definidos, aceptados y establecidos, si el riesgo es aceptable o necesita ser tratado.

Tratamiento de riesgos

En relación al tratamiento de riesgos deberán tenerse en cuenta las siguientes consideraciones:

- Diseñar y aplicar controles adecuados.
- Aceptar conscientemente el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para aceptación de los riesgos.
- Evitar el riesgo mediante el control y/o eliminación de las actividades que lo originan.
- Transferir el riesgo de forma total o parcialmente a terceros, como por ejemplo a proveedores de servicios (outsourcing), compañías aseguradoras, etc.

- Definir los controles para el tratamiento de riesgos.
- La dirección de la organización deberá aprobar los riesgos residuales.

Declaración de aplicabilidad (SOA)

En relación a la declaración de aplicabilidad deberán tenerse en cuenta las siguientes consideraciones:

- Incluir los objetivos de control y controles seleccionados y motivos para su elección.
- Incluir los objetivos de control y controles que actualmente están implantados.
- En caso de que haya controles excluidos deberán establecerse los argumentos.

DO= Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos. Que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos. Con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles. Definidos y seleccionados anteriormente que permitan llegar a los objetivos de control.
- Definir sistema de métricas. Con el propósito de obtener resultados comparables que permitan medir la eficacia de los controles o grupos de controles.
- Procurar diseñar e implementar programas de capacitación y concientización en relación a temas de seguridad de la información orientados a todo el personal de la organización.
- Gestionar las operaciones de SGSI.
- Gestionar los recursos destinados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos de control que permitan identificar oportunamente los incidentes de seguridad y dar un tratamiento eficiente a los mismos.
- Desarrollo de marco normativo, que involucre: normas, manuales, procedimientos e instrucciones.

CHECK= Monitorizar y revisar

La organización deberá tener en cuenta las siguientes consideraciones:
Llevar a cabo procedimientos de monitorización y revisión. Con el propósito de:

- Detectar oportunamente los errores en los resultados generados por el procesamiento de la información.
- Identificar vacíos e incidentes de seguridad.
- Ayudar a la organización a determinar si las actividades llevadas a cabo por las personas y los recursos tecnológicos para garantizar la seguridad de la información se comportan de acuerdo a lo previsto.
- Detectar y prevenir eventos e incidentes de seguridad de acuerdo a la utilización de indicadores.
- Determinar si las acciones tomadas para el tratamiento de los vacíos de seguridad surten efectos positivos.
- Revisar de forma regular la salud y efectividad del SGSI, basados en el cumplimiento de la política y objetivo del SGSI, los resultados arrojados por las auditorias de seguridad, incidentes, sugerencias y observaciones realizadas por las partes implicadas.
- Medir la efectividad de los controles con el propósito de comprobar si se cumple con los requisitos de seguridad.
- Revisar de forma periódica las evaluaciones de riesgo, los riesgos residuales y los niveles de aceptación de riesgos, previendo y considerando los posibles cambios que se hayan podido producir en la organización, la tecnología, objetivos y procesos de negocio, las amenazas, efectividad en los controles implementados, obligaciones contractuales, etc.
- Realizar de forma periódica y planificada auditorías internas al SGSI. Con el fin de determinar si los controles, procesos y procedimientos del SGSI se mantienen de acuerdo a las exigencias y lineamientos de la norma bajo el cual fue construido y observar si los requisitos y objetivos de seguridad de la organización son mantenidos y aplicados correctamente, evaluando además si efectivamente el rendimiento es el esperado.
- Revisión periódica del SGSI por parte de la alta dirección de la organización con el fin de verificar y determinar que el alcance definido sigue siendo el adecuado y determinar si es necesaria la implementación de mejoras al SGSI.
- Actualizar los planes de seguridad basados en nuevos hallazgos detectados durante las actividades de monitoreo y revisión.
- Registrar todo tipo de acciones y eventos que hayan impactado la efectividad y rendimiento del SGSI.

ACT= Mantener y mejorar

La organización deberá tener en cuenta las siguientes consideraciones:

- Implantar en el SGSI las mejoras que se hayan identificado.
- Realizar las acciones preventivas y correctivas a que haya lugar con la intención de prevenir potenciales no conformidades antes de que estas ocurran y dar soluciones a aquellas inconformidades que se hayan materializado.

- Divulgar las acciones de mejoras a todas las partes interesadas y de ser posible establecer en consenso la mejor forma de implementarlas.

Debe tenerse siempre presente que PDCA obedece a un ciclo de vida continuo, lo que en esencia quiere decir que concluida la fase ACT se regresara a la fase PLAN para iniciar un nuevo ciclo.

3.1.8 Normas y estándares para el diseño e implantación de un SGSI?. Para el diseño e implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) se suelen considerar entre otras las siguientes normas y estándares:

- La norma ISO/IEC 27001: "Especificaciones para los sistemas de gestión de la seguridad de la información", requeridas para obtener la certificación del SGSI implantado. Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tamaño o naturaleza.
- El estándar ISO/IEC 27002, "Código de Buenas prácticas para la gestión de la seguridad de la información". Estructurada en 11 dominios desglosados a su vez en 133 controles, que cubren todos los aspectos fundamentales de la seguridad en el tratamiento de la información.

3.1.9 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT). MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración y la sociedad en general, dependen cada vez mas de las tecnologías de la información para el cumplimiento de su misión.

La razón que dio origen a MAGERIT está directamente relacionada con la utilización generalizada de las tecnologías de la información, que si bien proporciona beneficios positivos y evidentes a la ciudadanía, también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT es una metodología destinada para su utilización por todas aquellas personas que trabajan con información digital y sistemas informáticos y cuyo interés se centra en cómo administrar de la mejor manera la información y los sistemas informáticos. MAGERIT les permitirá saber que tan importante es la

información y los servicios que se prestan, a que riesgos están expuestos y les ayudara a protegerlos. Conocer el riesgo al que están sometidos los elementos de trabajo, es imprescindible para poder gestionarlos. A través de MAGERIT se persigue una aproximación metódica en el que se elimine la improvisación y se evite todo tipo de arbitrariedades por parte del analista.

El análisis y gestión de los riesgos tiene como finalidad poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

Objetivos de MAGERIT

La metodología MAGERIT busca los siguientes objetivos:

- Concientizar a los responsables de las organizaciones de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar adecuadamente el tratamiento de los riesgos para mantenerlos bajo control.
- Preparar a la organización para eventuales procesos de evaluación, auditoria, certificación o acreditación.

MAGERIT es una metodología de carácter público, perteneciente al Ministerio de Hacienda y Administraciones Públicas del gobierno español, su utilización no requiere autorización previa. Su versión más actual es la versión 3 dada a conocer en el año 2012.

3.2 MARCO CONTEXTUAL

3.2.1 Misión. La Superintendencia de Notariado y Registro, como responsable de la guarda de la Fe pública, garantiza mediante la orientación, inspección, vigilancia y control, la seguridad jurídica y administración del servicio público registral inmobiliario; así como la actividad notarial. A partir de la innovación y efectividad en sus procesos y calidad de los servicios ofrecidos a nuestros clientes.

3.2.2 Visión. En el 2014 la SNR será una institución modelo en la prestación del servicio público registral y en la guarda de la Fe pública. Líder en proceso de protección, restitución y formalización para que los colombianos recuperen su tierra, con recurso humano calificado y tecnología de punta.

3.2.3 Valores. Son las creencias acerca de las conductas consideradas correctas y valiosas por la empresa. Son los que tienen mayor permanencia en consideración de la misión y la visión. No se trata de una declaración circunstancial o conveniencia, sino de creencias básicas esenciales.

Los valores que se proponen para facilitar el logro del Plan estratégico por parte de los servidores de la institución son:

- Honestidad
- Transparencia
- Compromiso
- Oportunidad
- Confianza

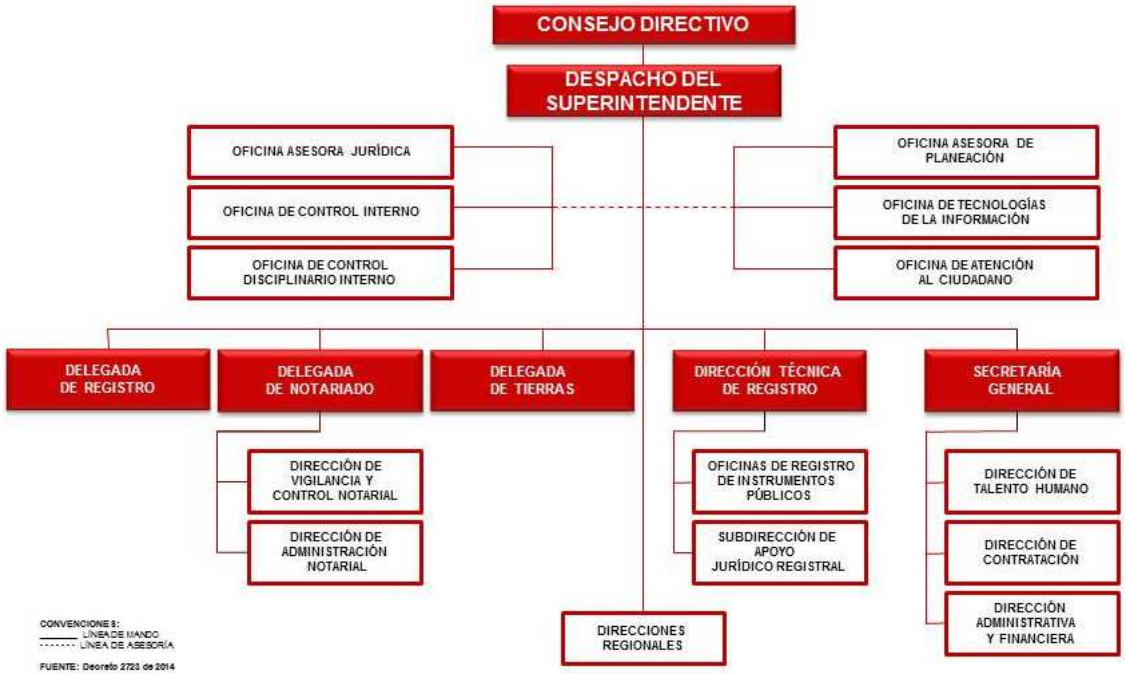
3.2.4 Dirección y administración. La Dirección y Administración de la Superintendencia de Notariado y Registro estará a cargo de un Consejo Directivo y del Superintendente de Notariado y Registro, quien para todos los efectos será su representante legal.

3.2.5 Estructura Superintendencia de Notariado y Registro. La estructura de la Superintendencia de Notariado y Registro es la siguiente:

1. Consejo Directivo de la Superintendencia.
2. Despacho del Superintendente.
2.1 Oficina Asesora Jurídica.
2.2 Oficina Asesora de Planeación.
2.3 Oficina de Control Interno.
2.4 Oficina de Tecnologías de la Información.
2.5 Oficina de Control Disciplinario Interno.
2.6 Oficina de Atención al Ciudadano.
2.7 Dirección Técnica de Registro.
2.7.1 Subdirección de Apoyo Jurídico Registral.
2.7.2 Oficinas de Registro de Instrumentos Públicos.
3. Superintendencia Delegada para el Registro.
4. Superintendencia Delegada para el Notariado.
4.1 Dirección de Administración Notarial.
4.2 Dirección de Vigilancia y Control Notarial.
5. Superintendencia Delegada para la Protección, Restitución y Formalización de Tierras.
6. Secretaría General.
6.1 Dirección de Talento Humano.
6.2 Dirección de Contratación.
6.3 Dirección Administrativa y Financiera.

7. Direcciones Regionales.
8. Órganos de Asesoría y Coordinación.
8.1 Comité de Coordinación del Sistema de Control Interno.

Figura 2. Organigrama



Fuente Superintendencia de Notariado y Registro (www.supernotariado.gov.co)

3.2.6 Oficina de Tecnologías de la Información

Conformación Oficina de Tecnologías de la Información

La Oficina de Tecnologías de la Información está compuesta por:

1. Grupo Centro de Computo

Quien tiene asignadas las siguientes funciones:

- Administración de la plataforma de hardware: servidores, librerías, etc.
- Administración de los dispositivos de comunicación: Firewalls, Switches, Puntos de Acceso Inalámbricos, Routers.
- Administración de las bases de datos.
- Velar por la funcionalidad de los aplicativos.

- Velar por la funcionalidad de los canales de comunicación e Internet, mediante supervisión a proveedor de comunicaciones.
- Velar por los temas de seguridad en relación a la red de datos.
- Supervisión de contratos.

2. Grupo Asistencia Técnica

Quien tiene asignada las siguientes funciones:

- Administración de la infraestructura eléctrica de la entidad.
- Elaborar y supervisar plan de mantenimiento de equipos (servidores, computadores, UPS, impresoras, etc.).
- Brindar soporte técnico sobre funcionalidad de equipos de cómputo directamente y a través de Mesa de Ayuda.
- Brindar soporte técnico sobre algunas aplicaciones.
- Suministro de equipos de cómputo y repuestos en general.
- Supervisión de contratos.

3. Grupo Desarrollo Informático

Quien tiene asignadas las siguientes funciones:

- Coordinar y supervisar el desarrollo de aplicaciones por parte de terceros.
- Brindar soporte técnico sobre aplicaciones directamente y a través de Mesa de Ayuda.
- Supervisión de contratos.

Cada uno de los grupos anteriormente mencionados están conformados por personal de planta y por contratistas. Con nivel de educación profesional y técnica.

Frecuentemente se están implementando proyectos para lo cual se contratan empresas privadas para su diseño y ejecución en la cual se involucra a veces tardíamente a personal propio de la entidad con el objeto de que la entidad se apersone de las tareas de administración.

3.3 MARCO LEGAL

Ley 1273

En Colombia se estableció un marco regulatorio para la protección de la información a través de la promulgación de la Ley 1273 del año 2009 “de la protección de la información y de los datos”.

En la que se establecen los lineamientos sobre la protección de la información y los datos, así como se estipulan las causales de penalización y las penas pertinentes las cuales están consignadas en el código penal colombiano.

La Ley está compuesta por múltiples artículos discriminados así:

Capítulo 1 (De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos)

Artículo 269A: Acceso abusivo a un sistema informático

El que sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Articulo 269B: Obstaculización ilegitima de sistema informático o red de telecomunicación

El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Articulo 269C: Interceptación de datos informáticos

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Articulo 269D: Daño informático

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Articulo 269E: Uso de software malicioso

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Articulo 269F: Violación de datos personales

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Articulo 269G: Suplantación de sitios web para capturar datos

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravara de una tercera parte a la mitad, si para consumarlo el agente ha reclutado victimas en la cadena del delito.

Articulo 269H: Circunstancias de agravación punitiva

Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentaran de la mitad a las tres cuartas partes si la conducta se cometiere:

1). Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2). Por servidor público en ejercicio de sus funciones.
3). Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4). Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5). Obteniendo provecho para sí o para un tercero.
6). Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7). Utilizando como instrumento a un tercero de buena fe.
8). Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Capítulo 2 (De los atentados informáticos y otras infracciones)

Articulo 269I: Hurto por medios informáticos y semejantes

El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Articulo 269J: Transferencia no consentida de activos

El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementara en la mitad.

3.4 MARCO METODOLOGICO

3.4.1 Tipo de investigación

Investigación descriptiva

La investigación que se planea llevar a cabo dadas sus características particulares corresponde a una investigación de tipo cuantitativa, específicamente una investigación descriptiva. Ya que se llevara a cabo un análisis inicial de la situación actual de la seguridad en el departamento de Informática de la Superintendencia de Notariado y Registro. Con lo que se pretende en primera instancia hacer un reconocimiento del departamento de Informática que nos permita conocer cómo opera, cuáles son sus procesos y procedimientos, con que activos cuenta, los riesgos a los que están expuestos sus activos.

Diseño de investigación

La estrategia que se aplicara para el desarrollo de la investigación es la investigación de campo. En donde se realizara la recolección de datos referentes al departamento de Informática de la Superintendencia de Notariado y Registro, utilizando para ello distintos mecanismos de recolección de información como por ejemplo entrevistas, observación directa, consulta y análisis de documentación pertinente.

3.4.2 Población. Básicamente el desarrollo de la investigación y ejecución del proyecto tendrá incidencia directa sobre el departamento de Informática de la Superintendencia de Notariado y Registro, quien actualmente está conformado por alrededor de 47 personas entre contratistas y personal de planta, quienes a su vez están asignados y distribuidos entre tres grupos definidos así: Asistencia Técnica, Desarrollo Informático y Centro de Computo. Todos estos grupos están subordinados a las orientaciones y supervisión de la jefatura del departamento de Informática.

4. FASES

4.1 FASE I – LEVANTAMIENTO INFORMACION

4.1.1 Descripción Superintendencia de Notariado y Registro (SNR)

4.1.1.1 Objetivos. La Superintendencia de Notariado y Registro tendrá como objetivo la orientación, inspección, vigilancia y control de los servicios públicos que prestan los Notarios y los Registradores de Instrumentos Públicos, la organización, administración, sostenimiento, vigilancia y control de las Oficinas de Registro de Instrumentos Públicos, con el fin de garantizar la guarda de la fe pública, la seguridad jurídica y administración del servicio público registral inmobiliario, para que estos servicios se desarrollen conforme a la ley y bajo los principios de eficiencia, eficacia y efectividad.

4.1.1.2 Dirección y administración. La Dirección y Administración de la Superintendencia de Notariado y Registro estará a cargo de un Consejo Directivo y del Superintendente de Notariado y Registro, quien para todos los efectos será su representante legal.

4.1.1.3 Integración del consejo directivo. El Consejo Directivo de la Superintendencia de Notariado y Registro estará integrado por:

1). El Ministro de Justicia y del Derecho o su delegado, quien lo presidirá.
2). El Ministro de Vivienda, Ciudad y Territorio o su delegado.
3). El Ministro de Agricultura o su delegado.
4). El Director del Instituto Geográfico Agustín Codazzi o su delegado.
5). Dos representantes del Presidente de la República, quienes no podrán ser Notarios ni Registradores en el ejercicio de sus cargos, ni haberlos desempeñado en el periodo inmediatamente anterior.

El Superintendente de Notariado y Registro asistirá con voz a las sesiones del Consejo.

4.1.1.4 Funciones de la Superintendencia de Notariado y Registro. Son funciones de la Superintendencia de Notariado y Registro, las siguientes:

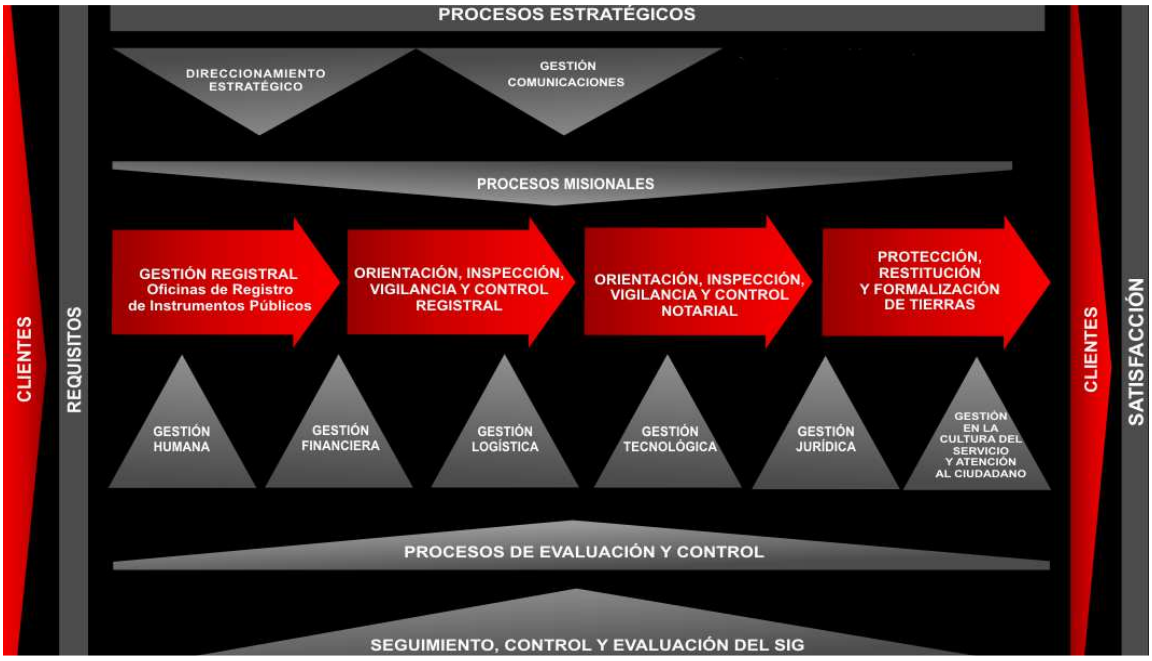
1). Proponer al Gobierno políticas, planes y programas sobre los servicios públicos de notariado y registro de instrumentos públicos.

2). Ejercer la inspección, vigilancia y control sobre el servicio público notarial en los términos establecidos en las normas vigentes.
3). Impartir las directrices e instrucciones para la eficiente prestación del servicio público de notariado mediante la expedición de conceptos, circulares y demás actos administrativos que se requieran con el fin de orientar el ejercicio de la actividad notarial.
4). Implementar sistemas administrativos y operativos para lograr la eficiente prestación de los servicios de notariado procurando su racionalización y modernización.
5). Realizar visitas generales, especiales, de seguimiento, por procedimientos virtuales o por cualquier otra modalidad a la actividad desarrollada por los Notarios y las Notarías.
6). Investigar y sancionar las faltas disciplinarias de los Notarios, en el desarrollo de sus funciones, sin perjuicio del poder preferente que podrá ejercer la Procuraduría General de la Nación.
7). Proponer al Gobierno Nacional la creación, supresión, fusión y recategorización de Notarías y sus círculos respectivos, de conformidad con las disposiciones legales vigentes.
8). Realizar directamente o por medio de entidades especializadas, los programas de capacitación formal y no formal que requieran los Notarios y empleados de Notarías.
9). Proponer al Gobierno Nacional la fijación de nuevas tarifas por concepto de derechos por la prestación del servicio público de notariado y modificación de las mismas.
10). Actualizar anualmente de acuerdo con el IPC las tarifas notariales.
11). Apoyar la realización de los concursos para proveer las vacantes en el cargo del notario, de conformidad con la delegación del Consejo Superior de Carrera Notarial.
12). Prestar el servicio público registral a través de las Oficinas de Registro de Instrumentos Públicos.
13). Llevar los registros de predios abandonados y de predios para reparación a víctimas de conformidad con la normativa vigente.
14). Ejercer la inspección, vigilancia y control de las Oficinas de Registro de Instrumentos Públicos, en los términos establecidos en las normas vigentes.
15). Realizar visitas generales, especiales, de seguimiento, por procedimientos virtuales, o por cualquier otra modalidad, a las Oficinas de Registro de Instrumentos Públicos.
16). Instruir a los Registradores de Instrumentos Públicos, sobre la aplicación de las normas que regulan su actividad.
17). Ordenar la suspensión inmediata de aquellas actuaciones irregulares de los Registradores de Instrumentos Públicos y disponer que se adopten las medidas correctivas del caso.
18). Investigar y sancionar las faltas disciplinarias de los Registradores de Instrumentos Públicos, en el desarrollo de sus funciones, sin perjuicio del poder preferente que podrá ejercer la Procuraduría General de la Nación.

19). Fijar los estándares de calidad requeridos para la prestación de los servicios públicos notarial y registral.
20). Implementar sistemas administrativos y operativos para lograr la eficiente prestación del servicio público de registro de instrumentos públicos procurando su racionalización y modernización.
21). Proponer al Gobierno Nacional la creación, supresión, fusión y modificación de Oficinas de Registro de Instrumentos Públicos y sus círculos respectivos, de conformidad con las disposiciones legales vigentes.
22). Fijar y actualizar las tarifas por concepto de derechos por la prestación de los servicios de registro de instrumentos públicos.
23). Proporcionar a los Órganos de Control y a la Fiscalía General de la Nación la información que solicite sobre los bienes inmuebles registrados en cumplimiento de sus funciones.
24). Apoyar, en los términos señalados en la ley y bajo las orientaciones del Consejo Superior de Carrera Registral, los concursos para proveer las vacantes en los empleos de Registradores de Instrumentos Públicos.
25). Adelantar y promover estudios, investigaciones y compilaciones en materia notarial y registral y divulgar sus resultados.
26). Las demás que señale la ley.

4.1.1.5 Procesos Generales de la Superintendencia de Notariado y Registro (SNR)

Figura 3. Procesos SNR



Fuente Superintendencia de Notariado y Registro (www.supernotariado.gov.co)

Procesos estratégicos

1). Gestión Direccionamiento Estratégico

Objetivo: Formular y emitir las directrices y lineamientos a través de los instrumentos de planeación que orienten la gestión de la SNR y a los actores, hacia el logro de la misión institucional.

Alcance:

- Inicia: Con el análisis de las directrices nacionales, necesidades del servicio en materia de Notariado y Registro derivadas de las exigencias de los ciudadanos y desarrollo económico del país.
- ¿Qué Hace?: Analizar información de los procesos y del contexto de la Superintendencia, toma decisiones y emite lineamientos.
- Termina: Seguimiento del cumplimiento de las directrices y los resultados de la gestión institucional.

Responsable: Superintendente.

2). Gestión Comunicaciones

Objetivo: Divulgar en forma oportuna, ágil y veraz, las políticas, planes y programas de la entidad con el propósito de que los clientes internos y externos accedan a la información institucional oportunamente.

Alcance:

- Inicia: La información que se genera al interior de la entidad, ciudadanía y entes externos relacionados con la misión institucional.
- ¿Qué Hace?: Recepcionar la información, clasificarla, determinar el medio para divulgarla, procesar el material.
- Termina: Publicación y seguimiento.

Responsable: Coordinador Grupo Divulgación.

Procesos misionales

1). Gestión de la Cultura del Servicio y Atención al Ciudadano

Objetivo: Resolver las peticiones, quejas, reclamos, sugerencias y consultas, de los ciudadanos, en relación con la prestación de los servicios públicos de notariado y registro.

Alcance:

- Inicia: Se reciben de los usuarios las PQRS y consultas (peticiones, quejas, reclamos, solicitudes, consultas, a través de: Pagina Web de atención.
- ¿Qué Hace?: Gestión de las PQRS y consultas de los usuarios internos y externos, realizando el debido seguimiento y registro de cada una de ellas.
- Termina: Con el proceso de registro y/o estado de finalización de las PQRS y CONSULTAS registrales y notariales a través del sistema SAC, del seguimiento a las PQRS y CONSULTAS que llevan por el cuadro EXCEL en el grupo, debidamente clasificadas y que permiten mejorar el índice de satisfacción al ciudadano, dándole resultados satisfactorios a sus requerimientos y tramites.

Responsable: Coordinador Grupo de Cultura del Servicio y Atención al Ciudadano.

2). Gestión Técnica Registral

Objetivo: Servir de modo en la tradición del derecho real de dominio, dar seguridad jurídica a la actividad inmobiliaria, certificar y publicar los actos y negocios jurídicos objeto de registro en Colombia, sujetos a dirección, orientación, inspección, vigilancia y control.

Alcance:

- Inicia: Formulación de planes, programas y proyectos para fortalecer la gestión registral.
- ¿Qué Hace?: Ejecutar y vigilar la gestión del servicio registral.
- Termina: Seguridad jurídica de la actividad inmobiliaria en Colombia.

Responsable: Superintendente Delegado para el Registro.

3). Orientación, Inspección, Vigilancia y Control de la Gestión Registral

Objetivo: Realizar las acciones relacionadas con la orientación, inspección, vigilancia y control de la gestión registral, dentro de una vigencia fiscal.

Alcance:

- Inicia: Con la estimación y proyección de costos para la ejecución de visitas de apoyo, de seguimiento e intervenciones. expedición de documentos para la orientación de la gestión registral. estudio recursos de apelación, queja o revocatoria directa. solicitudes de cambios de horario y/o suspensión de términos, nombramiento de Registradores Ad-Hoc, autorización de firma. Seguimiento a las solicitudes realizadas por las Oficinas de Registro, apoyo

funcional en la implementación del sistema de información registral, implementación de la Ventanilla Única de Registro en las Notarias y la interrelación Registro-Catastro.

- ¿Qué Hace?: Orientar, inspeccionar, vigilar y controlar la prestación del servicio registral en las Oficinas de Registro de Instrumentos Públicos. generar documentos que orienten la gestión registral, proyectar el acto administrativo que resuelve el recurso. Acompañamiento a las Oficinas de Registro en la implementación del sistema de información registral y seguimiento de las solicitudes enviadas a nivel central. ejecutar los proyectos.
- Termina: Informes de visitas y seguimiento de las acciones de acuerdo a los lineamientos formulados por la Delegada y Dirección de Registro. formalización de los documentos que orientan el servicio registral. Decisión a los recursos de apelación, quejas y revocatoria directa, resoluciones de cambios de horario y/o suspensión de términos, nombramiento de Registradores Ad-Hoc, autorización de firmas, ejecución del servicio VUR en las notarias seleccionadas, actualización de la información interrelacionada con Catastro, informes de auto evaluación y control de la gestión de seguimiento a planes y proyectos.

Responsable: Superintendente Delegado Para el Registro, Director de Registro y Director de Desarrollo Registral.

4). Orientación, Inspección, Vigilancia y Control de la Gestión Notarial

Objetivo: Gestionar la administración de la actividad notarial, la inspección, vigilancia y control del servicio público notarial que se desarrolla en el territorio nacional.

Alcance:

- Inicia: Fija directrices para la administración de la actividad notarial, la inspección, vigilancia y control del servicio público notarial.
- ¿Qué Hace?: Ejecuta programas y proyectos para la administración de la actividad notarial, la inspección, vigilancia y control del servicio público notarial.
- Termina: Evaluación, seguimiento y rediseño de la gestión de la administración de la actividad notarial, la inspección, vigilancia y control del servicio público notarial.

Responsable: Superintendente Delegado para el Notariado.

5). Gestión para la Protección, Restitución y Formalización de Tierras

Objetivo: Atender las disposiciones que la Ley de Victimas y Restitución de Tierras (Ley 1448 de 2011) y otras políticas públicas estatales, en materia de Protección, restitución y formalización de predios, impulsar el saneamiento jurídico de la propiedad inmobiliaria rural y urbana, en eventos tales como la ocupación, la posesión y la denominada falsa tradición, proteger los derechos sobre la propiedad a través de las inscripciones en los folios de matricula inmobiliaria de enajenar predios (RUPTA – Registro Único de Predios y Territorios Abandonados a causa de la violencia) sobre zonas declaradas en desplazamiento forzado y proveer información jurídica para las etapas administrativas y judiciales del proceso de restitución de tierras.

Alcance:

- Inicia: Recepción de solicitudes de estudios registrales de títulos requeridos por la Unidad de Restitución de Tierras del ministerio de agricultura, con las directrices del despacho de la Superintendencia de Notariado y Registro, con las iniciativas del Estado en materia de la política de tierras, con las iniciativas propias de la Delegada para la Protección, Restitución, Formalización de Tierras en el marco de sus funciones, con la ejecución del plan de formalización y el plan de visitas de inspección, vigilancia y control a las Oficinas de Registro de Instrumentos Públicos, con la recepción de los formulación de inscripción medidas de protección de predios por parte de las Oficinas de Instrumentos Públicos a nivel nacional, con el requerimiento de los municipios o la ciudadanía en cabeza de sus alcaldías para realizar jornadas de orientación y asesoría jurídica para la formalización de la propiedad de predios rurales y urbanos, con la suscripción de convenios interadministrativos con los municipios para la formalización de la propiedad irregular de predios.
- ¿Qué Hace?: Estudios de títulos jurídicos de los predios registrados reclamados por las víctimas de violencia, diagnósticos registrales para los procesos de restitución, formalización y protección judicial y administrativa como para el análisis de otros eventos de interés nacional o internacional sobre la propiedad rural en Colombia, ofrecer acceso oportuno al registro de la propiedad rural, formación en materia registral, notarial, agraria y derechos de humanos; coadministrar los sistemas de protección patrimonial, apoyo a las Oficinas de Registro de Instrumentos Públicos para la correcta prestación del servicio público registral, estudios traditicios de los folios protegidos, apoyo a la implementación de actuaciones administrativas, judiciales, fiscales y disciplinarias, realiza jornadas de orientación y asesoría jurídica a través de las unidades de registro móviles para impulsar la formalización de la propiedad en los casos de posesión, ocupación o propietario pero no ha registrado el titulo, determinar la cantidad de órdenes emanadas por los jueces y/o magistrados especializados en tierras, realizar visitas de inspección, vigilancia y control

a las oficinas de registro de instrumentos públicos en función de las actividades propias del macro procesó.

- Termina: Con la culminación de los estudios jurídicos de los folios de matricula inmobiliaria, con la presentación de los informes validados por el Superintendente Delegado para Tierras en el marco de la Ley de Tierras, con la ejecución de las jornadas de orientación jurídica para la formalización de la propiedad rural y urbana, con la culminación de los programas académicos impartidos, con el cambio de estado de las solicitudes de protección de las decisiones registrales de las ORIPs en el aplicativo RUPTA, con el envió de las instrucciones sobre modificaciones o actualizaciones en los procedimientos de registro de protección y los procesos de restitución a los notarios y registradores y con la recomendación de la conveniencia de inicio de actuaciones a los registradores sobre los hallazgos encontrados en los diagnósticos registrales, con la titulación de predios producto de las jornadas de orientación para la formalización de la propiedad y de los convenios firmados con los municipios para disminuir los índices de ocupación, posesión, y tenencia irregular de la tierra, con la presentación de un informe mensual con el estado del seguimiento de las sentencias por parte de la SNR a la Unidad Administrativa Especial de Gestión de Restitución de Tierras.

Responsable: Superintendente Delegado para la Protección, Restitución y Formalización de Tierras.

Procesos de Apoyo

1). Gestión Humana

Objetivo: Planear, desarrollar y evaluar el plan institucional de capacitación PIC para funcionarios y registradores, basados en las competencias laborales en el año 2011.

Alcance:

- Inicia: Diagnostico de necesidades de capacitación e identificación de problemas de los procesos para la elaboración del plan institucional de capacitación PIC para la SNR y diseño del plan de capacitación de notarios.
- ¿Qué Hace?: Planear, elaborar, ejecutar y hacer seguimiento al Plan Institucional de Capacitación (PIC) para funcionarios y registradores y Plan de Capacitación para Notarios.
- Termina: Evaluación y seguimiento del impacto de las actividades de capacitación.

Responsable: Jefe Oficina de Investigación y Capacitación.

2). Gestión Financiera

Objetivo: Proveer y controlar los recursos económicos a la SNR.

Alcance:

- Inicia: Elaboración del plan anual.
- ¿Qué Hace?: Dirigir, controlar y verificar la gestión de presupuesto, contabilidad y costos, tesorería, reconocimiento de pensiones y cartera de vivienda, recaudos y subsidios notariales.
- Termina: Con el cierre de la vigencia.

Responsable: Director financiero.

3). Gestión Administrativa (Este proceso no aparece definido al interior de la SNR)

4). Gestión Jurídica

Objetivo: Brindar la asesoría y apoyo jurídico a la Entidad, en lo relacionado con el consejo superior – de la carrera notarial y el servicio notarial, el servicio de registro de la propiedad inmobiliaria, la defensa judicial y el cobro coactivo y realizar la administración del concurso para el nombramiento de notarios en propiedad e ingreso a la carrera notarial.

Alcance:

- Inicia: Radicación de las solicitudes.
- ¿Qué Hace?: Estudiar, proyectar y sustentar las respuestas.
- Termina: Con la notificación de las respuestas y conceptos, al interesado o a las entidades competentes para continuar con el trámite, proferir el mandamiento ejecutivo de pago o archivo del proceso y con el fallo debidamente ejecutoriado, proyectos de decreto de nombramiento de notarios.

Responsable: Jefe de la Oficina Asesora Jurídica.

5). Gestión Tecnológica
6). Seguimiento, Control y Evaluación del SIG

Objetivo: Análisis, evaluación, seguimiento y mantenimiento del Sistema de Gestión de la Calidad (SGC), Sistema de Desarrollo Administrativo (SISTEDA) y Sistema de Control Interno (MECI) para proponer aspectos a mejorar que contribuyan a su mejoramiento y optimización.
Alcance:

- Inicia: Plan de auditorías de acuerdo a la Ley. Análisis del plan estratégico, planes anuales de gestión, de desarrollo administrativo y proyectos de inversión.
- ¿Qué Hace?: Planear y ejecutar la evaluación independiente y seguimiento del Sistema de Control Interno de la Entidad. Rendir informes a entes de control.
- Termina: Informes de evaluación y seguimiento con aspectos a mejorar para el mantenimiento continuo. Seguimiento a las recomendaciones de la OCI.

Responsable: Jefe de la Oficina de Control Interno de Gestión.

4.1.2 Descripción Departamento de Informática (Oficina de Tecnologías de la Información)

4.1.2.1 Funciones de la Oficina de Tecnologías de la Información

Las siguientes son las funciones de la Oficina de Tecnologías de la Información:

- Asesorar al Despacho del Superintendente en la definición de las políticas, planes, programas y procedimientos relacionados con el uso y aplicación de las tecnologías de la información, que contribuyan a incrementar la eficiencia y eficacia en las diferentes dependencias de la Superintendencia, así como a garantizar la calidad en la prestación de los servicios.
- Realizar el análisis, diseño, programación, documentación, implantación y mantenimiento de los sistemas de información requeridos por la Entidad.
- Adelantar acciones para que los sistemas de información de inspección, vigilancia y control de los servicios públicos del notariado y el registro de instrumentos públicos de la Superintendencia de Notariado y Registro, sean interoperables con los demás sistemas de información existentes y que se requieran para el cumplimiento de las funciones de la Entidad.
- Diseñar y proponer la política de uso y aplicación de las tecnologías de la información, estrategias y herramientas, para el mejoramiento continuo de los procesos relacionados con las tecnologías de la Información de la Superintendencia.
- Definir los protocolos tecnológicos, apoyar la capacitación y fomentar la cultura organizacional orientada a la utilización y adaptación de tecnologías de punta.
- Elaborar en coordinación con las diferentes dependencias de la Superintendencia, el plan de desarrollo tecnológico de la Entidad, ejecutarlo y realizar su seguimiento, control y evaluación, en coordinación con la Secretaría General.

- Promover e intervenir en todas las actividades y programas que tiendan a incorporar el uso de las tecnologías de la información en el desarrollo de los procesos relacionados con los objetivos estratégicos de la Superintendencia, como estrategia fundamental en la administración de indicadores de resultado, alertas de gestión del riesgo y calidad en la operación.
- Diseñar los mecanismos para aplicar, utilizar, adaptar, aprovechar y darle un buen uso a las tecnologías de la información.
- Evaluar la seguridad, calidad y flujo de la información de la Superintendencia a fin de permitir su acceso entre las diferentes Superintendencias Delegadas para el cumplimiento de los objetivos individuales e institucionales en materia de inspección, vigilancia y control.
- Administrar una plataforma unificada de los sistemas de información que permita articular las diferentes fuentes de información en una sola herramienta de gestión y efectuar análisis de información con procesamiento en tiempo real.
- Definir las acciones que garanticen la aplicación de los estándares, buenas prácticas y principios para el uso y manejo de la información estatal, alineado a las políticas y lineamientos impartidos por el Sector de las Tecnologías de la Información y las Comunicaciones.
- Elaborar en coordinación con las demás dependencias de la Superintendencia, el mapa de información, que permita contar de manera actualizada y completa con los procesos de información de la Superintendencia.
- Desarrollar estrategias para lograr un flujo eficiente de la información, como parte de la rendición de cuentas a la sociedad.
- Diseñar e implementar estrategias, instrumentos y herramientas con aplicación de tecnologías de punta adecuadas, que permitan brindar de manera constante y adecuada un buen servicio al ciudadano.
- Identificar las dificultades en la implementación de estándares y buenas prácticas en el cumplimiento de los principios para la información estatal y proponer las acciones de mejora necesarias.
- Definir las necesidades para la obtención, generación y sostenimiento de sistemas de información confiables que requiera la Superintendencia, coordinando su adquisición con la Secretaría General.
- Brindar asesoría técnica para el diseño, puesta en marcha y operación de los diferentes sistemas de información.
- Atender, proponer e implementar las políticas y acciones relativas a la seguridad de la información y de la plataforma tecnológica de la Superintendencia.
- Coordinar con las instancias pertinentes la incorporación de contenidos en la página Web y el óptimo aprovechamiento de las redes sociales, para la defensa de los derechos de los usuarios de los servicios prestados por la Superintendencia.

- Verificar que en los procesos tecnológicos de la Entidad se tengan en cuenta los estándares y lineamientos dictados por el Ministerio de Tecnologías de la Información y las Comunicaciones, que permitan la aplicación de las políticas que en materia de información expida el Departamento Nacional de Planeación (DNP) y el Departamento Nacional de Estadística (DANE).
- Definir, diseñar y asegurar el óptimo funcionamiento y mantenimiento de los sistemas de información de la infraestructura y plataforma tecnológica y de comunicaciones de la Superintendencia.
- Las demás que le sean asignadas y que correspondan a la naturaleza de la dependencia.

4.1.2.2 Procesos Internos del Departamento de Informática

Macroproceso - Gestión Tecnológica

Objetivo: Asegurar la disponibilidad del recurso tecnológico, garantizando la integridad, oportunidad, seguridad de la información, soportada en una plataforma tecnológica para el logro de la guarda de la fe pública como objetivo institucional.

Alcance:

- Inicia: Con la identificación de las necesidades y/o requerimientos de la Entidad, en materia de tecnología informática.
- ¿Qué Hace?: Desarrollar, implementar, mantener y administrar una plataforma tecnológica existente y asesorar la adquisición e implementación de nuevas tecnologías que brinden soluciones eficaces a las necesidades de la Entidad.
- Termina: Con la disponibilidad de la información y del recurso tecnológico a los usuarios internos y externos de la SNR.

Responsable: Jefe de Oficina de Informática.

Análisis Detallado Proceso de Gestión Tecnológica – Ciclo Básico

Cuadro 1. Ciclo básico de la gestión del proceso Gestión Tecnológica

Proveedores	**Entradas**	**P** **H** **V** **A**	**Actividades**	**Salidas**	**Clientes**
Gobierno nacional, usuarios, ciudadanos y procesos SNR.	Plan nacional de desarrollo, plan sectorial de desarrollo administrativo, programa nacional de servicio al ciudadano, plan estratégico institucional, plan anual de gestión (vigencia anterior).	P	Identificar las necesidades de actualización tecnológica propuestos para generar nuevos proyectos, que sean registrados en la ficha BPIN.	Plan maestro informático, plan anual de gestión, proyecto de inversión.	* Proceso de direccionamiento estratégico * Proceso de gestión tecnológica. * Proceso de apoyo * Departamento nacional de planeación
Proceso de gestión tecnológica.	Plan maestro informático, plan anual de gestión, proyectos de inversión.	H	Adaptación de la plataforma tecnológica.	Infraestructura tecnológica disponible.	Procesos de la SNR.
Procesos de apoyo.	Recursos: Financieros, humanos, tecnológicos.		Administrar la plataforma tecnológica.	Disponibilidad de la información.	Procesos de la SNR, usuarios.
Procesos de la SNR.	Infraestructura tecnológica disponible, necesidades.				
Proceso gestión tecnológica.	Ejecución: Plan anual de gestión, plan maestro informático y proyectos de inversión. Resultados de indicadores, seguimiento mapa de riesgos, plan de mejoramiento.	V	Evaluar y hacer seguimiento a la gestión del proceso.	Informes de seguimiento.	Procesos: Gestión tecnológica, seguimiento, control y evaluación del SIG, direccionamiento estratégico.
Procesos: Gestión tecnológica,	Lineamientos de la alta dirección, Informes de	A	Establecimiento de acciones correctivas,	Planes de mejoramiento.	Procesos: Gestión tecnológica,

Proveedores	Entradas	P	H	Actividades	Salidas	Clientes
		V	A			
seguimiento, control y evaluación del SGSI, direccionamiento estratégico.	seguimiento.			preventivas y de mejoras.		seguimiento, control y evaluación del SIG, direccionamiento estratégico.

Fuente Superintendencia de Notariado y Registro

Subprocesos del proceso de Gestión Tecnológica

El Macroproceso de Gestión tecnológica está compuesto a su vez por los siguientes subprocesos: Gestión Incorporación de Tecnología y Gestión de Recursos de Tecnología.

1). Proceso Gestión Incorporación de Tecnología

Caracterización del proceso

Objetivo: Estructurar e integrar proyectos de tecnología para satisfacer las necesidades de información a los clientes internos y externos de la Entidad, de manera oportuna, eficiente y segura.

Alcance:

- Inicia: Con la identificación de las necesidades y/o requerimientos de la Entidad, en materia de tecnología informática.
- ¿Qué Hace?: Desarrollar, implementar, mantener y administrar una plataforma tecnológica existente y asesorar la adquisición e implementación de nuevas tecnologías que brinden soluciones eficaces a las necesidades de la Entidad.
- Termina: Con la disponibilidad de la información y del recurso tecnológico a los usuarios internos y externos de la SNR.

Responsable: Jefe Oficina de Informática.

Análisis Detallado Proceso Gestión Incorporación de Tecnológica – Ciclo Básico

Cuadro 2. Ciclo básico de la gestión del proceso gestión incorporación de tecnología

Proveedores	**Entradas**	**P** / **V**	**H** / **A**	**Actividades**	**Salidas**	**Clientes**
Gobierno nacional, usuarios, ciudadanos y procesos SNR.	Plan nacional de desarrollo, plan sectorial de desarrollo administrativo, programa nacional de servicio al ciudadano, plan estratégico institucional, plan anual de gestión (vigencia anterior).	P		Identificar las necesidades de actualización tecnológica propuestos para generar nuevos proyectos, que sean registrados en la ficha BPIN.	Plan maestro informático, plan anual de gestión, proyecto de inversión.	* Proceso de direccionamiento estratégico. * Proceso de gestión tecnológica. *Procesos de apoyo. *Departamento nacional de planeación.
Proceso de gestión tecnológica, direccionamiento estratégico, plan anual de gestión.	Plan de compras, acuerdos de gestión, proyectos de inversión.			Incorporar tecnología a oficinas manuales.	Actualización de tecnologías.	Informe seguimiento proyecto de inversión, ciudadanía y usuarios.
Procesos de apoyo.	Recursos financieros, humanos, tecnológicos.				Disponibilidad de la información y de los aplicativos misionales.	
Proceso de gestión tecnológica, direccionamiento estratégico, plan anual de gestión.	Plan de compras, acuerdos de gestión, proyectos de inversión.			Ampliar cobertura de los servicios misionales a nivel nacional.	Promover la utilización de nuevas tecnologías.	Procesos de la SNR, ciudadanía y usuarios.
Proceso de apoyo.	Recursos: financieros, humanos, tecnológicos.				Disponibilidad de la información.	
Proceso Gestión Tecnológica.	Ejecución: Plan anual de gestión, plan maestro informático y proyectos de inversión, Resultados de	V		Evaluar y hacer seguimiento a la gestión del proceso.	Informes de seguimiento.	Procesos: Gestión tecnológica, seguimiento, control y evaluación del SIG; direccionamiento

Proveedores	Entradas	P	H	Actividades	Salidas	Clientes
		V	A			
	indicadores, seguimiento mapa de riesgos, plan de mejoramiento.					estratégico.
Procesos: Gestión tecnológica, seguimiento, control y evaluación del SIG; direccionamiento estratégico.	Lineamientos de la alta dirección, informes de seguimiento.	A		Establecimiento de acciones correctivas, preventivas y de mejora.	Planes de mejoramiento.	Procesos: Gestión tecnológica, seguimiento, control y evaluación del SIG; direccionamiento estratégico.

Fuente: Superintendencia de Notariado y Registro

Riesgos y controles del proceso

Cuadro 3. Riesgos y controles implícitos del proceso

Riesgos	Controles
Atraso o no ejecución de proyectos de tecnología programados.	1. Cumplir con los requisitos de ley (Pólizas de cumplimiento). 2. Todo contrato debe contener interventoria y/o supervisor. 3. hacer el seguimiento adecuado a los proyectos programados.
Ejecución de proyectos de tecnología que no cumplan a cabalidad con su objeto por falta de planeación en lo referente a la integración de las diferentes áreas de la Entidad y desconocimiento del factor tecnológico con que dispone la Oficina de Informática.	Elaborar acto administrativo donde indique que los proyectos de tecnología deben ser avalados por la Oficina de Informática.
Incumplimiento por parte de la Oficina de Informática en la implementación de actos administrativos emitidos por la Oficina Jurídica o Superintendencia Delegada para el Registro, dado que no se informa con antelación a la Oficina de Informática para que se realicen los ajustes necesarios en los aplicativos misionales con el fin de dar cumplimiento a las fechas de aplicabilidad de las mismas.	* Oficiar por parte de las dependencias que generan actos administrativos, con anticipación de cambios de normatividad de tal forma que esta oficina pueda planear la implementación. * Verificar y actualizar la información básica en los aplicativos misionales.
Cambio de las políticas de estado.	Adecuar la plataforma tecnológica de la Entidad a las competencias asignadas a la Entidad por orden gubernamental.

Fuente Superintendencia de Notariado y Registro

Procedimientos incorporados en el proceso

Los procedimientos incorporados en el proceso de Incorporación de Tecnología son los siguientes:

Procedimiento – Implantación Proyectos de Tecnologías de Información

- Objetivo y campo de aplicación: Estructurar, sistematizar y establecer los mecanismos necesarios que faciliten la ejecución y apoyo de forma integral, de los proyectos de tecnología informática en la SNR, ORIPs y Notarias para cumplir con la satisfactoria prestación de los servicios de la Entidad a la ciudadanía, cubriendo las necesidades de información de los clientes internos y externos, de manera oportuna, eficiente, segura, facilitando los diferentes procesos y convenios institucionales.

  Los clientes son la Superintendencia de Notariado y Registro, las Oficinas de Registro y las Notarias con el sistema SIN, Entidades, puntos externos y la ciudadanía.
- Alcance:
  Inicia: Delegación de Supervisores
  ¿Qué Hace?: Firma de acta de inicio, estudio y diagnostico de la situación actual, definición de cronograma de actividades, acompañamiento y seguimiento a la ejecución del proyecto.
  Termina: Con la implantación y socialización de los proyectos.
- Responsables:
  Responsable estratégico: Jefe Oficina de Informática.
  Responsable operativo: Coordinadores de Grupo (Desarrollo Informático, Asistencia Técnica, Centro de Computo), Profesional Especializado, Profesional Universitario, Analista de Sistemas y Técnicos Operativos y Administrativos.
- PHVA
  Planeación: Definir cronograma de actividades a desarrollar.
  Hacer: Firma de acta de inicio, estudio y diagnostico de la situación actual, definición de cronograma de actividades, acompañamiento y seguimiento a la ejecución del proyecto.
  Verificación: Revisión, pruebas y puesta en producción de los proyectos.
  Actuar: Mejoras y ajustes a los proyectos.

Procedimiento – Planeación, Desarrollo e Implementación de Proyectos de Tecnología

- Objetivo y campo de aplicación: Solucionar las necesidades técnicas a nivel de desarrollo y actualización de software para cumplir con los requerimientos y nuevas competencias de la SNR, ORIPs y Notarias.

Participar en el mejoramiento continuo de los procesos, ofreciendo nuevos servicios tanto funcionales como tecnológicos en pro de la excelencia en la prestación del servicio y satisfacción al ciudadano.

Los clientes son: La Superintendencia de Notariado y Registro, las Oficinas de Registro de Instrumentos Públicos, Notarias, Entidades y Puntos Externos.

- Alcance:
  Inicia: Identificación, análisis y evaluación de la necesidad o requerimiento.
  ¿Qué Hace?: Desarrollo, revisión y aceptación técnica; acompañamiento a la implementación de la solución; mejoramiento continuo de sistemas de información.
  Termina: Con la implantación de la solución.
- Responsables:
  Responsable estratégico: Jefe Oficina de Informática.
  Responsable operativo: Coordinador de Grupo (Desarrollo Informático, Asistencia Técnica, Centro de Computo), Profesional Especializado, Profesional Universitario, Analista de Sistemas y Técnico.
- PHVA
  Planeación: Definir estrategias de desarrollo y/o mejorar los sistemas de información basados en estudios previos de factibilidad y conveniencia.
  Hacer: Desarrollo, revisión y aceptación técnica; acompañamiento a la implementación de la solución; mejoramiento continuo de sistemas de información y elaborar cronogramas de actividades.
  Verificación: Validar que la solución se ajuste a la necesidad y normatividad.
  Actuar: Mejoramiento continúo del proceso.

Procedimiento – Supervisión e Interventoria de Contratos

- Objetivo y campo de aplicación: Vigilar, controlar y evaluar permanentemente la gestión de ejecución del objeto y obligaciones contractuales entre la SNR y la entidad interventora así como el seguimiento y evaluación de la ejecución del contrato dentro del plazo estipulado.

  Los clientes del proceso son: Superintendencia de Notariado y Registro.
- Alcance:
  Inicia: Con la designación del interventor, seguido del nombramiento formal del supervisor por parte de la SNR y termina con la evaluación del servicio prestado.
  ¿Qué Hace?: Elaborar actas de inicio, avance o seguimiento y finalización, verificar el cumplimiento de las clausulas del contrato, supervisar continuamente lo ofrecido, asistir y programar reuniones y presentar informes.

Tener en cuenta los criterios de: Calidad, Cantidad y Oportunidad.
Verificar y aprobar cada fase de ejecución de un contrato o convenio.
Controla, exigir y verificar la ejecución y cumplimiento del objeto del contrato de acuerdo a los términos de referencia y propuesta del contratista; esto aplica para los contratos o convenios celebrados con un tercero por la SNR.
Termina: Con el informe final y acta de liquidación del contrato.

- Responsables:
  Responsable estratégico: Jefe Oficina de Informática.
  Responsable operativo: Profesional o Técnico vinculado directamente con la SNR.
- PHVA
  Planeación: Planear cada una de las actividades frente al cronograma de ejecución.
  Hacer: Elaborar acta de inicio, verificar el cumplimiento de las clausulas del contrato, hacer seguimiento de lo ofrecido, presentar informes y actas de seguimiento.
  Verificación: Verificar y evaluar el cumplimiento de cada una de las actividades del contrato ajustado al cronograma de ejecución.
  Actuar: Determinar e informar al Ordenador del Gasto si existen desfases o incumplimientos en la ejecución del contrato, quienes tomaran las medidas correctivas al proceso.

2). Gestión de Recursos de Tecnología

Caracterización del proceso

Objetivo: Garantizar la planeación, administración, control, ejecución y seguimiento para la correcta operación y disponibilidad de los recursos de tecnología con los que cuenta la Superintendencia de Notariado y Registro para la efectiva prestación del servicio.

Alcance:

- Inicia: Elaboración del plan de gestión y administración de los recursos de tecnología (Plan de administración de las bases de datos, de servidores, de redes y comunicación, de sistemas de información, de asistencia y soporte técnico, de seguridad informática y auditorias de sistemas).
- ¿Qué Hace?: Planear, administrar, controlar y hacer seguimiento a la base de datos, servidores, redes y comunicaciones, sistemas de información, seguridad informática, asistencia y soporte técnico, auditorias de sistemas, para garantizar la operación efectiva de los recursos de tecnología.
- Termina: Informes de evaluación con indicadores sobre base de datos, de las redes y comunicaciones, sistemas de información, asistencia y soporte técnico, seguridad informática y auditorias de sistemas.

Responsable: Jefe Oficina de Informática.

Análisis Detallado Proceso Gestión de Recursos de Tecnología – Ciclo Básico

Cuadro 4. Ciclo básico de la gestión del proceso gestión de recursos de tecnología

Proveedores	**Entradas**	**P** **V**	**H** **A**	**Actividades**	**Salidas**	**Clientes**
Gobierno nacional, usuarios, ciudadanos y procesos SNR.	Plan nacional de desarrollo, plan sectorial de desarrollo administrativo, programa nacional de servicio al ciudadano, plan estratégico institucional, plan anual de gestión (vigencia anterior).	P		Identificar las necesidades de actualización tecnológica propuestos para generar nuestros proyectos, que sean registrados en la ficha BPIN.	Plan maestro informático, plan anual de gestión, proyectos de inversión.	* Proceso de direccionamiento estratégico * Proceso de gestión tecnológica * Procesos de apoyo * Departamento nacional de planeación.
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Garantías de los equipos.	H		Mantener disponible la plataforma tecnológica.	Dispositivos funcionando, hardware, software, comunicaciones incluyendo redes.	Proceso de gestión tecnológica.
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Un servidor de aplicaciones web y un firewall. Solicitudes de creación, modificación y eliminación de usuarios.			Administrar servicios de red, correo e Internet.	Reporte de cuentas o perfiles de usuarios creados para acceso a la red.	Proceso de gestión tecnológica.
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Herramientas administrativas, creación de perfiles de usuarios, licenciamientos de software, hardware.			Administrar la base de datos de aplicaciones.	Permisos según el perfil de usuario que va a subir a la base de datos, la realización de copias de seguridad (Backup).	Proceso de gestión tecnológica
Proceso de gestión tecnológica,	Administrador de las herramientas			Mantener y administrar las herramientas	Implementar la herramienta de anti virus en	Proceso de gestión tecnológica.

Proveedores	Entradas	P	H	Actividades	Salidas	Clientes
		V	A			
proveedores de herramientas y servicios tecnológicos.	de las aplicaciones para mitigar el riesgo de virus.			de protección contra virus.	todos los equipos de la SNR.	
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Plan de mantenimiento preventivo de la plataforma tecnológica e informática.			Hacer el mantenimiento preventivo y correctivo de hardware y software.	Mantenimiento preventivo y correctivo de hardware y software a todos los equipos a nivel nacional.	Proceso de gestión tecnológica.
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Políticas de seguridad informática.			Realizar Backups a las aplicaciones y bases de datos obtenidas en la SNR.	Copias de seguridad de las aplicaciones y bases de datos.	Proceso de gestión tecnológica.
Proceso de gestión tecnológica, proveedores de herramientas y servicios tecnológicos.	Requerimientos de los usuarios.			Asistir técnicamente a todos los requerimientos tecnológicos que demanden los usuarios de las aplicaciones de la SNR.	Soporte técnico a los requerimientos de los usuarios.	Proceso gestión tecnológica, Oficinas de Registro, nivel central de la SNR.
Proceso de gestión tecnológica	Ejecución: Plan anual de gestión, plan maestro informático y proyectos de inversión, resultados de indicadores, seguimiento mapa de riesgos, plan de mejoramiento.	V		Evaluar y hacer seguimiento a la gestión del proceso.	Informes de seguimiento.	Procesos: Gestión tecnológica; seguimiento, control y evaluación del SIG; direccionamiento estratégico.
Procesos: Gestión tecnológica; seguimiento, control y evaluación del SIG; direccionamient	Lineamientos de la alta dirección, informes de gestión.	A		Establecimiento de acciones correctivas, preventivas y de mejora.	Planes de mejoramiento.	Procesos: Gestión tecnológica; seguimiento, control y evaluación del SIG; direccionamient

Proveedores	Entradas	P	H	Actividades	Salidas	Clientes
		V	A			
o estratégico.						o estratégico.

Fuente Superintendencia de Notariado y Registro

Riesgos y controles del proceso

Cuadro 5. Riesgos y controles implícitos del proceso

Riesgos	Controles
No disponibilidad de la Mesa de Ayuda por vencimiento de contrato o falta del contratista.	1. Hacer estudios de previos para la contratación de un Outsourcing. 2. Solicitar asignación de recursos suficientes contratación de un Outsourcing.
Perdida de información.	1. Realizar Backups de manera periódica. 2. Revisar Backups realizados.
Fallas en hardware y/o software.	1. Controlar los mantenimientos preventivos y correctivos con límites de tiempo y como soporte técnico para los usuarios. 2. Elaborar un plan de adquisición de repuestos. 3. Hacer seguimiento a las garantías para los contratos de suministro de tecnología.

Fuente: Superintendencia de Notariado y Registro

Procedimientos incorporados en el proceso

Los procedimientos incorporados en el proceso de Gestión de Recursos de Tecnología son los siguientes:

Procedimiento – Administración de Hardware

- Objetivo y campo de aplicación: Planear, administrar y controlar los elementos técnicos a nivel de hardware, para garantizar su disponibilidad a los funcionarios de la SNR, ORIPs, Entidades y Puntos de Servicio Externo.

  Los clientes del proceso son: Superintendencia de Notariado y Registro, las Oficinas de Registro y Entidades Externas (INCODER, IGAC, GATASTRO).
- Alcance:
  Inicia: Plan de mantenimiento de hardware actualizado.
  ¿Qué Hace?: Verificar la disponibilidad del hardware, identificar los equipos objeto del mantenimiento preventivo, en caso de falla inmediata se direcciona a Mesa de Servicio.
  Termina: Actualización del plan de mantenimiento y la hoja de vida del equipo respectivo.
- Responsables:

Responsable estratégico: Jefe Oficina de Informática.
Responsable operativo: Profesional universitario y Analista de Sistemas (Grupo de Asistencia Técnica y Grupo Centro de Cómputo).

- PHVA
  Planeación: Planear el cronograma para llevar a cabo el plan de mantenimiento de hardware.
  Hacer: Verificar la disponibilidad del hardware, identificar los equipos objeto del mantenimiento preventivo, en caso de falla inmediata se direcciona a Mesa de Ayuda y actualizar las hojas de vida de los equipos respectivos.
  Verificación: Seguimiento al cumplimiento de cronograma de mantenimiento de hardware.
  Actuar: Corregir y actualizar el plan de mantenimiento de hardware.

Procedimiento – Administración Base de Datos

- Objetivo y campo de aplicación: El procedimiento administración de la base de datos tiene como objetivo, gestionar, administrar y garantizar la disponibilidad de las bases de datos, para brindar información en forma oportuna, segura y efectiva al ciudadano y en general a los usuarios que lo requieran.

  El procedimiento se desarrolla en el grupo Asistencia Técnica en compañía del Centro de Computo de la Superintendencia, en los Centros de Computo de las Oficinas de Registro sistematizadas con folio magnético, en el Data Center donde está la base de datos centralizada, por los sistemas de índices y RUPTA de las Oficinas de Registro manuales.

  Los clientes externos del procedimiento son: Entidades del estado, Notarias, Sistema Financiero y los Ciudadanos que requieran información. Los clientes internos son los funcionarios de la SNR nivel central y las Oficinas de Registro de Instrumentos Públicos y Notarias.
- Alcance:
  Inicia: Inventariar las bases de datos de las Oficinas de Registro y nivel central de la SNR de acuerdo a la normatividad.
  ¿Qué Hace?: Gestionar, administrar y verificar que los datos se encuentren actualizados, para brindar información en forma oportuna, segura y efectiva al ciudadano. Asegurar la disponibilidad de la información contenida en la base de datos.
  Termina: Verificación de la disponibilidad de la base de datos actualizada.
- Responsables:
  Responsable estratégico: Jefe Oficina de Informática.
  Responsable operativo: Coordinador Asistencia Técnica, Coordinador Centro de Computo, Coordinador de Desarrollo Informático, Administradores de los Centros de Computo de las Oficinas de Registro,

Registradores de Instrumentos Públicos y Operadores de los sistemas externos.

- PHVA

  Planeación: Planea los recursos logísticos, humanos y financieros para la gestión del procedimiento. Gestionar el mantenimiento preventivo y correctivo de las bases de datos y la capacitación a los responsables de ellas y actualización de las versiones de las bases de datos.

  Hacer: Gestionar, administrar y verificar que los datos se encuentren actualizados, para brindar información en forma oportuna, segura y efectiva al ciudadano. Asegurar la disponibilidad de la información contenida en la base de datos.

  Verificación: Verificar la disponibilidad de las bases de datos.

  Actuar: Definir estrategias de mejora continua en la administración de las bases de datos.

Procedimiento – Administración de Software

- Objetivo y campo de aplicación: Garantizar la disponibilidad del software realizando seguimiento a los diferentes compontes que integran el sistema de información.

  Los clientes del proceso son: Superintendencia de Notariado y Registro, las Oficinas de Registro, Entidades y Puntos externos.

- Alcance:

  Inicia: Verificar y actualizar el inventario de los diferentes tipos de software con los que cuenta la SNR y ORIPs.

  ¿Qué Hace?: Verificar la disponibilidad y funcionalidad de los diferentes tipos de software.

  Termina: Verificación y diligenciamiento de chequeo.

- Responsables:

  Responsable estratégico: Jefe Oficina de Informática.

  Responsable operativo: Profesional especializado, Profesional universitario y Analista de sistemas (Desarrollo Informático, Asistencia Técnica y Centro de Cómputo).

- PHVA

  Planeación: Verificación de la disponibilidad de planear el registro de incidentes técnicos desde la mesa de servicio, categorizar incidente y planear el tiempo de respuesta y la satisfacción al usuario.

  Hacer: Verificar la disponibilidad y funcionalidad de los diferentes tipos de software.

  Verificación: Evaluar el cumplimiento de la lista de chequeo.

  Actuar: Definir estrategias para el mejoramiento continuo del procedimiento, logrando así la satisfacción del usuario interno y externo.

Procedimiento – Administración de Redes y Comunicación

- Objetivo y campo de aplicación: Realizar la administración, instalación, adecuación, ampliación, operación y actualización de las redes de computo para agilizar los procesos administrativos en la operación de trámites y servicios que proporciona la SNR, ORIPs y Puntos externos, garantizándole al personal un fácil acceso a los aplicativos y servicios como correo electrónico, Internet, bases de datos, entre otros.

  El procedimiento se desarrolla en el Centro de Computo de la Superintendencia, en los Centros de Computo de las Oficinas de Registro y en el Data Center donde están las bases de datos centralizadas.

  Los clientes del proceso son: Los funcionarios de la Superintendencia de Notariado y Registro, Oficinas de Registro y Puntos externos.
- Alcance:
  Inicia: Desde la atención de un requerimiento, planeación topológica y ubicación de la red, hasta el monitoreo de las redes WAN y LAN.
  ¿Qué Hace?: Monitoreo de las redes, administración de las políticas en el uso de Internet, directorio activo, administración de usuarios, servidores y equipos activos de red, recepción y análisis del requerimiento.
  Termina: Validar la conectividad de los servicios y de los usuarios.
- Responsables:
  Responsable estratégico: Jefe Oficina de Informática.
  Responsable operativo: Profesional universitario, Analista de sistemas del Grupo Centro de Cómputo.
- PHVA
  Planeación: Planear inicialmente la topología y su ubicación, para hacer el diseño de la red, programar mantenimientos, adecuaciones físicas de las redes LAN y WAN.
  Hacer: Monitoreo de las redes, aplicación de las políticas de uso de Internet, directorio activo, usuarios, servidores y equipos activos de red, así como la recepción y análisis de requerimientos.
  Verificación: Verificar la funcionalidad de los servicios de telecomunicaciones, evaluar estado de los incidentes registrados vs tiempos de respuesta y hacer seguimiento al incidente.
  Actuar: Gestionar cambios, actualizaciones y correcciones de errores, copias de seguridad; realizar visitas de seguimiento.

Procedimiento – Administración de Usuarios

- Objetivo y campo de aplicación: Este procedimiento únicamente se deberá realizar en los sistemas que basen en contraseñas la identificación y autenticación de los usuarios y estará a cargo del grupo Centro de Cómputo – Nivel Central de la SNR.

Por lo tanto se debe definir un proceso de creación, desactivación y eliminación de usuarios de aplicaciones y bases de datos: Directorio Activo, Correo Electrónico, Apoteosys, ERP (Sistema de Correspondencia y Sistema de Atención al Ciudadano, Nomina, Contabilidad, Contratación, Inventarios), Reparto Notarial, SIN y Bloqueo, Desbloqueo, Cambio de Claves, entre otros.

Cabe aclarar que el manejo de cuentas de usuarios y contraseñas, es de carácter personal e intransferible, por lo tanto, las operaciones que pongan en riesgo los intereses de la SNR, serán de entera responsabilidad del usuario o funcionario.

Los clientes del proceso son: Superintendencia de Notariado y Registro, Oficinas de Registro y Notarias con el sistema SIN.

- Alcance:

  Inicia: Con el diligenciamiento y envió de la solicitud por los medios dispuestos para tal fin, debidamente autorizada por el Registrador de la ORIP o en su defecto por el Jefe, Director o Coordinador de Área a nivel SNR.

  ¿Qué Hace?: Diligenciar formulario y enviarlo al Centro de Cómputo nivel central, previamente autorizado por el Registrador de la ORIP, Jefe, Director o Coordinador de Dependencia.

  Termina: Asignar el responsable técnico del Centro de Computo o administrador de las cuentas de correo, según sea el caso y la notificación final el proceso.
- Responsables:

  Responsable estratégico: Jefe Oficina de Informática, Registrador de la ORIP, Jefe, Director o Coordinador de área o dependencia.

  Responsable operativo: Coordinador Centro de Cómputo, Mesa de Ayuda (Asistencia Técnica), Profesional especializado, Profesional universitario y/o Analista de sistemas.
- PHVA:

  Planeación: Garantizar que los funcionarios se obliguen a cumplir con la política de seguridad.

  Hacer: Diligenciar el formulario de solicitud por parte del funcionario debidamente autorizado y recibido por el responsable del Centro de Computo de la SNR, independientemente del medio por el cual haya sido enviado: Correo electrónico, oficio o fax; registrar todo requerimiento por parte del funcionario designado en la bitácora de control para administración de usuarios por el Centro de Computo nivel central y soporte de correo institucional; informar al usuario medidas de seguridad como caducidad, tamaño, bloqueo por intentos al momento de acceder una clave errada, sanciones por préstamo de claves o suplantación de usuarios.

  Verificación: Confirmar el cambio realizado al funcionario.

Actuar: Hacer uso del programa de divulgación de la entidad y/o socialización; hacer seguimiento al llenado de la bitácora de control.

Procedimiento – Administración de Seguridad Informática

- Objetivo y campo de aplicación: La administración de la Seguridad Informática depende de la Oficina de Informática de la Superintendencia de Notariado y Registro con alcance para los funcionarios, contratistas y pasantes de las Oficinas de Registro Sistematizadas (Folio Magnético y SIR), Oficinas de Registro manuales en proceso de sistematización.

  Los clientes externos son: Entidades del estado, Sistemas administrativos y financieros, Contratistas o Terceros.

  Los clientes internos son: Funcionarios vinculados directamente con la Superintendencia de Notariado y Registro, Oficinas de Registro y Notarias.
- Alcance:
  Inicia: Con el diagnostico y seguimiento a las diferentes amenazas informáticas en las que está expuesta la información de la Superintendencia de Notariado y Registro.
  ¿Qué Hace?: Conocer e identificar los activos de la Entidad, áreas funcionales; evaluar la seguridad de las comunicaciones, aplicativos y manejo de procesos; analizar, identificar, evaluar y valorar los riesgos.
  Termina: Con elaborar, ajustar y/o actualizar las Políticas de Seguridad, Plan de Recuperación de Desastres y el Plan de Continuidad del Negocio, Manual de Procesos y Procedimientos de las áreas de la Oficina de Informática y la socialización del tema de la seguridad informática.
- Responsables:
  Responsable operativo: Oficial de seguridad o profesional encargado de la misma apoyándose con los Coordinadores de los Grupos de Desarrollo Informático, Asistencia Técnica y Centro de Computo.
- PHVA:
  Planear: Especificar el alcance del sistema de gestión para la seguridad informática y las políticas de seguridad. Definir una metodología de evaluación de riesgos. Identificar los activos, amenazas y vulnerabilidades; analizar los riesgos; evaluar opciones para el tratamiento de los riesgos (Mitigar a través de controles, transferir haciendo uso de seguros y/o proveedores, aceptar y no hacer nada y evitar para que cese la actividad que origina) y definir una declaración de aplicabilidad.
  Hacer: Implantar y operar el sistema de gestión para la seguridad informática, enfocado a elaborar el plan de tratamiento de riesgos e implementar controles, definir un sistema de métricas para medir la eficacia de los controles, gestionar programas de formación y concienciación.
  Verificar: Monitorear y revisar el sistema de gestión para la seguridad informática, enfocado al control de procedimientos de revisión para

identificar, detectar y prevenir incidentes, realizar auditorías internas o evaluaciones periódicas de la efectividad del sistema de gestión, actualizar los planes de seguridad, ayudar a la alta dirección a determinar si las actividades realizadas por las personas y dispositivos tecnológicos se desarrollan en relación a lo previsto, registrar acciones y eventos que impacten la efectividad o rendimiento del sistema de seguridad informática.
Actuar: Implementar mejoras asociadas al sistema de gestión de calidad, realizar acciones correctivas y preventivas adecuadas en relación con la clausula 8 de ISO 27001, comunicar las acciones y mejoras a todas las partes interesadas asegurando cumplimiento de objetivos previstos.

Procedimiento – Asistencia y Soporte Técnico

- Objetivo y campo de aplicación: Atender los requerimientos a nivel de hardware, software, redes y comunicaciones de manera oportuna a los funcionarios de la SNR, ORIPs y Notarias que cuentan con el sistema SIN, ofreciendo una solución rápida y oportuna frente a los problemas que se puedan presentar en el desarrollo diario de las actividades, mediante herramientas tecnológicas como Mesa de servicio, directorio activo, sistema de seguridad informática y telecomunicaciones.

  Los clientes del proceso son: Superintendencia de Notariado y Registro, Oficinas de Registro, Notarias con el sistema SIN, Entidades y Puntos de atención externos.
- Alcance:
  Inicia: Solicitud telefónica o por correspondencia de los funcionarios de las ORIPs, SNR, Puntos de atención externos y Notarias, para la solución de problemas presentados a nivel de hardware, software, redes y comunicaciones, equipos de soporte eléctrico. Aplica para todos los requerimientos hechos por los funcionarios, desde la recepción de la solicitud de soporte.

  Para el caso de las ORIPs que cuentan con la base de datos centralizada administrada por un tercero, se atienden los requerimientos del desempeño del aplicativo en la mesa de servicio contratada.
  ¿Qué Hace?: Registrar la solicitud en el Sistema de Información de Mesa de Ayuda, Asignar el ticket manual o automáticamente a un profesional universitario o especializado, analista o técnico de acuerdo con el grupo, quien debe hacer seguimiento a la gestión del servicio en la solución del incidente.
  Termina: Con la solución del incidente dada telefónicamente o se escala al grupo respectivo (Asistencia Técnica, Centro de Computo, Desarrollo Informático) y cerrando el caso en la Mesa de Ayuda y registrando las actividades en la base de conocimiento.
- Responsables:

Responsable estratégico: Jefe Oficina de Informática
Responsable operativo: Coordinadores, Profesional universitario, Analista de sistemas, Técnicos (Centro de Cómputo, Asistencia Técnica y Desarrollo Informático).

- PHVA:

Planear: Planear el registro de incidentes desde la mesa de servicio, categorizar incidente y planear el tiempo de respuesta y la satisfacción al usuario.
Hacer: Registrar la solicitud en el Sistema de Información de la Mesa de Ayuda, Asignar el ticket manual o automáticamente a un profesional, analista o técnico de acuerdo con el grupo, quien debe hacer seguimiento a la gestión del servicio en la solución del incidente.
Verificación: Verificar el estado de los incidentes registrados, tiempo de respuesta y hacer seguimiento a la solución del mismo.
Actuar: Retro-alimentar adecuada y permanentemente la base de datos de conocimiento, con la solución de cada incidente reportados por los usuarios de los diferentes sistemas.

Procedimiento – Backup y Protección de la Información

- Objetivo y campo de aplicación: El Centro de Computo del Nivel Central de la SNR, se encargara de proteger y garantizar que los recursos del sistema de información (Aplicaciones y Bases de Datos) de la Superintendencia de Notariado y Registro, se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

Los clientes del proceso son: Superintendencia de Notariado y Registro Nivel Central, incluyendo las aplicaciones asignadas para su administración por parte de entes externos.

- Alcance:

Inicia: Inicia con la programación que se tiene definida en el Centro de Computo de la SNR para hacer copias de seguridad de las bases de datos de los sistemas de información.
¿Qué Hace?: Ejecutar procedimiento para cada base de datos y diligenciar bitácora de Backup de acuerdo a su periodicidad.
Termina: Con la verificación del Backup y posterior custodia de dichas copias de seguridad.

- Responsables:

Responsable estratégico: Jefe Oficina de Informática.
Responsable operativo: Coordinador Grupo Centro de Cómputo, Profesional especializado, Profesional universitario y Analista de sistemas

- PHVA:

Planear: Garantizar la realización de respaldo.
Hacer: Desarrollar cada una de las actividades contempladas en el proceso de Backup. Realizar recuperación de información cuando sea necesario.

Verificar: Registrar en la bitácora de control de Backup.
Actuar: Hacer seguimiento proceso de Backups.

4.1.3 Estudio situación actual de seguridad

4.1.3.1 Recaudo y revisión de información relacionada con la seguridad de la información en la Superintendencia de Notariado y Registro (SNR). La documentación relacionada con el tema de seguridad de la información al interior de la Superintendencia de Notariado y Registro está limitada a un documento general sobre políticas de seguridad titulado **"*Políticas de Seguridad en los Sistemas de Información*"**, Emitido a los directivos, registradores de instrumentos públicos y funcionarios a través de circular del 30 de mayo de 2008. Documento por demás desactualizado y al que se hacen revisiones eventuales sin llegar a concretarse un documento formal que pueda publicarse y ser divulgado. Además de circulares y oficios emitidos en su momento como consecuencia y con el propósito de palear determinada situación negativa de seguridad. Estos documentos pueden resumirse así:

- Circular No. 77 de 2008. A través de la cual se divulgan las políticas de seguridad de la Superintendencia de Notariado y Registro mediante documento "Políticas de Seguridad en los Sistemas de Información". Su contenido puede apreciarse en el **Anexo A.**
- Circular No. 230 de 2009. Emitida como complemento al documento "Políticas de Seguridad en los Sistemas de Información". Su contenido puede apreciarse en el **Anexo B.**
- Comunicado 003 de 2010. Donde se anuncian controles al servicio de Internet. Su contenido puede apreciarse en el **Anexo C.**

4.1.3.2 Levantamiento de información de activos. Mediante observación directa y consultas realizadas a las personas encargadas se realiza el siguiente levantamiento de información orientado a especificar los activos del Departamento de Informática (Oficina Tecnologías de la Información) de la Superintendencia de Notariado y Registro:

Activos

- Formato administración cuentas de usuarios
- Registros de recurso (DNS)
- Autenticación de usuarios
- Directorio activo
- Servicio de nombres de dominio
- DHCP

- BIOMETRICO
- Sistema de información notarial
- Sistema de personal y nomina
- IRIS documental
- Sistema de procesos judiciales
- Hoja de vida de notarios
- Sistema de control interno disciplinario
- Sistema de control interno disciplinario notarias
- Sistema integrado web
- Interrelación registro - catastro
- Botón de pago
- Ventanilla única de registro
- Netbackup
- Oracle Virtual Machine
- Endpointsecurity (antivirus)
- EXADATA
- EXALOGIC
- Servidores
- Computadores
- Portátiles
- Impresoras
- Switch
- Firewall
- Red LAN
- Internet
- Sistema de alimentación ininterrumpida (UPS)
- Fuentes de alimentación
- Aire acondicionado
- Arreglo de discos
- Librería de cintas
- Unidad DVD (servidores)
- Correo electrónico
- Portal
- Hosting y administración
- Centro de datos
- Administradores de sistemas
- Administradores de comunicaciones
- Administradores de bases de datos

4.1.3.3 Análisis de riesgos. Para el análisis de riesgo se utilizara la herramienta denominada PILAR, esta es una herramienta complementaria a la Metodología Magerit, que fue diseñada al igual que Magerit por el gobierno español con el único fin de realizar análisis de riesgo.

El análisis de riesgo que se llevara a cabo será un análisis de tipo cualitativo.

Activos

Activos - Identificación

Figura 4. Representación de activos

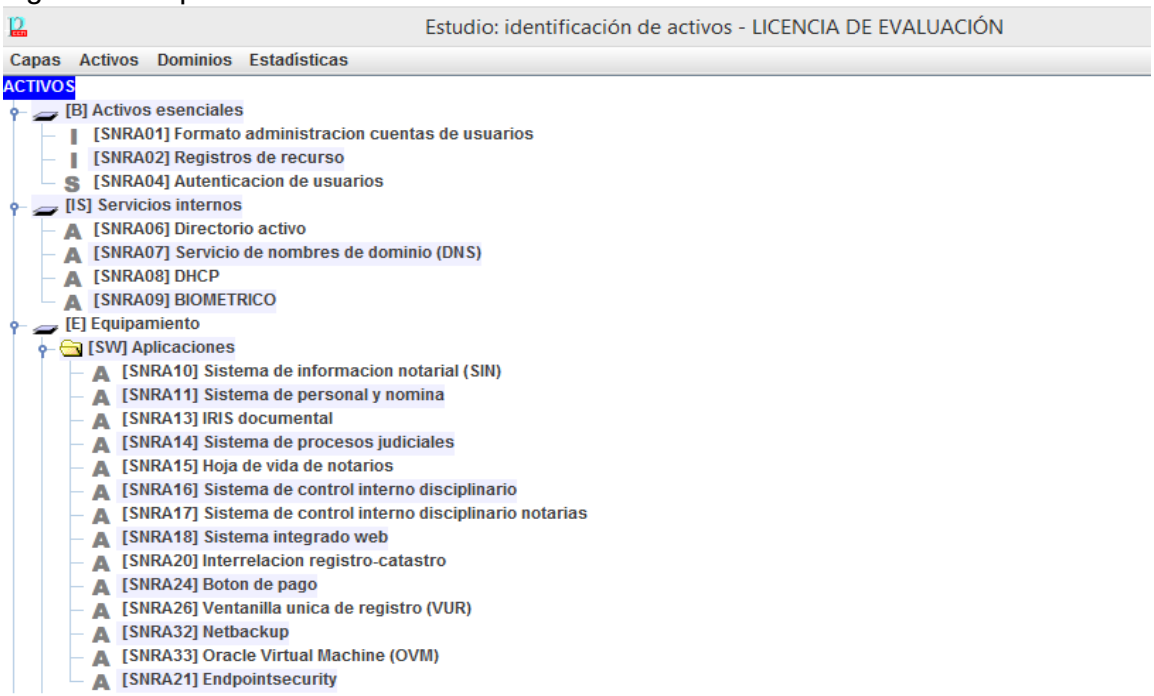
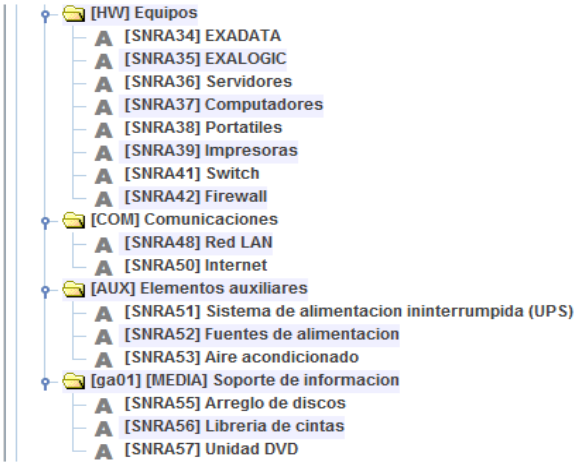
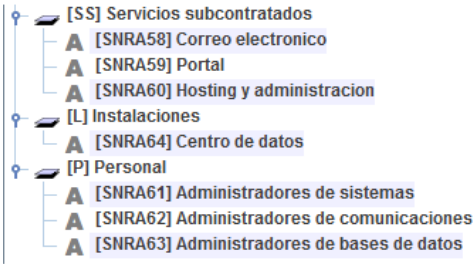


Figura 4. (Continuación)





Fuente El autor

Activos - Clases de activos

La herramienta PILAR tiene predefinidas las siguientes clases de activos, a través de las cuales se organizaran los activos.

[essential] Activos esenciales-[info] información-[vr] datos vitales (registros de la organización)

[essential] Activos esenciales-[service] servicio

[S] Servicios-[prov] proporcionado por nosotros-[idm] gestión de identidad

[S] Servicios-[prov] proporcionado por nosotros-[dns] servidor de nombres de dominio

[S] Servicios-[prov] proporcionado por nosotros-[int] interno (usuarios y medios de la propia organización)

[S] Servicios-[prov] proporcionado por nosotros-[pub] al público en general (sin relación contractual)

[SW] Aplicaciones (software)-[sub] desarrollo a medida (subcontratado)

[SW] Aplicaciones (software)-[std] estándar (off the shelf)-[backup] servicio de backup

[SW] Aplicaciones (software)-[std] estándar (off the shelf)-[hypervisor] hypervisor (gestor de la maquina virtual)

[SW] Aplicaciones (software)-[std] estándar (off the shelf)-[av] anti virus

[HW] Equipamiento informático (hardware)-[host] grandes equipos (host)

[HW] Equipamiento informático (hardware)-[mid] equipos medios

[HW] Equipamiento informático (hardware)-[pc] informática personal

[HW] Equipamiento informático (hardware)-[mobile] informática móvil

[HW] Equipamiento informático (hardware)-[peripheral] periféricos-[print] medios de impresión

[HW] Equipamiento informático (hardware)-[network] soporte de la red-[switch] conmutador
[HW] Equipamiento informático (hardware)-[network] soporte de la red-[other] otros

[COM] Redes de comunicaciones-[LAN] red local

[COM] Redes de comunicaciones-[Internet] Internet

[AUX] Equipamiento auxiliar-[ups] sai - sistemas de alimentación ininterrumpida

[AUX] Equipamiento auxiliar-[power] fuentes de alimentación

[AUX] Equipamiento auxiliar-[ac] equipos de climatización

[Media] Soportes de información-[electronic] electrónicos

[Media] Soportes de información-[electronic] electrónicos-[dvd] DVD

[S] Servicios-[3rd] contratado a una tercera parte-[email]-correo electrónico

[S] Servicios-[3rd] contratado a una tercera parte-[ISP] Proveedor de acceso a Internet

[S] Servicios-[3rd] contratado a una tercera parte-[ISP] Proveedor de acceso a Internet

[S] Servicios-[3rd] contratado a una tercera parte-[comms] transporte/comunicaciones

[S] Servicios-[3rd] contratado a una tercera parte-[email] correo electrónico

[S] Servicios-[3rd] contratado a una tercera parte-[www] alojamiento de servidor web

[S] Servicios-[3rd] contratado a una tercera parte-[hosting] alojamiento de aplicaciones

[S] Servicios-[3rd] contratado a una tercera parte-[housing] alojamiento de equipos

[L] Instalaciones-[local] cuarto

[P] Personal-[adm] administradores de sistemas

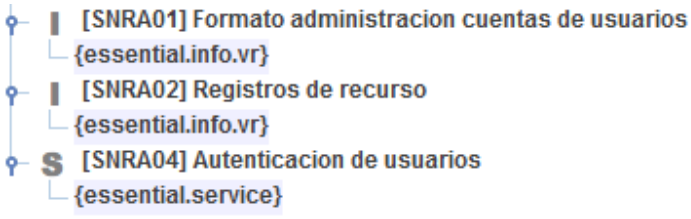
[P] Personal-[com] administradores de comunicaciones

[P] Personal-[dba] administradores de BBDD

A continuación se representan los activos y su pertenencia a cada clase de activos:

1). [B] Activos esenciales

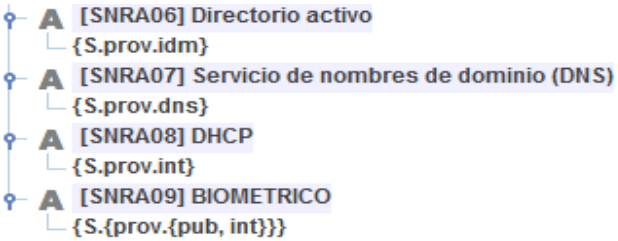
Figura 5. Representación de pertenencia a clases de los activos de activos esenciales



Fuente El autor

2). [IS] Servicios internos

Figura 6. Representación de pertenencia a clases de los activos de servicios internos

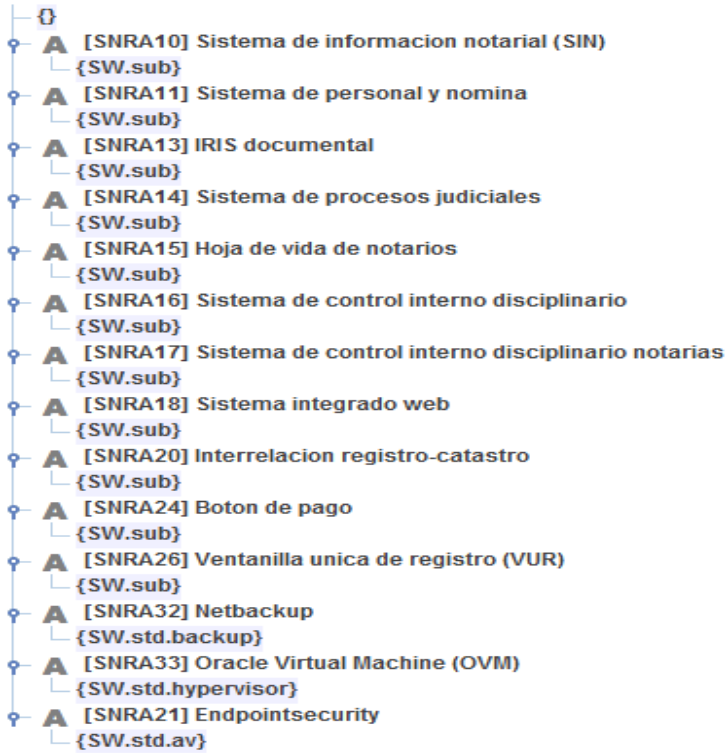


Fuente El autor

3). [E] equipamiento

[SW] Aplicaciones

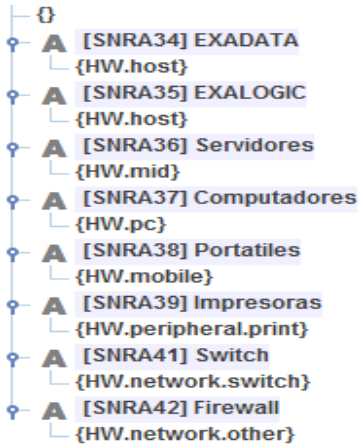
Figura 7. Representación de pertenencia a clases de los activos de equipamiento-aplicaciones



Fuente El autor

[HW] Equipos

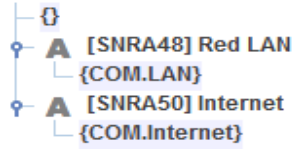
Figura 8. Representación de pertenencia a clases de los activos de equipamiento-equipos



Fuente El autor

[COM] Comunicaciones

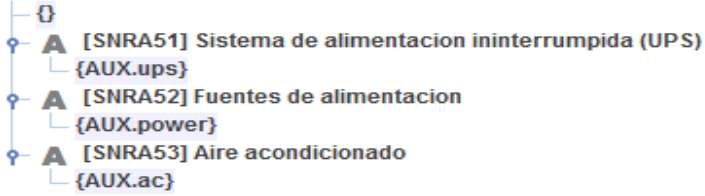
Figura 9. Representación de pertenencia a clases de los activos de equipamiento-comunicaciones



Fuente El autor

[AUX] Elementos auxiliares

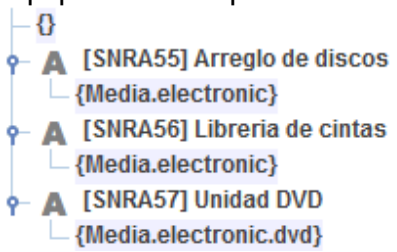
Figura 10. Representación de pertenencia a clases de los activos de equipamiento-elementos auxiliares



Fuente El autor

[MEDIA] Soporte de información

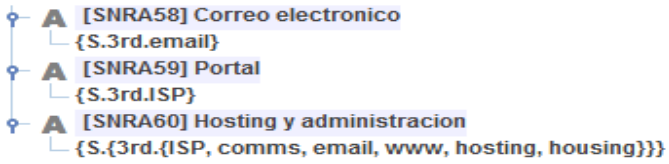
Figura 11. Representación de pertenencia a clases de los activos de equipamiento-soporte de información



Fuente El autor

4). [SS] Servicios subcontratados

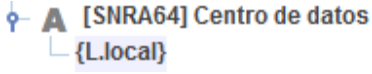
Figura 12. Representación de pertenencia a clases de los activos de servicios subcontratados



Fuente El autor

5). [L] Instalaciones

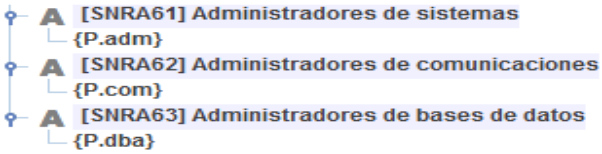
Figura 13. Representación de pertenencia a clases de los activos de instalaciones



Fuente El autor

6). [P] Personal

Figura 14. Representación de pertenencia a clases de los activos de personal

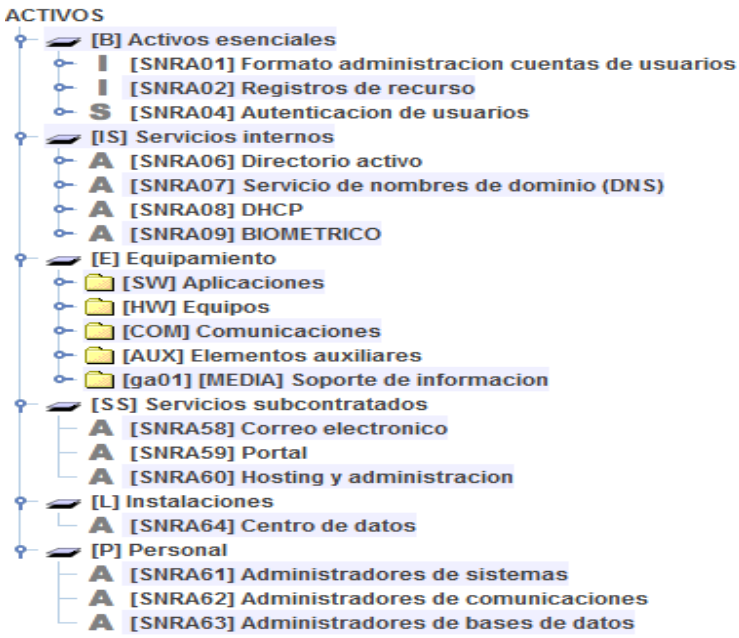


Fuente El autor

Activos - Dependencias

Descripción general

Figura 15. Representación general dependencias

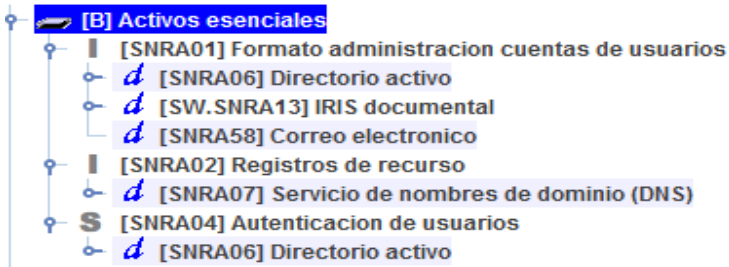


Fuente El autor

Descripción especifica

1). Activos esenciales

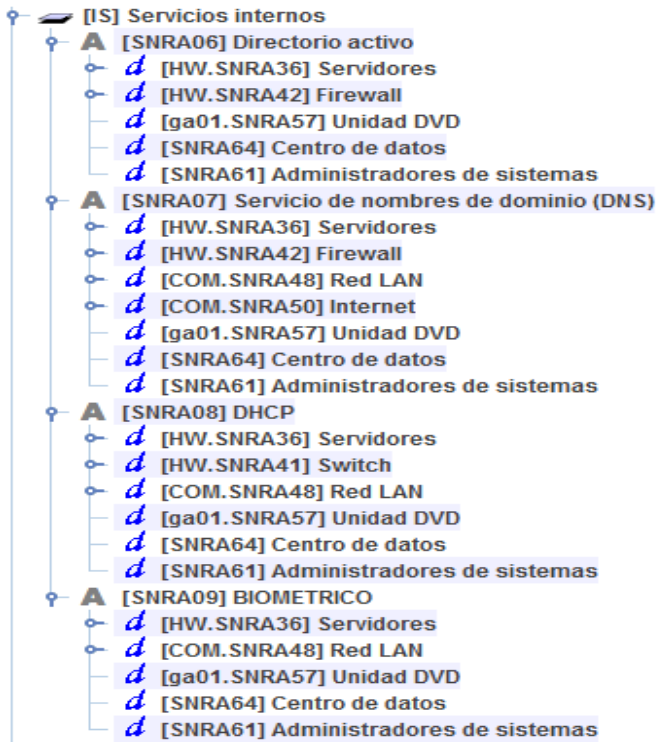
Figura 16. Representación de dependencias de los activos de activos esenciales



Fuente El autor

2). Servicios internos

Figura 17. Representación de dependencias de los activos de servicios internos



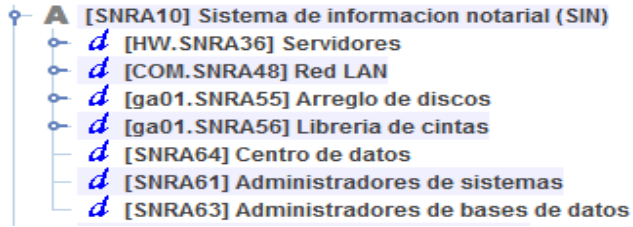
Fuente El autor

3). Equipamiento

[SW] Aplicaciones

a). Sistema de información notarial (SIN)

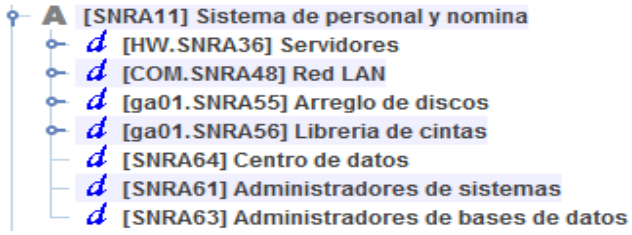
Figura 18. Representación de dependencias de sistema de información notarial



Fuente El autor

b). Sistema de personal y nomina

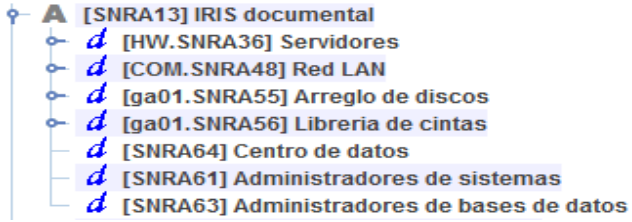
Figura 19. Representación de dependencias sistema de personal y nomina



Fuente El autor

c). IRIS documental

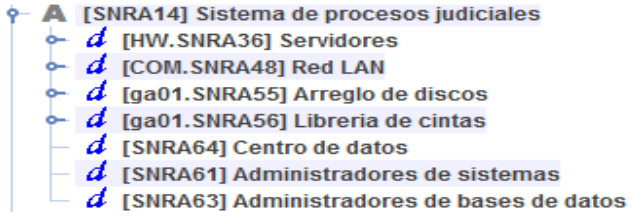
Figura 20. Representación de dependencias IRIS documental



Fuente El autor

d). Sistema de procesos judiciales

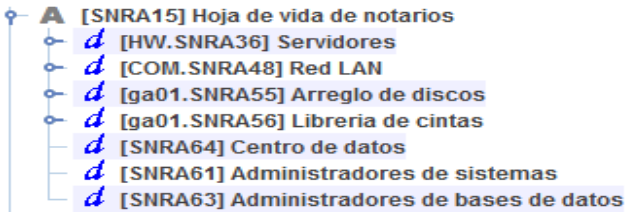
Figura 21. Representación de dependencias sistema de procesos judiciales



Fuente El autor

e). Hoja de vida de notarios

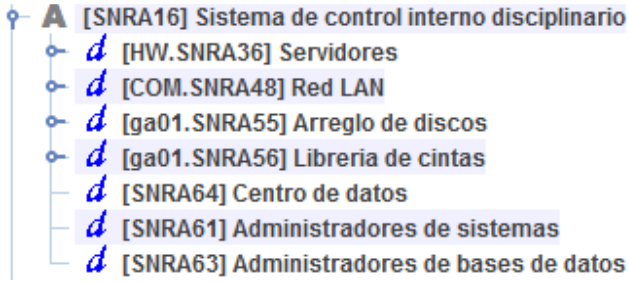
Figura 22. Representación de dependencias hoja de vida de notarios



Fuente El autor

f). Sistema de control interno disciplinario

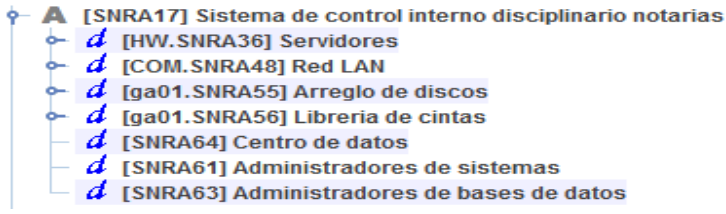
Figura 23. Representación de dependencias sistema de control interno disciplinario



Fuente El autor

g). Sistema de control interno disciplinario notarias

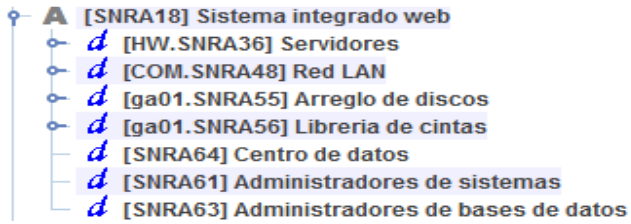
Figura 24. Representación de dependencias sistema de control interno disciplinario notarias



Fuente El autor

h). Sistema integrado web

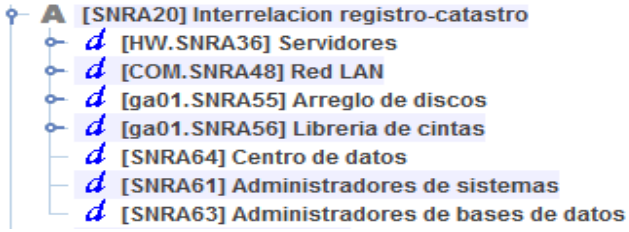
Figura 25. Representación de dependencias sistema integrado web



Fuente El autor

i). Interrelación registro - catastro

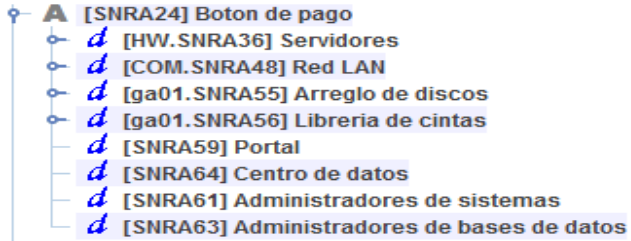
Figura 26. Representación de dependencias registro-catastro



Fuente El autor

j). Botón de pago

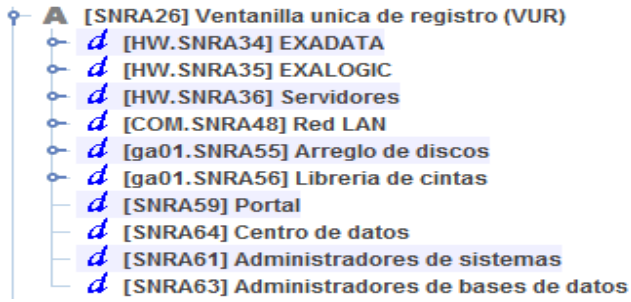
Figura 27. Representación de dependencias botón de pago



Fuente El autor

k). Ventanilla única de registro (VUR)

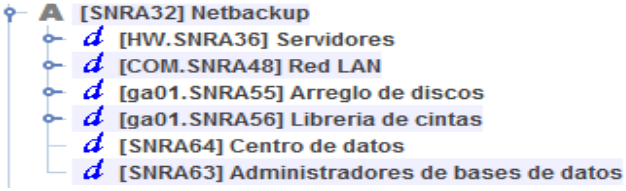
Figura 28. Representación de dependencias ventanilla única de registro



Fuente El autor

l). Netbackup

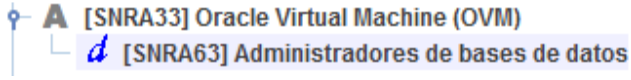
Figura 29. Representación de dependencias netbackup



Fuente El autor

m). Oracle Virtual Machine (OVM)

Figura 30. Representación de dependencias oracle virtual machine



Fuente El autor

n). Endpointsecurity

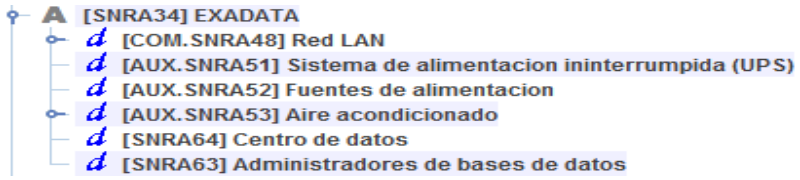
Figura 31. Representación de dependencias endpointsecurity

Fuente El autor

[HW] equipos

a). EXADATA

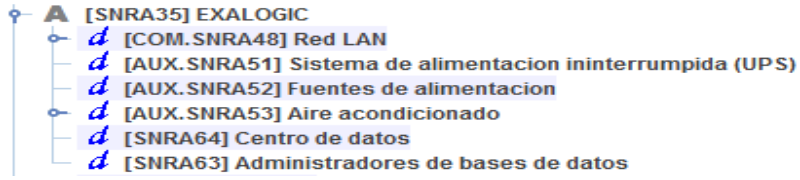
Figura 32. Representación de dependencias exadata



Fuente El autor

b). EXALOGIC

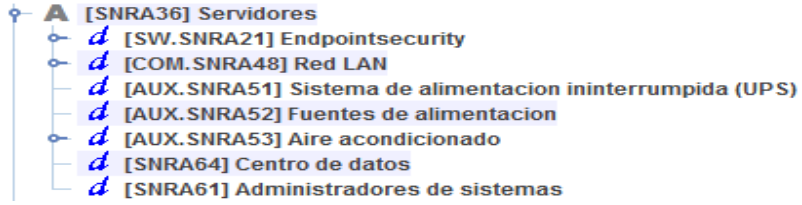
Figura 33. Representación de dependencias exalogic



Fuente El autor

c). Servidores

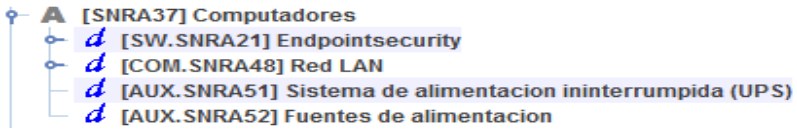
Figura 34. Representación de dependencias servidores



Fuente El autor

d). Computadores

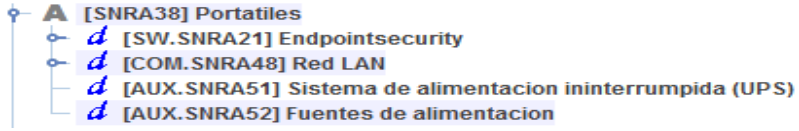
Figura 35. Representación de dependencias computadores



Fuente El autor

e). Portátiles

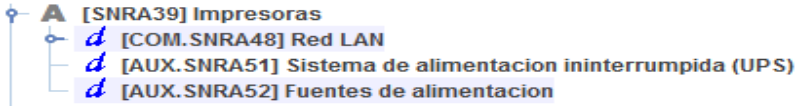
Figura 36. Representación de dependencias portátiles



Fuente El autor

f). Impresoras

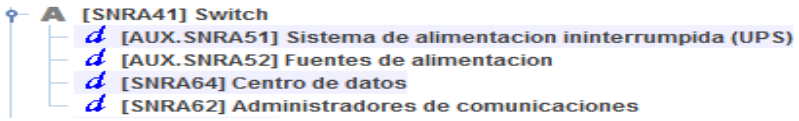
Figura 37. Representación de dependencias impresoras



Fuente El autor

g). Switch

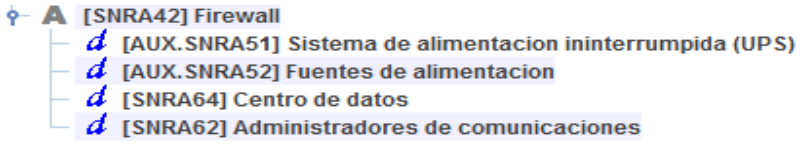
Figura 38. Representación de dependencias switch



Fuente El autor

h). Firewall

Figura 39. Representación de dependencias firewall

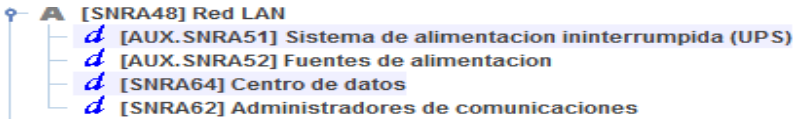


Fuente El autor

[COM] Comunicaciones

a). Red LAN

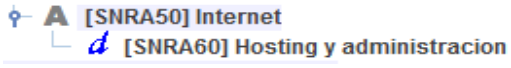
Figura 40. Representación de dependencias red LAN



Fuente El autor

b). Internet

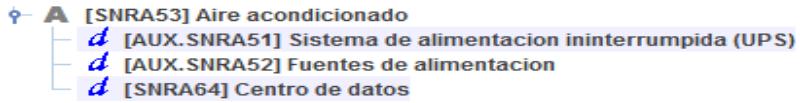
Figura 41. Representación de dependencias Internet



Fuente El autor

[AUX] Elementos auxiliares

Figura 42. Representación de dependencias aire acondicionado

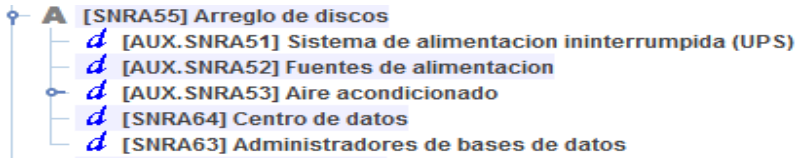


Fuente El autor

[MEDIA] Soporte de información

a). Arreglo de discos

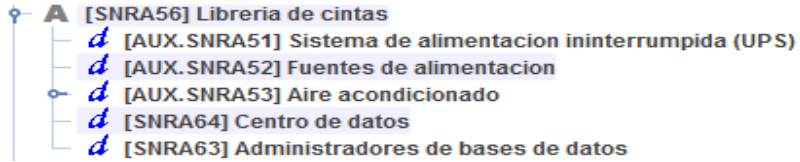
Figura 43. Representación de dependencias arreglo de discos



Fuente El autor

b). Librería de cintas

Figura 44. Representación de dependencias librería de cintas



Fuente El autor

Activos - Valoración de los activos

Cada uno de los activos fueron valorados independientemente.

Descripción general

Figura 45. Representación general de valoración de activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[SNRA01] Formato administracion cuentas de usuarios		[7]		[7]	
[SNRA02] Registros de recurso		[1]			
[SNRA04] Autenticacion de usuarios	[7]			[7]	
[IS] Servicios internos					
[SNRA06] Directorio activo	[7]			[7]	
[SNRA07] Servicio de nombres de dominio (DNS)	[7]				
[SNRA08] DHCP	[7]				
[SNRA09] BIOMETRICO	[3]				[3]
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[SNRA58] Correo electronico	[5]				
[SNRA59] Portal	[5]				
[SNRA60] Hosting y administracion	[7]				
[L] Instalaciones					
[SNRA64] Centro de datos	[7]				
[P] Personal					
[SNRA61] Administradores de sistemas	[5]				
[SNRA62] Administradores de comunicaciones	[7]				
[SNRA63] Administradores de bases de datos	[7]				

Fuente El autor

Descripción especifica

1). [B] Activos esenciales

Figura 46. Representación valoración de los activos de activos esenciales

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[SNRA01] Formato administracion cuentas de usuarios		[7]		[7]	
[SNRA02] Registros de recurso		[1]			
[SNRA04] Autenticacion de usuarios	[7]			[7]	
[IS] Servicios internos					
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

2). [IS] Servicios internos

Figura 47. Representación valoración de los activos de servicios internos

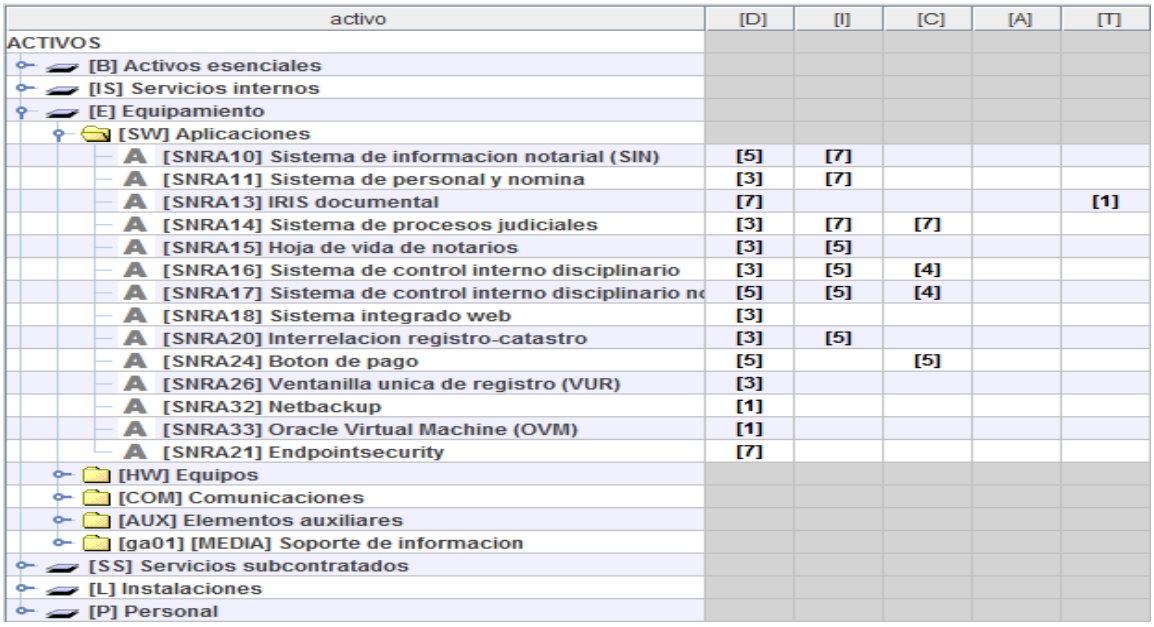
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[SNRA06] Directorio activo	[7]			[7]	
[SNRA07] Servicio de nombres de dominio (DNS)	[7]				
[SNRA08] DHCP	[7]				
[SNRA09] BIOMETRICO	[3]				[3]
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

3). [E] Equipamiento

[SW] Aplicaciones

Figura 48. Representación valoración de los activos de equipamiento-aplicaciones



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[SNRA10] Sistema de informacion notarial (SIN)	[5]	[7]			
[SNRA11] Sistema de personal y nomina	[3]	[7]			
[SNRA13] IRIS documental	[7]				[1]
[SNRA14] Sistema de procesos judiciales	[3]	[7]	[7]		
[SNRA15] Hoja de vida de notarios	[3]	[5]			
[SNRA16] Sistema de control interno disciplinario	[3]	[5]	[4]		
[SNRA17] Sistema de control interno disciplinario nc	[5]	[5]	[4]		
[SNRA18] Sistema integrado web	[3]				
[SNRA20] Interrelacion registro-catastro	[3]	[5]			
[SNRA24] Boton de pago	[5]		[5]		
[SNRA26] Ventanilla unica de registro (VUR)	[3]				
[SNRA32] Netbackup	[1]				
[SNRA33] Oracle Virtual Machine (OVM)	[1]				
[SNRA21] Endpointsecurity	[7]				
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

[HW] Equipos

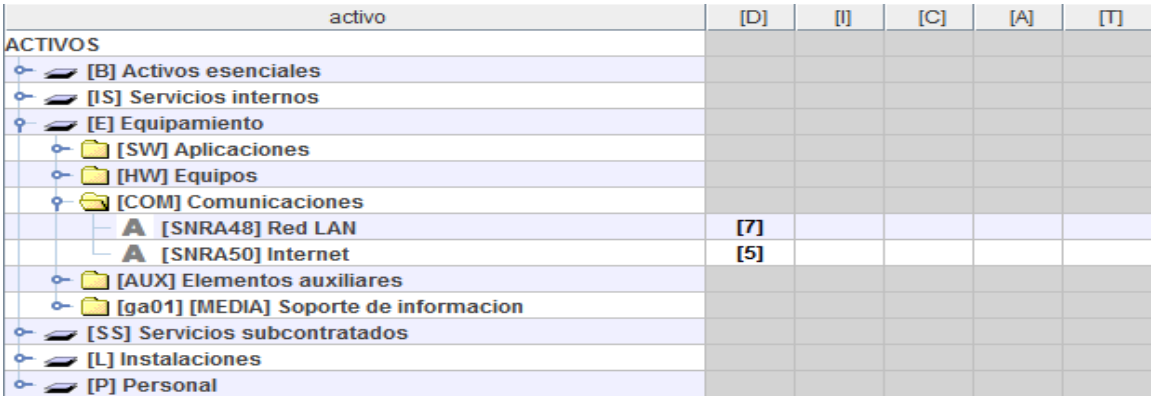
Figura 49. Representación valoración de los activos de equipamiento-equipos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[SNRA34] EXADATA	[7]				
[SNRA35] EXALOGIC	[7]				
[SNRA36] Servidores	[7]				
[SNRA37] Computadores	[3]				
[SNRA38] Portatiles	[3]				
[SNRA39] Impresoras	[1]				
[SNRA41] Switch	[5]				
[SNRA42] Firewall	[7]				
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

[COM] Comunicaciones

Figura 50. Representación valoración de los activos de equipamiento-comunicaciones

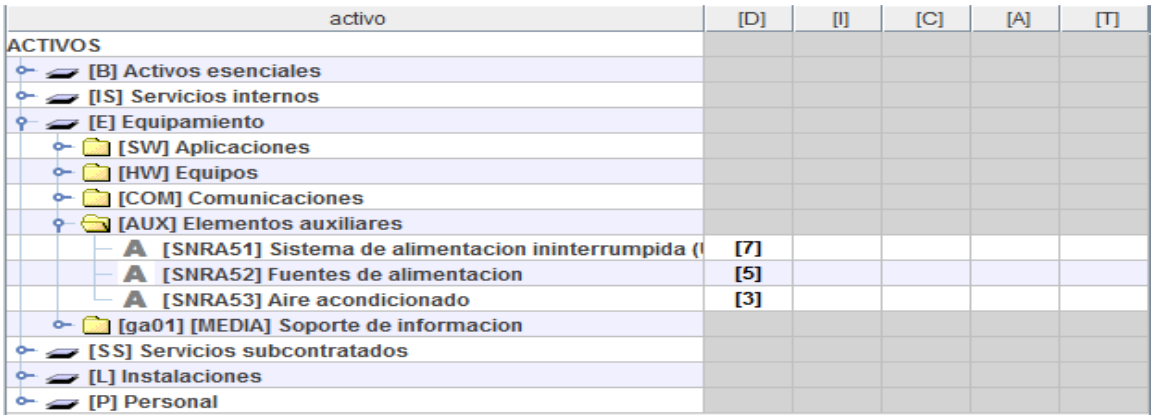


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[SNRA48] Red LAN	[7]				
[SNRA50] Internet	[5]				
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

[AUX] Elementos auxiliares

Figura 51. Representación valoración de los activos de equipamiento-elementos auxiliares

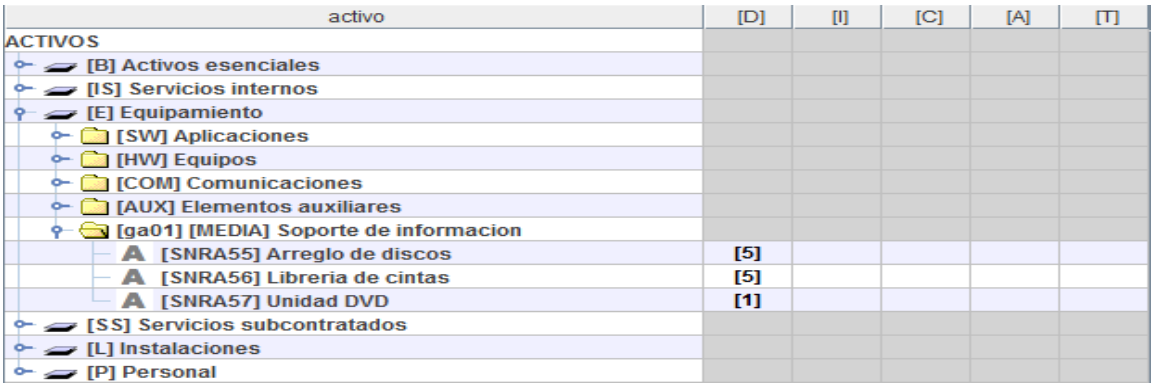


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SNRA51] Sistema de alimentacion ininterrumpida (	[7]				
[SNRA52] Fuentes de alimentacion	[5]				
[SNRA53] Aire acondicionado	[3]				
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

[MEDIA] Soporte de información

Figura 52. Representación valoración de los activos de equipamiento-soporte de información

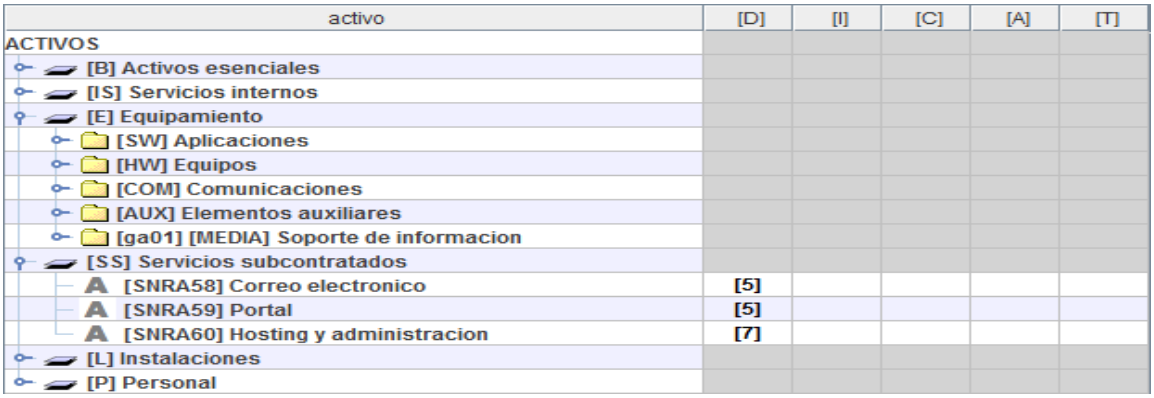


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SNRA55] Arreglo de discos	[5]				
[SNRA56] Libreria de cintas	[5]				
[SNRA57] Unidad DVD	[1]				
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Fuente El autor

4). [SS] Servicios subcontratados

Figura 53. Representación valoración de los activos de servicios subcontratados

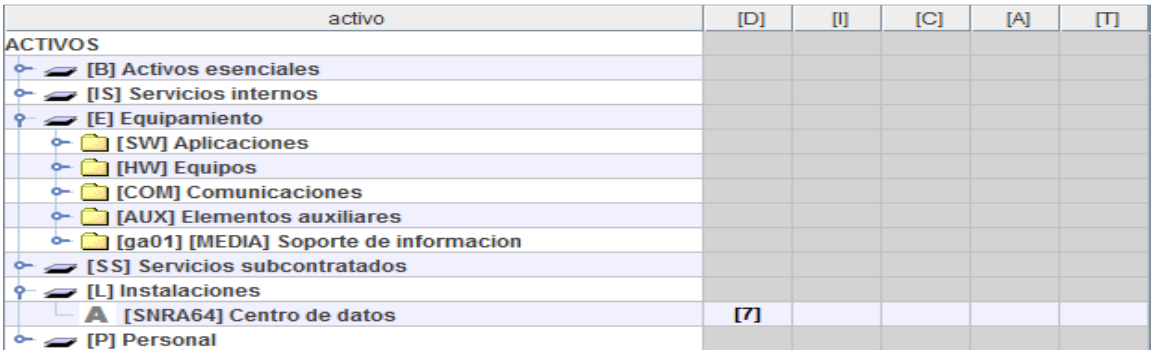


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[SNRA58] Correo electronico	[5]				
[SNRA59] Portal	[5]				
[SNRA60] Hosting y administracion	[7]				
[L] Instalaciones					
[P] Personal					

Fuente El autor

5). [L] Instalaciones

Figura 54. Representación valoración de los activos de instalaciones

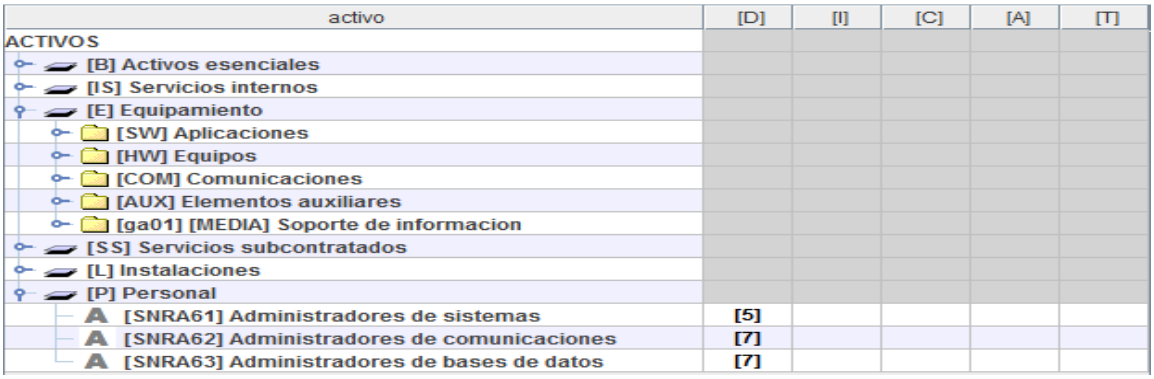


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[SNRA64] Centro de datos	[7]				
[P] Personal					

Fuente El autor

6). [P] Personal

Figura 55. Representación valoración de los activos de personal



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[ga01] [MEDIA] Soporte de informacion					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					
[SNRA61] Administradores de sistemas	[5]				
[SNRA62] Administradores de comunicaciones	[7]				
[SNRA63] Administradores de bases de datos	[7]				

Fuente El autor

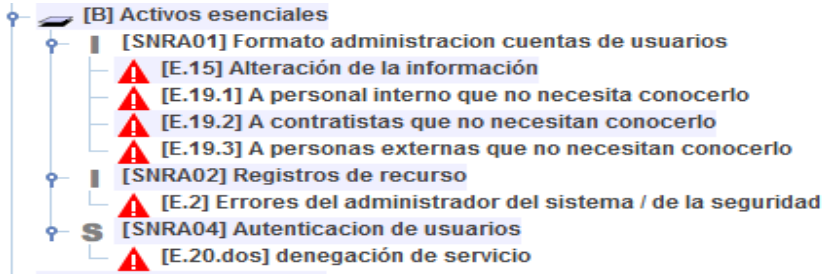
Amenazas

Amenazas - Identificación

Descripción especifica

1). [B] Activos esenciales

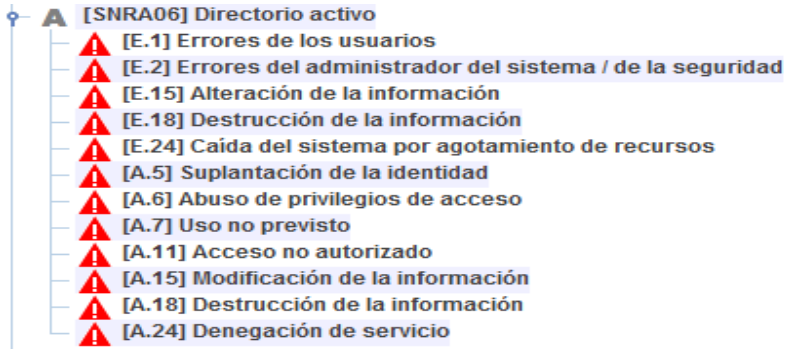
Figura 56. Representación de amenazas sobre los activos de activos esenciales



Fuente El autor

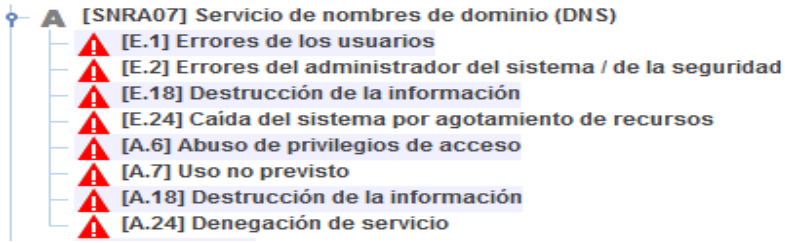
2). [IS] Servicios internos

Figura 57. Representación de amenazas sobre activo servicios internos-directorio activo



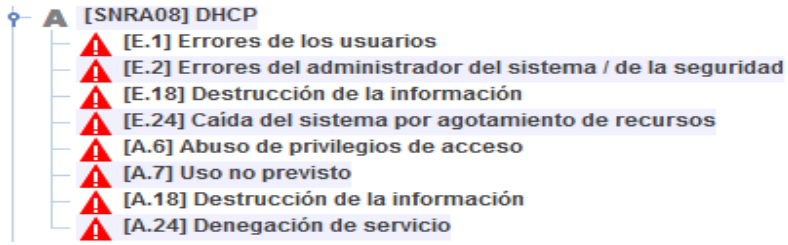
Fuente El autor

Figura 58. Representación de amenazas sobre activo servicios internos-DNS



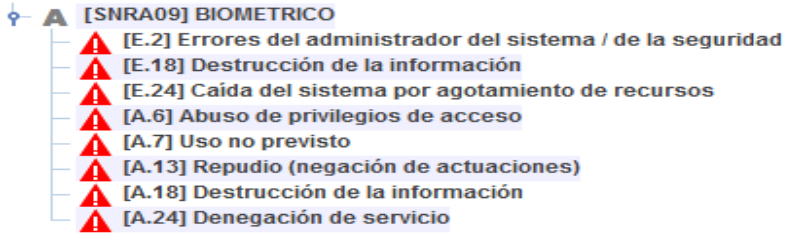
Fuente El autor

Figura 59. Representación de amenazas sobre activo servicios internos-DHCP



Fuente El autor

Figura 60. Representación de amenazas sobre activo servicios internos-BIOMETRICO

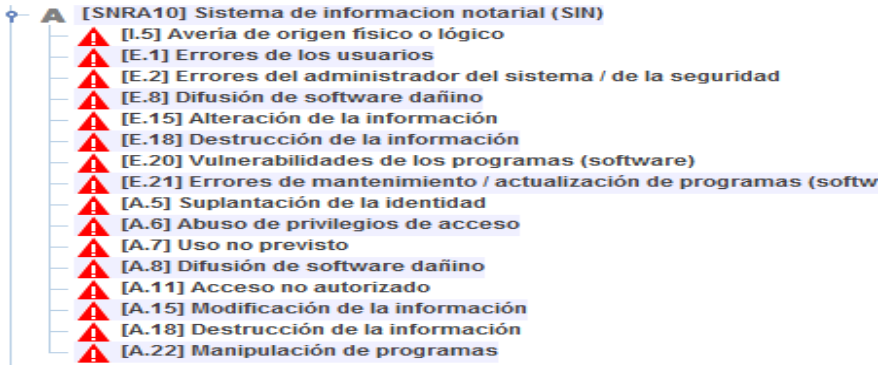


Fuente El autor

3). [E] Equipamientos

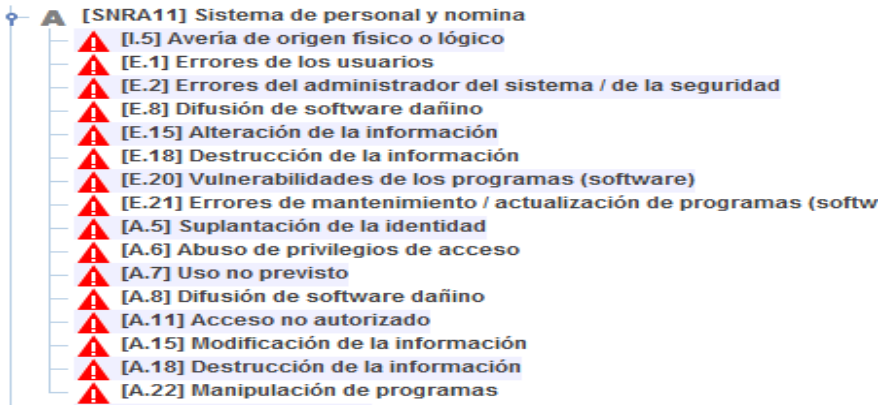
[SW] Aplicaciones

Figura 61. Representación de amenazas sobre activo aplicaciones-sistema de información notarial



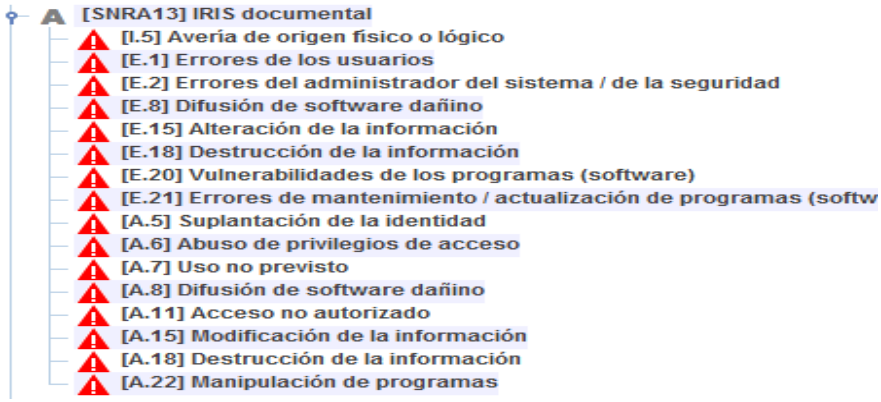
Fuente El autor

Figura 62. Representación de amenazas sobre activo aplicaciones-sistema de personal y nomina



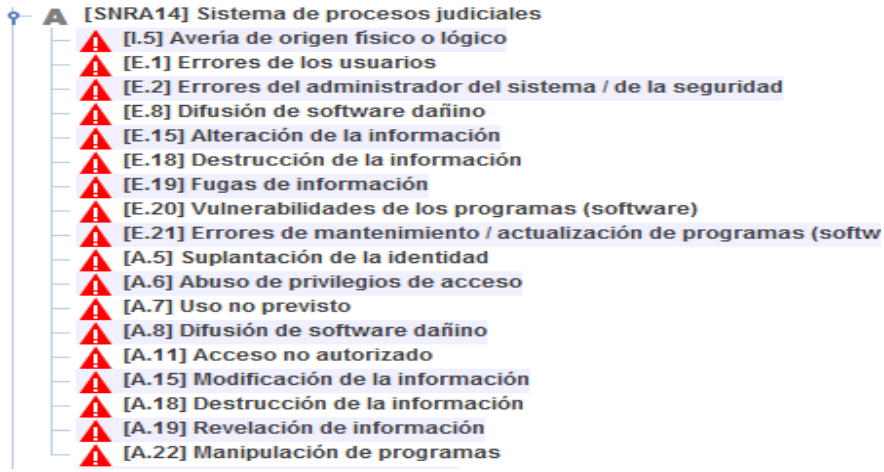
Fuente El autor

Figura 63. Representación de amenazas sobre activo aplicaciones-IRIS documental



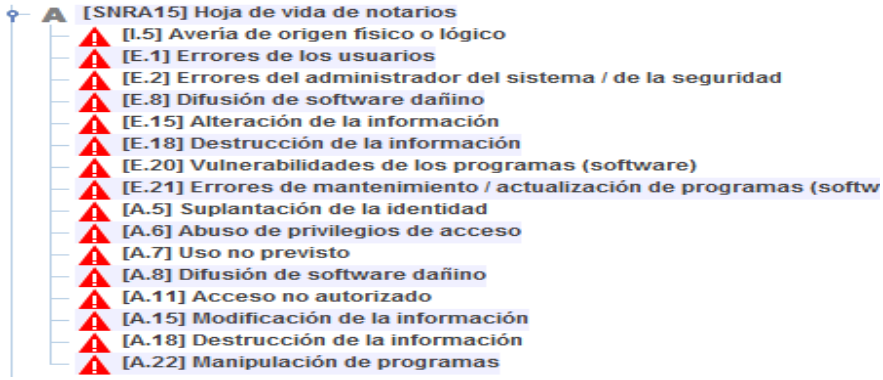
Fuente El autor

Figura 64. Representación de amenazas sobre activo aplicaciones-sistema de procesos judiciales



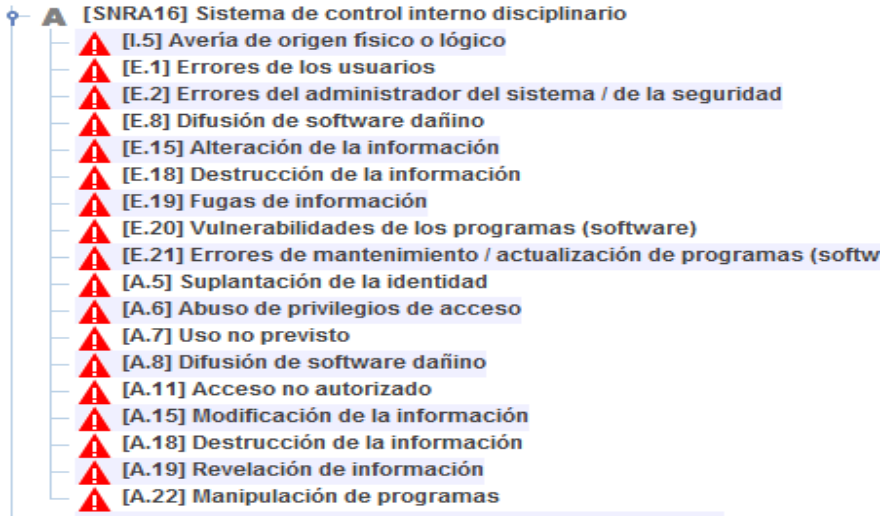
Fuente El autor

Figura 65. Representación de amenazas sobre activo aplicaciones-hoja de vida de notarios



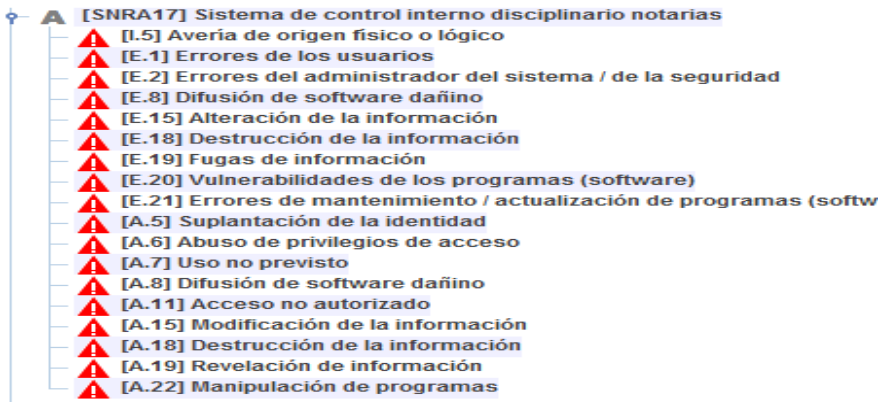
Fuente El autor

Figura 66. Representación de amenazas sobre activo aplicaciones-sistema de control interno disciplinario



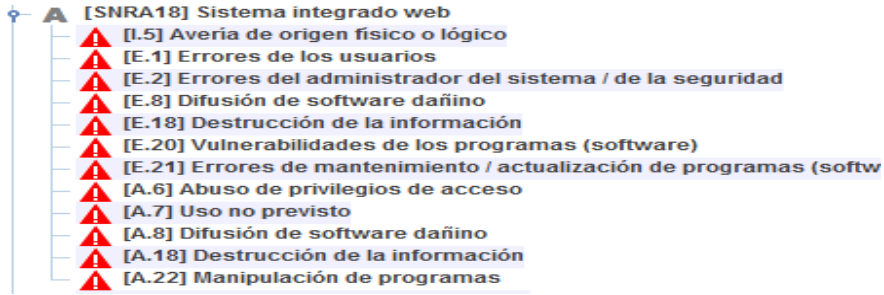
Fuente El autor

Figura 67. Representación de amenazas sobre activo aplicaciones-sistema de control interno disciplinario notarias



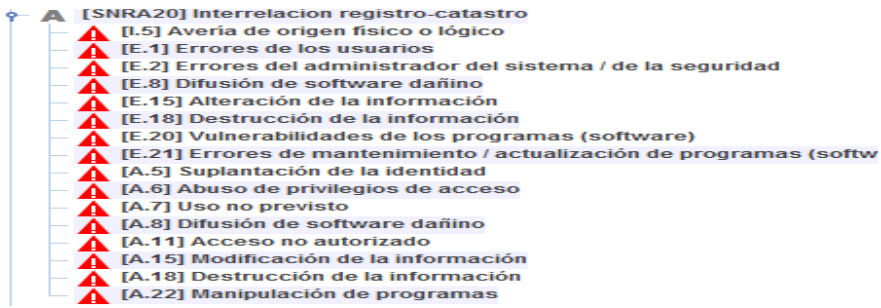
Fuente El autor

Figura 68. Representación de amenazas sobre activo aplicaciones-sistema integrado web



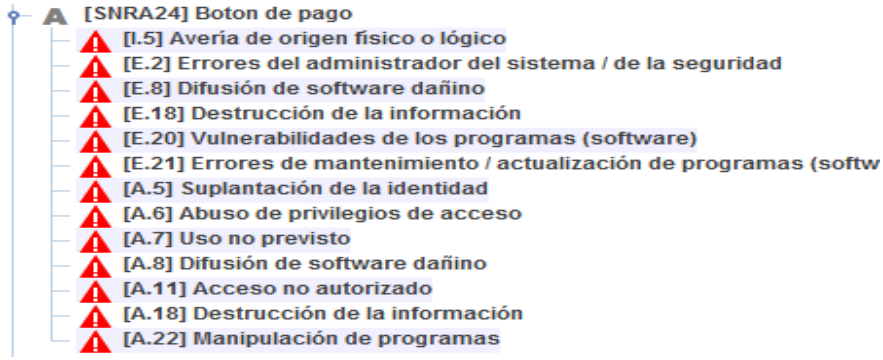
Fuente El autor

Figura 69. Representación de amenazas sobre activo aplicaciones-interrelación registro-catastro



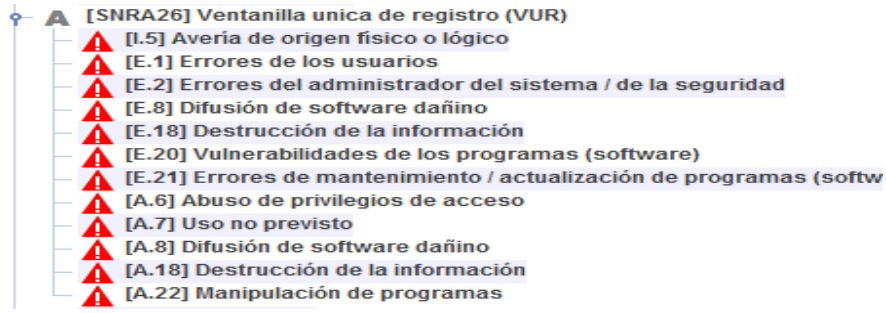
Fuente El autor

Figura 70. Representación de amenazas sobre activo aplicaciones-botón de pago



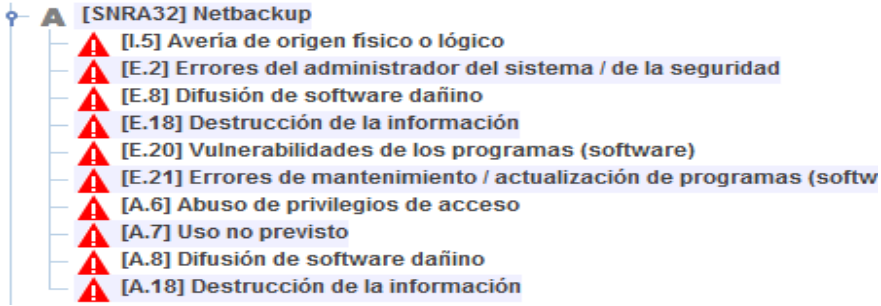
Fuente El autor

Figura 71. Representación de amenazas sobre activo aplicaciones-ventanilla única de registro



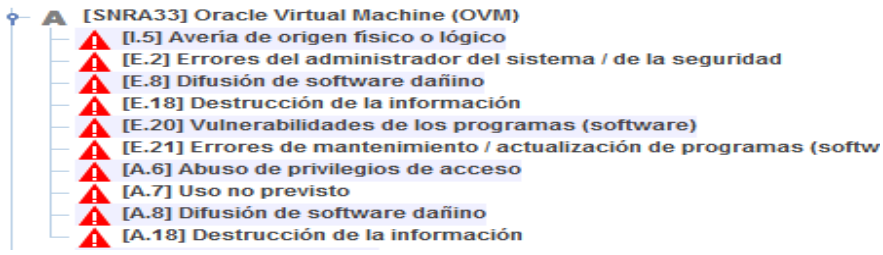
Fuente El autor

Figura 72. Representación de amenazas sobre activo aplicaciones-netbackup



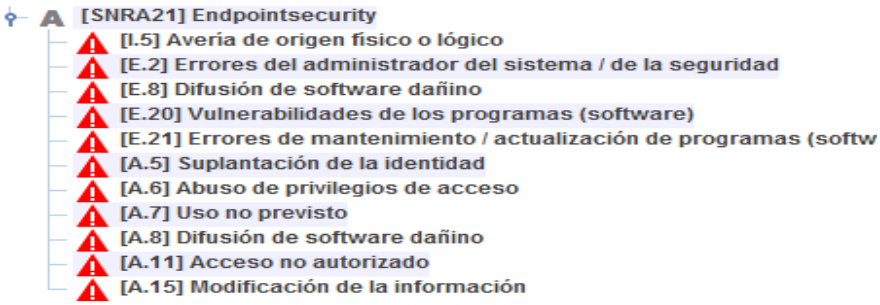
Fuente El autor

Figura 73. Representación de amenazas sobre activo aplicaciones-oracle virtual machine



Fuente El autor

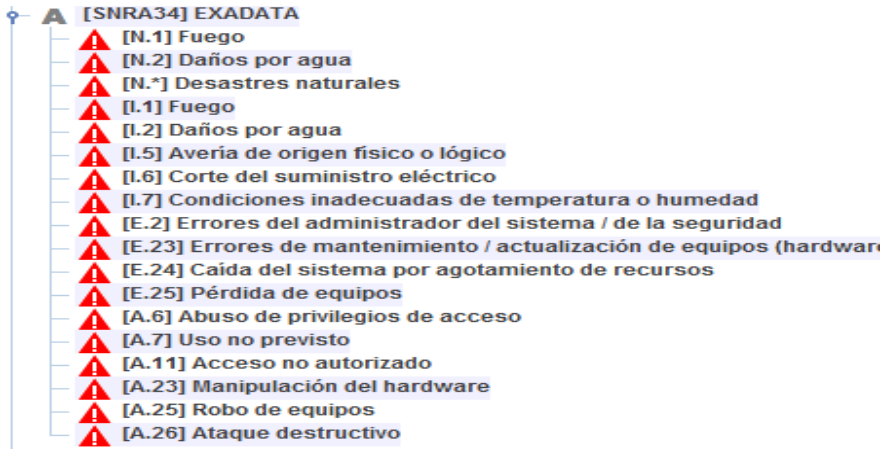
Figura 74. Representación de amenazas sobre activo aplicaciones-endpointsecurity



Fuente El autor

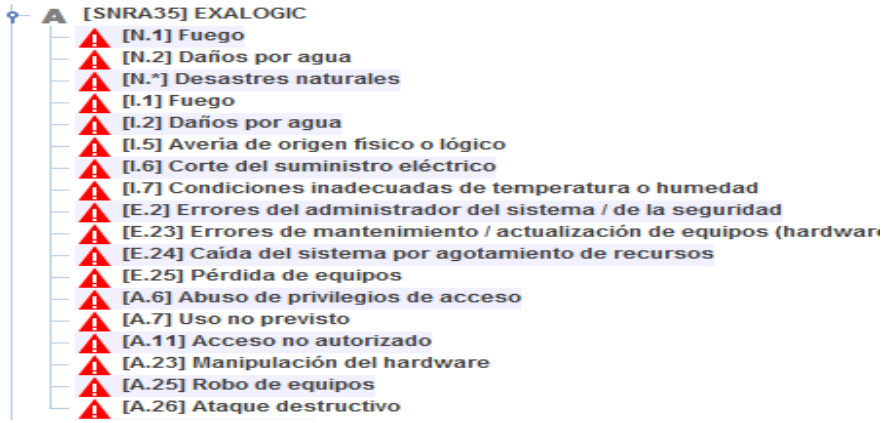
[HW] Equipos

Figura 75. Representación de amenazas sobre activo equipos-exadata



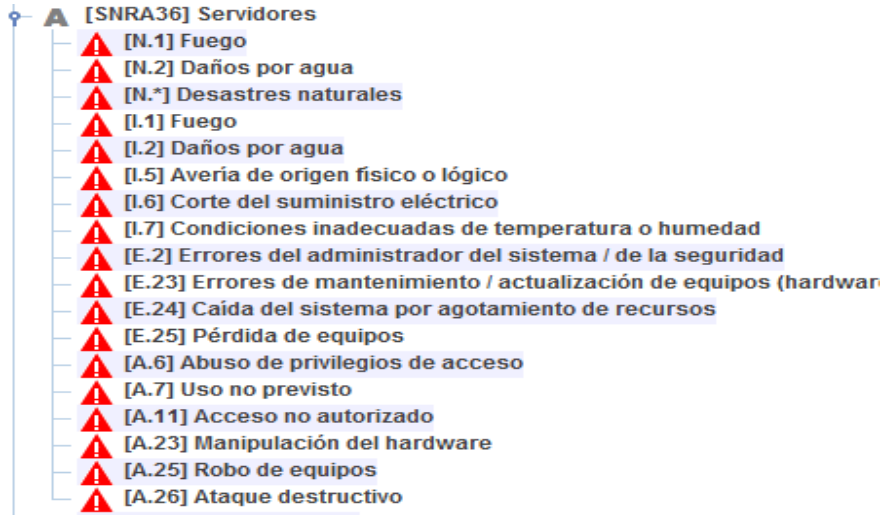
Fuente El autor

Figura 76. Representación de amenazas sobre activo equipos-exalogic



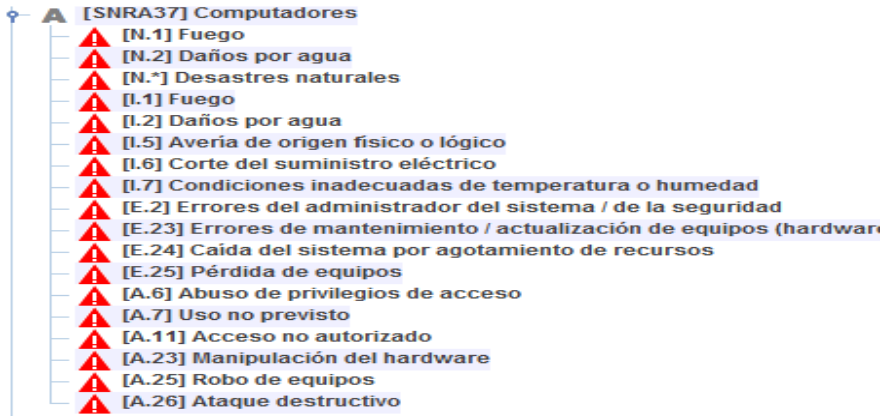
Fuente El autor

Figura 77. Representación de amenazas sobre activo equipos-servidores



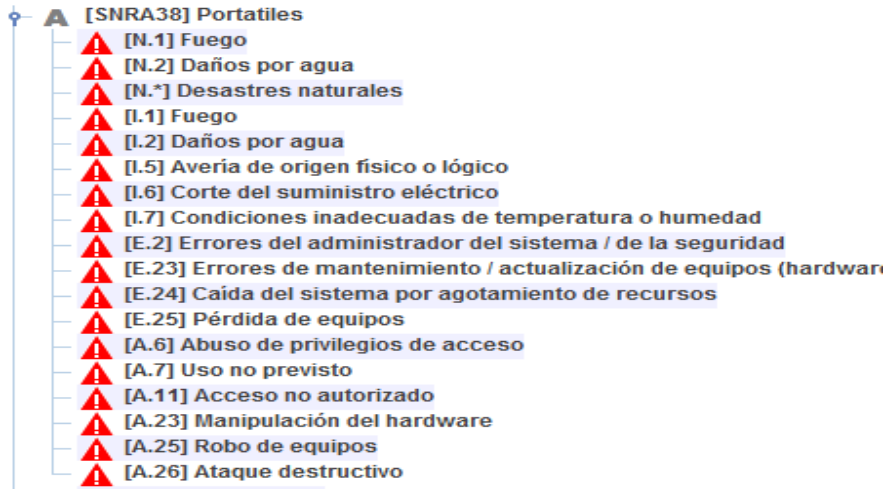
Fuente El autor

Figura 78. Representación de amenazas sobre activo equipos-computadores



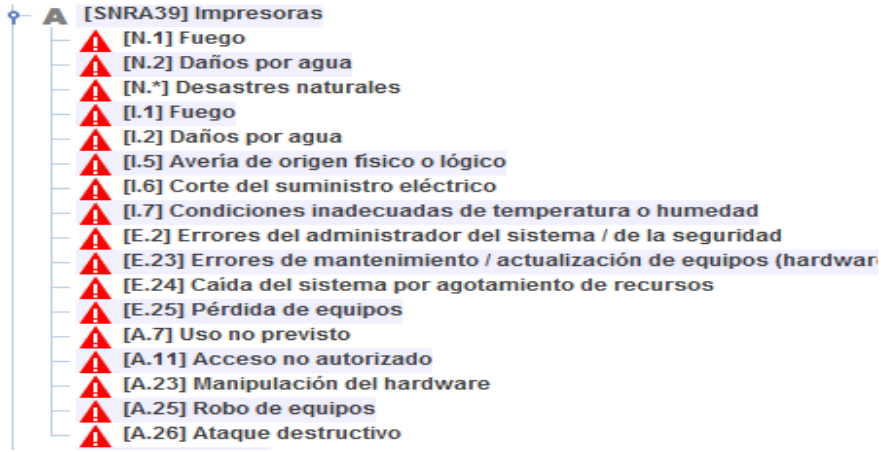
Fuente El autor

Figura 79. Representación de amenazas sobre activo equipos-portátiles



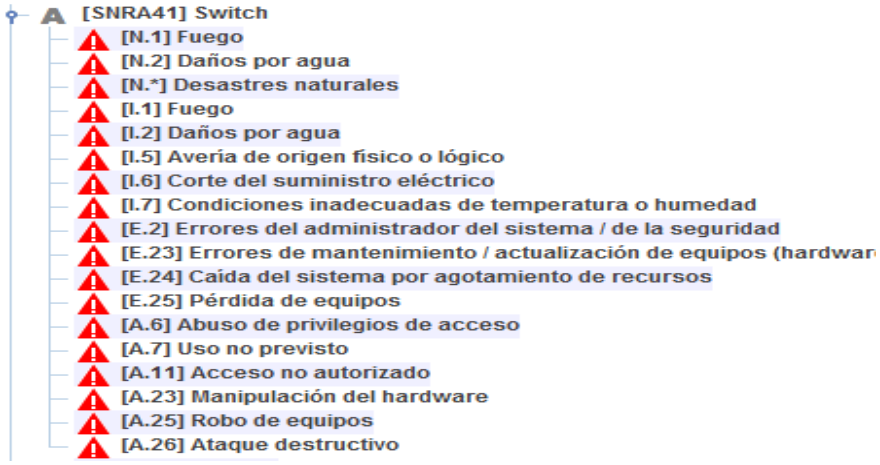
Fuente El autor

Figura 80. Representación de amenazas sobre activo equipos-impresoras



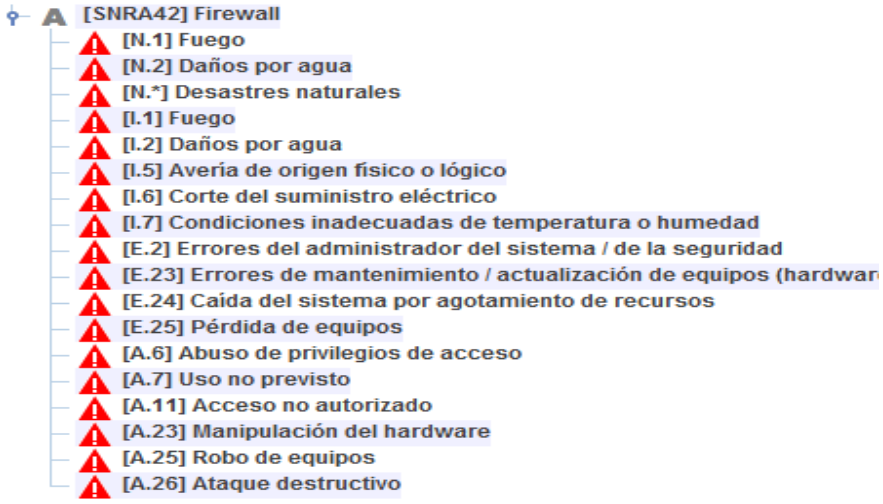
Fuente El autor

Figura 81. Representación de amenazas sobre activo equipos-switch



Fuente El autor

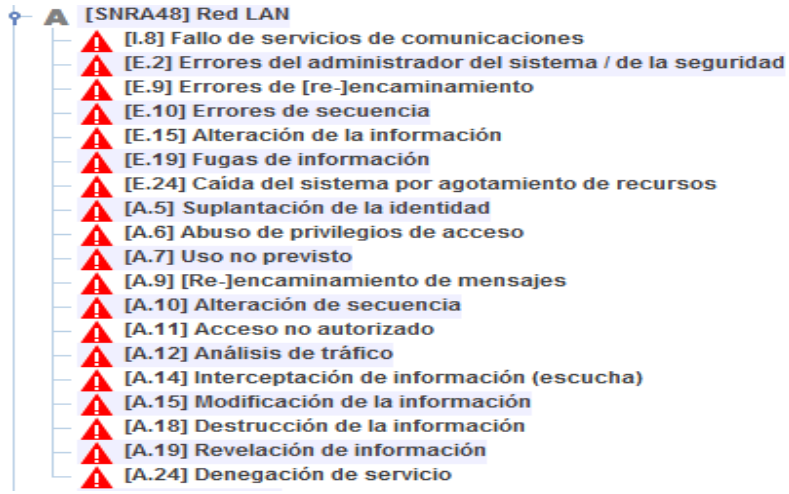
Figura 82. Representación de amenazas sobre activo equipos-firewall



Fuente El autor

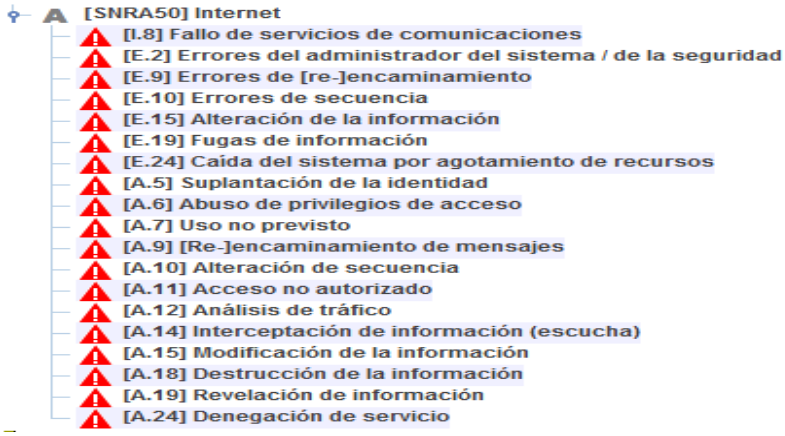
[COM] Comunicaciones

Figura 83. Representación de amenazas sobre activo comunicaciones-red LAN



Fuente El autor

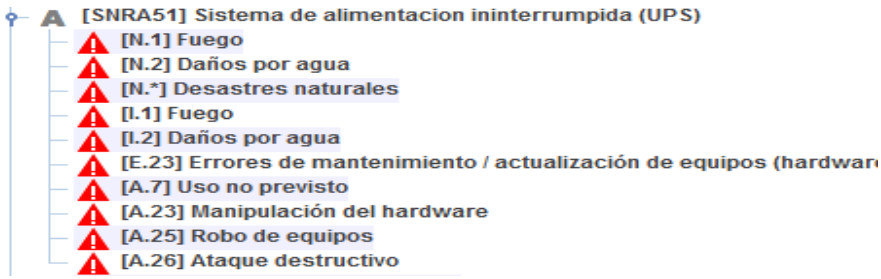
Figura 84. Representación de amenazas sobre activo comunicaciones-Internet



Fuente El autor

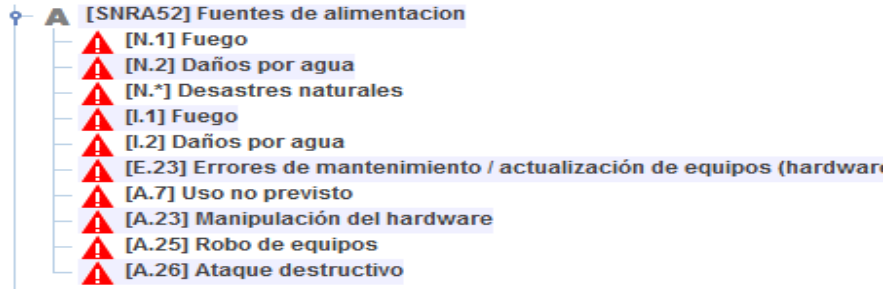
[AUX] Elementos auxiliares

Figura 85. Representación de amenazas sobre activo elementos auxiliares-ups



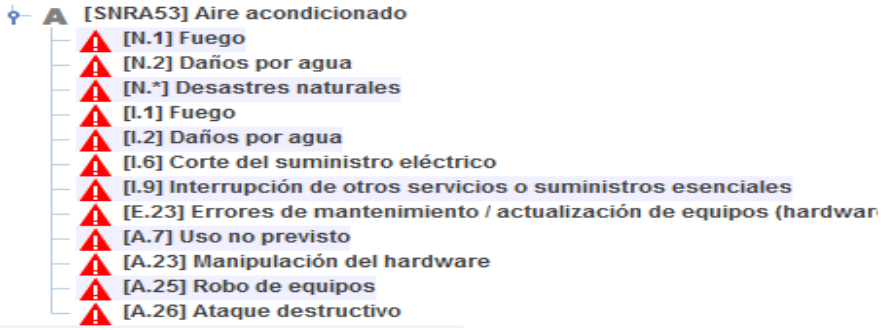
Fuente El autor

Figura 86. Representación de amenazas sobre activo elementos auxiliares-fuentes de alimentación



Fuente El autor

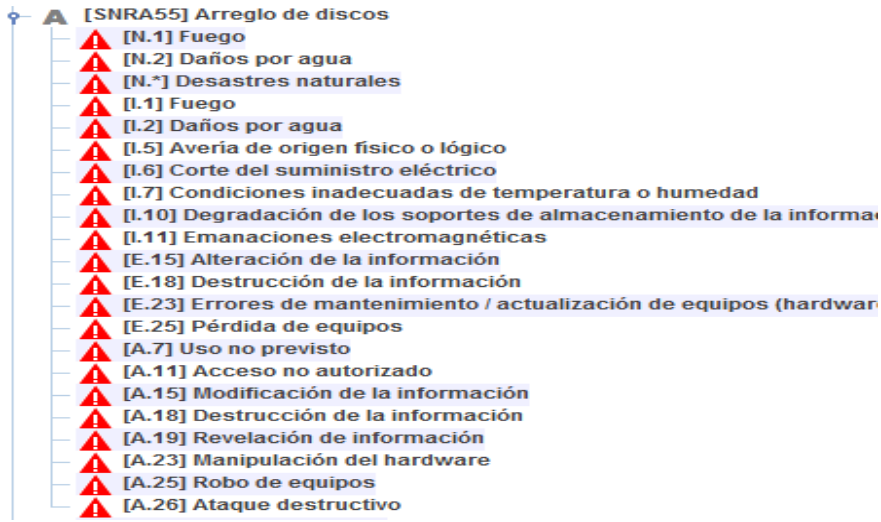
Figura 87. Representación de amenazas sobre activo elementos auxiliares-aire acondicionado



Fuente El autor

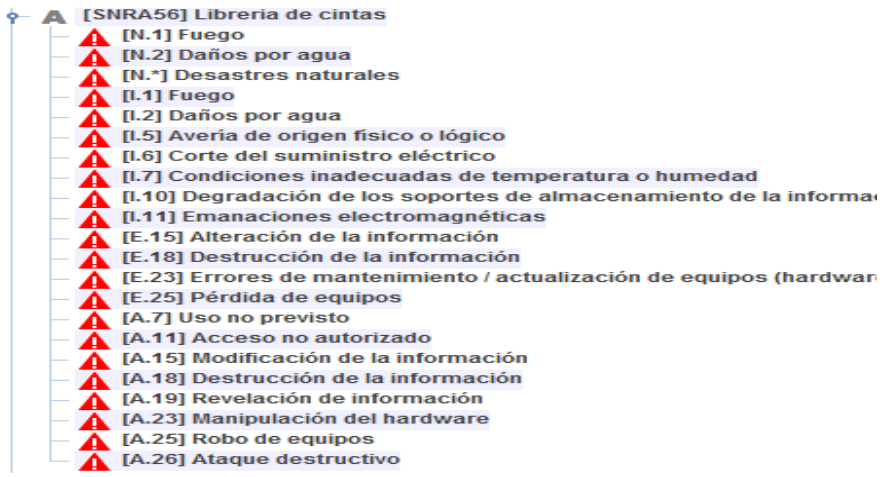
[MEDIA] Soporte de información

Figura 88. Representación de amenazas sobre activo soporte de información-arreglo de discos



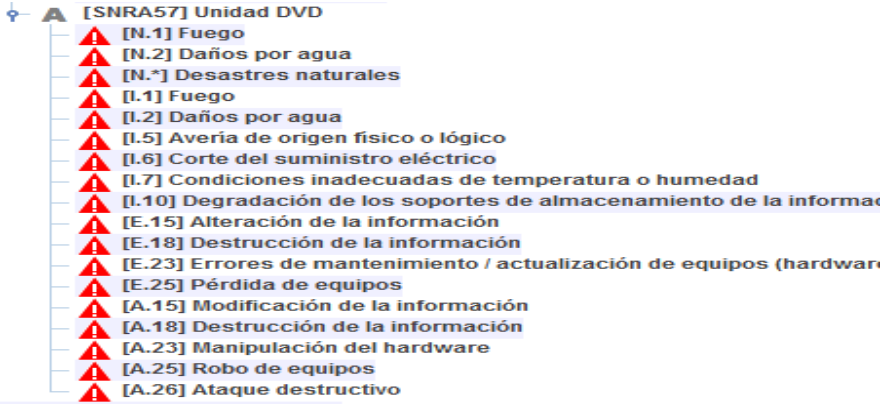
Fuente El autor

Figura 89. Representación de amenazas sobre activo soporte de información - librería de cintas



Fuente El autor

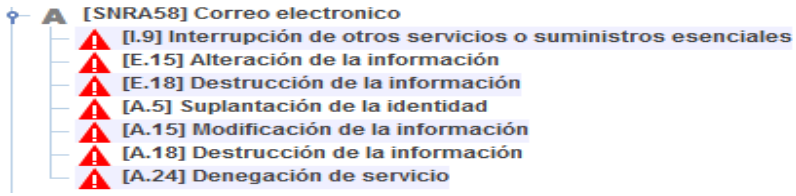
Figura 90. Representación de amenazas sobre activo soporte de información-dvd



Fuente El autor

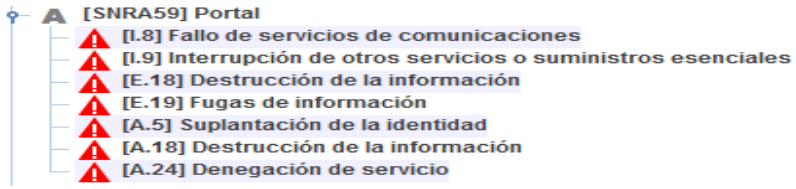
[SS] Servicios subcontratados

Figura 91. Representación de amenazas sobre activo servicios subcontratados-correo electrónico



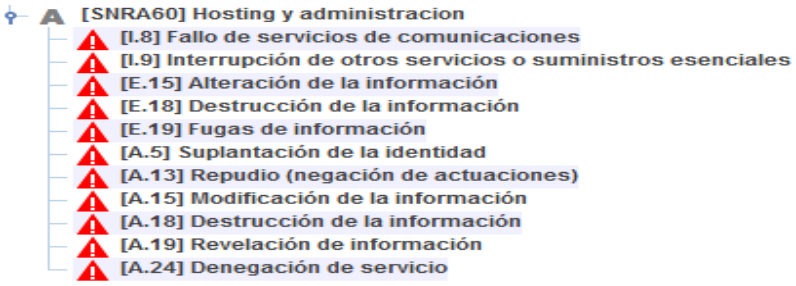
Fuente El autor

Figura 92. Representación de amenazas sobre activo servicios subcontratados-portal



Fuente El autor

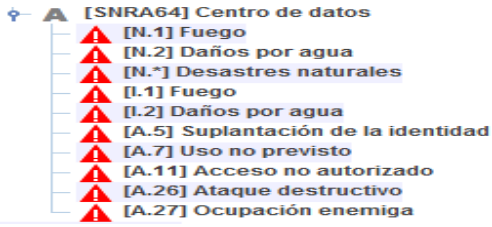
Figura 93. Representación de amenazas sobre activo servicios subcontratados-hosting y administración



Fuente El autor

[L] Instalaciones

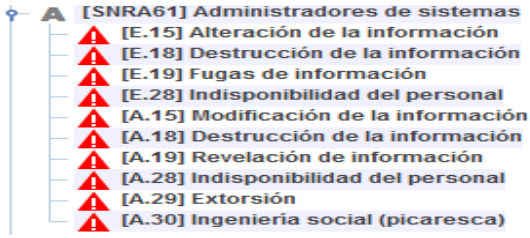
Figura 94. Representación de amenazas sobre activo instalaciones-centro de datos



Fuente El autor

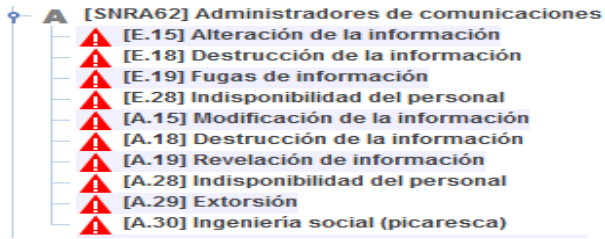
[P] Personal

Figura 95. Representación de amenazas sobre activo personal-administradores de sistemas



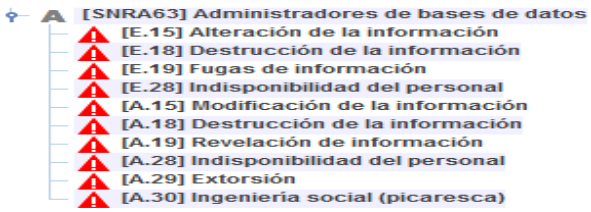
Fuente El autor

Figura 96. Representación de amenazas sobre activo personal-administradores de comunicaciones



Fuente El autor

Figura 97. Representación de amenazas sobre activo personal-administradores de bases de datos



Fuente El autor

Amenazas - Valoración

Descripción parámetros de valoración

Para la valoración de la afectación de las amenazas sobre los activos señalados se describen los siguientes parámetros de valoración:

* Las amenazas fueron establecidas de forma mixta así: Automático Programa PILAR + Asignación Manual. Como se puede apreciar en la convención en color rojo de la primera columna.
* La frecuencia o probabilidad de ocurrencia y materialización de las amenazas sobre los activos se califica de acuerdo a la siguiente escala:

10 - Frecuente (Alta)

1 - Normal (Media)

0.0 - 0.9 - Poco frecuente (Baja)

* Para la valoración de las amenazas sobre las dimensiones de seguridad (D-Disponibilidad, I-Integridad, C-Confidencialidad, A-Autenticación, T-Trazabilidad), es decir la degradación de cada uno de los activos se considera el siguiente rango:

o% - Ninguna

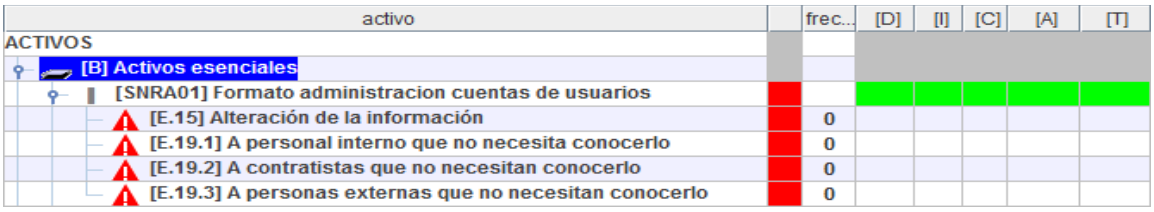
.

.

100% - Máxima

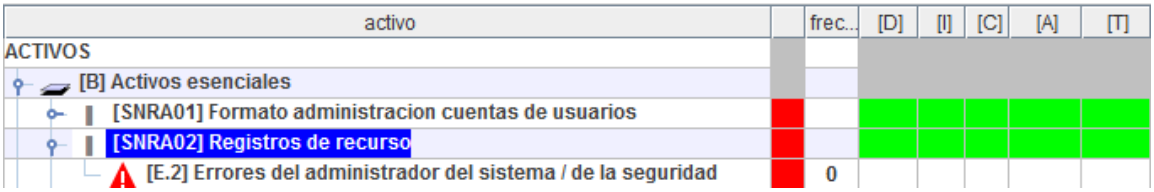
1). [B] Activos esenciales

Figura 98. Representación probabilidad ocurrencia amenazas y degradación sobre activo activos esenciales-formato administración cuentas de usuarios



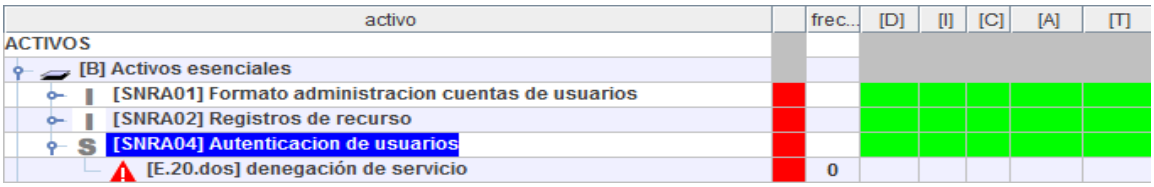
Fuente El autor

Figura 99. Representación probabilidad ocurrencia de amenazas y degradación sobre activo activos esenciales-registros de recurso



Fuente El autor

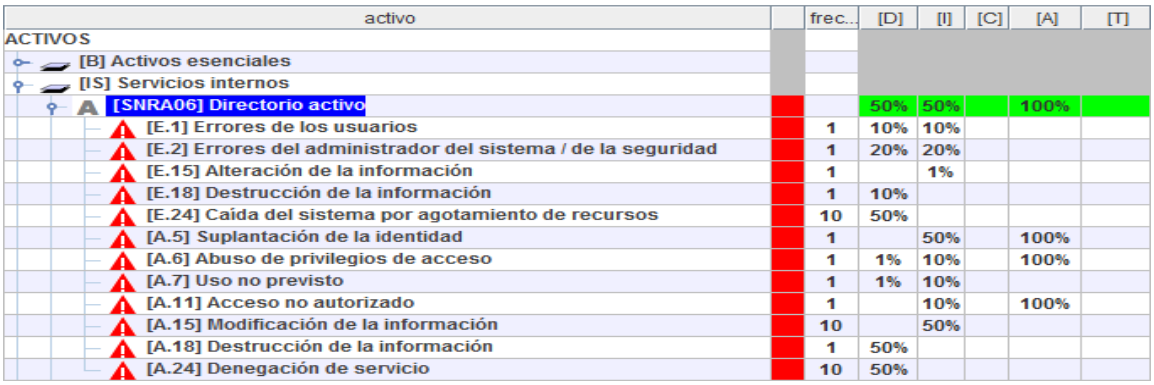
Figura 100. Representación probabilidad ocurrencia de amenazas y degradación sobre activo activos esenciales-autenticación de usuarios



Fuente El autor

2). [IS] Servicios internos

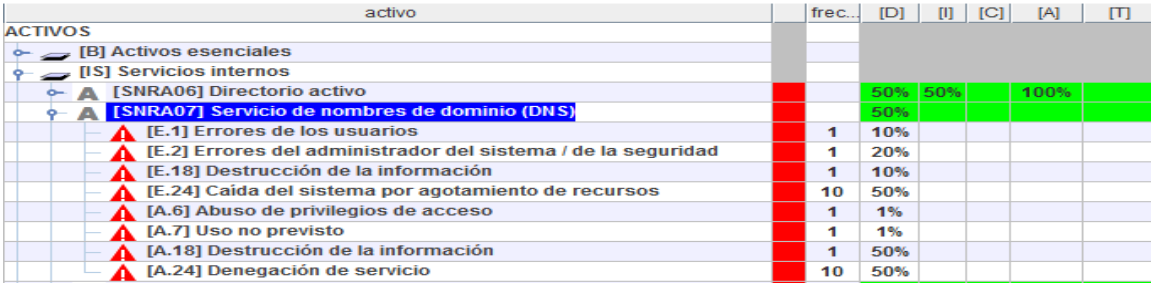
Figura 101. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos-directorio activo



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[SNRA06] Directorio activo			50%	50%		100%	
[E.1] Errores de los usuarios		1	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.5] Suplantación de la identidad		1		50%		100%	
[A.6] Abuso de privilegios de acceso		1	1%	10%		100%	
[A.7] Uso no previsto		1	1%	10%			
[A.11] Acceso no autorizado		1		10%		100%	
[A.15] Modificación de la información		10		50%			
[A.18] Destrucción de la información		1	50%				
[A.24] Denegación de servicio		10	50%				

Fuente El autor

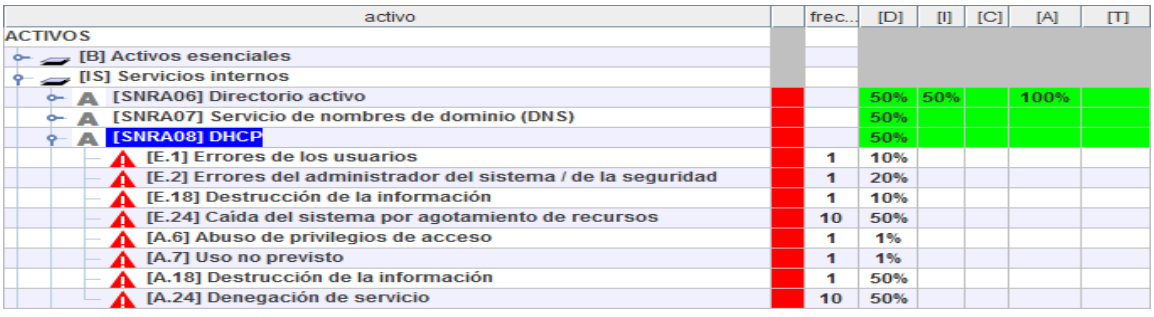
Figura 102. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos-dns



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[SNRA06] Directorio activo			50%	50%		100%	
[SNRA07] Servicio de nombres de dominio (DNS)			50%				
[E.1] Errores de los usuarios		1	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.18] Destrucción de la información		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.18] Destrucción de la información		1	50%				
[A.24] Denegación de servicio		10	50%				

Fuente El autor

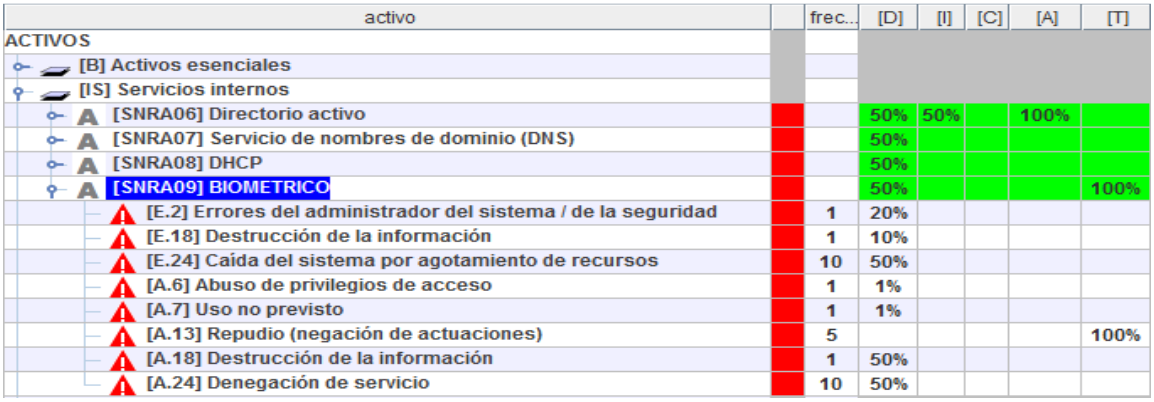
Figura 103. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos - dhcp



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[SNRA06] Directorio activo			50%	50%		100%	
[SNRA07] Servicio de nombres de dominio (DNS)			50%				
[SNRA08] DHCP			50%				
[E.1] Errores de los usuarios		1	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.18] Destrucción de la información		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.18] Destrucción de la información		1	50%				
[A.24] Denegación de servicio		10	50%				

Fuente El autor

Figura 104. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios internos-BIOMETRICO



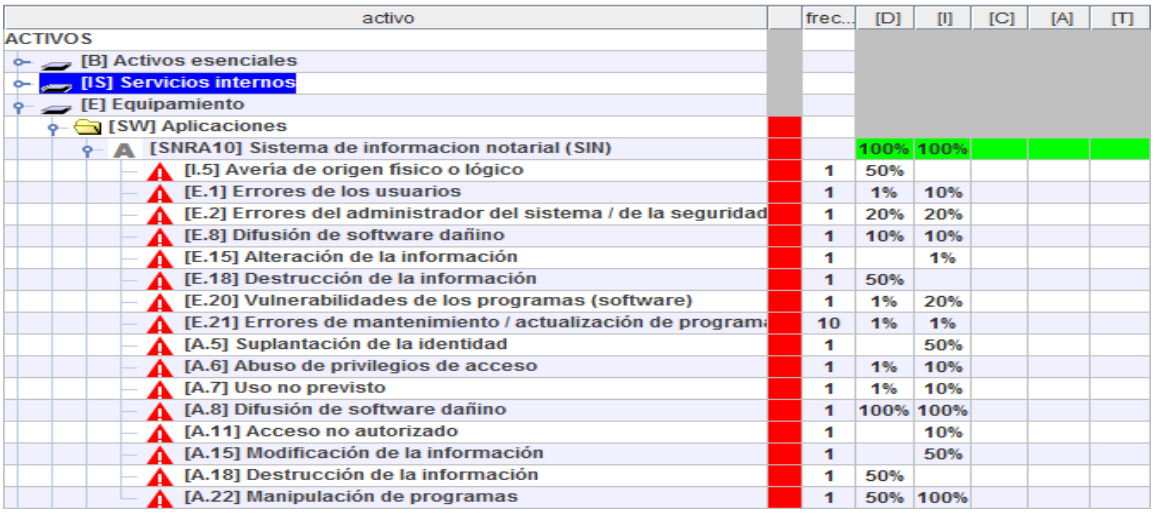
activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[SNRA06] Directorio activo			50%	50%		100%	
[SNRA07] Servicio de nombres de dominio (DNS)			50%				
[SNRA08] DHCP			50%				
[SNRA09] BIOMETRICO			50%				100%
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.18] Destrucción de la información		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.13] Repudio (negación de actuaciones)		5					100%
[A.18] Destrucción de la información		1	50%				
[A.24] Denegación de servicio		10	50%				

Fuente El autor

3). [E] Equipamiento

[SW] Aplicaciones

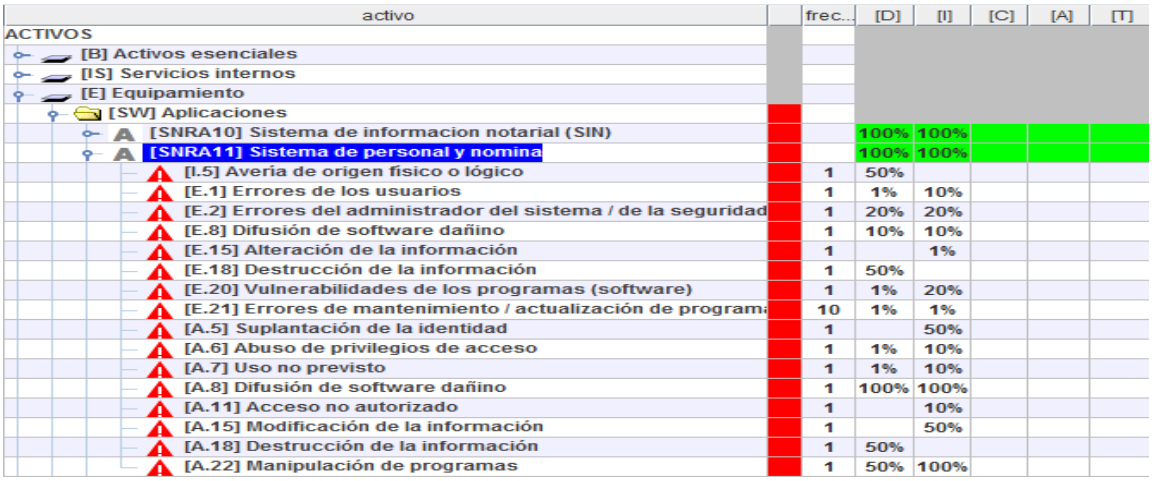
Figura 105. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema de información notarial



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SNRA10] Sistema de informacion notarial (SIN)			100%	100%			
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%			
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%			
[A.6] Abuso de privilegios de acceso		1	1%	10%			
[A.7] Uso no previsto		1	1%	10%			
[A.8] Difusión de software dañino		1	100%	100%			
[A.11] Acceso no autorizado		1		10%			
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%			

Fuente El autor

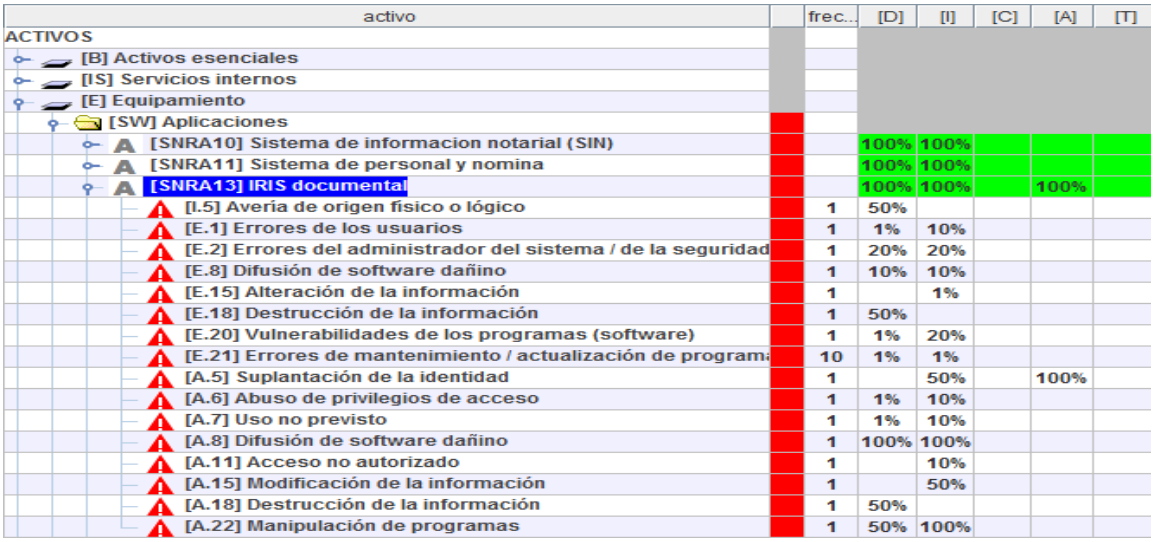
Figura 106. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema de personal y nomina



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SNRA10] Sistema de informacion notarial (SIN)			100%	100%			
[SNRA11] Sistema de personal y nomina			100%	100%			
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%			
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%			
[A.6] Abuso de privilegios de acceso		1	1%	10%			
[A.7] Uso no previsto		1	1%	10%			
[A.8] Difusión de software dañino		1	100%	100%			
[A.11] Acceso no autorizado		1		10%			
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%			

Fuente El autor

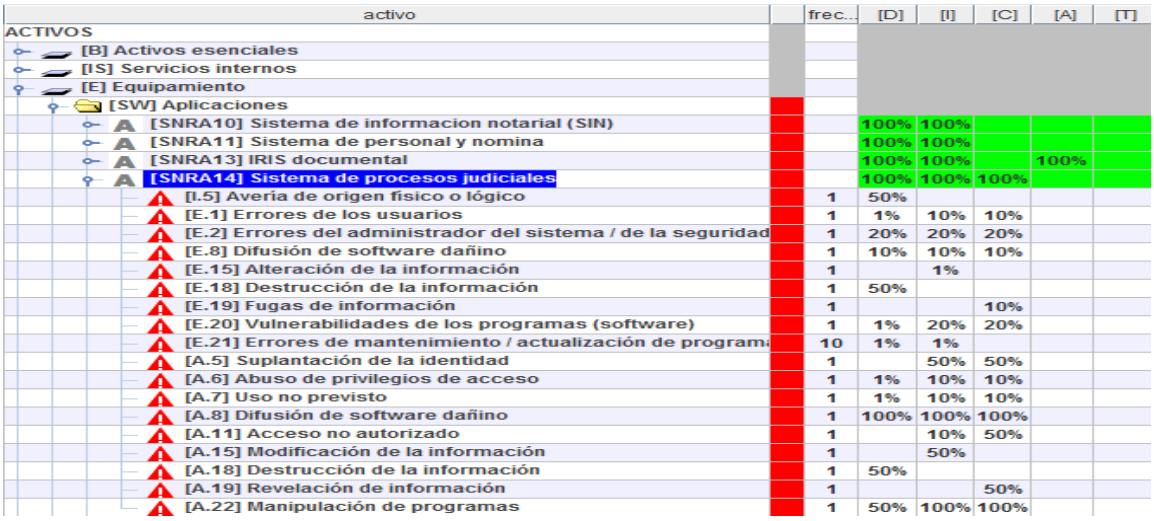
Figura 107. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-IRIS documental



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SNRA10] Sistema de informacion notarial (SIN)			100%	100%			
[SNRA11] Sistema de personal y nomina			100%	100%			
[SNRA13] IRIS documental			100%	100%		100%	
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%			
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%		100%	
[A.6] Abuso de privilegios de acceso		1	1%	10%			
[A.7] Uso no previsto		1	1%	10%			
[A.8] Difusión de software dañino		1	100%	100%			
[A.11] Acceso no autorizado		1		10%			
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%			

Fuente El autor

Figura 108. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema de procesos judiciales



activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SNRA10] Sistema de informacion notarial (SIN)			100%	100%			
[SNRA11] Sistema de personal y nomina			100%	100%			
[SNRA13] IRIS documental			100%	100%		100%	
[SNRA14] Sistema de procesos judiciales			100%	100%	100%		
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de progra		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%	50%		
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%		
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		1		10%	50%		
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.19] Revelación de información		1			50%		
[A.22] Manipulación de programas		1	50%	100%	100%		

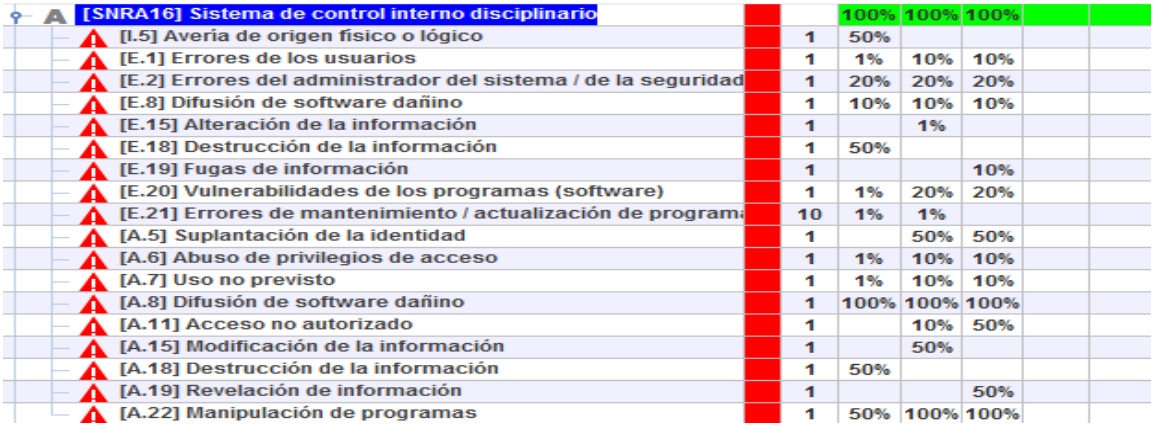
Fuente El autor

Figura 109. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-hoja de vida de notarios

activo		frec...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SNRA10] Sistema de informacion notarial (SIN)			100%	100%			
[SNRA11] Sistema de personal y nomina			100%	100%			
[SNRA13] IRIS documental			100%	100%		100%	
[SNRA14] Sistema de procesos judiciales			100%	100%	100%		
[SNRA15] Hoja de vida de notarios			100%	100%			
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%			
[E.21] Errores de mantenimiento / actualización de progra		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%			
[A.6] Abuso de privilegios de acceso		1	1%	10%			
[A.7] Uso no previsto		1	1%	10%			
[A.8] Difusión de software dañino		1	100%	100%			
[A.11] Acceso no autorizado		1		10%			
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%			

Fuente El autor

Figura 110. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema de control interno disciplinario



[SNRA16] Sistema de control interno disciplinario			100%	100%	100%		
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%	50%		
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%		
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		1		10%	50%		
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.19] Revelación de información		1			50%		
[A.22] Manipulación de programas		1	50%	100%	100%		

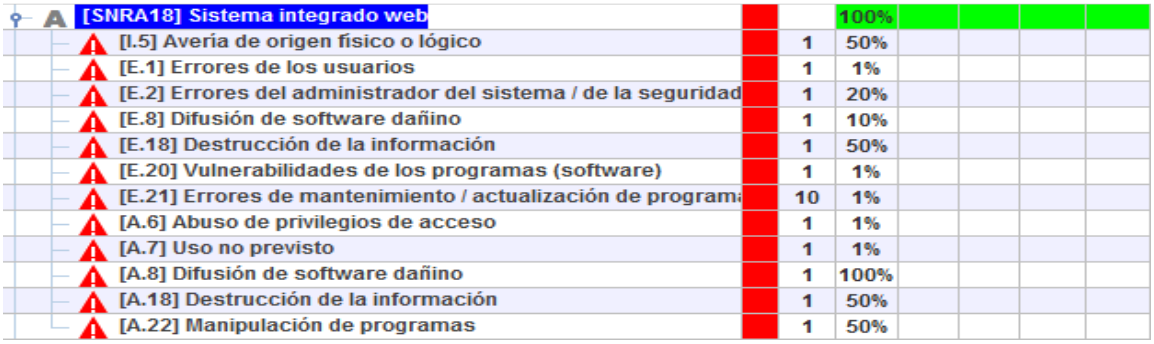
Fuente El autor

Figura 111. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema de control interno disciplinario notarias

[SNRA17] Sistema de control interno disciplinario notarias			100%	100%	100%		
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%	50%		
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%		
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		1		10%	50%		
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.19] Revelación de información		1			50%		
[A.22] Manipulación de programas		1	50%	100%	100%		

Fuente El autor

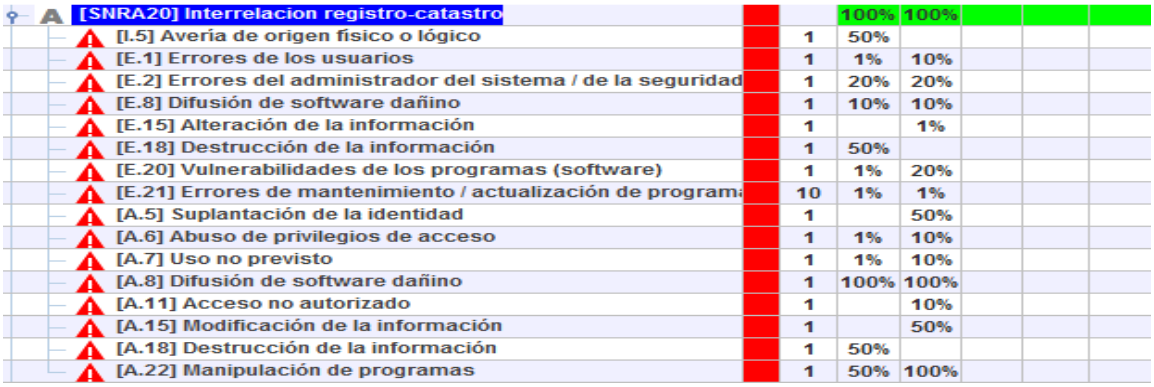
Figura 112. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-sistema integrado web



[SNRA18] Sistema integrado web			100%				
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.8] Difusión de software dañino		1	10%				
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%				
[E.21] Errores de mantenimiento / actualización de programa		10	1%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.8] Difusión de software dañino		1	100%				
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%				

Fuente El autor

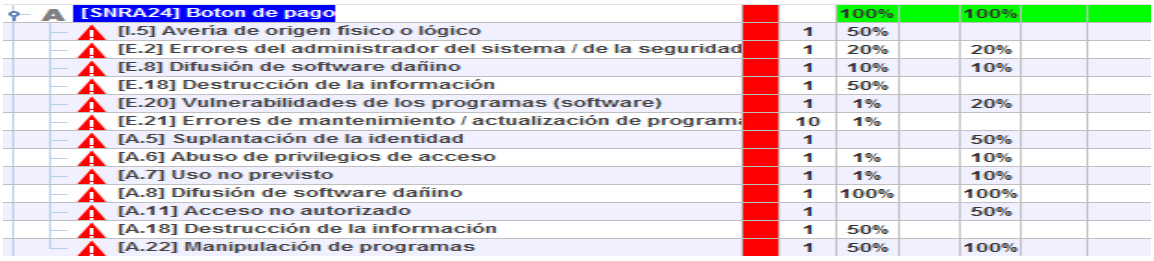
Figura 113. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-interrelación registro-catastro



[SNRA20] Interrelacion registro-catastro			100%	100%			
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%			
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%			
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%			
[A.6] Abuso de privilegios de acceso		1	1%	10%			
[A.7] Uso no previsto		1	1%	10%			
[A.8] Difusión de software dañino		1	100%	100%			
[A.11] Acceso no autorizado		1		10%			
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%			

Fuente El autor

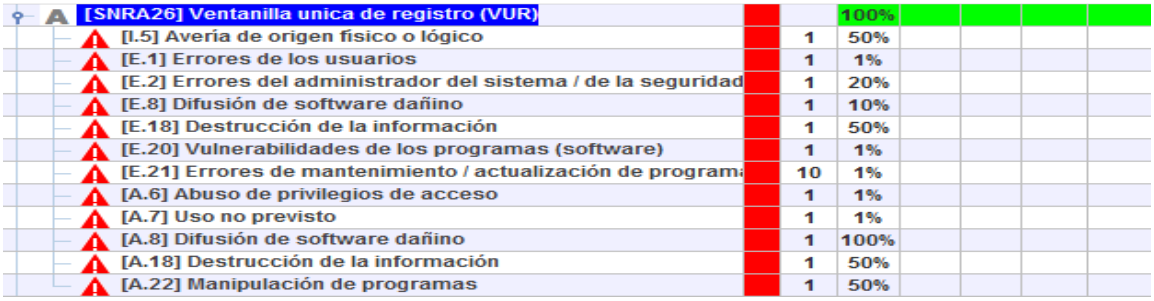
Figura 114. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-botón de pago



[SNRA24] Boton de pago			100%		100%		
[I.5] Avería de origen físico o lógico		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%		20%		
[E.8] Difusión de software dañino		1	10%		10%		
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%		
[E.21] Errores de mantenimiento / actualización de programa		10	1%				
[A.5] Suplantación de la identidad		1			50%		
[A.6] Abuso de privilegios de acceso		1	1%		10%		
[A.7] Uso no previsto		1	1%		10%		
[A.8] Difusión de software dañino		1	100%		100%		
[A.11] Acceso no autorizado		1			50%		
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%		100%		

Fuente El autor

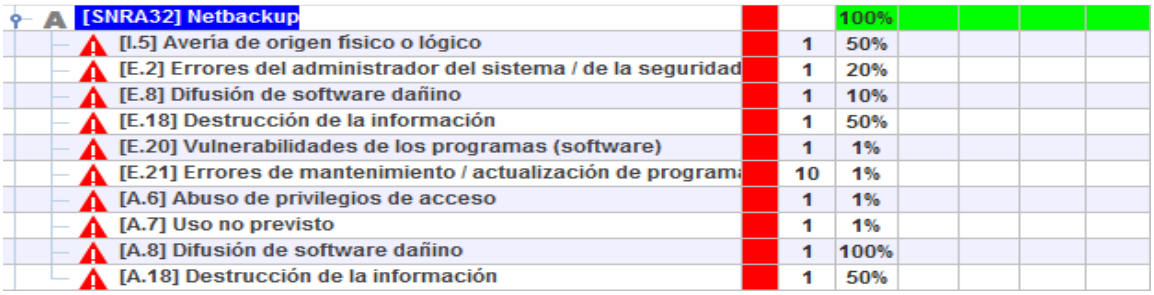
Figura 115. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-ventanilla única de registro



[SNRA26] Ventanilla unica de registro (VUR)			100%				
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	1%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.8] Difusión de software dañino		1	10%				
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%				
[E.21] Errores de mantenimiento / actualización de programa		10	1%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.8] Difusión de software dañino		1	100%				
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%				

Fuente El autor

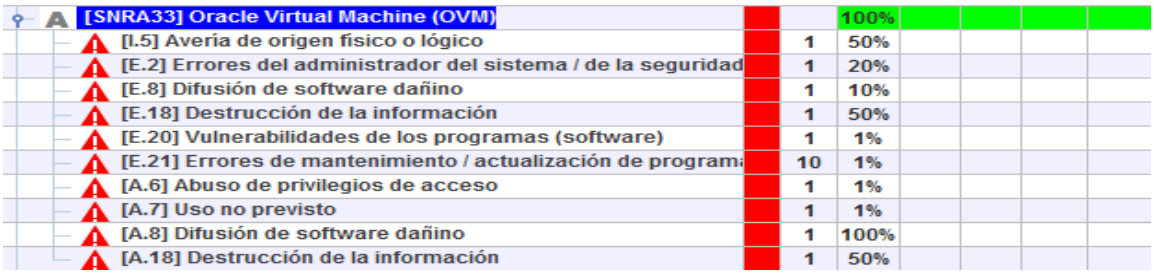
Figura 116. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-netbackup



[SNRA32] Netbackup			100%				
[I.5] Avería de origen físico o lógico		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.8] Difusión de software dañino		1	10%				
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%				
[E.21] Errores de mantenimiento / actualización de programa		10	1%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.8] Difusión de software dañino		1	100%				
[A.18] Destrucción de la información		1	50%				

Fuente El autor

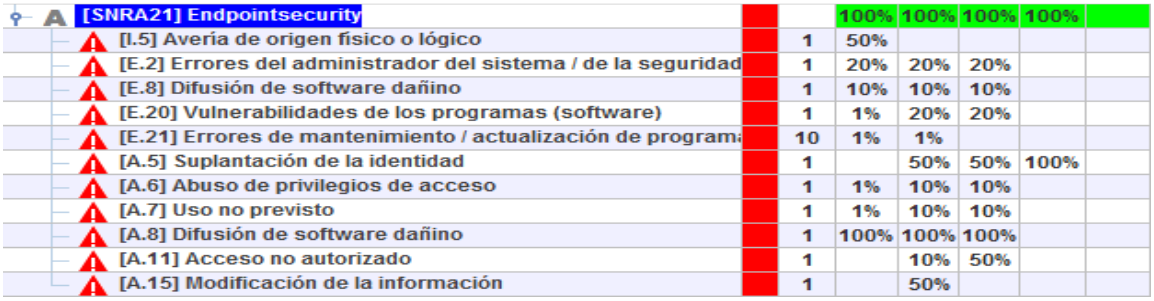
Figura 117. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-oracle virtual machine



[SNRA33] Oracle Virtual Machine (OVM)			100%				
[I.5] Avería de origen físico o lógico		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.8] Difusión de software dañino		1	10%				
[E.18] Destrucción de la información		1	50%				
[E.20] Vulnerabilidades de los programas (software)		1	1%				
[E.21] Errores de mantenimiento / actualización de programa		10	1%				
[A.6] Abuso de privilegios de acceso		1	1%				
[A.7] Uso no previsto		1	1%				
[A.8] Difusión de software dañino		1	100%				
[A.18] Destrucción de la información		1	50%				

Fuente El autor

Figura 118. Representación probabilidad ocurrencia de amenazas y degradación sobre activo aplicaciones-endpointsecurity

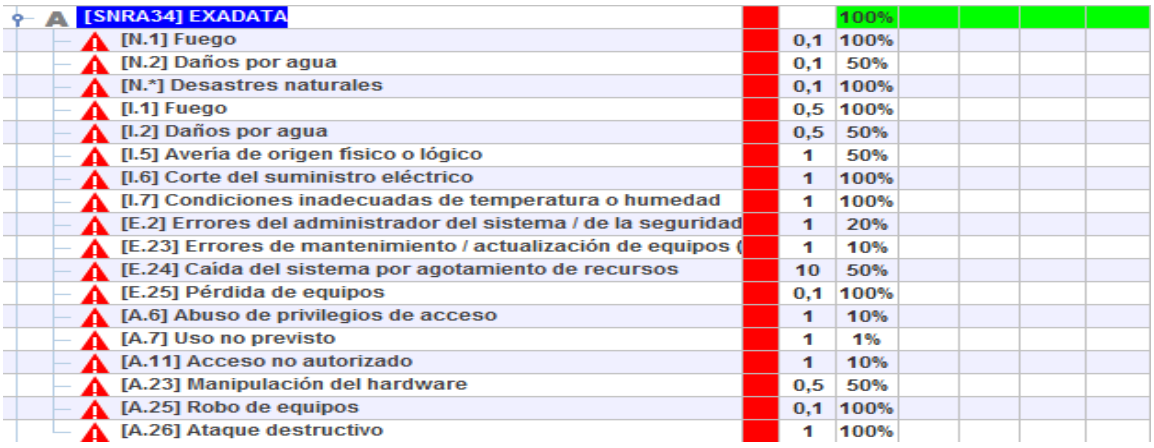


[SNRA21] Endpointsecurity			100%	100%	100%	100%	
[I.5] Avería de origen físico o lógico		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programa		10	1%	1%			
[A.5] Suplantación de la identidad		1		50%	50%	100%	
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%		
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		1		10%	50%		
[A.15] Modificación de la información		1		50%			

Fuente El autor

[HW] Equipos

Figura 119. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-exadata



[SNRA34] EXADATA			100%				
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.5] Avería de origen físico o lógico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%				
[E.23] Errores de mantenimiento / actualización de equipos (		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		0,1	100%				
[A.6] Abuso de privilegios de acceso		1	10%				
[A.7] Uso no previsto		1	1%				
[A.11] Acceso no autorizado		1	10%				
[A.23] Manipulación del hardware		0,5	50%				
[A.25] Robo de equipos		0,1	100%				
[A.26] Ataque destructivo		1	100%				

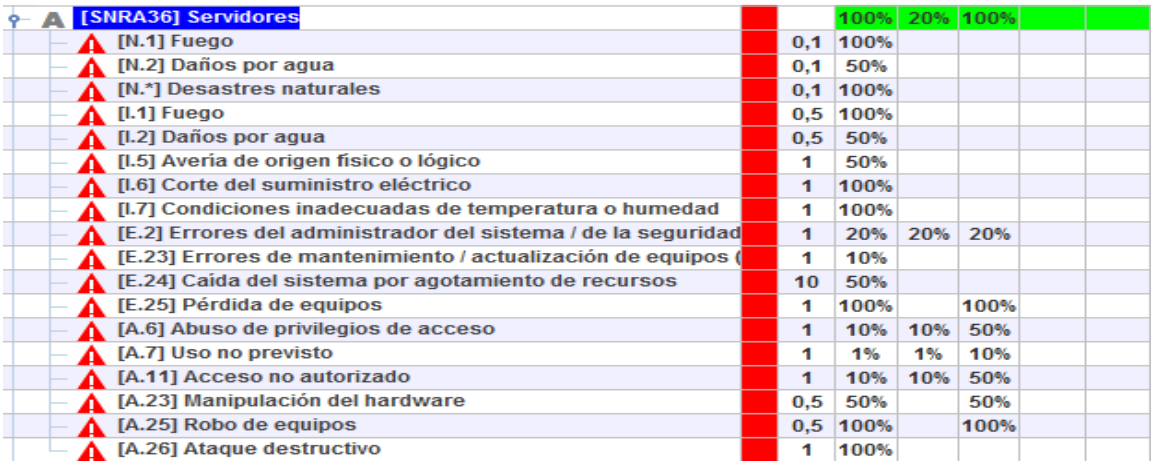
Fuente El autor

Figura 120. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-exalogic

[SNRA35] EXALOGIC		100%				
[N.1] Fuego	0,1	100%				
[N.2] Daños por agua	0,1	50%				
[N.*] Desastres naturales	0,1	100%				
[I.1] Fuego	0,5	100%				
[I.2] Daños por agua	0,5	50%				
[I.5] Avería de origen físico o lógico	1	50%				
[I.6] Corte del suministro eléctrico	1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%				
[E.2] Errores del administrador del sistema / de la seguridad	1	20%				
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%				
[E.24] Caída del sistema por agotamiento de recursos	10	50%				
[E.25] Pérdida de equipos	0,1	100%				
[A.6] Abuso de privilegios de acceso	1	10%				
[A.7] Uso no previsto	1	1%				
[A.11] Acceso no autorizado	1	10%				
[A.23] Manipulación del hardware	0,5	50%				
[A.25] Robo de equipos	0,1	100%				
[A.26] Ataque destructivo	1	100%				

Fuente El autor

Figura 121. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-servidores



[SNRA36] Servidores		100%	20%	100%		
[N.1] Fuego	0,1	100%				
[N.2] Daños por agua	0,1	50%				
[N.*] Desastres naturales	0,1	100%				
[I.1] Fuego	0,5	100%				
[I.2] Daños por agua	0,5	50%				
[I.5] Avería de origen físico o lógico	1	50%				
[I.6] Corte del suministro eléctrico	1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%				
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%				
[E.24] Caída del sistema por agotamiento de recursos	10	50%				
[E.25] Pérdida de equipos	1	100%		100%		
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%		
[A.7] Uso no previsto	1	1%	1%	10%		
[A.11] Acceso no autorizado	1	10%	10%	50%		
[A.23] Manipulación del hardware	0,5	50%		50%		
[A.25] Robo de equipos	0,5	100%		100%		
[A.26] Ataque destructivo	1	100%				

Fuente El autor

Figura 122. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-computadores

[SNRA37] Computadores		100%
[N.1] Fuego	0,1	100%
[N.2] Daños por agua	0,1	50%
[N.*] Desastres naturales	0,1	100%
[I.1] Fuego	0,5	100%
[I.2] Daños por agua	0,5	50%
[I.5] Avería de origen físico o lógico	1	50%
[I.6] Corte del suministro eléctrico	1	100%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%
[E.24] Caída del sistema por agotamiento de recursos	10	50%
[E.25] Pérdida de equipos	5	5%
[A.6] Abuso de privilegios de acceso	1	10%
[A.7] Uso no previsto	1	10%
[A.11] Acceso no autorizado	1	10%
[A.23] Manipulación del hardware	0,5	50%
[A.25] Robo de equipos	5	5%
[A.26] Ataque destructivo	1	100%

Fuente El autor

Figura 123. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-portátiles

[SNRA38] Portatiles		100%
[N.1] Fuego	0,1	100%
[N.2] Daños por agua	0,1	50%
[N.*] Desastres naturales	0,1	100%
[I.1] Fuego	0,5	100%
[I.2] Daños por agua	0,5	50%
[I.5] Avería de origen físico o lógico	1	50%
[I.6] Corte del suministro eléctrico	1	100%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%
[E.24] Caída del sistema por agotamiento de recursos	10	50%
[E.25] Pérdida de equipos	20	1%
[A.6] Abuso de privilegios de acceso	1	10%
[A.7] Uso no previsto	1	5%
[A.11] Acceso no autorizado	1	10%
[A.23] Manipulación del hardware	0,5	50%
[A.25] Robo de equipos	20	1%
[A.26] Ataque destructivo	1	100%

Fuente El autor

Figura 124. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-impresoras

[SNRA39] Impresoras		100%
[N.1] Fuego	0,1	100%
[N.2] Daños por agua	0,1	50%
[N.*] Desastres naturales	0,1	100%
[I.1] Fuego	0,5	100%
[I.2] Daños por agua	0,5	50%
[I.5] Avería de origen físico o lógico	1	50%
[I.6] Corte del suministro eléctrico	1	100%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%
[E.24] Caída del sistema por agotamiento de recursos	10	50%
[E.25] Pérdida de equipos	1	100%
[A.7] Uso no previsto	1	10%
[A.11] Acceso no autorizado	1	10%
[A.23] Manipulación del hardware	0,5	50%
[A.25] Robo de equipos	0,5	100%
[A.26] Ataque destructivo	1	100%

Fuente El autor

Figura 125. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-switch

[SNRA41] Switch		100%
[N.1] Fuego	0,1	100%
[N.2] Daños por agua	0,1	50%
[N.*] Desastres naturales	0,1	100%
[I.1] Fuego	0,5	100%
[I.2] Daños por agua	0,5	50%
[I.5] Avería de origen físico o lógico	1	50%
[I.6] Corte del suministro eléctrico	1	100%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
[E.2] Errores del administrador del sistema / de la seguridad	1	20%
[E.23] Errores de mantenimiento / actualización de equipos (	1	10%
[E.24] Caída del sistema por agotamiento de recursos	10	50%
[E.25] Pérdida de equipos	1	20%
[A.6] Abuso de privilegios de acceso	1	10%
[A.7] Uso no previsto	1	10%
[A.11] Acceso no autorizado	1	10%
[A.23] Manipulación del hardware	0,5	100%
[A.25] Robo de equipos	0,5	20%
[A.26] Ataque destructivo	1	100%

Fuente El autor

Figura 126. Representación probabilidad ocurrencia de amenazas y degradación sobre activo equipos-firewall

[SNRA42] Firewall			100%	20%			
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.5] Avería de origen físico o lógico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%			
[E.23] Errores de mantenimiento / actualización de equipos (		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	20%				
[A.6] Abuso de privilegios de acceso		1	10%	10%			
[A.7] Uso no previsto		1	10%	1%			
[A.11] Acceso no autorizado		1	10%	10%			
[A.23] Manipulación del hardware		0,5	100%				
[A.25] Robo de equipos		0,5	20%				
[A.26] Ataque destructivo		1	100%				

Fuente El autor

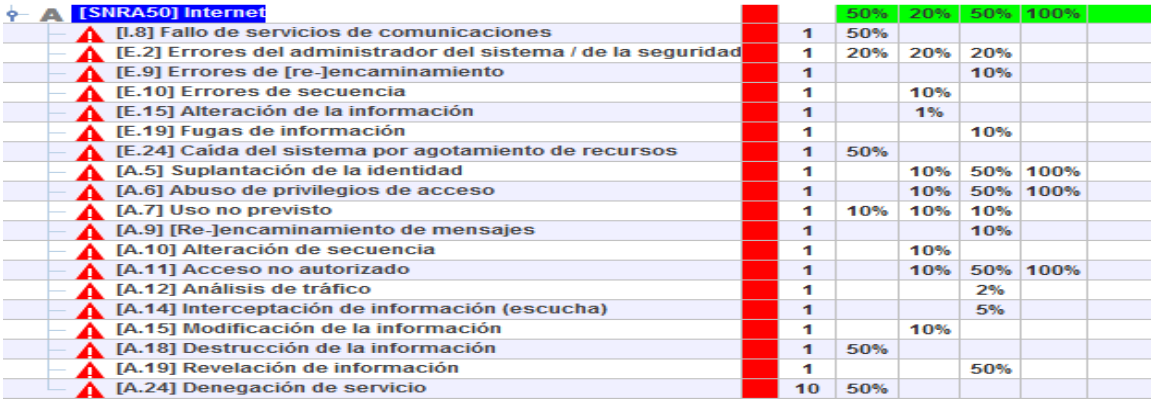
[COM] Comunicaciones

Figura 127. Representación probabilidad ocurrencia de amenazas y degradación sobre activo comunicaciones-red LAN

[SNRA48] Red LAN			50%	20%	50%	100%	
[I.8] Fallo de servicios de comunicaciones		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.9] Errores de [re-]encaminamiento		1			10%		
[E.10] Errores de secuencia		1		10%			
[E.15] Alteración de la información		1		1%			
[E.19] Fugas de información		1			10%		
[E.24] Caída del sistema por agotamiento de recursos		1	50%				
[A.5] Suplantación de la identidad		1		10%	50%	100%	
[A.6] Abuso de privilegios de acceso		1		10%	50%	100%	
[A.7] Uso no previsto		1	10%	10%	10%		
[A.9] [Re-]encaminamiento de mensajes		1			10%		
[A.10] Alteración de secuencia		1		10%			
[A.11] Acceso no autorizado		1		10%	50%	100%	
[A.12] Análisis de tráfico		1			2%		
[A.14] Interceptación de información (escucha)		1			1%		
[A.15] Modificación de la información		1		10%			
[A.18] Destrucción de la información		1	50%				
[A.19] Revelación de información		1			50%		
[A.24] Denegación de servicio		10	50%				

Fuente El autor

Figura 128. Representación probabilidad ocurrencia de amenazas y degradación sobre activo comunicaciones-Internet

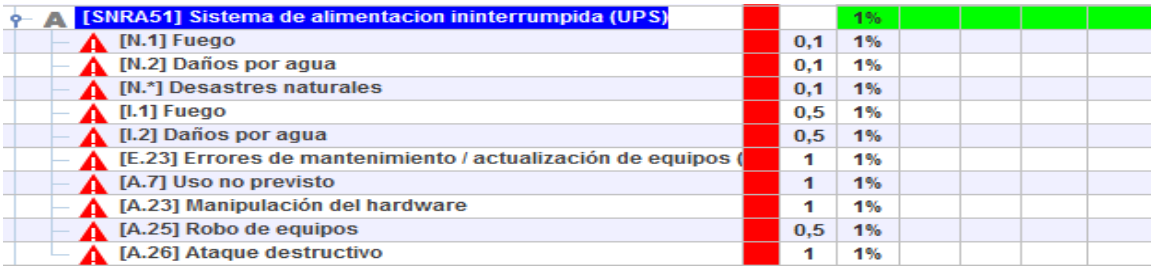


[SNRA50] Internet			50%	20%	50%	100%	
[I.8] Fallo de servicios de comunicaciones		1	50%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.9] Errores de [re-]encaminamiento		1			10%		
[E.10] Errores de secuencia		1		10%			
[E.15] Alteración de la información		1		1%			
[E.19] Fugas de información		1			10%		
[E.24] Caída del sistema por agotamiento de recursos		1	50%				
[A.5] Suplantación de la identidad		1		10%	50%	100%	
[A.6] Abuso de privilegios de acceso		1		10%	50%	100%	
[A.7] Uso no previsto		1	10%	10%	10%		
[A.9] [Re-]encaminamiento de mensajes		1			10%		
[A.10] Alteración de secuencia		1		10%			
[A.11] Acceso no autorizado		1		10%	50%	100%	
[A.12] Análisis de tráfico		1			2%		
[A.14] Interceptación de información (escucha)		1			5%		
[A.15] Modificación de la información		1		10%			
[A.18] Destrucción de la información		1	50%				
[A.19] Revelación de información		1			50%		
[A.24] Denegación de servicio		10	50%				

Fuente El autor

[AUX] Elementos auxiliares

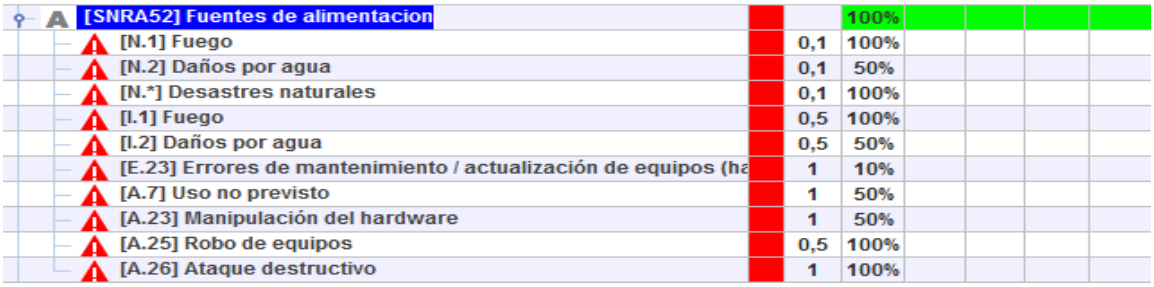
Figura 129. Representación probabilidad ocurrencia de amenazas y degradación sobre activo elementos auxiliares-ups



[SNRA51] Sistema de alimentacion ininterrumpida (UPS)			1%				
[N.1] Fuego		0,1	1%				
[N.2] Daños por agua		0,1	1%				
[N.*] Desastres naturales		0,1	1%				
[I.1] Fuego		0,5	1%				
[I.2] Daños por agua		0,5	1%				
[E.23] Errores de mantenimiento / actualización de equipos (		1	1%				
[A.7] Uso no previsto		1	1%				
[A.23] Manipulación del hardware		1	1%				
[A.25] Robo de equipos		0,5	1%				
[A.26] Ataque destructivo		1	1%				

Fuente El autor

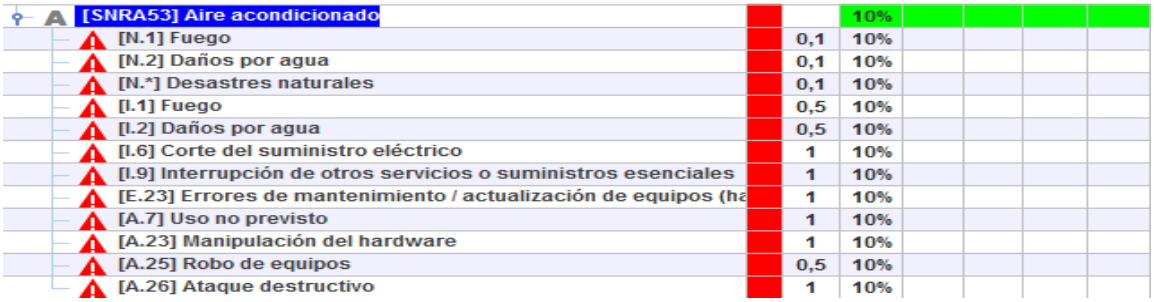
Figura 130. Representación probabilidad de ocurrencia de amenazas y degradación sobre activo elementos auxiliares-fuentes de alimentación



[SNRA52] Fuentes de alimentacion			100%				
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[E.23] Errores de mantenimiento / actualización de equipos (ha		1	10%				
[A.7] Uso no previsto		1	50%				
[A.23] Manipulación del hardware		1	50%				
[A.25] Robo de equipos		0,5	100%				
[A.26] Ataque destructivo		1	100%				

Fuente El autor

Figura 131. Representación probabilidad de ocurrencia de amenazas y degradación sobre activo elementos auxiliares-aire acondicionado



[SNRA53] Aire acondicionado		10%				
[N.1] Fuego	0,1	10%				
[N.2] Daños por agua	0,1	10%				
[N.*] Desastres naturales	0,1	10%				
[I.1] Fuego	0,5	10%				
[I.2] Daños por agua	0,5	10%				
[I.6] Corte del suministro eléctrico	1	10%				
[I.9] Interrupción de otros servicios o suministros esenciales	1	10%				
[E.23] Errores de mantenimiento / actualización de equipos (ha	1	10%				
[A.7] Uso no previsto	1	10%				
[A.23] Manipulación del hardware	1	10%				
[A.25] Robo de equipos	0,5	10%				
[A.26] Ataque destructivo	1	10%				

Fuente El autor

[MEDIA] Soporte de información

Figura 132. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información-arreglo de discos

[SNRA55] Arreglo de discos		100%	100%	100%		
[N.1] Fuego	0,1	100%				
[N.2] Daños por agua	0,1	50%				
[N.*] Desastres naturales	0,1	100%				
[I.1] Fuego	0,5	100%				
[I.2] Daños por agua	0,5	50%				
[I.5] Avería de origen físico o lógico	1	50%				
[I.6] Corte del suministro eléctrico	1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%				
[I.10] Degradación de los soportes de almacenamiento de la	1	100%				
[I.11] Emanaciones electromagnéticas	1			1%		
[E.15] Alteración de la información	1		1%			
[E.18] Destrucción de la información	1	100%				
[E.23] Errores de mantenimiento / actualización de equipos (	1	100%				
[E.25] Pérdida de equipos	1	10%		50%		
[A.7] Uso no previsto	1	1%		1%		
[A.11] Acceso no autorizado	1		1%	50%		
[A.15] Modificación de la información	5		100%			
[A.18] Destrucción de la información	1	100%				
[A.19] Revelación de información	1			10%		
[A.23] Manipulación del hardware	0,1	50%		50%		
[A.25] Robo de equipos	1	10%		100%		
[A.26] Ataque destructivo	1	10%				

Fuente El autor

Figura 133. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información - librería de cintas

[SNRA56] Libreria de cintas			100%	100%	100%		
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.5] Avería de origen físico o lógico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.10] Degradación de los soportes de almacenamiento de la		1	100%				
[I.11] Emanaciones electromagnéticas		1			1%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	100%				
[E.23] Errores de mantenimiento / actualización de equipos (		1	100%				
[E.25] Pérdida de equipos		1	10%		50%		
[A.7] Uso no previsto		1	1%		1%		
[A.11] Acceso no autorizado		1		1%	50%		
[A.15] Modificación de la información		5		100%			
[A.18] Destrucción de la información		1	100%				
[A.19] Revelación de información		1			10%		
[A.23] Manipulación del hardware		0,1	50%		50%		
[A.25] Robo de equipos		1	10%		100%		
[A.26] Ataque destructivo		1	10%				

Fuente El autor

Figura 134. Representación probabilidad ocurrencia de amenazas y degradación sobre activo soporte de información-dvd

[SNRA57] Unidad DVD			100%	100%			
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.5] Avería de origen físico o lógico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.10] Degradación de los soportes de almacenamiento de la in		1	100%				
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	100%				
[E.23] Errores de mantenimiento / actualización de equipos (ha		1	100%				
[E.25] Pérdida de equipos		1	10%				
[A.15] Modificación de la información		5		100%			
[A.18] Destrucción de la información		1	100%				
[A.23] Manipulación del hardware		0,1	50%				
[A.25] Robo de equipos		1	10%				
[A.26] Ataque destructivo		1	10%				

Fuente El autor

4). [SS] Servicios subcontratados

Figura 135. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados-correo electrónico

[SNRA58] Correo electronico		50%	100%		100%	
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%				
[E.15] Alteración de la información	1		10%			
[E.18] Destrucción de la información	1	10%				
[A.5] Suplantación de la identidad	0,2		100%		100%	
[A.15] Modificación de la información	1		50%			
[A.18] Destrucción de la información	1	50%				
[A.24] Denegación de servicio	1	50%				

Fuente El autor

Figura 136. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados-portal

[SNRA59] Portal		100%		100%		
[I.8] Fallo de servicios de comunicaciones	1	100%				
[I.9] Interrupción de otros servicios o suministros esenciales	0	50%				
[E.18] Destrucción de la información	1	10%				
[E.19] Fugas de información	1			10%		
[A.5] Suplantación de la identidad	0,2			100%		
[A.18] Destrucción de la información	1	50%				
[A.24] Denegación de servicio	1	50%				

Fuente El autor

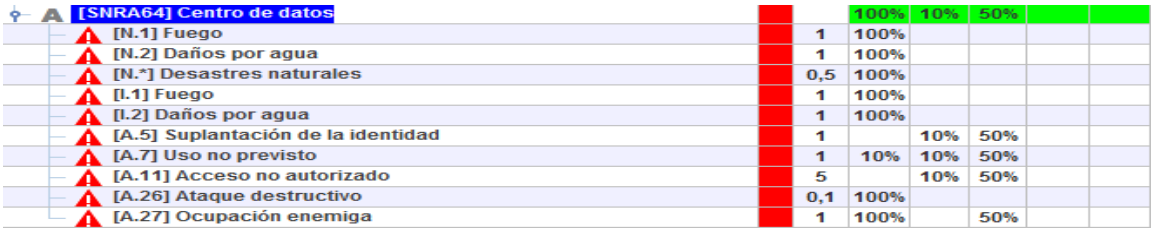
Figura 137. Representación probabilidad ocurrencia de amenazas y degradación sobre activo servicios subcontratados-hosting y administración

[SNRA60] Hosting y administracion		100%	100%	100%	100%	100%
[I.8] Fallo de servicios de comunicaciones	1	100%				
[I.9] Interrupción de otros servicios o suministros esenciales	0	50%				
[E.15] Alteración de la información	1		10%			
[E.18] Destrucción de la información	1	10%				
[E.19] Fugas de información	1			10%		
[A.5] Suplantación de la identidad	0,2		100%	100%	100%	
[A.13] Repudio (negación de actuaciones)	1					100%
[A.15] Modificación de la información	1		50%			
[A.18] Destrucción de la información	1	50%				
[A.19] Revelación de información	1			50%		
[A.24] Denegación de servicio	1	50%				

Fuente El autor

[L] Instalaciones

Figura 138. Representación probabilidad ocurrencia de amenazas y degradación sobre activo instalaciones-centro de datos

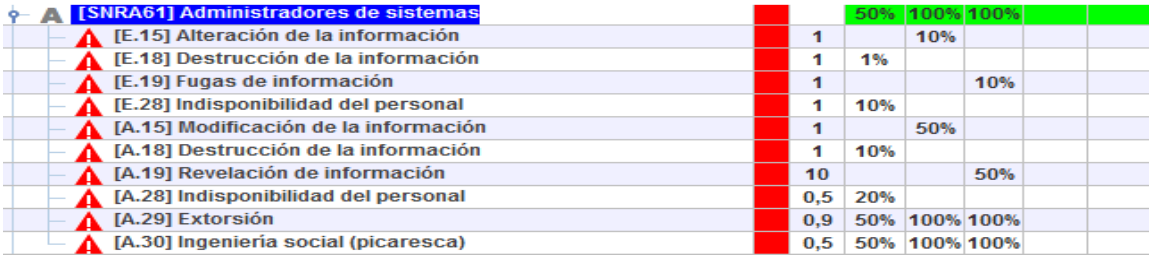


[SNRA64] Centro de datos			100%	10%	50%		
[N.1] Fuego		1	100%				
[N.2] Daños por agua		1	100%				
[N.*] Desastres naturales		0,5	100%				
[I.1] Fuego		1	100%				
[I.2] Daños por agua		1	100%				
[A.5] Suplantación de la identidad		1		10%	50%		
[A.7] Uso no previsto		1	10%	10%	50%		
[A.11] Acceso no autorizado		5		10%	50%		
[A.26] Ataque destructivo		0,1	100%				
[A.27] Ocupación enemiga		1	100%		50%		

Fuente El autor

[P] Personal

Figura 139. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal -administradores de sistemas



[SNRA61] Administradores de sistemas			50%	100%	100%		
[E.15] Alteración de la información		1		10%			
[E.18] Destrucción de la información		1	1%				
[E.19] Fugas de información		1			10%		
[E.28] Indisponibilidad del personal		1	10%				
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	10%				
[A.19] Revelación de información		10			50%		
[A.28] Indisponibilidad del personal		0,5	20%				
[A.29] Extorsión		0,9	50%	100%	100%		
[A.30] Ingeniería social (picaresca)		0,5	50%	100%	100%		

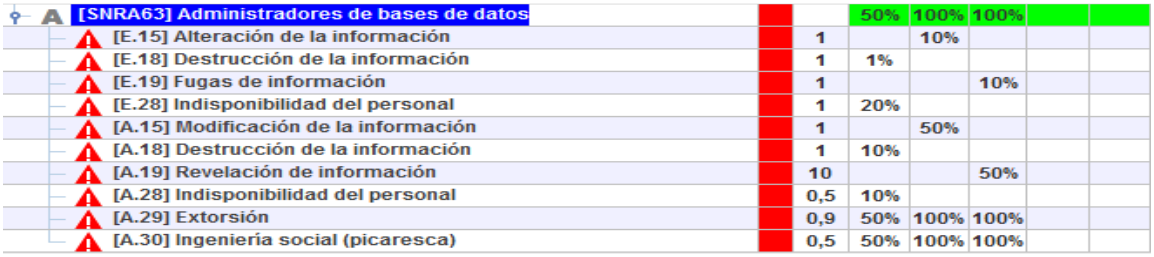
Fuente El autor

Figura 140. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal -administradores de comunicaciones

[SNRA62] Administradores de comunicaciones			50%	50%	50%		
[E.15] Alteración de la información		1		10%			
[E.18] Destrucción de la información		1	1%				
[E.19] Fugas de información		1			10%		
[E.28] Indisponibilidad del personal		1	10%				
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	10%				
[A.19] Revelación de información		1			50%		
[A.28] Indisponibilidad del personal		0,5	20%				
[A.29] Extorsión		0,9	50%	50%	50%		
[A.30] Ingeniería social (picaresca)		0,5	50%	50%	50%		

Fuente El autor

Figura 141. Representación probabilidad ocurrencia de amenazas y degradación sobre activo personal -administradores de bases de datos



[SNRA63] Administradores de bases de datos			50%	100%	100%		
[E.15] Alteración de la información		1		10%			
[E.18] Destrucción de la información		1	1%				
[E.19] Fugas de información		1			10%		
[E.28] Indisponibilidad del personal		1	20%				
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	10%				
[A.19] Revelación de información		10			50%		
[A.28] Indisponibilidad del personal		0,5	10%				
[A.29] Extorsión		0,9	50%	100%	100%		
[A.30] Ingeniería social (picaresca)		0,5	50%	100%	100%		

Fuente El autor

Salvaguardas

Son realmente pocas las salvaguardas existentes y que puedan contribuir a garantizar la seguridad de la información y la infraestructura tecnológica a través de la cual se administra. Entre las pocas medidas de salvaguarda existentes y efectivas podrían mencionarse las siguientes:

a). Como mecanismo para asegurar la protección de las comunicaciones desde y hacia fuera de la entidad existen actualmente configurados dos firewall en un esquema redundante de tal manera que ante la caída de uno de estos dispositivos habrá un dispositivo listo para asumir las funciones del dispositivo en problemas.
b). Como mecanismo para asegurar la disponibilidad del servicio de autenticación de los usuarios tanto del departamento de informática como de toda la entidad a sus equipos de trabajo, existen en el departamento de informática 2 servidores denominados controladores de dominio que deberán asegurar la prestación permanente del servicio. Así mismo existen otros cinco servidores (controladores de dominio) distribuidos por varias ciudades para fortalecer este ambiente de alta disponibilidad.
c). Como mecanismo para asegurar la disponibilidad del servicio de resolución de nombres (DNS) los servidores denominados controladores de dominio también fueron configurados como servidores DNS.
d). Como mecanismo de protección frente a la presencia de software maligno, existe configurado para el departamento de informática y la entidad en general una solución de antivirus dedicada. La cual se encuentra ubicada en la Nube.
e). Para asegurar un ambiente optimo de temperatura para los equipos ubicados en el centro de datos de la entidad se dispone de dos maquinas de aire acondicionado, aunque de muy distintas capacidades.
f). Para la protección de los equipos ubicados en el centro de datos de la entidad, se dispone de espacio totalmente cerrado y el establecimiento de dispositivos biométricos para la entrada y salida a dicho sitio.

g). El entorno adyacente al centro de datos cuenta con la señalización pertinente en donde se informa de la ubicación de una zona de carácter restringido.
h). En la puerta principal del centro de datos existe una carpeta en donde se registra la entrada y salida de personas que por razones diversas deban ingresar al centro de datos. Aunque su diligenciamiento no se supervisa de forma estricta.
i). Se cuenta con la disposición de un centro de datos alterno ubicado en las instalaciones del proveedor de servicio de hosting. Aunque solo se utiliza para el almacenamiento y operación de algunas aplicaciones.
j). Como mecanismo de protección frente a la perdida de fluido eléctrico existen dos UPS establecidas en un esquema de redundancia.
k). Existen dispuestos dos canales de comunicación independiente. Un primer canal destinado para aplicaciones y servicios en general. Un segundo canal dispuesto exclusivamente para la prestación del servicio de Internet.

Impacto y riesgo

Niveles de criticidad - Código de colores

La herramienta PILAR representa los niveles de riesgo en el rango comprendido de 0.00 a 9.9, con una coloración cuyo propósito es el de resaltar la visibilidad.

Figura 142. Código de colores niveles de criticidad

Fuente Centro criptologico nacional (ccn-cert)

Valores acumulados - Impacto

Descripción general

Figura 143. Representación general de impacto

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[7]	[7]	[7]	[7]	[3]
[B] Activos esenciales					
[IS] Servicios internos	[6]	[6]		[7]	[3]
[SNRA06] Directorio activo	[6]	[6]		[7]	
[SNRA07] Servicio de nombres de dominio (DNS)	[6]				
[SNRA08] DHCP	[6]				
[SNRA09] BIOMETRICO	[2]				[3]
[E] Equipamiento	[7]	[7]	[7]	[7]	
[SW] Aplicaciones	[7]	[7]	[7]	[7]	
[HW] Equipos	[7]	[5]	[7]		
[COM] Comunicaciones	[6]	[5]	[6]	[7]	
[AUX] Elementos auxiliares	[7]				
[ga01] [MEDIA] Soporte de informacion	[7]	[7]	[7]		
[SS] Servicios subcontratados	[7]	[7]	[7]	[7]	[3]
[SNRA58] Correo electronico	[4]	[7]		[7]	
[SNRA59] Portal	[5]		[5]		
[SNRA60] Hosting y administracion	[7]	[7]	[7]	[7]	[3]
[L] Instalaciones	[7]	[4]	[6]		
[SNRA64] Centro de datos	[7]	[4]	[6]		
[P] Personal	[6]	[7]	[7]		
[SNRA61] Administradores de sistemas	[6]	[7]	[7]		
[SNRA62] Administradores de comunicaciones	[6]	[6]	[6]		
[SNRA63] Administradores de bases de datos	[6]	[7]	[7]		

Fuente El autor

Descripción especifica

1). [B] Activos esenciales

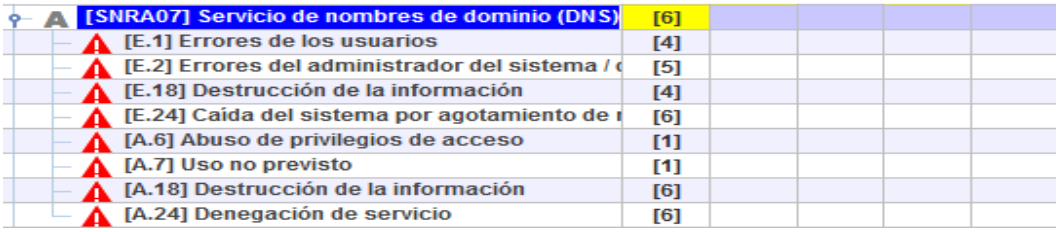
2). [IS] Servicios internos

Figura 144. Representación de impacto sobre activo servicios internos-Directorio activo

[SNRA06] Directorio activo	[6]	[6]		[7]	
[E.1] Errores de los usuarios	[4]	[4]			
[E.2] Errores del administrador del sistema /	[5]	[5]			
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[4]				
[E.24] Caída del sistema por agotamiento de	[6]				
[A.5] Suplantación de la identidad		[6]		[7]	
[A.6] Abuso de privilegios de acceso	[1]	[4]		[7]	
[A.7] Uso no previsto	[1]	[4]			
[A.11] Acceso no autorizado		[4]		[7]	
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[6]				
[A.24] Denegación de servicio	[6]				

Fuente El autor

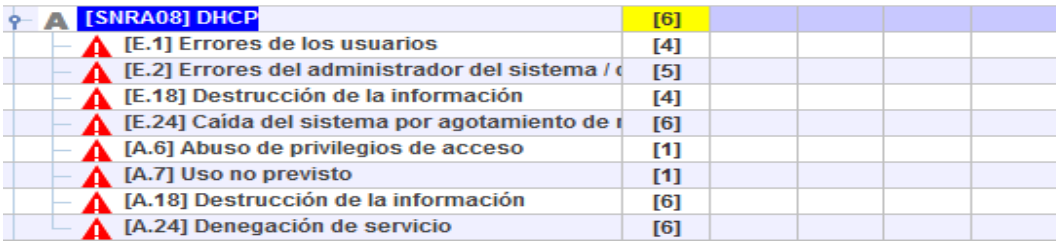
Figura 145. Representación de impacto sobre activo servicios internos-Servicio de nombres de dominio (DNS)



[SNRA07] Servicio de nombres de dominio (DNS)	[6]					
[E.1] Errores de los usuarios	[4]					
[E.2] Errores del administrador del sistema /	[5]					
[E.18] Destrucción de la información	[4]					
[E.24] Caída del sistema por agotamiento de	[6]					
[A.6] Abuso de privilegios de acceso	[1]					
[A.7] Uso no previsto	[1]					
[A.18] Destrucción de la información	[6]					
[A.24] Denegación de servicio	[6]					

Fuente El autor

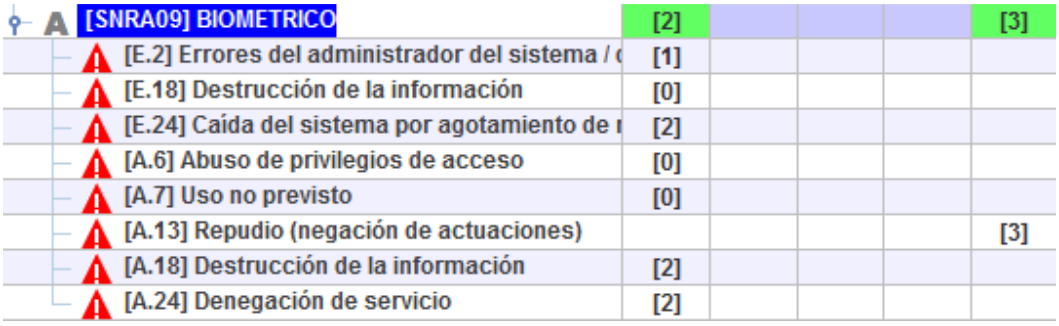
Figura 146. Representación de impacto sobre activo servicios internos-DHCP



[SNRA08] DHCP	[6]					
[E.1] Errores de los usuarios	[4]					
[E.2] Errores del administrador del sistema /	[5]					
[E.18] Destrucción de la información	[4]					
[E.24] Caída del sistema por agotamiento de	[6]					
[A.6] Abuso de privilegios de acceso	[1]					
[A.7] Uso no previsto	[1]					
[A.18] Destrucción de la información	[6]					
[A.24] Denegación de servicio	[6]					

Fuente El autor

Figura 147. Representación de impacto sobre activo servicios internos-BIOMETRICO



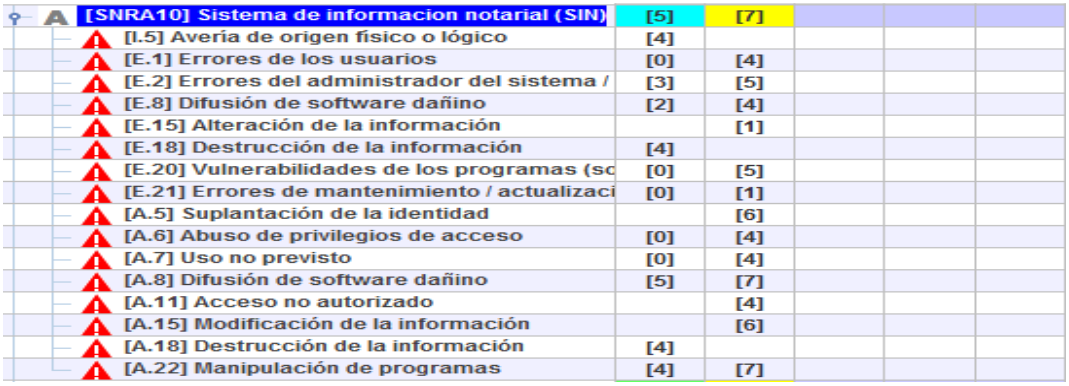
[SNRA09] BIOMETRICO	[2]					[3]
[E.2] Errores del administrador del sistema /	[1]					
[E.18] Destrucción de la información	[0]					
[E.24] Caída del sistema por agotamiento de	[2]					
[A.6] Abuso de privilegios de acceso	[0]					
[A.7] Uso no previsto	[0]					
[A.13] Repudio (negación de actuaciones)						[3]
[A.18] Destrucción de la información	[2]					
[A.24] Denegación de servicio	[2]					

Fuente El autor

3). [E] Equipamiento

[SW] Aplicaciones

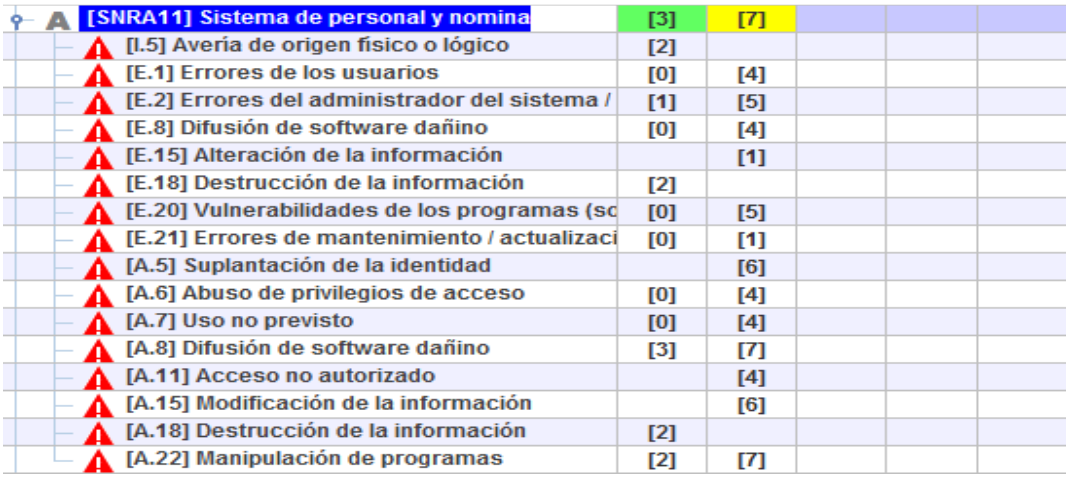
Figura 148. Representación de impacto sobre activo aplicaciones-sistema de información notarial (SIN)



[SNRA10] Sistema de informacion notarial (SIN)	[5]	[7]			
[I.5] Avería de origen físico o lógico	[4]				
[E.1] Errores de los usuarios	[0]	[4]			
[E.2] Errores del administrador del sistema /	[3]	[5]			
[E.8] Difusión de software dañino	[2]	[4]			
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[4]				
[E.20] Vulnerabilidades de los programas (sc	[0]	[5]			
[E.21] Errores de mantenimiento / actualizaci	[0]	[1]			
[A.5] Suplantación de la identidad		[6]			
[A.6] Abuso de privilegios de acceso	[0]	[4]			
[A.7] Uso no previsto	[0]	[4]			
[A.8] Difusión de software dañino	[5]	[7]			
[A.11] Acceso no autorizado		[4]			
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[4]				
[A.22] Manipulación de programas	[4]	[7]			

Fuente El autor

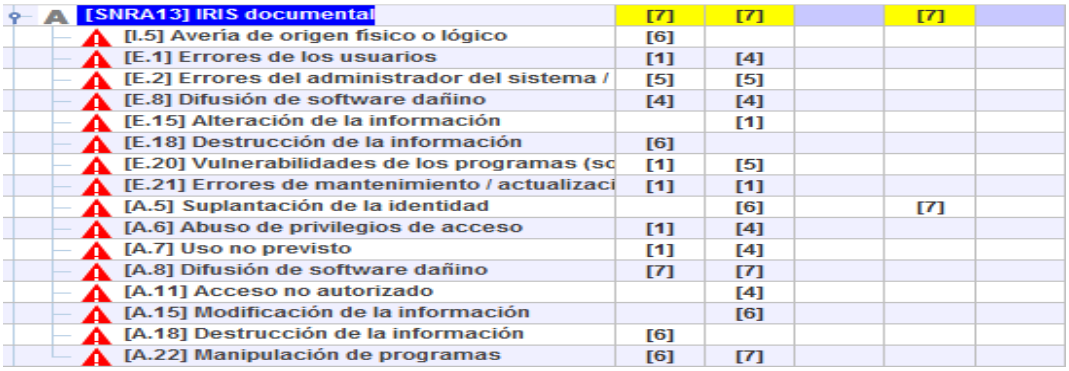
Figura 149. Representación de impacto sobre activo aplicaciones-sistema de personal y nomina



[SNRA11] Sistema de personal y nomina	[3]	[7]			
[I.5] Avería de origen físico o lógico	[2]				
[E.1] Errores de los usuarios	[0]	[4]			
[E.2] Errores del administrador del sistema /	[1]	[5]			
[E.8] Difusión de software dañino	[0]	[4]			
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[2]				
[E.20] Vulnerabilidades de los programas (sc	[0]	[5]			
[E.21] Errores de mantenimiento / actualizaci	[0]	[1]			
[A.5] Suplantación de la identidad		[6]			
[A.6] Abuso de privilegios de acceso	[0]	[4]			
[A.7] Uso no previsto	[0]	[4]			
[A.8] Difusión de software dañino	[3]	[7]			
[A.11] Acceso no autorizado		[4]			
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[2]				
[A.22] Manipulación de programas	[2]	[7]			

Fuente El autor

Figura 150. Representación de impacto sobre activo aplicaciones-IRIS documental



[SNRA13] IRIS documental	[7]	[7]		[7]	
[I.5] Avería de origen físico o lógico	[6]				
[E.1] Errores de los usuarios	[1]	[4]			
[E.2] Errores del administrador del sistema /	[5]	[5]			
[E.8] Difusión de software dañino	[4]	[4]			
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[6]				
[E.20] Vulnerabilidades de los programas (sc	[1]	[5]			
[E.21] Errores de mantenimiento / actualizaci	[1]	[1]			
[A.5] Suplantación de la identidad		[6]		[7]	
[A.6] Abuso de privilegios de acceso	[1]	[4]			
[A.7] Uso no previsto	[1]	[4]			
[A.8] Difusión de software dañino	[7]	[7]			
[A.11] Acceso no autorizado		[4]			
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[6]				
[A.22] Manipulación de programas	[6]	[7]			

Fuente El autor

Figura 151. Representación de impacto sobre activo aplicaciones-sistema de procesos judiciales

[SNRA14] Sistema de procesos judiciales	[3]	[7]	[7]		
[I.5] Avería de origen físico o lógico	[2]				
[E.1] Errores de los usuarios	[0]	[4]	[4]		
[E.2] Errores del administrador del sistema /	[1]	[5]	[5]		
[E.8] Difusión de software dañino	[0]	[4]	[4]		
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[2]				
[E.19] Fugas de información			[4]		
[E.20] Vulnerabilidades de los programas (sc	[0]	[5]	[5]		
[E.21] Errores de mantenimiento / actualizaci	[0]	[1]			
[A.5] Suplantación de la identidad		[6]	[6]		
[A.6] Abuso de privilegios de acceso	[0]	[4]	[4]		
[A.7] Uso no previsto	[0]	[4]	[4]		
[A.8] Difusión de software dañino	[3]	[7]	[7]		
[A.11] Acceso no autorizado		[4]	[6]		
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[2]				
[A.19] Revelación de información			[6]		
[A.22] Manipulación de programas	[2]	[7]	[7]		

Fuente El autor

Figura 152. Representación de impacto sobre activo aplicaciones-hoja de vida de notarios

[SNRA15] Hoja de vida de notarios	[3]	[5]			
[I.5] Avería de origen físico o lógico	[2]				
[E.1] Errores de los usuarios	[0]	[2]			
[E.2] Errores del administrador del sistema /	[1]	[3]			
[E.8] Difusión de software dañino	[0]	[2]			
[E.15] Alteración de la información		[0]			
[E.18] Destrucción de la información	[2]				
[E.20] Vulnerabilidades de los programas (sc	[0]	[3]			
[E.21] Errores de mantenimiento / actualizaci	[0]	[0]			
[A.5] Suplantación de la identidad		[4]			
[A.6] Abuso de privilegios de acceso	[0]	[2]			
[A.7] Uso no previsto	[0]	[2]			
[A.8] Difusión de software dañino	[3]	[5]			
[A.11] Acceso no autorizado		[2]			
[A.15] Modificación de la información		[4]			
[A.18] Destrucción de la información	[2]				
[A.22] Manipulación de programas	[2]	[5]			

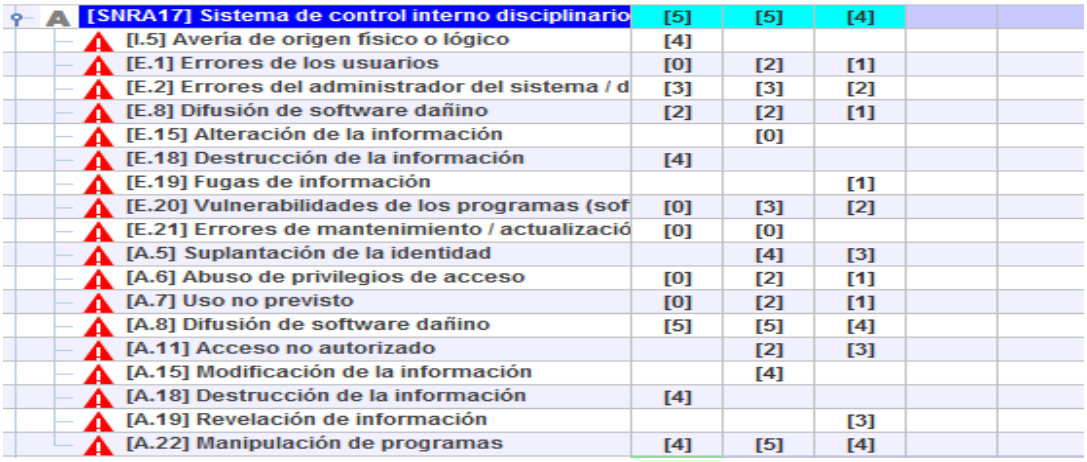
Fuente El autor

Figura 153. Representación de impacto sobre activo aplicaciones-sistema de control interno disciplinario

[SNRA16] Sistema de control interno disciplinario	[3]	[5]	[4]
[I.5] Avería de origen físico o lógico	[2]		
[E.1] Errores de los usuarios	[0]	[2]	[1]
[E.2] Errores del administrador del sistema / d	[1]	[3]	[2]
[E.8] Difusión de software dañino	[0]	[2]	[1]
[E.15] Alteración de la información		[0]	
[E.18] Destrucción de la información	[2]		
[E.19] Fugas de información			[1]
[E.20] Vulnerabilidades de los programas (sof	[0]	[3]	[2]
[E.21] Errores de mantenimiento / actualizació	[0]	[0]	
[A.5] Suplantación de la identidad		[4]	[3]
[A.6] Abuso de privilegios de acceso	[0]	[2]	[1]
[A.7] Uso no previsto	[0]	[2]	[1]
[A.8] Difusión de software dañino	[3]	[5]	[4]
[A.11] Acceso no autorizado		[2]	[3]
[A.15] Modificación de la información		[4]	
[A.18] Destrucción de la información	[2]		
[A.19] Revelación de información			[3]
[A.22] Manipulación de programas	[2]	[5]	[4]

Fuente El autor

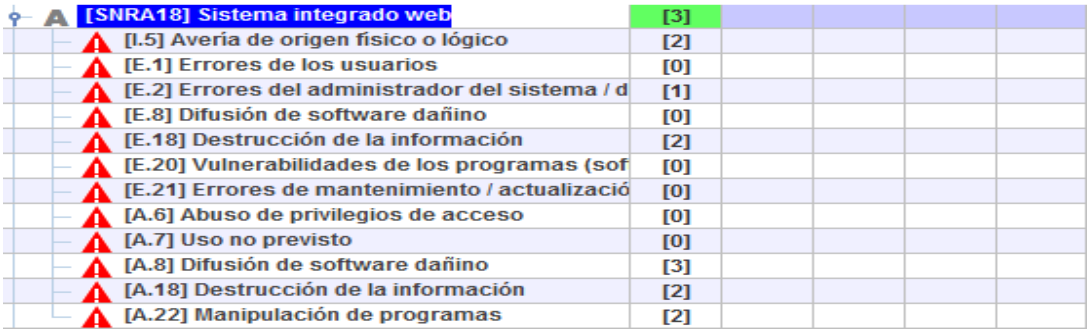
Figura 154. Representación de impacto sobre activo aplicaciones-sistema de control interno disciplinario notarias



[SNRA17] Sistema de control interno disciplinario	[5]	[5]	[4]
[I.5] Avería de origen físico o lógico	[4]		
[E.1] Errores de los usuarios	[0]	[2]	[1]
[E.2] Errores del administrador del sistema / d	[3]	[3]	[2]
[E.8] Difusión de software dañino	[2]	[2]	[1]
[E.15] Alteración de la información		[0]	
[E.18] Destrucción de la información	[4]		
[E.19] Fugas de información			[1]
[E.20] Vulnerabilidades de los programas (sof	[0]	[3]	[2]
[E.21] Errores de mantenimiento / actualizació	[0]	[0]	
[A.5] Suplantación de la identidad		[4]	[3]
[A.6] Abuso de privilegios de acceso	[0]	[2]	[1]
[A.7] Uso no previsto	[0]	[2]	[1]
[A.8] Difusión de software dañino	[5]	[5]	[4]
[A.11] Acceso no autorizado		[2]	[3]
[A.15] Modificación de la información		[4]	
[A.18] Destrucción de la información	[4]		
[A.19] Revelación de información			[3]
[A.22] Manipulación de programas	[4]	[5]	[4]

Fuente El autor

Figura 155. Representación de impacto sobre activo aplicaciones-sistema integrado web



[SNRA18] Sistema integrado web	[3]
[I.5] Avería de origen físico o lógico	[2]
[E.1] Errores de los usuarios	[0]
[E.2] Errores del administrador del sistema / d	[1]
[E.8] Difusión de software dañino	[0]
[E.18] Destrucción de la información	[2]
[E.20] Vulnerabilidades de los programas (sof	[0]
[E.21] Errores de mantenimiento / actualizació	[0]
[A.6] Abuso de privilegios de acceso	[0]
[A.7] Uso no previsto	[0]
[A.8] Difusión de software dañino	[3]
[A.18] Destrucción de la información	[2]
[A.22] Manipulación de programas	[2]

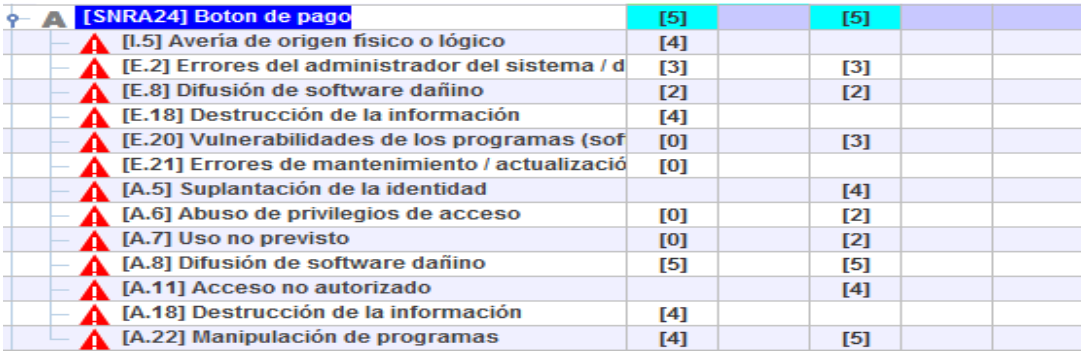
Fuente El autor

Figura 156. Representación de impacto sobre activo aplicaciones-interrelación registro-catastro

[SNRA20] Interrelacion registro-catastro	[3]	[5]
[I.5] Avería de origen físico o lógico	[2]	
[E.1] Errores de los usuarios	[0]	[2]
[E.2] Errores del administrador del sistema / d	[1]	[3]
[E.8] Difusión de software dañino	[0]	[2]
[E.15] Alteración de la información		[0]
[E.18] Destrucción de la información	[2]	
[E.20] Vulnerabilidades de los programas (sof	[0]	[3]
[E.21] Errores de mantenimiento / actualizació	[0]	[0]
[A.5] Suplantación de la identidad		[4]
[A.6] Abuso de privilegios de acceso	[0]	[2]
[A.7] Uso no previsto	[0]	[2]
[A.8] Difusión de software dañino	[3]	[5]
[A.11] Acceso no autorizado		[2]
[A.15] Modificación de la información		[4]
[A.18] Destrucción de la información	[2]	
[A.22] Manipulación de programas	[2]	[5]

Fuente El autor

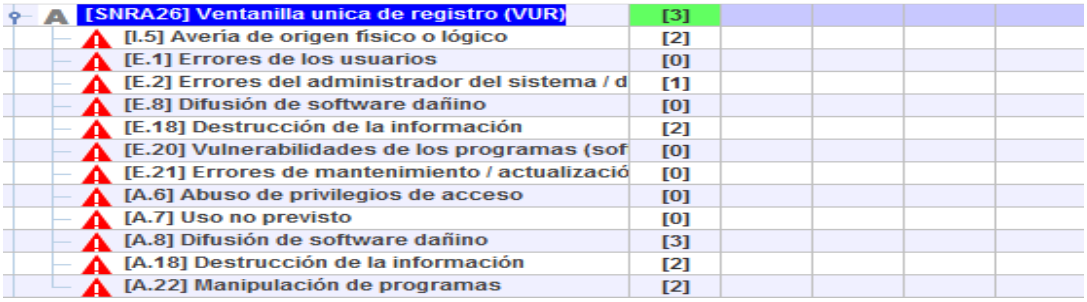
Figura 157. Representación de impacto sobre activo aplicaciones-botón de pago



[SNRA24] Boton de pago	[5]	[5]
[I.5] Avería de origen físico o lógico	[4]	
[E.2] Errores del administrador del sistema / d	[3]	[3]
[E.8] Difusión de software dañino	[2]	[2]
[E.18] Destrucción de la información	[4]	
[E.20] Vulnerabilidades de los programas (sof	[0]	[3]
[E.21] Errores de mantenimiento / actualizació	[0]	
[A.5] Suplantación de la identidad		[4]
[A.6] Abuso de privilegios de acceso	[0]	[2]
[A.7] Uso no previsto	[0]	[2]
[A.8] Difusión de software dañino	[5]	[5]
[A.11] Acceso no autorizado		[4]
[A.18] Destrucción de la información	[4]	
[A.22] Manipulación de programas	[4]	[5]

Fuente El autor

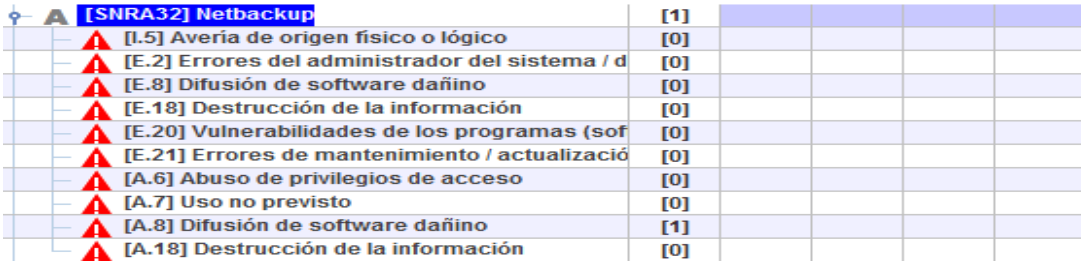
Figura 158. Representación de impacto sobre activo aplicaciones-ventanilla única de registro (VUR)



[SNRA26] Ventanilla unica de registro (VUR)	[3]
[I.5] Avería de origen físico o lógico	[2]
[E.1] Errores de los usuarios	[0]
[E.2] Errores del administrador del sistema / d	[1]
[E.8] Difusión de software dañino	[0]
[E.18] Destrucción de la información	[2]
[E.20] Vulnerabilidades de los programas (sof	[0]
[E.21] Errores de mantenimiento / actualizació	[0]
[A.6] Abuso de privilegios de acceso	[0]
[A.7] Uso no previsto	[0]
[A.8] Difusión de software dañino	[3]
[A.18] Destrucción de la información	[2]
[A.22] Manipulación de programas	[2]

Fuente El autor

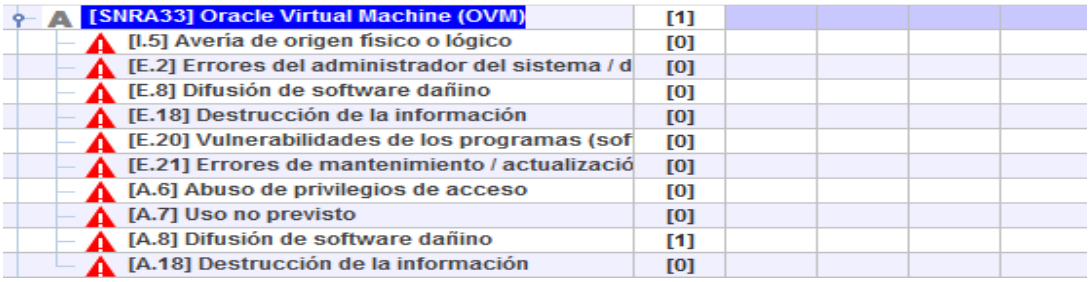
Figura 159. Representación de impacto sobre activo aplicaciones-netbackup



[SNRA32] Netbackup	[1]
[I.5] Avería de origen físico o lógico	[0]
[E.2] Errores del administrador del sistema / d	[0]
[E.8] Difusión de software dañino	[0]
[E.18] Destrucción de la información	[0]
[E.20] Vulnerabilidades de los programas (sof	[0]
[E.21] Errores de mantenimiento / actualizació	[0]
[A.6] Abuso de privilegios de acceso	[0]
[A.7] Uso no previsto	[0]
[A.8] Difusión de software dañino	[1]
[A.18] Destrucción de la información	[0]

Fuente El autor

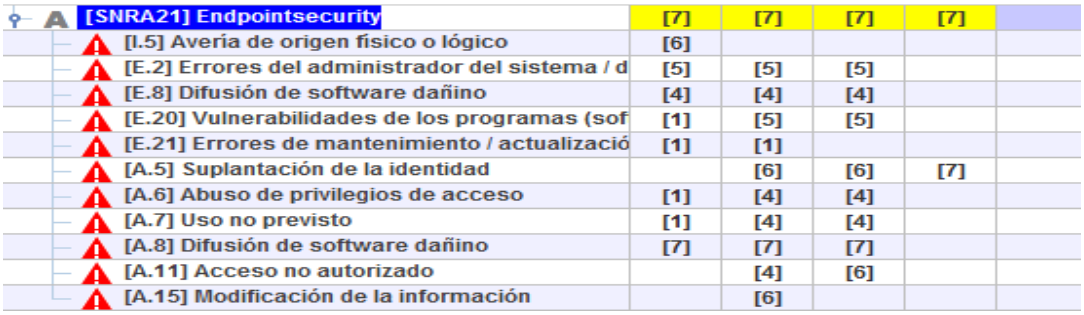
Figura 160. Representación de impacto sobre activo aplicaciones-oracle virtual machine (OVM)



[SNRA33] Oracle Virtual Machine (OVM)	[1]
[I.5] Avería de origen físico o lógico	[0]
[E.2] Errores del administrador del sistema / d	[0]
[E.8] Difusión de software dañino	[0]
[E.18] Destrucción de la información	[0]
[E.20] Vulnerabilidades de los programas (sof	[0]
[E.21] Errores de mantenimiento / actualizació	[0]
[A.6] Abuso de privilegios de acceso	[0]
[A.7] Uso no previsto	[0]
[A.8] Difusión de software dañino	[1]
[A.18] Destrucción de la información	[0]

Fuente El autor

Figura 161. Representación de impacto sobre activo aplicaciones-endpointsecurity



[SNRA21] Endpointsecurity	[7]	[7]	[7]	[7]	
[I.5] Avería de origen físico o lógico	[6]				
[E.2] Errores del administrador del sistema / d	[5]	[5]	[5]		
[E.8] Difusión de software dañino	[4]	[4]	[4]		
[E.20] Vulnerabilidades de los programas (sof	[1]	[5]	[5]		
[E.21] Errores de mantenimiento / actualizació	[1]	[1]			
[A.5] Suplantación de la identidad		[6]	[6]	[7]	
[A.6] Abuso de privilegios de acceso	[1]	[4]	[4]		
[A.7] Uso no previsto	[1]	[4]	[4]		
[A.8] Difusión de software dañino	[7]	[7]	[7]		
[A.11] Acceso no autorizado		[4]	[6]		
[A.15] Modificación de la información		[6]			

Fuente El autor

[HW] Equipos

Figura 162. Representación de impacto sobre activo equipos-exadata

[SNRA34] EXADATA	[7]				
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura	[7]				
[E.2] Errores del administrador del sistema / d	[5]				
[E.23] Errores de mantenimiento / actualizació	[4]				
[E.24] Caída del sistema por agotamiento de r	[6]				
[E.25] Pérdida de equipos	[7]				
[A.6] Abuso de privilegios de acceso	[4]				
[A.7] Uso no previsto	[1]				
[A.11] Acceso no autorizado	[4]				
[A.23] Manipulación del hardware	[6]				
[A.25] Robo de equipos	[7]				
[A.26] Ataque destructivo	[7]				

Fuente El autor

Figura 163. Representación de impacto sobre activo equipos-exalogic

[SNRA35] EXALOGIC	[7]				
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura	[7]				
[E.2] Errores del administrador del sistema / d	[5]				
[E.23] Errores de mantenimiento / actualizació	[4]				
[E.24] Caída del sistema por agotamiento de r	[6]				
[E.25] Pérdida de equipos	[7]				
[A.6] Abuso de privilegios de acceso	[4]				
[A.7] Uso no previsto	[1]				
[A.11] Acceso no autorizado	[4]				
[A.23] Manipulación del hardware	[6]				
[A.25] Robo de equipos	[7]				
[A.26] Ataque destructivo	[7]				

Fuente El autor

Figura 164. Representación de impacto sobre activo equipos-servidores

[SNRA36] Servidores	[7]	[5]	[7]		
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura	[7]				
[E.2] Errores del administrador del sistema / d	[5]	[5]	[5]		
[E.23] Errores de mantenimiento / actualizació	[4]				
[E.24] Caída del sistema por agotamiento de r	[6]				
[E.25] Pérdida de equipos	[7]		[7]		
[A.6] Abuso de privilegios de acceso	[4]	[4]	[6]		
[A.7] Uso no previsto	[1]	[1]	[4]		
[A.11] Acceso no autorizado	[4]	[4]	[6]		
[A.23] Manipulación del hardware	[6]		[6]		
[A.25] Robo de equipos	[7]		[7]		
[A.26] Ataque destructivo	[7]				

Fuente El autor

Figura 165. Representación de impacto sobre activo equipos-computadores

[SNRA37] Computadores	[3]				
[N.1] Fuego	[3]				
[N.2] Daños por agua	[2]				
[N.*] Desastres naturales	[3]				
[I.1] Fuego	[3]				
[I.2] Daños por agua	[2]				
[I.5] Avería de origen físico o lógico	[2]				
[I.6] Corte del suministro eléctrico	[3]				
[I.7] Condiciones inadecuadas de temperatura	[3]				
[E.2] Errores del administrador del sistema / d	[1]				
[E.23] Errores de mantenimiento / actualizació	[0]				
[E.24] Caída del sistema por agotamiento de r	[2]				
[E.25] Pérdida de equipos	[0]				
[A.6] Abuso de privilegios de acceso	[0]				
[A.7] Uso no previsto	[0]				
[A.11] Acceso no autorizado	[0]				
[A.23] Manipulación del hardware	[2]				
[A.25] Robo de equipos	[0]				
[A.26] Ataque destructivo	[3]				

Fuente El autor

Figura 166. Representación de impacto sobre activo equipos-portátiles

[SNRA38] Portatiles	[3]				
[N.1] Fuego	[3]				
[N.2] Daños por agua	[2]				
[N.*] Desastres naturales	[3]				
[I.1] Fuego	[3]				
[I.2] Daños por agua	[2]				
[I.5] Avería de origen físico o lógico	[2]				
[I.6] Corte del suministro eléctrico	[3]				
[I.7] Condiciones inadecuadas de temperatura	[3]				
[E.2] Errores del administrador del sistema / d	[1]				
[E.23] Errores de mantenimiento / actualizació	[0]				
[E.24] Caída del sistema por agotamiento de r	[2]				
[E.25] Pérdida de equipos	[0]				
[A.6] Abuso de privilegios de acceso	[0]				
[A.7] Uso no previsto	[0]				
[A.11] Acceso no autorizado	[0]				
[A.23] Manipulación del hardware	[2]				
[A.25] Robo de equipos	[0]				
[A.26] Ataque destructivo	[3]				

Fuente El autor

Figura 167. Representación de impacto sobre activo equipos-impresoras

[SNRA39] Impresoras	[1]
[N.1] Fuego	[1]
[N.2] Daños por agua	[0]
[N.*] Desastres naturales	[1]
[I.1] Fuego	[1]
[I.2] Daños por agua	[0]
[I.5] Avería de origen físico o lógico	[0]
[I.6] Corte del suministro eléctrico	[1]
[I.7] Condiciones inadecuadas de temperatura	[1]
[E.2] Errores del administrador del sistema / d	[0]
[E.23] Errores de mantenimiento / actualizació	[0]
[E.24] Caída del sistema por agotamiento de r	[0]
[E.25] Pérdida de equipos	[1]
[A.7] Uso no previsto	[0]
[A.11] Acceso no autorizado	[0]
[A.23] Manipulación del hardware	[0]
[A.25] Robo de equipos	[1]
[A.26] Ataque destructivo	[1]

Fuente El autor

Figura 168. Representación de impacto sobre activo equipos-switch

[SNRA41] Switch	[7]
[N.1] Fuego	[7]
[N.2] Daños por agua	[6]
[N.*] Desastres naturales	[7]
[I.1] Fuego	[7]
[I.2] Daños por agua	[6]
[I.5] Avería de origen físico o lógico	[6]
[I.6] Corte del suministro eléctrico	[7]
[I.7] Condiciones inadecuadas de temperatura	[7]
[E.2] Errores del administrador del sistema / d	[5]
[E.23] Errores de mantenimiento / actualizació	[4]
[E.24] Caída del sistema por agotamiento de r	[6]
[E.25] Pérdida de equipos	[5]
[A.6] Abuso de privilegios de acceso	[4]
[A.7] Uso no previsto	[4]
[A.11] Acceso no autorizado	[4]
[A.23] Manipulación del hardware	[7]
[A.25] Robo de equipos	[5]
[A.26] Ataque destructivo	[7]

Fuente El autor

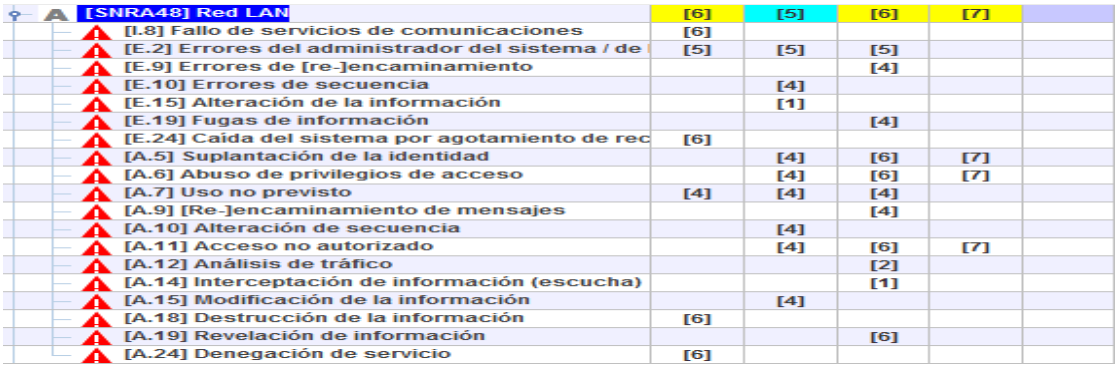
Figura 169. Representación de impacto sobre activo equipos-firewall

[SNRA42] Firewall	[7]	[5]
[N.1] Fuego	[7]	
[N.2] Daños por agua	[6]	
[N.*] Desastres naturales	[7]	
[I.1] Fuego	[7]	
[I.2] Daños por agua	[6]	
[I.5] Avería de origen físico o lógico	[6]	
[I.6] Corte del suministro eléctrico	[7]	
[I.7] Condiciones inadecuadas de temperatura	[7]	
[E.2] Errores del administrador del sistema / d	[5]	[5]
[E.23] Errores de mantenimiento / actualizació	[4]	
[E.24] Caída del sistema por agotamiento de r	[6]	
[E.25] Pérdida de equipos	[5]	
[A.6] Abuso de privilegios de acceso	[4]	[4]
[A.7] Uso no previsto	[4]	[1]
[A.11] Acceso no autorizado	[4]	[4]
[A.23] Manipulación del hardware	[7]	
[A.25] Robo de equipos	[5]	
[A.26] Ataque destructivo	[7]	

Fuente El autor

[COM] Comunicaciones

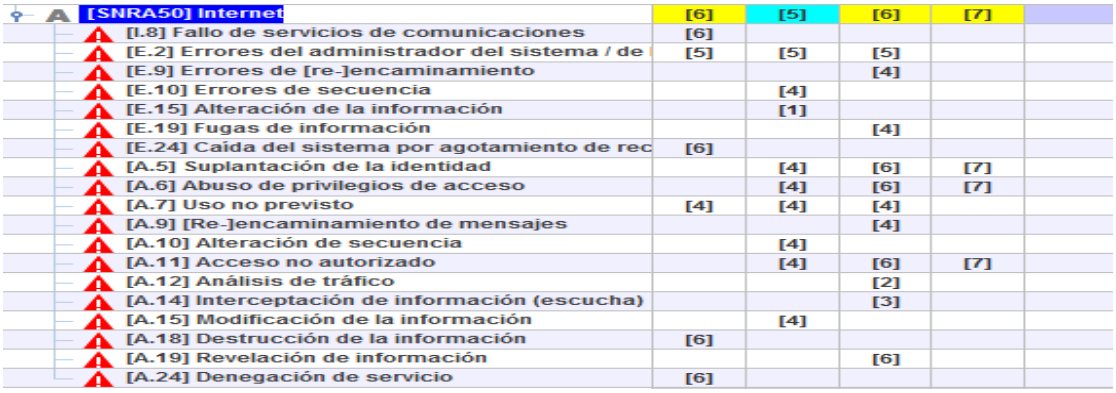
Figura 170. Representación de impacto sobre activo comunicaciones-red LAN



[SNRA48] Red LAN	[6]	[5]	[6]	[7]
[I.8] Fallo de servicios de comunicaciones	[6]			
[E.2] Errores del administrador del sistema / de	[5]	[5]	[5]	
[E.9] Errores de [re-]encaminamiento			[4]	
[E.10] Errores de secuencia		[4]		
[E.15] Alteración de la información		[1]		
[E.19] Fugas de información			[4]	
[E.24] Caída del sistema por agotamiento de rec	[6]			
[A.5] Suplantación de la identidad		[4]	[6]	[7]
[A.6] Abuso de privilegios de acceso		[4]	[6]	[7]
[A.7] Uso no previsto	[4]	[4]	[4]	
[A.9] [Re-]encaminamiento de mensajes			[4]	
[A.10] Alteración de secuencia		[4]		
[A.11] Acceso no autorizado		[4]	[6]	[7]
[A.12] Análisis de tráfico			[2]	
[A.14] Interceptación de información (escucha)			[1]	
[A.15] Modificación de la información		[4]		
[A.18] Destrucción de la información	[6]			
[A.19] Revelación de información			[6]	
[A.24] Denegación de servicio	[6]			

Fuente El autor

Figura 171. Representación de impacto sobre activo comunicaciones-internet

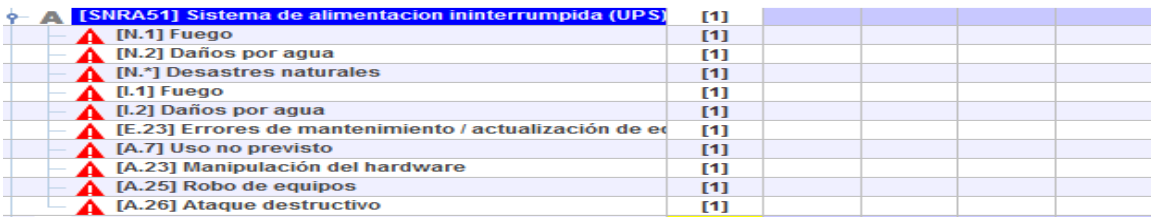


[SNRA50] Internet	[6]	[5]	[6]	[7]
[I.8] Fallo de servicios de comunicaciones	[6]			
[E.2] Errores del administrador del sistema / de	[5]	[5]	[5]	
[E.9] Errores de [re-]encaminamiento			[4]	
[E.10] Errores de secuencia		[4]		
[E.15] Alteración de la información		[1]		
[E.19] Fugas de información			[4]	
[E.24] Caída del sistema por agotamiento de rec	[6]			
[A.5] Suplantación de la identidad		[4]	[6]	[7]
[A.6] Abuso de privilegios de acceso		[4]	[6]	[7]
[A.7] Uso no previsto	[4]	[4]	[4]	
[A.9] [Re-]encaminamiento de mensajes			[4]	
[A.10] Alteración de secuencia		[4]		
[A.11] Acceso no autorizado		[4]	[6]	[7]
[A.12] Análisis de tráfico			[2]	
[A.14] Interceptación de información (escucha)			[3]	
[A.15] Modificación de la información		[4]		
[A.18] Destrucción de la información	[6]			
[A.19] Revelación de información			[6]	
[A.24] Denegación de servicio	[6]			

Fuente El autor

[AUX] Elementos auxiliares

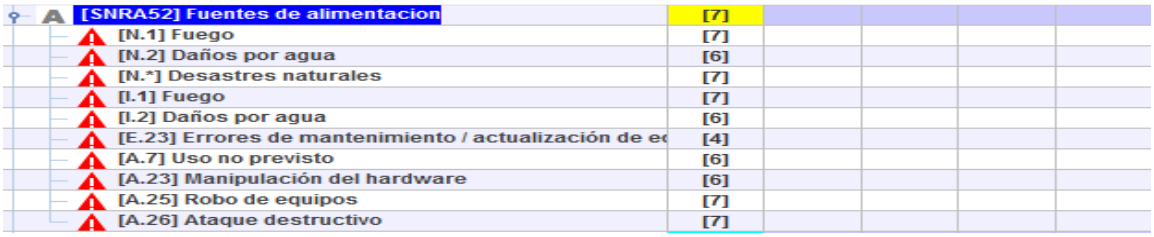
Figura 172. Representación de impacto sobre activo elementos auxiliares-sistema de alimentación ininterrumpida (UPS)



[SNRA51] Sistema de alimentacion ininterrumpida (UPS)	[1]
[N.1] Fuego	[1]
[N.2] Daños por agua	[1]
[N.*] Desastres naturales	[1]
[I.1] Fuego	[1]
[I.2] Daños por agua	[1]
[E.23] Errores de mantenimiento / actualización de e	[1]
[A.7] Uso no previsto	[1]
[A.23] Manipulación del hardware	[1]
[A.25] Robo de equipos	[1]
[A.26] Ataque destructivo	[1]

Fuente El autor

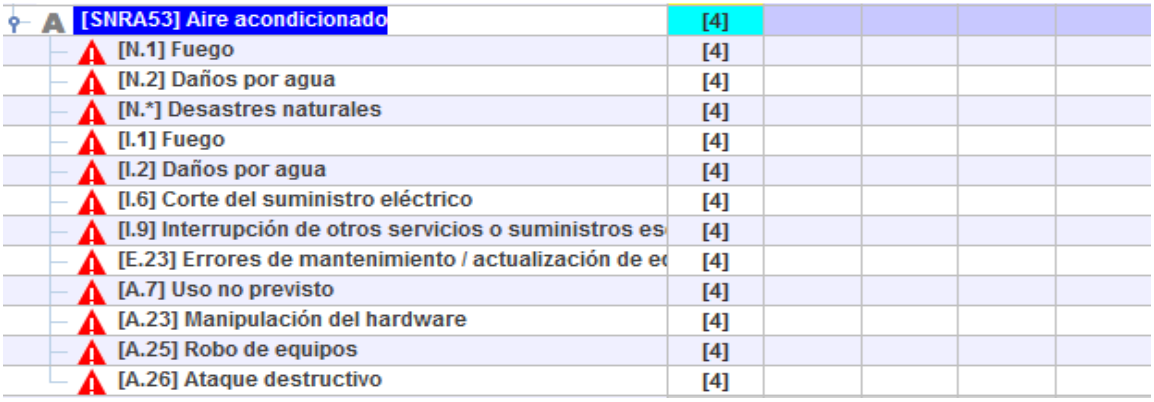
Figura 173. Representación de impacto sobre activo elementos auxiliares-fuentes de alimentación



[SNRA52] Fuentes de alimentacion	[7]
[N.1] Fuego	[7]
[N.2] Daños por agua	[6]
[N.*] Desastres naturales	[7]
[I.1] Fuego	[7]
[I.2] Daños por agua	[6]
[E.23] Errores de mantenimiento / actualización de e	[4]
[A.7] Uso no previsto	[6]
[A.23] Manipulación del hardware	[6]
[A.25] Robo de equipos	[7]
[A.26] Ataque destructivo	[7]

Fuente El autor

Figura 174. Representación de impacto sobre activo elementos auxiliares-aire acondicionado



[SNRA53] Aire acondicionado	[4]
[N.1] Fuego	[4]
[N.2] Daños por agua	[4]
[N.*] Desastres naturales	[4]
[I.1] Fuego	[4]
[I.2] Daños por agua	[4]
[I.6] Corte del suministro eléctrico	[4]
[I.9] Interrupción de otros servicios o suministros es	[4]
[E.23] Errores de mantenimiento / actualización de e	[4]
[A.7] Uso no previsto	[4]
[A.23] Manipulación del hardware	[4]
[A.25] Robo de equipos	[4]
[A.26] Ataque destructivo	[4]

Fuente El autor

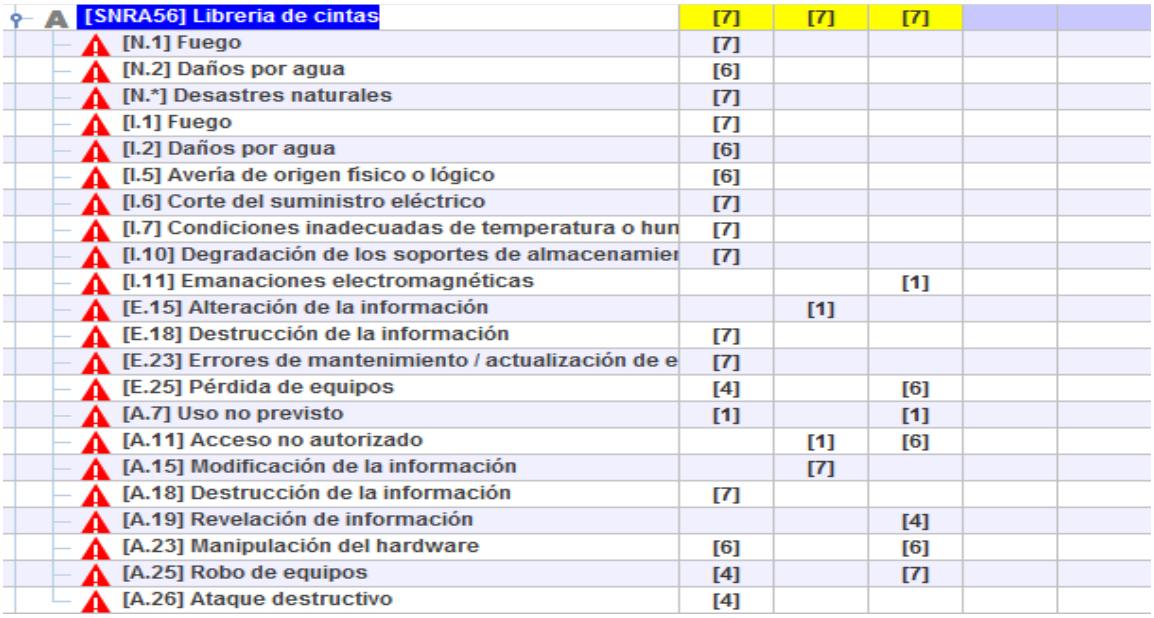
[MEDIA] Soporte de información

Figura 175. Representación de impacto sobre activo soporte de información- arreglo de discos

[SNRA55] Arreglo de discos	[7]	[7]	[7]		
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura o hun	[7]				
[I.10] Degradación de los soportes de almacenamier	[7]				
[I.11] Emanaciones electromagnéticas			[1]		
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[7]				
[E.23] Errores de mantenimiento / actualización de e	[7]				
[E.25] Pérdida de equipos	[4]		[6]		
[A.7] Uso no previsto	[1]		[1]		
[A.11] Acceso no autorizado		[1]	[6]		
[A.15] Modificación de la información		[7]			
[A.18] Destrucción de la información	[7]				
[A.19] Revelación de información			[4]		
[A.23] Manipulación del hardware	[6]		[6]		
[A.25] Robo de equipos	[4]		[7]		
[A.26] Ataque destructivo	[4]				

Fuente El autor

Figura 176. Representación de impacto sobre activo soporte de información - librería de cintas



[SNRA56] Libreria de cintas	[7]	[7]	[7]		
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura o hun	[7]				
[I.10] Degradación de los soportes de almacenamier	[7]				
[I.11] Emanaciones electromagnéticas			[1]		
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[7]				
[E.23] Errores de mantenimiento / actualización de e	[7]				
[E.25] Pérdida de equipos	[4]		[6]		
[A.7] Uso no previsto	[1]		[1]		
[A.11] Acceso no autorizado		[1]	[6]		
[A.15] Modificación de la información		[7]			
[A.18] Destrucción de la información	[7]				
[A.19] Revelación de información			[4]		
[A.23] Manipulación del hardware	[6]		[6]		
[A.25] Robo de equipos	[4]		[7]		
[A.26] Ataque destructivo	[4]				

Fuente El autor

Figura 177. Representación de impacto sobre activo soporte de información - unidad dvd

[SNRA57] Unidad DVD	[7]	[7]			
[N.1] Fuego	[7]				
[N.2] Daños por agua	[6]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[6]				
[I.5] Avería de origen físico o lógico	[6]				
[I.6] Corte del suministro eléctrico	[7]				
[I.7] Condiciones inadecuadas de temperatura o hum	[7]				
[I.10] Degradación de los soportes de almacenamien	[7]				
[E.15] Alteración de la información		[1]			
[E.18] Destrucción de la información	[7]				
[E.23] Errores de mantenimiento / actualización de e	[7]				
[E.25] Pérdida de equipos	[4]				
[A.15] Modificación de la información		[7]			
[A.18] Destrucción de la información	[7]				
[A.23] Manipulación del hardware	[6]				
[A.25] Robo de equipos	[4]				
[A.26] Ataque destructivo	[4]				

Fuente El autor

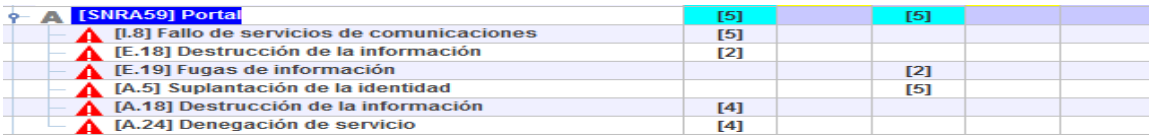
[SS] Servicios subcontratados

Figura 178. Representación de impacto sobre activo servicios subcontratados-correo electrónico

[SNRA58] Correo electronico	[4]	[7]		[7]	
[I.9] Interrupción de otros servicios o suministros esenc	[4]				
[E.15] Alteración de la información		[4]			
[E.18] Destrucción de la información	[2]				
[A.5] Suplantación de la identidad		[7]		[7]	
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[4]				
[A.24] Denegación de servicio	[4]				

Fuente El autor

Figura 179. Representación de impacto sobre activo servicios subcontratados-portal



[SNRA59] Portal	[5]		[5]		
[I.8] Fallo de servicios de comunicaciones	[5]				
[E.18] Destrucción de la información	[2]				
[E.19] Fugas de información			[2]		
[A.5] Suplantación de la identidad			[5]		
[A.18] Destrucción de la información	[4]				
[A.24] Denegación de servicio	[4]				

Fuente El autor

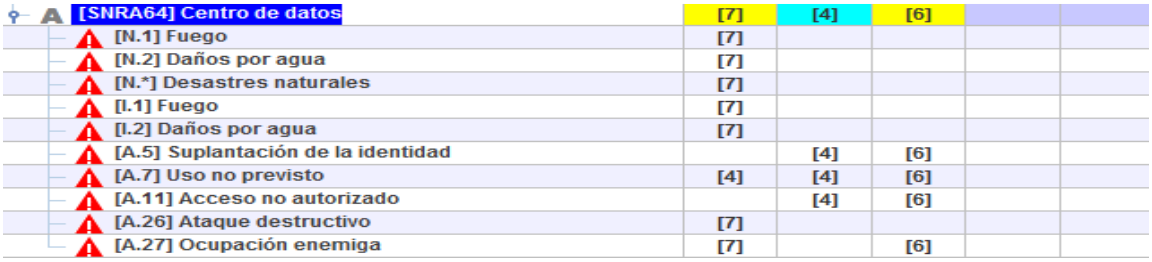
Figura 180. Representación de impacto sobre activo servicios subcontratados - hosting y administración

[SNRA60] Hosting y administracion	[7]	[7]	[7]	[7]	[3]
[I.8] Fallo de servicios de comunicaciones	[7]				
[E.15] Alteración de la información		[4]			
[E.18] Destrucción de la información	[4]				
[E.19] Fugas de información			[4]		
[A.5] Suplantación de la identidad		[7]	[7]	[7]	
[A.13] Repudio (negación de actuaciones)					[3]
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[6]				
[A.19] Revelación de información			[6]		
[A.24] Denegación de servicio	[6]				

Fuente El autor

[L] Instalaciones

Figura 181. Representación de impacto sobre activo instalaciones-centro de datos

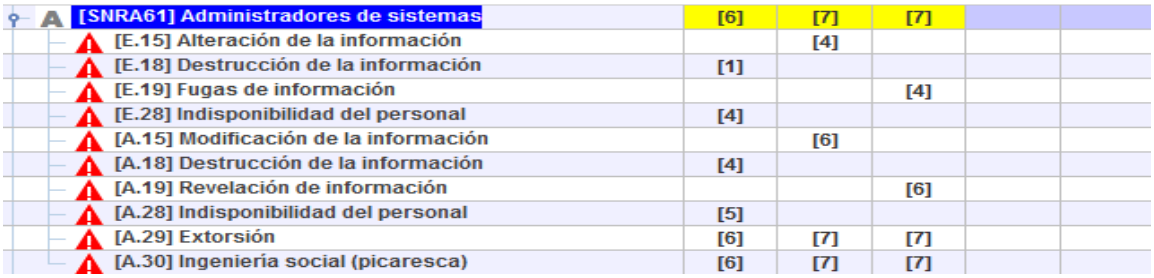


[SNRA64] Centro de datos	[7]	[4]	[6]		
[N.1] Fuego	[7]				
[N.2] Daños por agua	[7]				
[N.*] Desastres naturales	[7]				
[I.1] Fuego	[7]				
[I.2] Daños por agua	[7]				
[A.5] Suplantación de la identidad		[4]	[6]		
[A.7] Uso no previsto	[4]	[4]	[6]		
[A.11] Acceso no autorizado		[4]	[6]		
[A.26] Ataque destructivo	[7]				
[A.27] Ocupación enemiga	[7]		[6]		

Fuente El autor

[P] Personal

Figura 182. Representación de impacto sobre activo personal-administradores de sistemas



[SNRA61] Administradores de sistemas	[6]	[7]	[7]		
[E.15] Alteración de la información		[4]			
[E.18] Destrucción de la información	[1]				
[E.19] Fugas de información			[4]		
[E.28] Indisponibilidad del personal	[4]				
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[4]				
[A.19] Revelación de información			[6]		
[A.28] Indisponibilidad del personal	[5]				
[A.29] Extorsión	[6]	[7]	[7]		
[A.30] Ingeniería social (picaresca)	[6]	[7]	[7]		

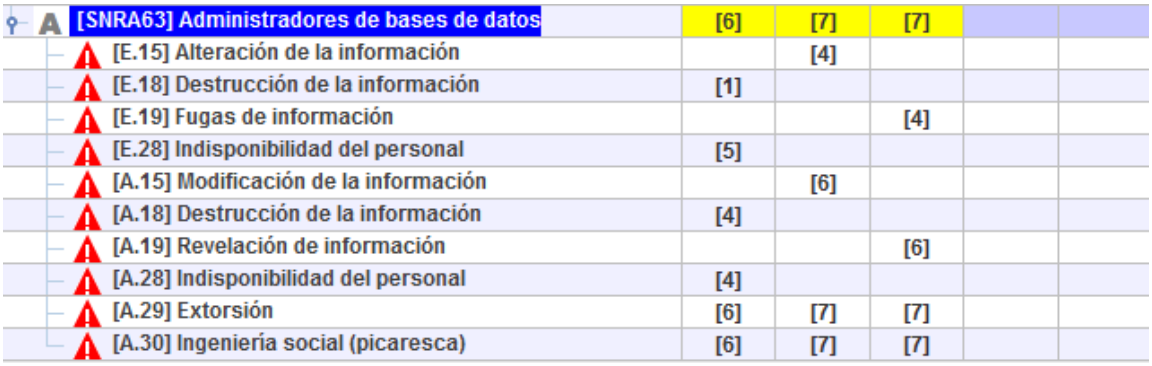
Fuente El autor

Figura 183. Representación de impacto sobre activo personal-administradores de comunicaciones

[SNRA62] Administradores de comunicaciones	[6]	[6]	[6]		
[E.15] Alteración de la información		[4]			
[E.18] Destrucción de la información	[1]				
[E.19] Fugas de información			[4]		
[E.28] Indisponibilidad del personal	[4]				
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[4]				
[A.19] Revelación de información			[6]		
[A.28] Indisponibilidad del personal	[5]				
[A.29] Extorsión	[6]	[6]	[6]		
[A.30] Ingeniería social (picaresca)	[6]	[6]	[6]		

Fuente El autor

Figura 184. Representación de impacto sobre activo personal-administradores de bases de datos



[SNRA63] Administradores de bases de datos	[6]	[7]	[7]		
[E.15] Alteración de la información		[4]			
[E.18] Destrucción de la información	[1]				
[E.19] Fugas de información			[4]		
[E.28] Indisponibilidad del personal	[5]				
[A.15] Modificación de la información		[6]			
[A.18] Destrucción de la información	[4]				
[A.19] Revelación de información			[6]		
[A.28] Indisponibilidad del personal	[4]				
[A.29] Extorsión	[6]	[7]	[7]		
[A.30] Ingeniería social (picaresca)	[6]	[7]	[7]		

Fuente El autor

Valores acumulados - Riesgo

Descripción general

Figura 185. Representación de riesgos sobre activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{5,4}	{5,7}	{5,4}	{5,1}	{3,3}
[B] Activos esenciales					
[IS] Servicios internos	{5,4}	{5,4}		{5,1}	{3,3}
[SNRA06] Directorio activo	{5,4}	{5,4}		{5,1}	
[SNRA07] Servicio de nombres de dominio (DNS)	{5,4}				
[SNRA08] DHCP	{5,4}				
[SNRA09] BIOMETRICO	{3,1}				{3,3}
[E] Equipamiento	{5,4}	{5,7}	{5,1}	{5,1}	
[SW] Aplicaciones	{5,1}	{5,1}	{5,1}	{5,1}	
[HW] Equipos	{5,4}	{3,8}	{5,1}		
[COM] Comunicaciones	{5,4}	{3,8}	{4,5}	{5,1}	
[AUX] Elementos auxiliares	{5,1}				
[ga01] [MEDIA] Soporte de informacion	{5,1}	{5,7}	{5,1}		
[SS] Servicios subcontratados	{5,1}	{4,5}	{4,5}	{4,5}	{2,7}
[SNRA58] Correo electronico	{3,4}	{4,5}		{4,5}	
[SNRA59] Portal	{3,9}		{3,3}		
[SNRA60] Hosting y administracion	{5,1}	{4,5}	{4,5}	{4,5}	{2,7}
[L] Instalaciones	{5,1}	{3,9}	{5,2}		
[SNRA64] Centro de datos	{5,1}	{3,9}	{5,2}		
[P] Personal	{4,5}	{5,0}	{5,4}		
[SNRA61] Administradores de sistemas	{4,5}	{5,0}	{5,4}		
[SNRA62] Administradores de comunicaciones	{4,5}	{4,5}	{4,5}		
[SNRA63] Administradores de bases de datos	{4,5}	{5,0}	{5,4}		

Fuente El autor

Descripción especifica

1). [B] Activos esenciales

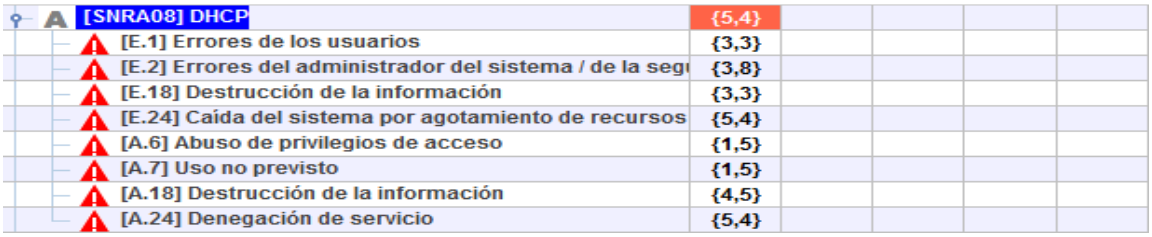
2). [IS] Servicios internos

Figura 186. Representación de riesgos sobre activo servicios internos-Servicio de nombres de dominio (DNS)

[SNRA07] Servicio de nombres de dominio (DNS)	{5,4}
[E.1] Errores de los usuarios	{3,3}
[E.2] Errores del administrador del sistema / de la seg	{3,8}
[E.18] Destrucción de la información	{3,3}
[E.24] Caida del sistema por agotamiento de recursos	{5,4}
[A.6] Abuso de privilegios de acceso	{1,5}
[A.7] Uso no previsto	{1,5}
[A.18] Destrucción de la información	{4,5}
[A.24] Denegación de servicio	{5,4}

Fuente el autor

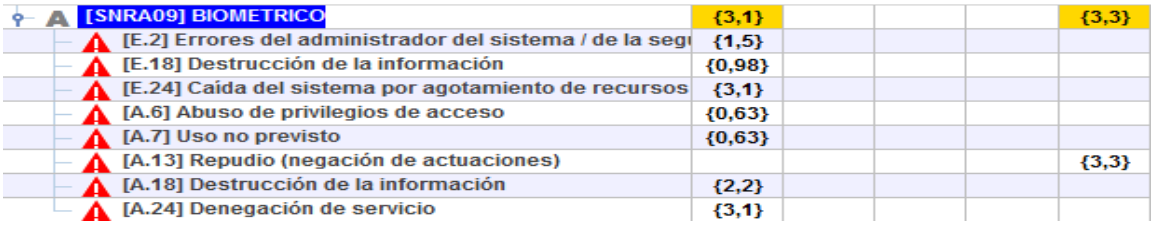
Figura 187. Representación de riesgos sobre activo servicios internos-DHCP



[SNRA08] DHCP	{5,4}
[E.1] Errores de los usuarios	{3,3}
[E.2] Errores del administrador del sistema / de la segu	{3,8}
[E.18] Destrucción de la información	{3,3}
[E.24] Caída del sistema por agotamiento de recursos	{5,4}
[A.6] Abuso de privilegios de acceso	{1,5}
[A.7] Uso no previsto	{1,5}
[A.18] Destrucción de la información	{4,5}
[A.24] Denegación de servicio	{5,4}

Fuente El autor

Figura 188. Representación de riesgos sobre activo servicios internos-BIOMETRICO



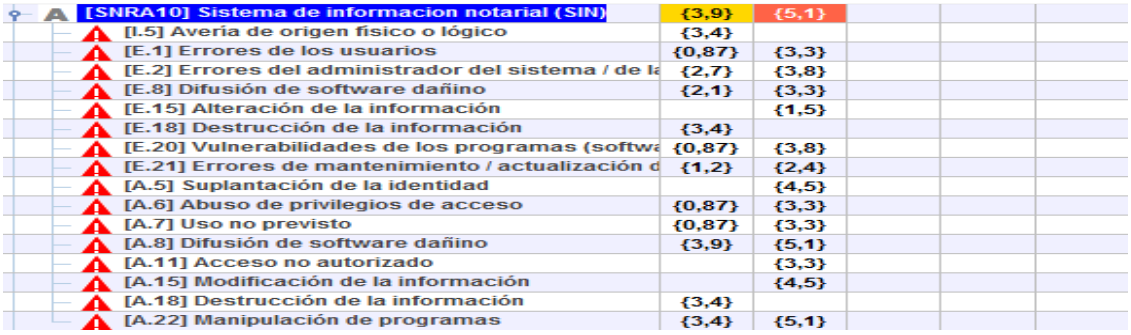
[SNRA09] BIOMETRICO	{3,1}				{3,3}
[E.2] Errores del administrador del sistema / de la segu	{1,5}				
[E.18] Destrucción de la información	{0,98}				
[E.24] Caída del sistema por agotamiento de recursos	{3,1}				
[A.6] Abuso de privilegios de acceso	{0,63}				
[A.7] Uso no previsto	{0,63}				
[A.13] Repudio (negación de actuaciones)					{3,3}
[A.18] Destrucción de la información	{2,2}				
[A.24] Denegación de servicio	{3,1}				

Fuente El autor

3). [E] Equipamiento

[SW] Aplicaciones

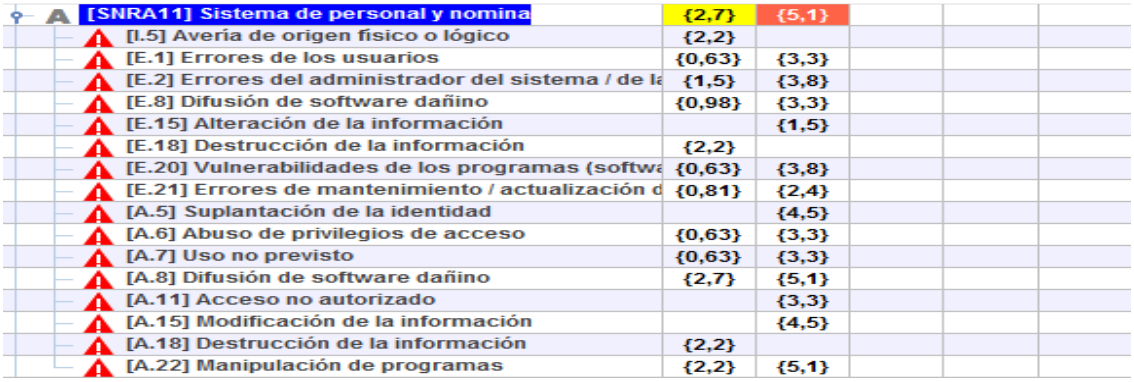
Figura 189. Representación de riesgos sobre activo aplicaciones-Sistema de información notarial (SIN)



[SNRA10] Sistema de informacion notarial (SIN)	{3,9}	{5,1}			
[I.5] Avería de origen físico o lógico	{3,4}				
[E.1] Errores de los usuarios	{0,87}	{3,3}			
[E.2] Errores del administrador del sistema / de la	{2,7}	{3,8}			
[E.8] Difusión de software dañino	{2,1}	{3,3}			
[E.15] Alteración de la información		{1,5}			
[E.18] Destrucción de la información	{3,4}				
[E.20] Vulnerabilidades de los programas (softwa	{0,87}	{3,8}			
[E.21] Errores de mantenimiento / actualización d	{1,2}	{2,4}			
[A.5] Suplantación de la identidad		{4,5}			
[A.6] Abuso de privilegios de acceso	{0,87}	{3,3}			
[A.7] Uso no previsto	{0,87}	{3,3}			
[A.8] Difusión de software dañino	{3,9}	{5,1}			
[A.11] Acceso no autorizado		{3,3}			
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{3,4}				
[A.22] Manipulación de programas	{3,4}	{5,1}			

Fuente El autor

Figura 190. Representación de riesgos sobre activo aplicaciones-Sistema de personal y nomina



[SNRA11] Sistema de personal y nomina	{2,7}	{5,1}			
[I.5] Avería de origen físico o lógico	{2,2}				
[E.1] Errores de los usuarios	{0,63}	{3,3}			
[E.2] Errores del administrador del sistema / de la	{1,5}	{3,8}			
[E.8] Difusión de software dañino	{0,98}	{3,3}			
[E.15] Alteración de la información		{1,5}			
[E.18] Destrucción de la información	{2,2}				
[E.20] Vulnerabilidades de los programas (softwa	{0,63}	{3,8}			
[E.21] Errores de mantenimiento / actualización d	{0,81}	{2,4}			
[A.5] Suplantación de la identidad		{4,5}			
[A.6] Abuso de privilegios de acceso	{0,63}	{3,3}			
[A.7] Uso no previsto	{0,63}	{3,3}			
[A.8] Difusión de software dañino	{2,7}	{5,1}			
[A.11] Acceso no autorizado		{3,3}			
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{2,2}				
[A.22] Manipulación de programas	{2,2}	{5,1}			

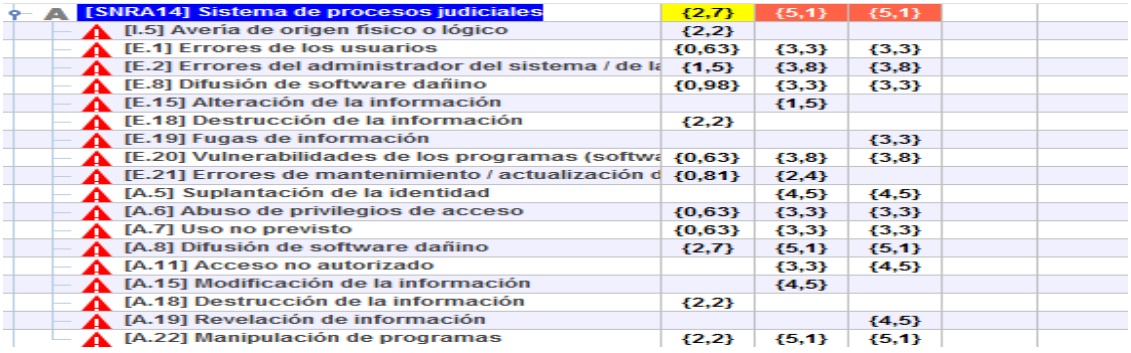
Fuente El autor

Figura 191. Representación de riesgos sobre activo aplicaciones-IRIS documental

[SNRA13] IRIS documental	{5,1}	{5,1}		{5,1}	
[I.5] Avería de origen físico o lógico	{4,5}				
[E.1] Errores de los usuarios	{1,5}	{3,3}			
[E.2] Errores del administrador del sistema / de la	{3,8}	{3,8}			
[E.8] Difusión de software dañino	{3,3}	{3,3}			
[E.15] Alteración de la información		{1,5}			
[E.18] Destrucción de la información	{4,5}				
[E.20] Vulnerabilidades de los programas (softwa	{1,5}	{3,8}			
[E.21] Errores de mantenimiento / actualización d	{2,4}	{2,4}			
[A.5] Suplantación de la identidad		{4,5}		{5,1}	
[A.6] Abuso de privilegios de acceso	{1,5}	{3,3}			
[A.7] Uso no previsto	{1,5}	{3,3}			
[A.8] Difusión de software dañino	{5,1}	{5,1}			
[A.11] Acceso no autorizado		{3,3}			
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{4,5}				
[A.22] Manipulación de programas	{4,5}	{5,1}			

Fuente El autor

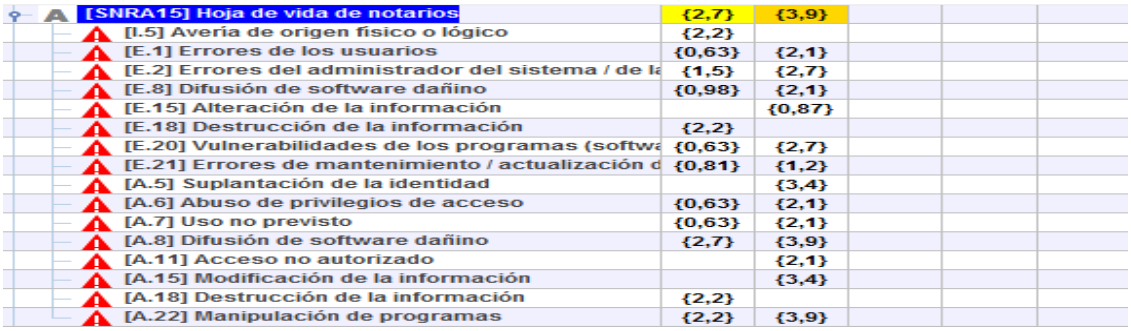
Figura 192. Representación de riesgos sobre activo aplicaciones-Sistema de procesos judiciales



[SNRA14] Sistema de procesos judiciales	{2,7}	{5,1}	{5,1}		
[I.5] Avería de origen físico o lógico	{2,2}				
[E.1] Errores de los usuarios	{0,63}	{3,3}	{3,3}		
[E.2] Errores del administrador del sistema / de la	{1,5}	{3,8}	{3,8}		
[E.8] Difusión de software dañino	{0,98}	{3,3}	{3,3}		
[E.15] Alteración de la información		{1,5}			
[E.18] Destrucción de la información	{2,2}				
[E.19] Fugas de información			{3,3}		
[E.20] Vulnerabilidades de los programas (softwa	{0,63}	{3,8}	{3,8}		
[E.21] Errores de mantenimiento / actualización d	{0,81}	{2,4}			
[A.5] Suplantación de la identidad		{4,5}	{4,5}		
[A.6] Abuso de privilegios de acceso	{0,63}	{3,3}	{3,3}		
[A.7] Uso no previsto	{0,63}	{3,3}	{3,3}		
[A.8] Difusión de software dañino	{2,7}	{5,1}	{5,1}		
[A.11] Acceso no autorizado		{3,3}	{4,5}		
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{2,2}				
[A.19] Revelación de información			{4,5}		
[A.22] Manipulación de programas	{2,2}	{5,1}	{5,1}		

Fuente El autor

Figura 193. Representación de riesgos sobre activo aplicaciones-Hoja de vida de notarios



[SNRA15] Hoja de vida de notarios	{2,7}	{3,9}
[I.5] Avería de origen físico o lógico	{2,2}	
[E.1] Errores de los usuarios	{0,63}	{2,1}
[E.2] Errores del administrador del sistema / de la	{1,5}	{2,7}
[E.8] Difusión de software dañino	{0,98}	{2,1}
[E.15] Alteración de la información		{0,87}
[E.18] Destrucción de la información	{2,2}	
[E.20] Vulnerabilidades de los programas (softwa	{0,63}	{2,7}
[E.21] Errores de mantenimiento / actualización d	{0,81}	{1,2}
[A.5] Suplantación de la identidad		{3,4}
[A.6] Abuso de privilegios de acceso	{0,63}	{2,1}
[A.7] Uso no previsto	{0,63}	{2,1}
[A.8] Difusión de software dañino	{2,7}	{3,9}
[A.11] Acceso no autorizado		{2,1}
[A.15] Modificación de la información		{3,4}
[A.18] Destrucción de la información	{2,2}	
[A.22] Manipulación de programas	{2,2}	{3,9}

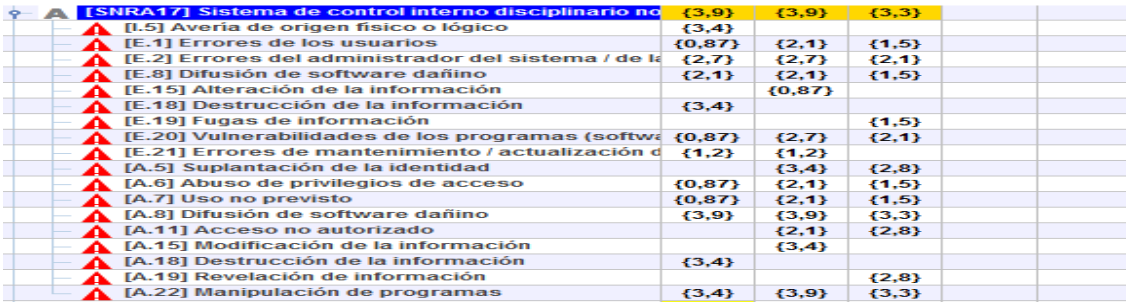
Fuente El autor

Figura 194. Representación de riesgos sobre activo aplicaciones-Sistema de control interno disciplinario

[SNRA16] Sistema de control interno disciplinario	{2,7}	{3,9}	{3,3}
[I.5] Avería de origen físico o lógico	{2,2}		
[E.1] Errores de los usuarios	{0,63}	{2,1}	{1,5}
[E.2] Errores del administrador del sistema / de la	{1,5}	{2,7}	{2,1}
[E.8] Difusión de software dañino	{0,98}	{2,1}	{1,5}
[E.15] Alteración de la información		{0,87}	
[E.18] Destrucción de la información	{2,2}		
[E.19] Fugas de información			{1,5}
[E.20] Vulnerabilidades de los programas (softwa	{0,63}	{2,7}	{2,1}
[E.21] Errores de mantenimiento / actualización d	{0,81}	{1,2}	
[A.5] Suplantación de la identidad		{3,4}	{2,8}
[A.6] Abuso de privilegios de acceso	{0,63}	{2,1}	{1,5}
[A.7] Uso no previsto	{0,63}	{2,1}	{1,5}
[A.8] Difusión de software dañino	{2,7}	{3,9}	{3,3}
[A.11] Acceso no autorizado		{2,1}	{2,8}
[A.15] Modificación de la información		{3,4}	
[A.18] Destrucción de la información	{2,2}		
[A.19] Revelación de información			{2,8}
[A.22] Manipulación de programas	{2,2}	{3,9}	{3,3}

Fuente El autor

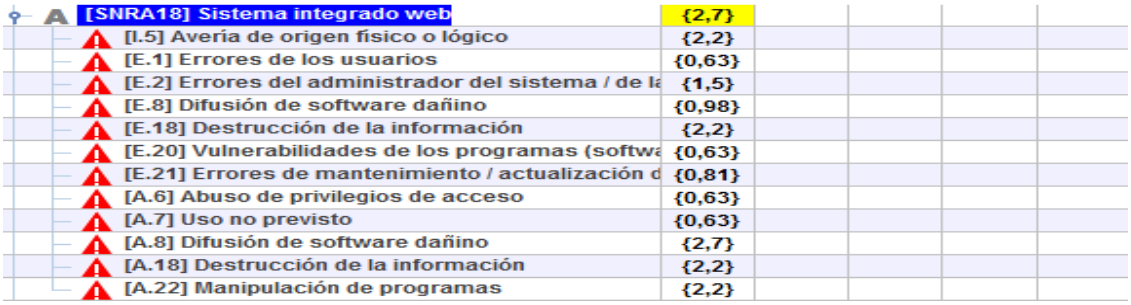
Figura 195. Representación de riesgos sobre activo aplicaciones-Sistema de control interno disciplinario notarias



[SNRA17] Sistema de control interno disciplinario no	{3,9}	{3,9}	{3,3}
[I.5] Avería de origen físico o lógico	{3,4}		
[E.1] Errores de los usuarios	{0,87}	{2,1}	{1,5}
[E.2] Errores del administrador del sistema / de la	{2,7}	{2,7}	{2,1}
[E.8] Difusión de software dañino	{2,1}	{2,1}	{1,5}
[E.15] Alteración de la información		{0,87}	
[E.18] Destrucción de la información	{3,4}		
[E.19] Fugas de información			{1,5}
[E.20] Vulnerabilidades de los programas (softwa	{0,87}	{2,7}	{2,1}
[E.21] Errores de mantenimiento / actualización d	{1,2}	{1,2}	
[A.5] Suplantación de la identidad		{3,4}	{2,8}
[A.6] Abuso de privilegios de acceso	{0,87}	{2,1}	{1,5}
[A.7] Uso no previsto	{0,87}	{2,1}	{1,5}
[A.8] Difusión de software dañino	{3,9}	{3,9}	{3,3}
[A.11] Acceso no autorizado		{2,1}	{2,8}
[A.15] Modificación de la información		{3,4}	
[A.18] Destrucción de la información	{3,4}		
[A.19] Revelación de información			{2,8}
[A.22] Manipulación de programas	{3,4}	{3,9}	{3,3}

Fuente El autor

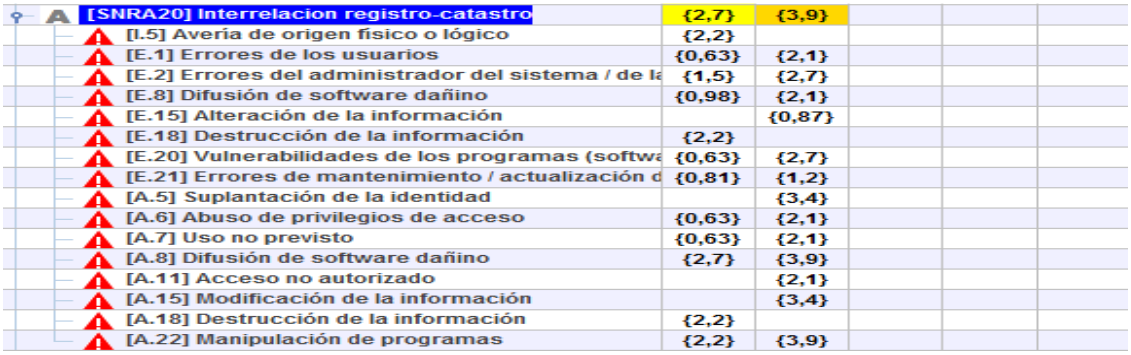
Figura 196. Representación de riesgos sobre activo aplicaciones-Sistema integrado web



[SNRA18] Sistema integrado web	{2,7}
[I.5] Avería de origen físico o lógico	{2,2}
[E.1] Errores de los usuarios	{0,63}
[E.2] Errores del administrador del sistema / de la	{1,5}
[E.8] Difusión de software dañino	{0,98}
[E.18] Destrucción de la información	{2,2}
[E.20] Vulnerabilidades de los programas (softwa	{0,63}
[E.21] Errores de mantenimiento / actualización d	{0,81}
[A.6] Abuso de privilegios de acceso	{0,63}
[A.7] Uso no previsto	{0,63}
[A.8] Difusión de software dañino	{2,7}
[A.18] Destrucción de la información	{2,2}
[A.22] Manipulación de programas	{2,2}

Fuente El autor

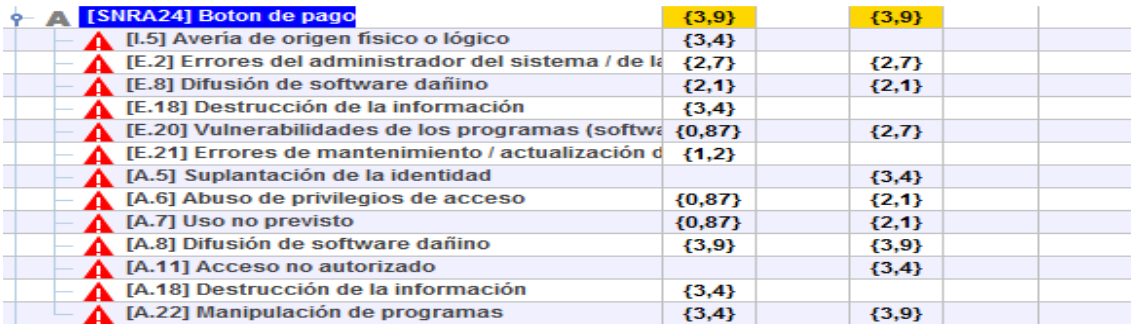
Figura 197. Representación de riesgos sobre activo aplicaciones-Interrelación registro-catastro



[SNRA20] Interrelacion registro-catastro	{2,7}	{3,9}
[I.5] Avería de origen físico o lógico	{2,2}	
[E.1] Errores de los usuarios	{0,63}	{2,1}
[E.2] Errores del administrador del sistema / de la	{1,5}	{2,7}
[E.8] Difusión de software dañino	{0,98}	{2,1}
[E.15] Alteración de la información		{0,87}
[E.18] Destrucción de la información	{2,2}	
[E.20] Vulnerabilidades de los programas (softwa	{0,63}	{2,7}
[E.21] Errores de mantenimiento / actualización d	{0,81}	{1,2}
[A.5] Suplantación de la identidad		{3,4}
[A.6] Abuso de privilegios de acceso	{0,63}	{2,1}
[A.7] Uso no previsto	{0,63}	{2,1}
[A.8] Difusión de software dañino	{2,7}	{3,9}
[A.11] Acceso no autorizado		{2,1}
[A.15] Modificación de la información		{3,4}
[A.18] Destrucción de la información	{2,2}	
[A.22] Manipulación de programas	{2,2}	{3,9}

Fuente El autor

Figura 198. Representación de riesgos sobre activo aplicaciones-Botón de pago



[SNRA24] Boton de pago	{3,9}	{3,9}
[I.5] Avería de origen físico o lógico	{3,4}	
[E.2] Errores del administrador del sistema / de la	{2,7}	{2,7}
[E.8] Difusión de software dañino	{2,1}	{2,1}
[E.18] Destrucción de la información	{3,4}	
[E.20] Vulnerabilidades de los programas (softwa	{0,87}	{2,7}
[E.21] Errores de mantenimiento / actualización d	{1,2}	
[A.5] Suplantación de la identidad		{3,4}
[A.6] Abuso de privilegios de acceso	{0,87}	{2,1}
[A.7] Uso no previsto	{0,87}	{2,1}
[A.8] Difusión de software dañino	{3,9}	{3,9}
[A.11] Acceso no autorizado		{3,4}
[A.18] Destrucción de la información	{3,4}	
[A.22] Manipulación de programas	{3,4}	{3,9}

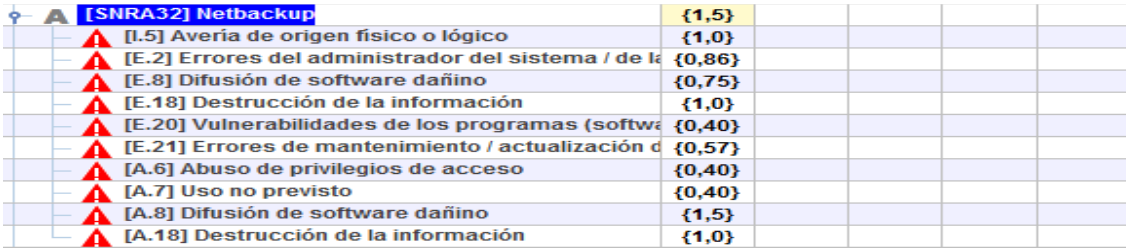
Fuente El autor

Figura 199. Representación de riesgos sobre activo aplicaciones-Ventanilla única de registro (VUR9

[SNRA26] Ventanilla unica de registro (VUR)	{2,7}
[I.5] Avería de origen físico o lógico	{2,2}
[E.1] Errores de los usuarios	{0,63}
[E.2] Errores del administrador del sistema / de la	{1,5}
[E.8] Difusión de software dañino	{0,98}
[E.18] Destrucción de la información	{2,2}
[E.20] Vulnerabilidades de los programas (softwa	{0,63}
[E.21] Errores de mantenimiento / actualización d	{0,81}
[A.6] Abuso de privilegios de acceso	{0,63}
[A.7] Uso no previsto	{0,63}
[A.8] Difusión de software dañino	{2,7}
[A.18] Destrucción de la información	{2,2}
[A.22] Manipulación de programas	{2,2}

Fuente El autor

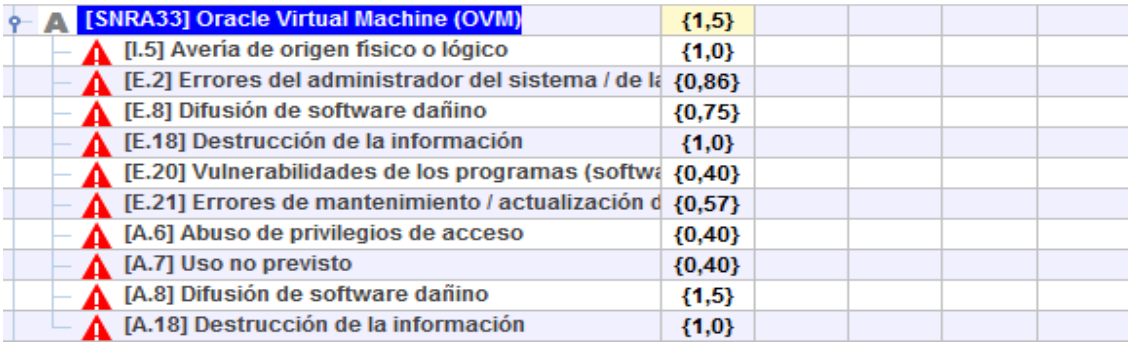
Figura 200. Representación de riesgos sobre activo aplicaciones-Netbackup



[SNRA32] Netbackup	{1,5}
[I.5] Avería de origen físico o lógico	{1,0}
[E.2] Errores del administrador del sistema / de la	{0,86}
[E.8] Difusión de software dañino	{0,75}
[E.18] Destrucción de la información	{1,0}
[E.20] Vulnerabilidades de los programas (softwa	{0,40}
[E.21] Errores de mantenimiento / actualización d	{0,57}
[A.6] Abuso de privilegios de acceso	{0,40}
[A.7] Uso no previsto	{0,40}
[A.8] Difusión de software dañino	{1,5}
[A.18] Destrucción de la información	{1,0}

Fuente El autor

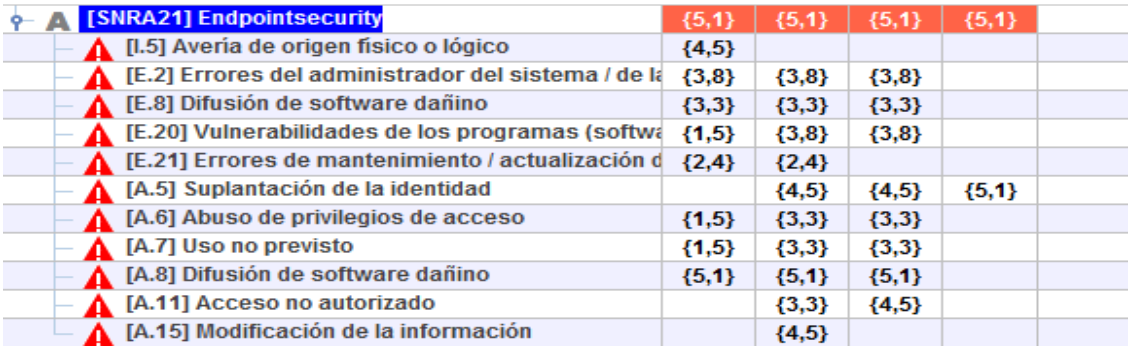
Figura 201. Representación de riesgos sobre activo aplicaciones-Oracle virtual machine



[SNRA33] Oracle Virtual Machine (OVM)	{1,5}
[I.5] Avería de origen físico o lógico	{1,0}
[E.2] Errores del administrador del sistema / de la	{0,86}
[E.8] Difusión de software dañino	{0,75}
[E.18] Destrucción de la información	{1,0}
[E.20] Vulnerabilidades de los programas (softwa	{0,40}
[E.21] Errores de mantenimiento / actualización d	{0,57}
[A.6] Abuso de privilegios de acceso	{0,40}
[A.7] Uso no previsto	{0,40}
[A.8] Difusión de software dañino	{1,5}
[A.18] Destrucción de la información	{1,0}

Fuente El autor

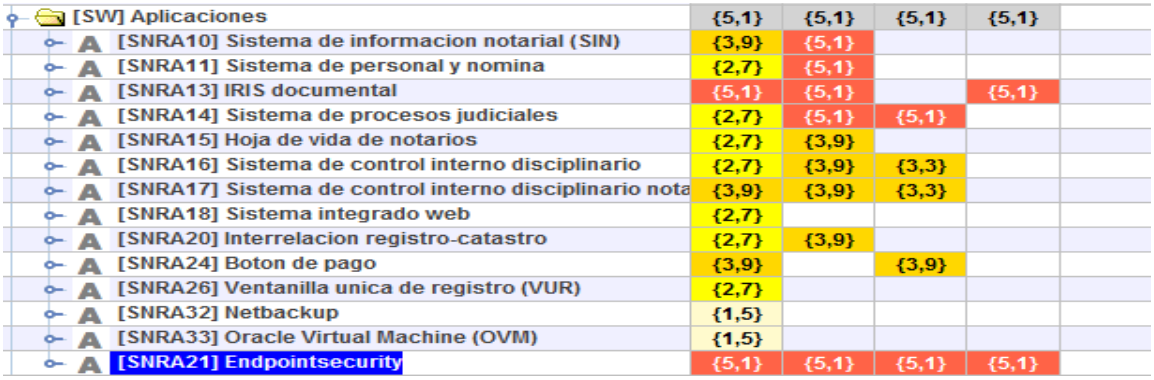
Figura 202. Representación de riesgos sobre activo aplicaciones-Endpointsecurity



[SNRA21] Endpointsecurity	{5,1}	{5,1}	{5,1}	{5,1}
[I.5] Avería de origen físico o lógico	{4,5}			
[E.2] Errores del administrador del sistema / de la	{3,8}	{3,8}	{3,8}	
[E.8] Difusión de software dañino	{3,3}	{3,3}	{3,3}	
[E.20] Vulnerabilidades de los programas (softwa	{1,5}	{3,8}	{3,8}	
[E.21] Errores de mantenimiento / actualización d	{2,4}	{2,4}		
[A.5] Suplantación de la identidad		{4,5}	{4,5}	{5,1}
[A.6] Abuso de privilegios de acceso	{1,5}	{3,3}	{3,3}	
[A.7] Uso no previsto	{1,5}	{3,3}	{3,3}	
[A.8] Difusión de software dañino	{5,1}	{5,1}	{5,1}	
[A.11] Acceso no autorizado		{3,3}	{4,5}	
[A.15] Modificación de la información		{4,5}		

Fuente El autor

Figura 203. Representación de riesgos sobre activo aplicaciones



[SW] Aplicaciones	{5,1}	{5,1}	{5,1}	{5,1}
[SNRA10] Sistema de informacion notarial (SIN)	{3,9}	{5,1}		
[SNRA11] Sistema de personal y nomina	{2,7}	{5,1}		
[SNRA13] IRIS documental	{5,1}	{5,1}		{5,1}
[SNRA14] Sistema de procesos judiciales	{2,7}	{5,1}	{5,1}	
[SNRA15] Hoja de vida de notarios	{2,7}	{3,9}		
[SNRA16] Sistema de control interno disciplinario	{2,7}	{3,9}	{3,3}	
[SNRA17] Sistema de control interno disciplinario nota	{3,9}	{3,9}	{3,3}	
[SNRA18] Sistema integrado web	{2,7}			
[SNRA20] Interrelacion registro-catastro	{2,7}	{3,9}		
[SNRA24] Boton de pago	{3,9}		{3,9}	
[SNRA26] Ventanilla unica de registro (VUR)	{2,7}			
[SNRA32] Netbackup	{1,5}			
[SNRA33] Oracle Virtual Machine (OVM)	{1,5}			
[SNRA21] Endpointsecurity	{5,1}	{5,1}	{5,1}	{5,1}

Fuente El autor

[HW] Equipos

Figura 204. Representación de riesgos sobre activo equipos-Exadata

[SNRA34] EXADATA	{5,4}
[N.1] Fuego	{4,2}
[N.2] Daños por agua	{3,7}
[N.*] Desastres naturales	{4,2}
[I.1] Fuego	{4,8}
[I.2] Daños por agua	{4,3}
[I.5] Avería de origen físico o lógico	{4,5}
[I.6] Corte del suministro eléctrico	{5,1}
[I.7] Condiciones inadecuadas de temperatura o	{5,1}
[E.2] Errores del administrador del sistema / de la	{3,8}
[E.23] Errores de mantenimiento / actualización d	{3,3}
[E.24] Caída del sistema por agotamiento de recu	{5,4}
[E.25] Pérdida de equipos	{4,2}
[A.6] Abuso de privilegios de acceso	{3,3}
[A.7] Uso no previsto	{1,5}
[A.11] Acceso no autorizado	{3,3}
[A.23] Manipulación del hardware	{4,3}
[A.25] Robo de equipos	{4,2}
[A.26] Ataque destructivo	{5,1}

Fuente El autor

Figura 205. Representación de riesgos sobre activo equipos-Exalogic

[SNRA35] EXALOGIC	{5,4}
[N.1] Fuego	{4,2}
[N.2] Daños por agua	{3,7}
[N.*] Desastres naturales	{4,2}
[I.1] Fuego	{4,8}
[I.2] Daños por agua	{4,3}
[I.5] Avería de origen físico o lógico	{4,5}
[I.6] Corte del suministro eléctrico	{5,1}
[I.7] Condiciones inadecuadas de temperatura o	{5,1}
[E.2] Errores del administrador del sistema / de la	{3,8}
[E.23] Errores de mantenimiento / actualización d	{3,3}
[E.24] Caída del sistema por agotamiento de recu	{5,4}
[E.25] Pérdida de equipos	{4,2}
[A.6] Abuso de privilegios de acceso	{3,3}
[A.7] Uso no previsto	{1,5}
[A.11] Acceso no autorizado	{3,3}
[A.23] Manipulación del hardware	{4,3}
[A.25] Robo de equipos	{4,2}
[A.26] Ataque destructivo	{5,1}

Fuente El autor

Figura 206. Representación de riesgos sobre activo equipos-Servidores

[SNRA36] Servidores	{5,4}	{3,8}	{5,1}
[N.1] Fuego	{4,2}		
[N.2] Daños por agua	{3,7}		
[N.*] Desastres naturales	{4,2}		
[I.1] Fuego	{4,8}		
[I.2] Daños por agua	{4,3}		
[I.5] Avería de origen físico o lógico	{4,5}		
[I.6] Corte del suministro eléctrico	{5,1}		
[I.7] Condiciones inadecuadas de temperatura o	{5,1}		
[E.2] Errores del administrador del sistema / de la	{3,8}	{3,8}	{3,8}
[E.23] Errores de mantenimiento / actualización d	{3,3}		
[E.24] Caída del sistema por agotamiento de recu	{5,4}		
[E.25] Pérdida de equipos	{5,1}		{5,1}
[A.6] Abuso de privilegios de acceso	{3,3}	{3,3}	{4,5}
[A.7] Uso no previsto	{1,5}	{1,5}	{3,3}
[A.11] Acceso no autorizado	{3,3}	{3,3}	{4,5}
[A.23] Manipulación del hardware	{4,3}		{4,3}
[A.25] Robo de equipos	{4,8}		{4,8}
[A.26] Ataque destructivo	{5,1}		

Fuente El autor

Figura 207. Representación de riesgos sobre activo equipos-Computadores

[SNRA37] Computadores	{3,1}
[N.1] Fuego	{1,8}
[N.2] Daños por agua	{1,3}
[N.*] Desastres naturales	{1,8}
[I.1] Fuego	{2,4}
[I.2] Daños por agua	{1,9}
[I.5] Avería de origen físico o lógico	{2,2}
[I.6] Corte del suministro eléctrico	{2,7}
[I.7] Condiciones inadecuadas de temperatura o	{2,7}
[E.2] Errores del administrador del sistema / de la	{1,5}
[E.23] Errores de mantenimiento / actualización d	{0,98}
[E.24] Caída del sistema por agotamiento de recu	{3,1}
[E.25] Pérdida de equipos	{1,0}
[A.6] Abuso de privilegios de acceso	{0,98}
[A.7] Uso no previsto	{0,98}
[A.11] Acceso no autorizado	{0,98}
[A.23] Manipulación del hardware	{1,9}
[A.25] Robo de equipos	{1,0}
[A.26] Ataque destructivo	{2,7}

Fuente El autor

Figura 208. Representación de riesgos sobre activo equipos-Portátiles

[SNRA38] Portatiles	{3,1}
[N.1] Fuego	{1,8}
[N.2] Daños por agua	{1,3}
[N.*] Desastres naturales	{1,8}
[I.1] Fuego	{2,4}
[I.2] Daños por agua	{1,9}
[I.5] Avería de origen físico o lógico	{2,2}
[I.6] Corte del suministro eléctrico	{2,7}
[I.7] Condiciones inadecuadas de temperatura o	{2,7}
[E.2] Errores del administrador del sistema / de la	{1,5}
[E.23] Errores de mantenimiento / actualización d	{0,98}
[E.24] Caída del sistema por agotamiento de recu	{3,1}
[E.25] Pérdida de equipos	{0,86}
[A.6] Abuso de privilegios de acceso	{0,98}
[A.7] Uso no previsto	{0,88}
[A.11] Acceso no autorizado	{0,98}
[A.23] Manipulación del hardware	{1,9}
[A.25] Robo de equipos	{0,86}
[A.26] Ataque destructivo	{2,7}

Fuente El autor

Figura 209. Representación de riesgos sobre activo equipos-Impresoras

[SNRA39] Impresoras	{1,9}
[N.1] Fuego	{0,93}
[N.2] Daños por agua	{0,82}
[N.*] Desastres naturales	{0,93}
[I.1] Fuego	{1,3}
[I.2] Daños por agua	{0,94}
[I.5] Avería de origen físico o lógico	{1,0}
[I.6] Corte del suministro eléctrico	{1,5}
[I.7] Condiciones inadecuadas de temperatura o	{1,5}
[E.2] Errores del administrador del sistema / de la	{0,86}
[E.23] Errores de mantenimiento / actualización d	{0,75}
[E.24] Caída del sistema por agotamiento de recu	{1,9}
[E.25] Pérdida de equipos	{1,5}
[A.7] Uso no previsto	{0,75}
[A.11] Acceso no autorizado	{0,75}
[A.23] Manipulación del hardware	{0,94}
[A.25] Robo de equipos	{1,3}
[A.26] Ataque destructivo	{1,5}

Fuente El autor

Figura 210. Representación de riesgos sobre activo equipos-Switch

[SNRA41] Switch	{5,4}
[N.1] Fuego	{4,2}
[N.2] Daños por agua	{3,7}
[N.*] Desastres naturales	{4,2}
[I.1] Fuego	{4,8}
[I.2] Daños por agua	{4,3}
[I.5] Avería de origen físico o lógico	{4,5}
[I.6] Corte del suministro eléctrico	{5,1}
[I.7] Condiciones inadecuadas de temperatura o	{5,1}
[E.2] Errores del administrador del sistema / de la	{3,8}
[E.23] Errores de mantenimiento / actualización d	{3,3}
[E.24] Caída del sistema por agotamiento de recu	{5,4}
[E.25] Pérdida de equipos	{3,8}
[A.6] Abuso de privilegios de acceso	{3,3}
[A.7] Uso no previsto	{3,3}
[A.11] Acceso no autorizado	{3,3}
[A.23] Manipulación del hardware	{4,8}
[A.25] Robo de equipos	{3,6}
[A.26] Ataque destructivo	{5,1}

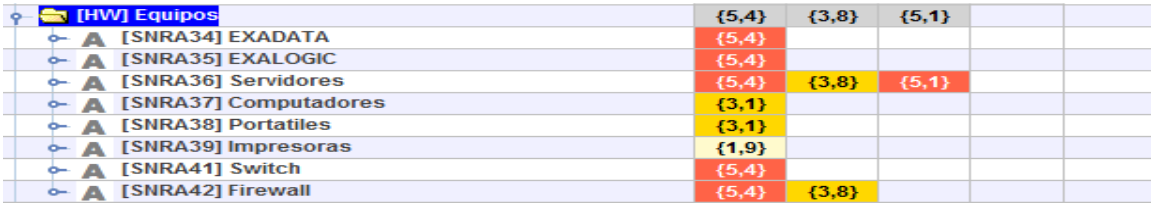
Fuente El autor

Figura 211. Representación de riesgos sobre activo equipos-Firewall

[SNRA42] Firewall	{5,4}	{3,8}			
[N.1] Fuego	{4,2}				
[N.2] Daños por agua	{3,7}				
[N.*] Desastres naturales	{4,2}				
[I.1] Fuego	{4,8}				
[I.2] Daños por agua	{4,3}				
[I.5] Avería de origen físico o lógico	{4,5}				
[I.6] Corte del suministro eléctrico	{5,1}				
[I.7] Condiciones inadecuadas de temperatura o	{5,1}				
[E.2] Errores del administrador del sistema / de la	{3,8}	{3,8}			
[E.23] Errores de mantenimiento / actualización d	{3,3}				
[E.24] Caída del sistema por agotamiento de recu	{5,4}				
[E.25] Pérdida de equipos	{3,8}				
[A.6] Abuso de privilegios de acceso	{3,3}	{3,3}			
[A.7] Uso no previsto	{3,3}	{1,5}			
[A.11] Acceso no autorizado	{3,3}	{3,3}			
[A.23] Manipulación del hardware	{4,8}				
[A.25] Robo de equipos	{3,6}				
[A.26] Ataque destructivo	{5,1}				

Fuente El autor

Figura 212. Representación de riesgos sobre activos equipos

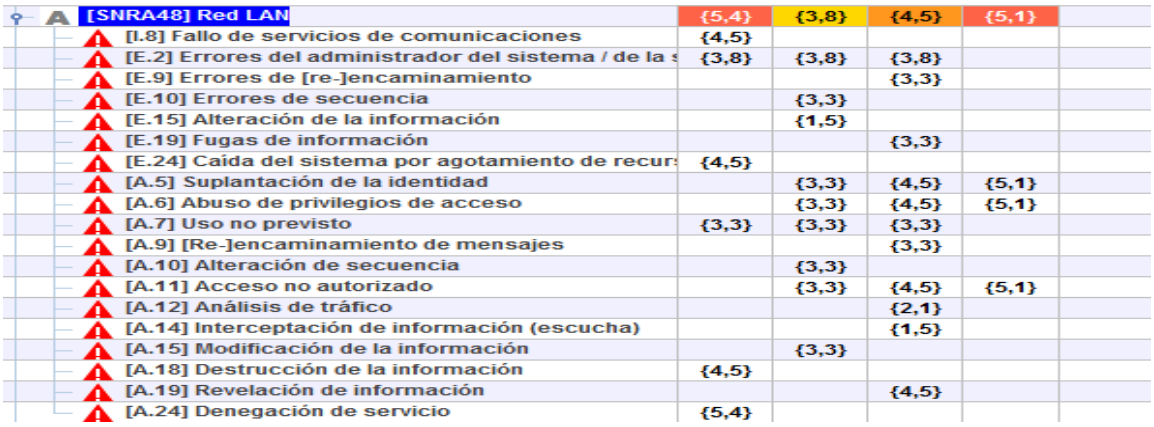


[HW] Equipos	{5,4}	{3,8}	{5,1}	
[SNRA34] EXADATA	{5,4}			
[SNRA35] EXALOGIC	{5,4}			
[SNRA36] Servidores	{5,4}	{3,8}	{5,1}	
[SNRA37] Computadores	{3,1}			
[SNRA38] Portatiles	{3,1}			
[SNRA39] Impresoras	{1,9}			
[SNRA41] Switch	{5,4}			
[SNRA42] Firewall	{5,4}	{3,8}		

Fuente El autor

[COM] Comunicaciones

Figura 213. Representación de riesgos sobre activo comunicaciones-Red LAN



[SNRA48] Red LAN	{5,4}	{3,8}	{4,5}	{5,1}
[I.8] Fallo de servicios de comunicaciones	{4,5}			
[E.2] Errores del administrador del sistema / de la	{3,8}	{3,8}	{3,8}	
[E.9] Errores de [re-]encaminamiento			{3,3}	
[E.10] Errores de secuencia		{3,3}		
[E.15] Alteración de la información		{1,5}		
[E.19] Fugas de información			{3,3}	
[E.24] Caída del sistema por agotamiento de recur	{4,5}			
[A.5] Suplantación de la identidad		{3,3}	{4,5}	{5,1}
[A.6] Abuso de privilegios de acceso		{3,3}	{4,5}	{5,1}
[A.7] Uso no previsto	{3,3}	{3,3}	{3,3}	
[A.9] [Re-]encaminamiento de mensajes			{3,3}	
[A.10] Alteración de secuencia		{3,3}		
[A.11] Acceso no autorizado		{3,3}	{4,5}	{5,1}
[A.12] Análisis de tráfico			{2,1}	
[A.14] Interceptación de información (escucha)			{1,5}	
[A.15] Modificación de la información		{3,3}		
[A.18] Destrucción de la información	{4,5}			
[A.19] Revelación de información			{4,5}	
[A.24] Denegación de servicio	{5,4}			

Fuente El autor

Figura 214. Representación de riesgos sobre activo comunicaciones-Internet

[SNRA50] Internet	{5,4}	{3,8}	{4,5}	{5,1}
[I.8] Fallo de servicios de comunicaciones	{4,5}			
[E.2] Errores del administrador del sistema / de la s	{3,8}	{3,8}	{3,8}	
[E.9] Errores de [re-]encaminamiento			{3,3}	
[E.10] Errores de secuencia		{3,3}		
[E.15] Alteración de la información		{1,5}		
[E.19] Fugas de información			{3,3}	
[E.24] Caída del sistema por agotamiento de recurs	{4,5}			
[A.5] Suplantación de la identidad		{3,3}	{4,5}	{5,1}
[A.6] Abuso de privilegios de acceso		{3,3}	{4,5}	{5,1}
[A.7] Uso no previsto	{3,3}	{3,3}	{3,3}	
[A.9] [Re-]encaminamiento de mensajes			{3,3}	
[A.10] Alteración de secuencia		{3,3}		
[A.11] Acceso no autorizado		{3,3}	{4,5}	{5,1}
[A.12] Análisis de tráfico			{2,1}	
[A.14] Interceptación de información (escucha)			{2,8}	
[A.15] Modificación de la información		{3,3}		
[A.18] Destrucción de la información	{4,5}			
[A.19] Revelación de información			{4,5}	
[A.24] Denegación de servicio	{5,4}			

Fuente El autor

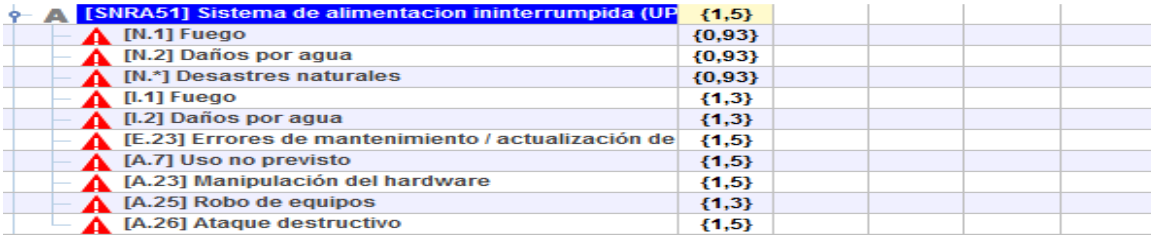
Figura 215. Representación de riesgos sobre activos comunicaciones

[COM] Comunicaciones	{5,4}	{3,8}	{4,5}	{5,1}
[SNRA48] Red LAN	{5,4}	{3,8}	{4,5}	{5,1}
[SNRA50] Internet	{5,4}	{3,8}	{4,5}	{5,1}

Fuente El autor

[AUX] Elementos auxiliares

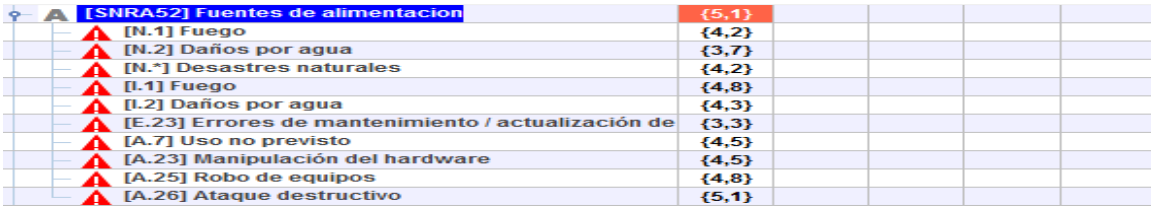
Figura 216. Representación de riesgos sobre activo elementos auxiliares-Sistema de alimentación ininterrumpida (UPS)



[SNRA51] Sistema de alimentacion ininterrumpida (UP	{1,5}
[N.1] Fuego	{0,93}
[N.2] Daños por agua	{0,93}
[N.*] Desastres naturales	{0,93}
[I.1] Fuego	{1,3}
[I.2] Daños por agua	{1,3}
[E.23] Errores de mantenimiento / actualización de	{1,5}
[A.7] Uso no previsto	{1,5}
[A.23] Manipulación del hardware	{1,5}
[A.25] Robo de equipos	{1,3}
[A.26] Ataque destructivo	{1,5}

Fuente El autor

Figura 217. Representación de riesgos sobre activo elementos auxiliares-Fuentes de alimentación



[SNRA52] Fuentes de alimentacion	{5,1}
[N.1] Fuego	{4,2}
[N.2] Daños por agua	{3,7}
[N.*] Desastres naturales	{4,2}
[I.1] Fuego	{4,8}
[I.2] Daños por agua	{4,3}
[E.23] Errores de mantenimiento / actualización de	{3,3}
[A.7] Uso no previsto	{4,5}
[A.23] Manipulación del hardware	{4,5}
[A.25] Robo de equipos	{4,8}
[A.26] Ataque destructivo	{5,1}

Fuente El autor

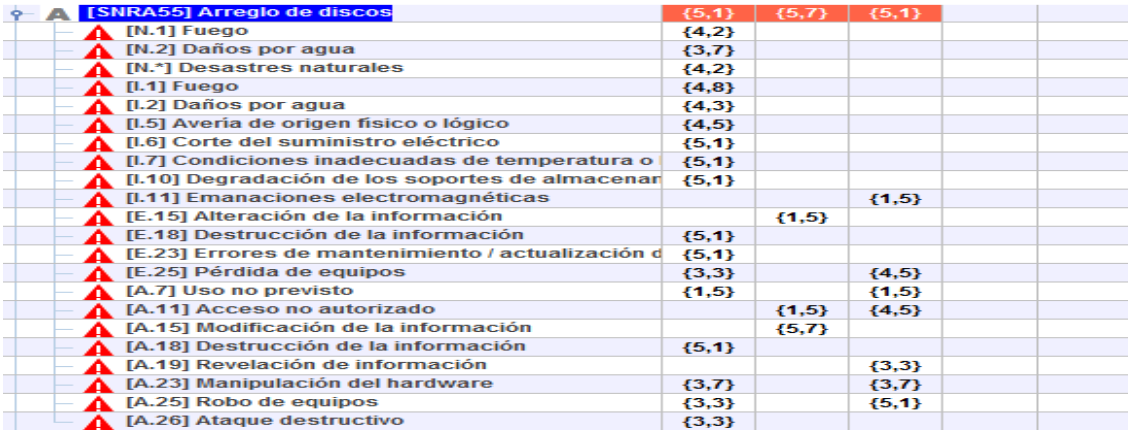
Figura 218. Representación de riesgos sobre activo elementos auxiliares-Aire acondicionado

[SNRA53] Aire acondicionado	{3,3}
[N.1] Fuego	{2,4}
[N.2] Daños por agua	{2,4}
[N.*] Desastres naturales	{2,4}
[I.1] Fuego	{3,0}
[I.2] Daños por agua	{3,0}
[I.6] Corte del suministro eléctrico	{3,3}
[I.9] Interrupción de otros servicios o suministros	{3,3}
[E.23] Errores de mantenimiento / actualización de	{3,3}
[A.7] Uso no previsto	{3,3}
[A.23] Manipulación del hardware	{3,3}
[A.25] Robo de equipos	{3,0}
[A.26] Ataque destructivo	{3,3}

Fuente El autor

[MEDIA] Soporte de información

Figura 219. Representación de riesgos sobre activo soporte de información-arreglo de discos



[SNRA55] Arreglo de discos	{5,1}	{5,7}	{5,1}
[N.1] Fuego	{4,2}		
[N.2] Daños por agua	{3,7}		
[N.*] Desastres naturales	{4,2}		
[I.1] Fuego	{4,8}		
[I.2] Daños por agua	{4,3}		
[I.5] Avería de origen físico o lógico	{4,5}		
[I.6] Corte del suministro eléctrico	{5,1}		
[I.7] Condiciones inadecuadas de temperatura o	{5,1}		
[I.10] Degradación de los soportes de almacenar	{5,1}		
[I.11] Emanaciones electromagnéticas			{1,5}
[E.15] Alteración de la información		{1,5}	
[E.18] Destrucción de la información	{5,1}		
[E.23] Errores de mantenimiento / actualización d	{5,1}		
[E.25] Pérdida de equipos	{3,3}		{4,5}
[A.7] Uso no previsto	{1,5}		{1,5}
[A.11] Acceso no autorizado		{1,5}	{4,5}
[A.15] Modificación de la información		{5,7}	
[A.18] Destrucción de la información	{5,1}		
[A.19] Revelación de información			{3,3}
[A.23] Manipulación del hardware	{3,7}		{3,7}
[A.25] Robo de equipos	{3,3}		{5,1}
[A.26] Ataque destructivo	{3,3}		

Fuente El autor

Figura 220. Representación de riesgos sobre activo soporte de información - Librería de cintas

[SNRA56] Libreria de cintas	{5,1}	{5,7}	{5,1}
[N.1] Fuego	{4,2}		
[N.2] Daños por agua	{3,7}		
[N.*] Desastres naturales	{4,2}		
[I.1] Fuego	{4,8}		
[I.2] Daños por agua	{4,3}		
[I.5] Avería de origen físico o lógico	{4,5}		
[I.6] Corte del suministro eléctrico	{5,1}		
[I.7] Condiciones inadecuadas de temperatura o	{5,1}		
[I.10] Degradación de los soportes de almacenar	{5,1}		
[I.11] Emanaciones electromagnéticas			{1,5}
[E.15] Alteración de la información		{1,5}	
[E.18] Destrucción de la información	{5,1}		
[E.23] Errores de mantenimiento / actualización d	{5,1}		
[E.25] Pérdida de equipos	{3,3}		{4,5}
[A.7] Uso no previsto	{1,5}		{1,5}
[A.11] Acceso no autorizado		{1,5}	{4,5}
[A.15] Modificación de la información		{5,7}	
[A.18] Destrucción de la información	{5,1}		
[A.19] Revelación de información			{3,3}
[A.23] Manipulación del hardware	{3,7}		{3,7}
[A.25] Robo de equipos	{3,3}		{5,1}
[A.26] Ataque destructivo	{3,3}		

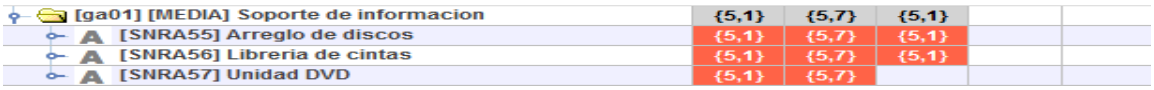
Fuente El autor

Figura 221. Representación de riesgos sobre activo soporte de información- Unidad DVD

[SNRA57] Unidad DVD	{5,1}	{5,7}	
[N.1] Fuego	{4,2}		
[N.2] Daños por agua	{3,7}		
[N.*] Desastres naturales	{4,2}		
[I.1] Fuego	{4,8}		
[I.2] Daños por agua	{4,3}		
[I.5] Avería de origen físico o lógico	{4,5}		
[I.6] Corte del suministro eléctrico	{5,1}		
[I.7] Condiciones inadecuadas de temperatura o	{5,1}		
[I.10] Degradación de los soportes de almacenar	{5,1}		
[E.15] Alteración de la información		{1,5}	
[E.18] Destrucción de la información	{5,1}		
[E.23] Errores de mantenimiento / actualización d	{5,1}		
[E.25] Pérdida de equipos	{3,3}		
[A.15] Modificación de la información		{5,7}	
[A.18] Destrucción de la información	{5,1}		
[A.23] Manipulación del hardware	{3,7}		
[A.25] Robo de equipos	{3,3}		
[A.26] Ataque destructivo	{3,3}		

Fuente El autor

Figura 222. Representación de riesgos sobre activos soporte de información



[ga01] [MEDIA] Soporte de informacion	{5,1}	{5,7}	{5,1}
[SNRA55] Arreglo de discos	{5,1}	{5,7}	{5,1}
[SNRA56] Libreria de cintas	{5,1}	{5,7}	{5,1}
[SNRA57] Unidad DVD	{5,1}	{5,7}	

Fuente El autor

[SS] Servicios subcontratados

Figura 223. Representación de riesgos sobre activo servicios subcontratados-Correo electrónico

[SNRA58] Correo electronico	{3,4}	{4,5}		{4,5}	
[I.9] Interrupción de otros servicios o suministros esei	{3,4}				
[E.15] Alteración de la información		{3,3}			
[E.18] Destrucción de la información	{2,1}				
[A.5] Suplantación de la identidad		{4,5}		{4,5}	
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{3,4}				
[A.24] Denegación de servicio	{3,4}				

Fuente El autor

Figura 224. Representación de riesgos sobre activo servicios subcontratados-Portal

[SNRA59] Portal	{3,9}		{3,3}		
[I.8] Fallo de servicios de comunicaciones	{3,9}				
[E.18] Destrucción de la información	{2,1}				
[E.19] Fugas de información			{2,1}		
[A.5] Suplantación de la identidad			{3,3}		
[A.18] Destrucción de la información	{3,4}				
[A.24] Denegación de servicio	{3,4}				

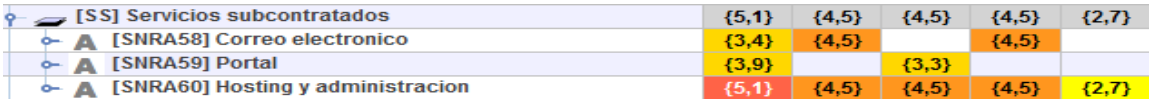
Fuente El autor

Figura 225. Representación de riesgos sobre activo servicios subcontratados-Hosting y administración

[SNRA60] Hosting y administracion	{5,1}	{4,5}	{4,5}	{4,5}	{2,7}
[I.8] Fallo de servicios de comunicaciones	{5,1}				
[E.15] Alteración de la información		{3,3}			
[E.18] Destrucción de la información	{3,3}				
[E.19] Fugas de información			{3,3}		
[A.5] Suplantación de la identidad		{4,5}	{4,5}	{4,5}	
[A.13] Repudio (negación de actuaciones)					{2,7}
[A.15] Modificación de la información		{4,5}			
[A.18] Destrucción de la información	{4,5}				
[A.19] Revelación de información			{4,5}		
[A.24] Denegación de servicio	{4,5}				

Fuente El autor

Figura 226. Representación de riesgos sobre activos servicios subcontratados

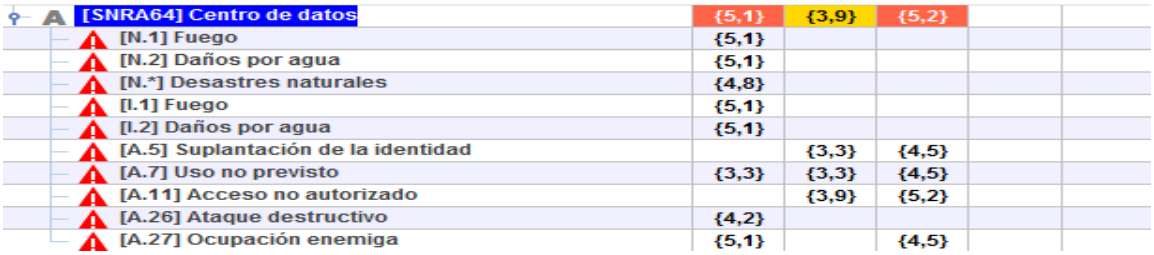


[SS] Servicios subcontratados	{5,1}	{4,5}	{4,5}	{4,5}	{2,7}
[SNRA58] Correo electronico	{3,4}	{4,5}		{4,5}	
[SNRA59] Portal	{3,9}		{3,3}		
[SNRA60] Hosting y administracion	{5,1}	{4,5}	{4,5}	{4,5}	{2,7}

Fuente El autor

[L] Instalaciones

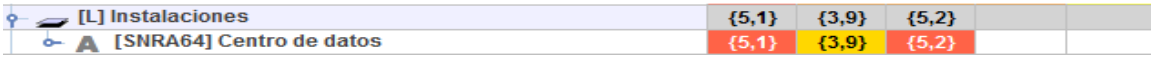
Figura 227. Representación de riesgos sobre activo instalaciones-Centro de datos



[SNRA64] Centro de datos	{5,1}	{3,9}	{5,2}
[N.1] Fuego	{5,1}		
[N.2] Daños por agua	{5,1}		
[N.*] Desastres naturales	{4,8}		
[I.1] Fuego	{5,1}		
[I.2] Daños por agua	{5,1}		
[A.5] Suplantación de la identidad		{3,3}	{4,5}
[A.7] Uso no previsto	{3,3}	{3,3}	{4,5}
[A.11] Acceso no autorizado		{3,9}	{5,2}
[A.26] Ataque destructivo	{4,2}		
[A.27] Ocupación enemiga	{5,1}		{4,5}

Fuente El autor

Figura 228. Representación de riesgos sobre activos instalaciones

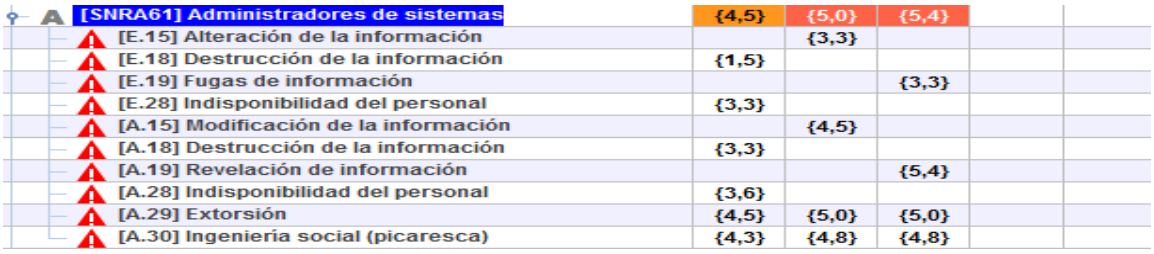


[L] Instalaciones	{5,1}	{3,9}	{5,2}
[SNRA64] Centro de datos	{5,1}	{3,9}	{5,2}

Fuente El autor

[P] Personal

Figura 229. Representación de riesgos sobre activo personal-Administradores de sistemas



[SNRA61] Administradores de sistemas	{4,5}	{5,0}	{5,4}
[E.15] Alteración de la información		{3,3}	
[E.18] Destrucción de la información	{1,5}		
[E.19] Fugas de información			{3,3}
[E.28] Indisponibilidad del personal	{3,3}		
[A.15] Modificación de la información		{4,5}	
[A.18] Destrucción de la información	{3,3}		
[A.19] Revelación de información			{5,4}
[A.28] Indisponibilidad del personal	{3,6}		
[A.29] Extorsión	{4,5}	{5,0}	{5,0}
[A.30] Ingeniería social (picaresca)	{4,3}	{4,8}	{4,8}

Fuente El autor

Figura 230. Representación de riesgos sobre activo personal-Administradores de comunicaciones

[SNRA62] Administradores de comunicaciones	{4,5}	{4,5}	{4,5}
[E.15] Alteración de la información		{3,3}	
[E.18] Destrucción de la información	{1,5}		
[E.19] Fugas de información			{3,3}
[E.28] Indisponibilidad del personal	{3,3}		
[A.15] Modificación de la información		{4,5}	
[A.18] Destrucción de la información	{3,3}		
[A.19] Revelación de información			{4,5}
[A.28] Indisponibilidad del personal	{3,6}		
[A.29] Extorsión	{4,5}	{4,5}	{4,5}
[A.30] Ingeniería social (picaresca)	{4,3}	{4,3}	{4,3}

Fuente El autor

Figura 231. Representación de riesgos sobre activo personal-Administradores de bases de datos

[SNRA63] Administradores de bases de datos	{4,5}	{5,0}	{5,4}
[E.15] Alteración de la información		{3,3}	
[E.18] Destrucción de la información	{1,5}		
[E.19] Fugas de información			{3,3}
[E.28] Indisponibilidad del personal	{3,8}		
[A.15] Modificación de la información		{4,5}	
[A.18] Destrucción de la información	{3,3}		
[A.19] Revelación de información			{5,4}
[A.28] Indisponibilidad del personal	{3,0}		
[A.29] Extorsión	{4,5}	{5,0}	{5,0}
[A.30] Ingeniería social (picaresca)	{4,3}	{4,8}	{4,8}

Fuente El autor

Figura 232. Representación de riesgos sobre activos personal

[P] Personal	{4,5}	{5,0}	{5,4}
[SNRA61] Administradores de sistemas	{4,5}	{5,0}	{5,4}
[SNRA62] Administradores de comunicaciones	{4,5}	{4,5}	{4,5}
[SNRA63] Administradores de bases de datos	{4,5}	{5,0}	{5,4}

Fuente El autor

Valores repercutidos - Impacto

Figura 233. Representación impacto sobre activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[7]	[7]	[7]	[7]	[3]
[SNRA01] Formato administracion cuentas de usuarios		[7]		[7]	
[I] integridad de los datos		[7]			
[A] autenticidad de los usuarios y de la información				[7]	
[SNRA02] Registros de recurso					
[I] integridad de los datos					
[SNRA04] Autenticacion de usuarios	[7]			[7]	
[D] disponibilidad	[7]				
[A] autenticidad de los usuarios y de la información				[7]	
[SNRA06] Directorio activo	[7]			[7]	
[D] disponibilidad	[7]				
[A] autenticidad de los usuarios y de la información				[7]	
[SNRA07] Servicio de nombres de dominio (DNS)	[7]				
[D] disponibilidad	[7]				
[SNRA08] DHCP	[7]				
[D] disponibilidad	[7]				
[SNRA09] BIOMETRICO	[3]				[3]
[D] disponibilidad	[3]				
[T] trazabilidad del servicio y de los datos					[3]
[SW.SNRA10] Sistema de informacion notarial (SIN)	[5]	[7]			
[D] disponibilidad	[5]				
[I] integridad de los datos		[7]			
[SW.SNRA11] Sistema de personal y nomina	[3]	[7]			
[D] disponibilidad	[3]				
[I] integridad de los datos		[7]			
[SW.SNRA13] IRIS documental	[7]				[1]
[D] disponibilidad	[7]				
[T] trazabilidad del servicio y de los datos					[1]

Fuente El autor

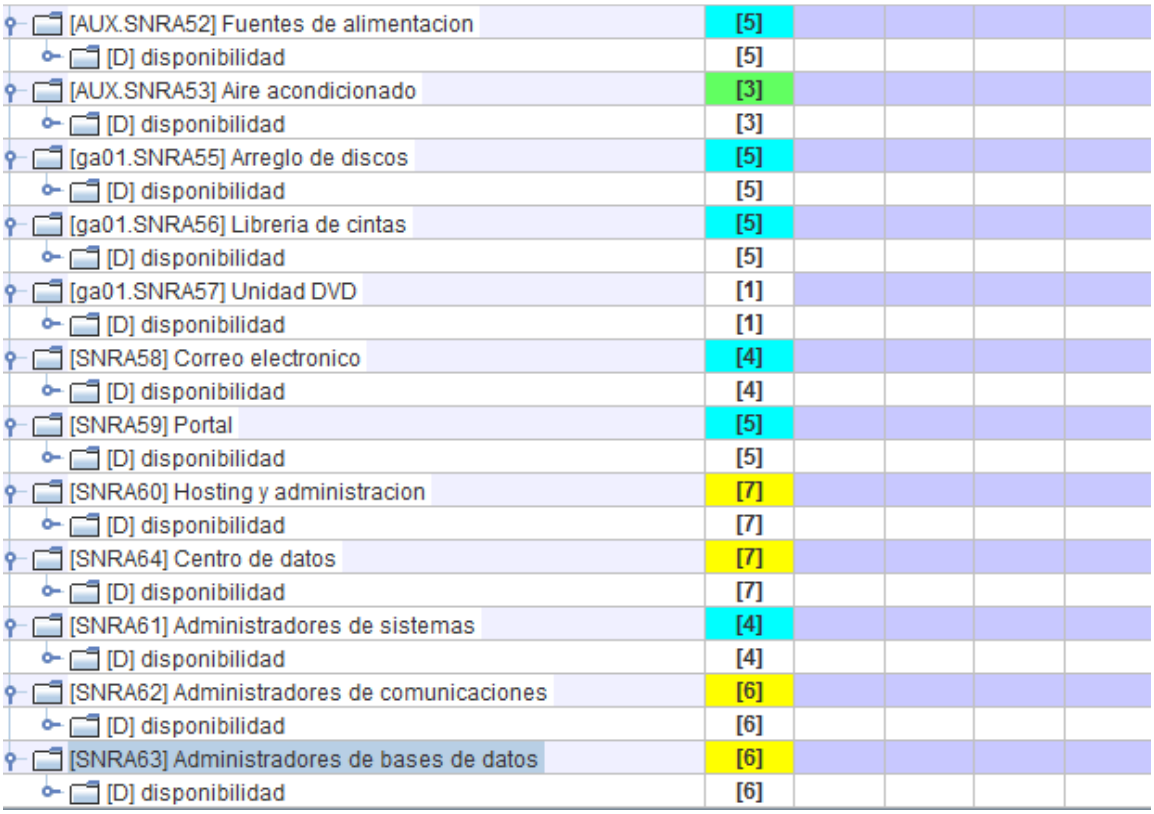
Figura 233. (Continuación)

[SW.SNRA14] Sistema de procesos judiciales	[3]	[7]	[7]		
[D] disponibilidad	[3]				
[I] integridad de los datos		[7]			
[C] confidencialidad de los datos			[7]		
[SW.SNRA15] Hoja de vida de notarios	[3]	[5]			
[D] disponibilidad	[3]				
[I] integridad de los datos		[5]			
[SW.SNRA16] Sistema de control interno disciplinario	[3]	[5]	[4]		
[D] disponibilidad	[3]				
[I] integridad de los datos		[5]			
[C] confidencialidad de los datos			[4]		
[SW.SNRA17] Sistema de control interno disciplinario notarias	[5]	[5]	[4]		
[D] disponibilidad	[5]				
[I] integridad de los datos		[5]			
[C] confidencialidad de los datos			[4]		
[SW.SNRA18] Sistema integrado web	[3]				
[D] disponibilidad	[3]				
[SW.SNRA20] Interrelacion registro-catastro	[3]	[5]			
[D] disponibilidad	[3]				
[I] integridad de los datos		[5]			
[SW.SNRA24] Boton de pago	[5]		[5]		
[D] disponibilidad	[5]				
[C] confidencialidad de los datos			[5]		
[SW.SNRA26] Ventanilla unica de registro (VUR)	[3]				
[D] disponibilidad	[3]				

Figura 233. (Continuación)

[SW.SNRA32] Netbackup	[1]				
[D] disponibilidad	[1]				
[SW.SNRA33] Oracle Virtual Machine (OVM)	[1]				
[D] disponibilidad	[1]				
[SW.SNRA21] Endpointsecurity	[7]				
[D] disponibilidad	[7]				
[HW.SNRA34] EXADATA	[7]				
[D] disponibilidad	[7]				
[HW.SNRA35] EXALOGIC	[7]				
[D] disponibilidad	[7]				
[HW.SNRA36] Servidores	[7]				
[D] disponibilidad	[7]				
[HW.SNRA37] Computadores	[3]				
[D] disponibilidad	[3]				
[HW.SNRA38] Portatiles	[3]				
[D] disponibilidad	[3]				
[HW.SNRA39] Impresoras	[1]				
[D] disponibilidad	[1]				
[HW.SNRA41] Switch	[5]				
[D] disponibilidad	[5]				
[HW.SNRA42] Firewall	[7]				
[D] disponibilidad	[7]				
[COM.SNRA48] Red LAN	[7]				
[D] disponibilidad	[7]				
[COM.SNRA50] Internet	[5]				
[D] disponibilidad	[5]				
[AUX.SNRA51] Sistema de alimentacion ininterrumpida (UPS)	[1]				
[D] disponibilidad	[1]				

Figura 233. (Continuación)



[AUX.SNRA52] Fuentes de alimentacion	[5]				
[D] disponibilidad	[5]				
[AUX.SNRA53] Aire acondicionado	[3]				
[D] disponibilidad	[3]				
[ga01.SNRA55] Arreglo de discos	[5]				
[D] disponibilidad	[5]				
[ga01.SNRA56] Libreria de cintas	[5]				
[D] disponibilidad	[5]				
[ga01.SNRA57] Unidad DVD	[1]				
[D] disponibilidad	[1]				
[SNRA58] Correo electronico	[4]				
[D] disponibilidad	[4]				
[SNRA59] Portal	[5]				
[D] disponibilidad	[5]				
[SNRA60] Hosting y administracion	[7]				
[D] disponibilidad	[7]				
[SNRA64] Centro de datos	[7]				
[D] disponibilidad	[7]				
[SNRA61] Administradores de sistemas	[4]				
[D] disponibilidad	[4]				
[SNRA62] Administradores de comunicaciones	[6]				
[D] disponibilidad	[6]				
[SNRA63] Administradores de bases de datos	[6]				
[D] disponibilidad	[6]				

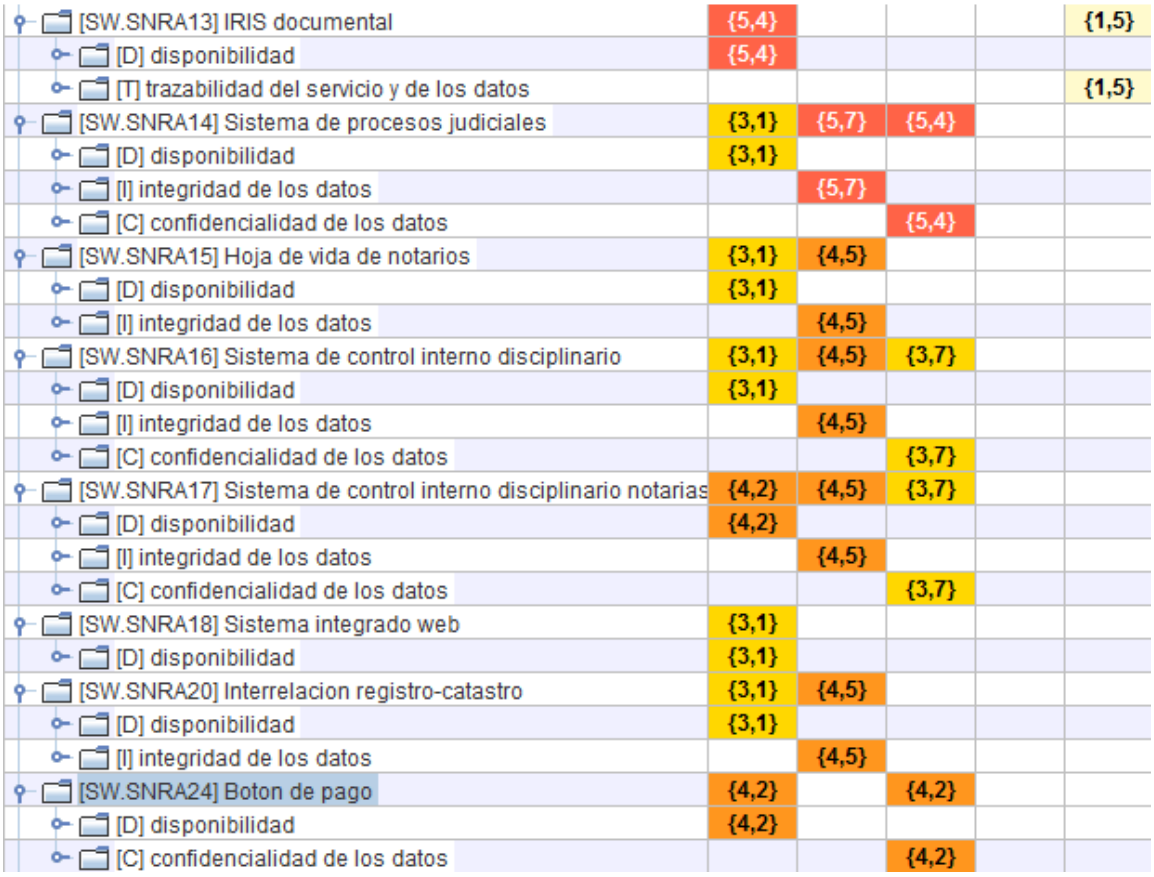
Valores repercutidos - Riesgo

Figura 234. Representación riesgos sobre activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{5,4}	{5,7}	{5,4}	{5,7}	{3,3}
[SNRA01] Formato administracion cuentas de usuarios		{5,7}		{5,7}	
[I] integridad de los datos		{5,7}			
[A] autenticidad de los usuarios y de la información				{5,7}	
[SNRA02] Registros de recurso					
[I] integridad de los datos					
[SNRA04] Autenticacion de usuarios	{5,4}			{5,7}	
[D] disponibilidad	{5,4}				
[A] autenticidad de los usuarios y de la información				{5,7}	
[SNRA06] Directorio activo	{5,4}			{5,1}	
[D] disponibilidad	{5,4}				
[A] autenticidad de los usuarios y de la información				{5,1}	
[SNRA07] Servicio de nombres de dominio (DNS)	{5,4}				
[D] disponibilidad	{5,4}				
[SNRA08] DHCP	{5,4}				
[D] disponibilidad	{5,4}				
[SNRA09] BIOMETRICO	{3,1}				{3,3}
[D] disponibilidad	{3,1}				
[T] trazabilidad del servicio y de los datos					{3,3}
[SW.SNRA10] Sistema de informacion notarial (SIN)	{4,2}	{5,7}			
[D] disponibilidad	{4,2}				
[I] integridad de los datos		{5,7}			
[SW.SNRA11] Sistema de personal y nomina	{3,1}	{5,7}			
[D] disponibilidad	{3,1}				
[I] integridad de los datos		{5,7}			

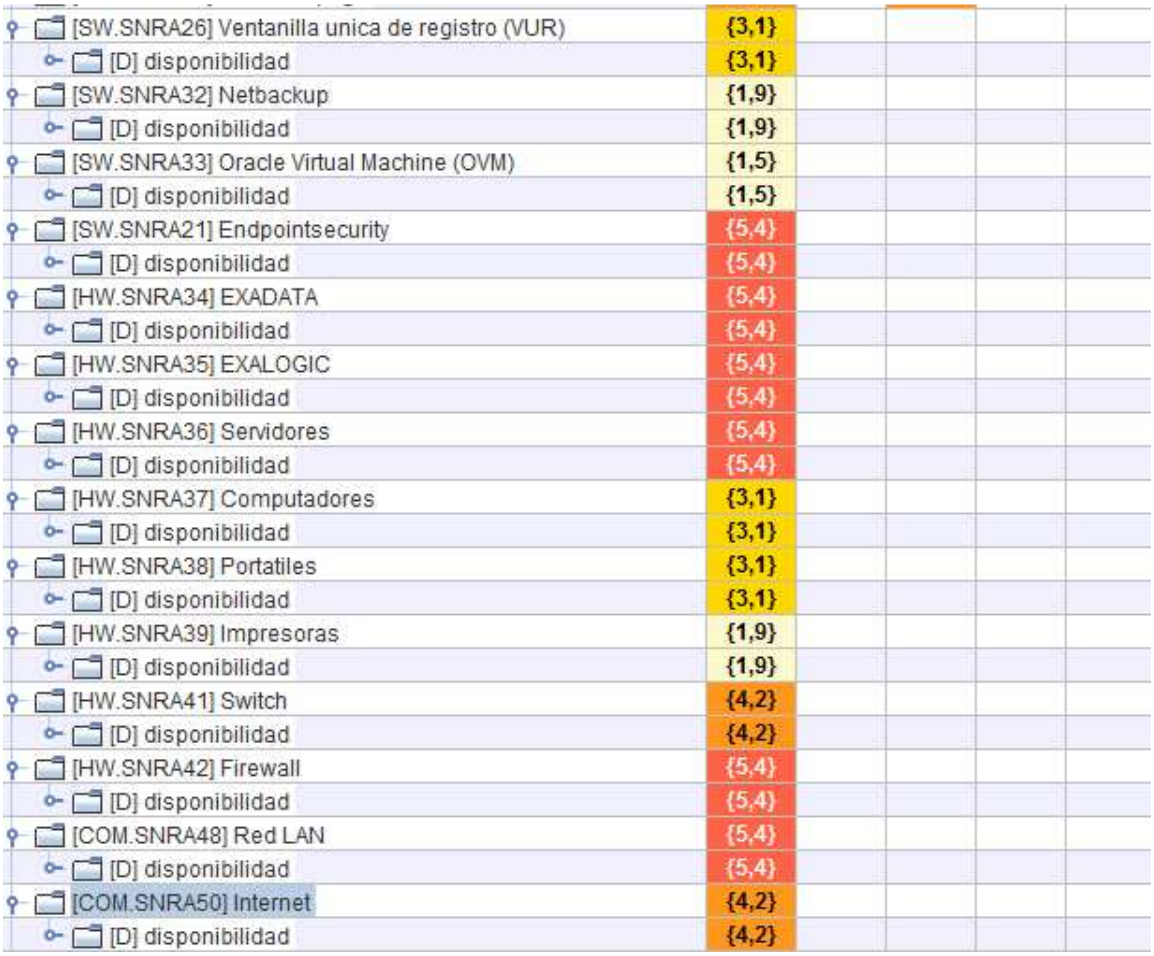
Fuente El autor

Figura 234. (Continuación)



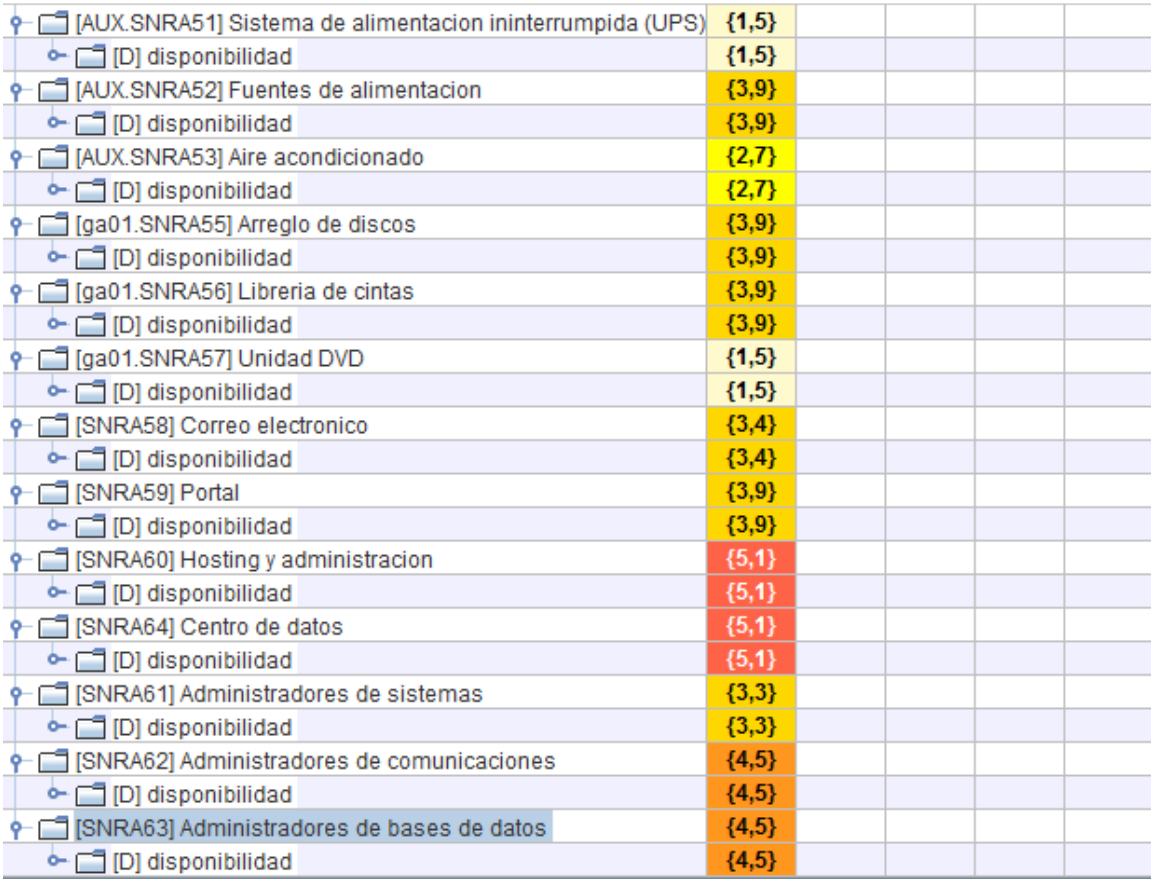
[SW.SNRA13] IRIS documental	{5,4}				{1,5}
[D] disponibilidad	{5,4}				
[T] trazabilidad del servicio y de los datos					{1,5}
[SW.SNRA14] Sistema de procesos judiciales	{3,1}	{5,7}	{5,4}		
[D] disponibilidad	{3,1}				
[I] integridad de los datos		{5,7}			
[C] confidencialidad de los datos			{5,4}		
[SW.SNRA15] Hoja de vida de notarios	{3,1}	{4,5}			
[D] disponibilidad	{3,1}				
[I] integridad de los datos		{4,5}			
[SW.SNRA16] Sistema de control interno disciplinario	{3,1}	{4,5}	{3,7}		
[D] disponibilidad	{3,1}				
[I] integridad de los datos		{4,5}			
[C] confidencialidad de los datos			{3,7}		
[SW.SNRA17] Sistema de control interno disciplinario notarias	{4,2}	{4,5}	{3,7}		
[D] disponibilidad	{4,2}				
[I] integridad de los datos		{4,5}			
[C] confidencialidad de los datos			{3,7}		
[SW.SNRA18] Sistema integrado web	{3,1}				
[D] disponibilidad	{3,1}				
[SW.SNRA20] Interrelacion registro-catastro	{3,1}	{4,5}			
[D] disponibilidad	{3,1}				
[I] integridad de los datos		{4,5}			
[SW.SNRA24] Boton de pago	{4,2}		{4,2}		
[D] disponibilidad	{4,2}				
[C] confidencialidad de los datos			{4,2}		

Figura 234. (Continuación)



[SW.SNRA26] Ventanilla unica de registro (VUR)	{3,1}
[D] disponibilidad	{3,1}
[SW.SNRA32] Netbackup	{1,9}
[D] disponibilidad	{1,9}
[SW.SNRA33] Oracle Virtual Machine (OVM)	{1,5}
[D] disponibilidad	{1,5}
[SW.SNRA21] Endpointsecurity	{5,4}
[D] disponibilidad	{5,4}
[HW.SNRA34] EXADATA	{5,4}
[D] disponibilidad	{5,4}
[HW.SNRA35] EXALOGIC	{5,4}
[D] disponibilidad	{5,4}
[HW.SNRA36] Servidores	{5,4}
[D] disponibilidad	{5,4}
[HW.SNRA37] Computadores	{3,1}
[D] disponibilidad	{3,1}
[HW.SNRA38] Portatiles	{3,1}
[D] disponibilidad	{3,1}
[HW.SNRA39] Impresoras	{1,9}
[D] disponibilidad	{1,9}
[HW.SNRA41] Switch	{4,2}
[D] disponibilidad	{4,2}
[HW.SNRA42] Firewall	{5,4}
[D] disponibilidad	{5,4}
[COM.SNRA48] Red LAN	{5,4}
[D] disponibilidad	{5,4}
[COM.SNRA50] Internet	{4,2}
[D] disponibilidad	{4,2}

Figura 234. (Continuación)



[AUX.SNRA51] Sistema de alimentacion ininterrumpida (UPS)	{1,5}
[D] disponibilidad	{1,5}
[AUX.SNRA52] Fuentes de alimentacion	{3,9}
[D] disponibilidad	{3,9}
[AUX.SNRA53] Aire acondicionado	{2,7}
[D] disponibilidad	{2,7}
[ga01.SNRA55] Arreglo de discos	{3,9}
[D] disponibilidad	{3,9}
[ga01.SNRA56] Libreria de cintas	{3,9}
[D] disponibilidad	{3,9}
[ga01.SNRA57] Unidad DVD	{1,5}
[D] disponibilidad	{1,5}
[SNRA58] Correo electronico	{3,4}
[D] disponibilidad	{3,4}
[SNRA59] Portal	{3,9}
[D] disponibilidad	{3,9}
[SNRA60] Hosting y administracion	{5,1}
[D] disponibilidad	{5,1}
[SNRA64] Centro de datos	{5,1}
[D] disponibilidad	{5,1}
[SNRA61] Administradores de sistemas	{3,3}
[D] disponibilidad	{3,3}
[SNRA62] Administradores de comunicaciones	{4,5}
[D] disponibilidad	{4,5}
[SNRA63] Administradores de bases de datos	{4,5}
[D] disponibilidad	{4,5}

Análisis de riesgos - Lectura y resultados

Identificación

De acuerdo al esquema de la herramienta PILAR para la identificación de los activos, estos fueron organizados en capas y grupos. Lo que permite apreciar que los activos son de muy distinta naturaleza lo que exige la consideración de medidas de diversa índole para su protección.

Dependencias

Gran parte de los activos están íntimamente relacionados en mayor o menor grado, Lo que conlleva a considerar que la afectación de seguridad de un activo puede repercutir en el activo (s) que dependen de él.

En el caso particular de la red LAN puede apreciarse lo siguiente:

1). Su dependencia de otros activos tales como: sistema de alimentación interrumpida UPS, fuentes de alimentación, centro de datos, administradores de comunicaciones.
2). La casi totalidad de los activos tienen una gran dependencia del activo red LAN.

Valoración

- La Disponibilidad es el dominio de seguridad donde se ubican los activos con mayor valoración. Lo que lleva a considerar en primera instancia que los activos cuya disponibilidad resultan ser esenciales para la operación del departamento de informática son: Autenticación de usuarios, directorio activo, DNS, DHCP, hosting y administración, administradores de comunicaciones, administradores de bases de datos, correo electrónico, portal, administradores de sistemas, red LAN.

En el caso particular del activo red LAN su valoración en la dimensión de seguridad disponibilidad permite concluir que es imprescindible en el desarrollo de las actividades darías del departamento de informática y la entidad en general.

- La Integridad es el dominio de seguridad donde se aprecia que las aplicaciones reportan los mayores valores de importancia, especialmente las siguientes aplicaciones: Sistema de información notarial (SIN), sistema de personal y nomina, sistema de procesos judiciales. Sin embargo también se visualiza la importancia que tienen los datos que se registran en el activo formato administración cuentas de usuarios.
- Los valores que se observan en el dominio de seguridad confidencialidad permiten determinar que son especialmente relevantes las aplicaciones que involucran el tratamiento de información de carácter reservado como procesos judiciales y disciplinarios (sistema de procesos judiciales, sistema de control interno disciplinario, sistema de control interno disciplinario notarias). Así como aplicaciones que exigen la reserva de información de usuarios como es el caso de la aplicación botón de pago.
- Los valores que se observan en el dominio de seguridad autenticidad permiten inferir que para el departamento de informática son de extremada importancia como elementos de control e identificación los activos formato administración cuentas de usuarios, autenticación de usuarios y directorio activo.

Amenazas

- Los tipos de amenazas con mayor predominio a las que están expuestos los activos son: Errores y fallos no intencionados, ataques deliberados, de origen industrial y desastres naturales.

- En el caso del activo red LAN es apreciable que el mayor numero de amenazas que podrían afectarle son las amenazas enmarcadas dentro del tipo ataques deliberados, que dicho en otras palabras son amenazas de origen interno o externo propiciados para perjudicar la operación del departamento de informática y por ende de la entidad.
- Las amenazas que registran mayor valor de frecuencia o probabilidad de ocurrencia sobre los activos (diferente de aplicaciones) son:

1). [E.24] Caída del sistema por agotamiento de recursos Frec.:10
2). [A.15] Modificación de la información Frec.:10
3). [A.24] Denegación de servicio Frec.:10
4). [A.19] Revelación de información Frec.:10

Lo que quiere decir que la probabilidad de ocurrencia es alta.
- Las amenazas que registran mayor valor de frecuencia o probabilidad de ocurrencia sobre los activos aplicaciones son:

1). [E.21] Errores de mantenimiento/actualización de programas Frec.:10

Lo que quiere decir que la probabilidad de ocurrencia es alta.
- En el caso del activo red LAN se pueden establecer las siguientes consideraciones:

1). En general la frecuencia o probabilidad de ocurrencia de las amenazas a las que está expuesto son de valoración baja (1). Sin embargo existe una amenaza de especial consideración "denegación de servicio" que tiene una frecuencia o probabilidad de ocurrencia de valoración alta (10). Al tener tal valor de probabilidad significa que puede ocurrir en cualquier momento lo que afectaría por completo las actividades del departamento de informática y la entidad en general al no poder hacer uso de las aplicaciones y servicios.
2). Los niveles de degradación son variables presentándose los valores más altos en la dimensión de seguridad autenticidad en donde por ejemplo ante la materialización de una amenaza dentro de la categoría de ataque deliberado como por ejemplo "acceso no autorizado" (suponga acceso a los gabinetes de comunicaciones) podría degradar el activo en valor de 100% lo que significa un perjuicio total sobre el activo.

Impacto y Riesgo

Valores repercutidos - Impacto

- La materialización de las amenazas sobre los activos del departamento de Informática podrían afectar muy negativamente el estado de los mismos y generar distintos niveles de impactó. Si se tiene en cuenta que en general todas las dimensiones de seguridad registran valores de afectación con valores de impacto

que van desde 7 lo que significa una valoración extremadamente crítica hasta 1 lo que significa una valoración baja.

- En la dimensión de seguridad disponibilidad se aprecian la mayor cantidad de valores de impacto. Lo que indica que ante la materialización de las amenazas lo que más impactaría al departamento de informática seria la disponibilidad de los activos. De acuerdo a lo anterior los activos que registrarían mayor índice de impacto ante la materialización de las amenazas serian: directorio activo, Dns, Dhcp, IRIS documental, endpointsecurity, exadata, exalogic, servidores, firewall, red LAN, hosting y administración, centro de datos. Con valoración de 7 lo que significa extremadamente crítico.
- En la dimensión de seguridad integridad los activos que registran mayor nivel de impacto ante la materialización de cualquier amenaza serian: formato administración cuentas de usuarios, sistema de información notarial SIN, sistema de personal y nomina, sistema de procesos judiciales. Con valoración de 7 lo que significa extremadamente crítico.
- En la dimensión de seguridad confidencialidad los activos que registran mayor nivel de impacto ante la materialización de cualquier amenaza serian: sistema de procesos judiciales. Con valoración de 7 lo que significa extremadamente crítico.
- En la dimensión de seguridad autenticidad los activos que registran mayor nivel de impacto ante la materialización de cualquier amenaza serian: formato administración de cuentas de usuarios, directorio activo, autenticación de usuarios. Con valoración de 7 lo que significa extremadamente crítico.
- En la dimensión de seguridad trazabilidad los activos que registran mayor nivel de impacto ante la materialización de cualquier amenaza serian: Biométrico. Con valoración de 3 lo que significa alto.
- En relación al activo red LAN, se puede apreciar que ante la materialización de cualquier amenaza su nivel de impacto es muy alto con valoración de 7 lo que significa extremadamente crítico. De tal manera que su afectación en relación a la disponibilidad impactaría enormemente la operación del departamento de informática y por ende a toda la entidad.

Valores repercutidos - Riesgo

- En general el nivel de riesgo de los activos del departamento de Informática es muy alto si se consideran los siguientes valores generales: Disponibilidad (5,4), Integridad (5,7), Confidencialidad (5,4), Autenticidad (5,7), Trazabilidad (3,3).
- En resumen los activos con mayor nivel de riesgo (dentro del rango de valoración crítica) están organizados bajo el siguiente orden:

1). Riesgos disponibilidad. Donde se pueden ver afectados en gran medida los activos agrupados especialmente en: servicios internos, equipamiento-equipos, equipamiento-comunicaciones, servicios subcontratados, instalaciones.
2). Riesgos integridad. Donde se pueden ver afectados en gran medida los activos agrupados especialmente en: equipamiento-aplicaciones.

3). Riesgos confidencialidad. Donde se pueden ver afectados en gran medida los activos agrupados especialmente en: equipamiento-aplicaciones.
4). Riesgos autenticidad. Donde se pueden ver afectados en gran medida los activos agrupados especialmente en: activos esenciales, servicios internos.

- En relación al activo red LAN su nivel de riesgo está enmarcado solo dentro de la dimensión de seguridad disponibilidad y su valoración se ubica dentro del nivel crítico. Lo que significa que existe un alto riesgo que ante la materialización de cualquier amenaza la disponibilidad de la red se vea afectada con un impacto muy crítico. Lo que a su vez exige el mayor nivel de atención posible considerando todas las medidas de seguridad que sean posibles para asegurar ante todo su disponibilidad sin olvidar que la casi totalidad de los activos del departamento de informática como se puede apreciar en el grafo de dependencias dependen directamente del mismo.

4.1.3.4 Resumen valoración situación actual. Como resultado del recaudo, estudio y análisis de la información obtenida durante la fase de levantamiento de la información, así como producto del análisis de riesgo es necesario considerar las siguientes situaciones:

- Si bien es cierto existen algunos procedimientos que podrían orientar en la ejecución de algunas actividades, muchos de tales procedimientos no han sido revisados y renovados para adaptarse a las nuevas necesidades. Así mismo su existencia no es divulgada y por lo tanto no son considerados y tenidos en cuenta por las personas adscritas al departamento de informática, de hecho se ha podido evidenciar como resultado de procesos de auditoría de calidad que existe un desconocimiento total de los procesos y procedimiento propios del departamento de informática.
- Aunque existe un documento oficial denominado "Políticas de seguridad en los sistemas de información". Donde se establecen las políticas de seguridad de la entidad y que en su momento fue diseñado por el departamento de informática. valorado y aprobado formalmente por la dirección general. se evidencian las siguientes situaciones:

a). Desde su diseño y promulgación en el año 2008, el documento de políticas de seguridad de la entidad no han sido revisadas formalmente para su ajuste a las nuevas necesidades.
b). Al interior del departamento de informática no existe ninguna persona responsable de evaluar que las políticas de seguridad se estén aplicando correctamente tanto en el departamento de informática como en toda la entidad. Por lo tanto existe un desconocimiento total acerca de la efectividad o no de las políticas de seguridad existentes actualmente.
c). Debido a la modernización permanente de la entidad desde el punto de vista tecnológico y al ofrecimiento regular de servicios a la ciudadanía. se hace

absolutamente necesario la revisión y actualización de las actuales políticas de seguridad que se ajusten a las nuevas realidades.
d). Las políticas de seguridad de la entidad no son divulgadas a través de ningún medio para conocimiento de los usuarios.
e). A las personas que se incorporan a la entidad y en concreto al departamento de informática ya sea que se incorporen como funcionarios o contratistas no se les hace una presentación oficial de las políticas de seguridad existentes en la entidad.
e). Existe un desconocimiento generalizado sobre las políticas de seguridad por parte de los actuales funcionarios y contratistas del departamento de informática.
f). A las empresas contratadas para la prestación de servicios o implementación de soluciones tecnológicas no se les presenta, ni se les exige la observación y aplicación de las políticas de seguridad de la entidad.
g). En el diseño e implementación de proyectos no se tienen en cuenta las políticas de seguridad de la entidad.
h). No existe un grupo de seguridad o en su defecto una persona con el entrenamiento y conocimiento necesario en temas de seguridad que se responsabilice de la aplicación y seguimiento de las políticas de seguridad, así como del planteamiento de nuevas políticas de seguridad.

- El proceso de creación de las cuentas de usuarios y contraseñas no se encuentra estandarizado, de tal manera que cada administrador de aplicaciones o sistemas de información define autónomamente como proceder.
- Los administradores de aplicaciones y sistemas de información no aplican ningún control de seguridad que exija el cambio de contraseñas de manera periódica.
- Los administradores de aplicaciones y sistemas de información en muchos casos desconocen las características generales de las plataformas en las que se encuentran almacenadas tales aplicaciones.
- En muchos casos no se evidencia que los administradores de aplicaciones y sistemas de información registren formalmente la creación y/o eliminación de las cuentas de usuarios.
- En la mayoría de los casos los administradores de sistemas y aplicaciones utilizan la cuenta de usuario root o de administrador local principal para llevar a cabo sus tareas habituales.
- Los administradores de sistemas y aplicaciones no siguen un procedimiento formal para el registro de contraseñas de la cuenta local administrador (root, administrador, administrator). Sino que por el contrario esta es aprendida de memoria por parte de la persona responsable del sistema o aplicación.
- Los administradores de sistemas y aplicaciones no llevan una documentación formal (hoja de vida de servidores, características generales de aplicaciones, administración de aplicaciones y servicios, procedimientos de copia de seguridad, procedimientos de apagado y encendido, etc.). De los activos bajo su responsabilidad. Lo que genera serios inconvenientes cuando la persona responsable de la administración del activo renuncia o se le termina el contrato. Situación que se agrava mucho más si se tiene en cuenta que por costumbre a las

personas se les asigna la responsabilidad de administración de cualquier activo pero no se asignan otras personas que apoyen en su administración y ante la ausencia del responsable principal la segunda persona a cargo pueda seguir llevando a cabo la administración sin inconveniente alguno.

- En muchos casos los administradores de sistemas y aplicaciones permiten el acceso remoto a terceros para efecto de revisar o solucionar problemas técnicos sin considerar las mínimas medidas de seguridad. Así como también es común que los administradores de sistemas y aplicaciones ingresen a los activos bajo su responsabilidad desde sus hogares sin que de antemano se evalúen los riesgos a que pueden estar expuestos los activos y especialmente la información. No se evalúan los mínimos requisitos de seguridad que debe cumplir toda persona responsable de administrar activos para acceder a los mismos desde fuera de las instalaciones del departamento de informática.

No existen herramientas formales y aprobadas institucionalmente para el acceso remoto a los activos, De tal manera que se hace uso de herramientas poco seguras y de acceso público como TeamViewer.

- Para la asignación de responsabilidades no siempre son tenidos en cuenta los perfiles de las personas y normalmente obedece a decisiones inconsultas por parte de la dirección del departamento de informática.
- A las personas sean funcionarios o contratistas se les asigna la administración de los activos, algunos con información relevante y trascendental para la organización sin considerar la aplicación de un documento de confidencialidad que garantice la confidencialidad y privacidad de la información.
- No existen controles de auditoría que permitan identificar si las personas responsables de sistemas y aplicaciones están administrando correctamente la información. Al igual que no existen controles que permitan salvaguardar la información frente a robo, alteración, etc., Por parte de los administradores o responsables.
- No se diseñan planes de capacitación que permitan mantener actualizados los conocimientos de las personas encargadas de administrar los distintos sistemas y aplicaciones. Lo que incrementa las posibilidades de que se comentan errores que puedan afectar la funcionalidad de los sistemas. En cuanto al tema de seguridad de la información por parte de los administradores de sistemas y aplicaciones, se aprecia una ignorancia total del tema.
- El formulario para la administración de usuarios nuevos, activos e inactivos. Que se utiliza para la creación de cuentas de usuarios, puede convertirse en un problema de seguridad ya que no existe la forma de evidenciar la legitimidad de las firmas de las personas que tienen la autoridad para emitir tales solicitudes.
- Ante la falta de conciencia y como consecuencia de la falta total de jornadas periódicas de inducción y capacitación sobre seguridad de la información y sobre las políticas de seguridad definidas en la entidad las personas suelen llevar a cabo practicas indebidas como: prestar sus cuentas de usuarios, divulgar sus contraseñas, dejar desprotegidas sus inicios de sesión, etc. Lo que evidentemente puede dar lugar a la materialización de amenazas como robo, alteración, borrado, etc., de la información propiedad de la persona titular de la cuenta de usuario.

- Por la falta de lineamientos institucionales se observa que si bien las personas suelen ingresar a la entidad bajo nombramiento o contrato. En el momento del ingreso a la institución se suele generar ticket o se emiten oficios para la creación de cuentas de usuarios y asignación de permisos. Pero desafortunadamente no suelen aplicarse los mismo mecanismos para cuando una persona abandona la entidad con lo cual muchas veces prevalecen cuentas de usuarios activas de personas que ya no laboran en la entidad generándose un riesgo de seguridad importante que puede dar lugar a la suplantación de identidad.
- Ante la falta de supervisión y aplicación de las políticas de seguridad existen situaciones y conductas que permiten la proliferación de software dañino al interior del departamento de informática y la entidad en general. Se pueden evidenciar las siguientes conductas que facilitan la presencia y distribución de software dañino:

a). El uso de dispositivos de almacenamiento extraíbles no se encuentra restringido.

b). El uso de cuentas de correos privadas (Yahoo, Gmail, etc.). No se encuentra restringido.

c). El servicio de Internet a los usuarios se habilita sin mayores exigencias.

d). En el caso de los usuarios del departamento de informática, suelen ingresar a los equipos con cuentas de administrador local lo que les permite la instalación de programas sin ningún tipo de restricción. Esto a pesar de que existe un dominio local en donde cada individuo deberá tener asignada una cuenta de usuario de dominio y operar su equipo de trabajo con tal cuenta.

- En razón a que algunos usuarios suelen trabajar en sus equipos con cuenta local administrador. Con frecuencia alteran o modifican las configuraciones de seguridad de los equipos para según ellos solventar alguna necesidad.
- Los equipos de los usuarios, al igual que los servidores no cuentan con las ultimas actualizaciones de seguridad. No se es responsable con la verificación habitual de las actualizaciones de seguridad.
- No existe un plan constante de mantenimiento preventivo y correctivo de los equipos que permita evaluar y valorar su estado. Normalmente se espera a que ocurran situaciones negativas para proceder a la atención de los mismos.
- No se aplica ningún tipo de procedimiento que permita evaluar la capacidad de los equipos y proyectar el uso eficiente del mismo en el tiempo.

4.2 FASE II – CONSTRUCCION DE DISEÑO

4.2.1 Argumentación necesidad de Sistema de Gestión de Seguridad de la Información (SGSI). La información es considerada como el activo más importante de cualquier organización y por lo tanto deben disponerse todos los mecanismos necesarios para su protección.

El departamento de informática de la Superintendencia de Notariado y de Registro es el gran responsable de la seguridad de la información al interior de la entidad. Al tener asignada la responsabilidad de administrar los recursos tecnológicos de la organización es su obligación velar por la seguridad de tales recursos y la aplicación estricta de los lineamientos de seguridad reflejados en políticas de seguridad. Sin embargo la realidad es otra y se ha podido evidenciar que la seguridad de la información es bastante precaria.

Existen razones suficientes para advertir la necesidad que tiene la Superintendencia de Notariado y Registro, específicamente su departamento de informática de contar con un Sistema de Gestión de Seguridad de la Información (SGSI). Entre tales razones se pueden exponer las siguientes:

- Un Sistema de Gestión de Seguridad de la Información (SGSI), brindaría las herramientas necesarias para la correcta utilización y administración de la información y toda la infraestructura técnica alrededor de la información.
- Al interior del departamento de informática no se maneja un inventario formal de activos en el que se identifiquen los responsables de cada uno de ellos. Lo que genera en determinado momento confusión cuando se requieren respuestas al momento de llevar a cabo actualizaciones o implementaciones de soluciones que puedan influir en el desempeño de los sistemas y aplicaciones existentes. El SGSI permitiría asignar formalmente los responsables de cada activo, así como las responsabilidades que se asumen con la asignación tanto en la operación y administración, como en lo pertinente a la seguridad del activo. De esta manera cada individuo al interior del departamento de informática sabrá a quien dirigir o encausar los requerimientos técnicos a que haya lugar.
- Nunca se ha llevado a cabo un análisis de riesgo de los activos que se encuentran bajo la responsabilidad del departamento de informática. De tal manera que en estos momentos el departamento de informática si bien es consciente de la importancia de ciertos activos ignora a si mismo que clases de amenazas podrían atentar contra el desempeño de tales activos, desconoce el grado de dependencia entre los activos lo que se ha evidenciado en distintas circunstancias cuando ha habido problemas con determinado sistema o aplicación en donde los tiempos de respuesta frente al inconveniente son en algunos casos muy altos por el desconocimiento por parte de los administradores de los activos de la interrelación o dependencias entre los mismos. A través del SGSI se podrían identificar las distintas amenazas y vulnerabilidades a los que pueden estar expuestos los activos, podrá identificarse la importancia que tiene cada activo dentro de las labores diarias de la entidad, podrán identificarse las dependencias entre los activos lo que resulta ser un asunto de gran importancia a la hora de verificar la influencia de un activo sobre el otro e identificar en su momento las posibles causas de los problemas técnicos.

- La existencia de un SGSI, obligaría a la ejecución de tareas habituales de análisis de riesgo lo que permitiría tener un conocimiento actualizado acerca de las amenazas y riesgos latentes sobre los activos. Así como la consideración e implementación de un plan de tratamiento de riesgos que permita minimizar las consecuencias negativas que se puedan generar si llegara a materializarse la exposición de tales riesgos.
- La existencia de un SGSI permitiría estructurar las políticas de seguridad alrededor de las verdaderas necesidades de seguridad sobre los activos. Fundamentado en labores de análisis de riesgo. La presencia de un SGSI obligaría a la revisión permanente de las políticas de seguridad, lo que permitirá mantenerlas actualizadas y acordes a las necesidades de seguridad del departamento y la entidad. Así como el seguimiento a la aplicación de las políticas de seguridad. De acuerdo a las exigencias establecidas en las normas ISO/IEC 27001 e ISO/IEC 27002. Recordemos que el departamento de informática no hace ninguna revisión formal de las políticas de seguridad, ni tampoco vela por su cumplimiento.
- La existencia de un SGSI exigiría la conformación de un grupo de seguridad o por lo menos la designación de un responsable general de la seguridad de la información en el departamento de informática. Quien entre otras cosas se encargaría de la revisión constante de la salud del SGSI, exigirá además su revisión y auditoria, será responsable de establecer los mecanismos de divulgación de las políticas de seguridad tanto al interior del departamento de informática como de la entidad en general, velara por el cumplimiento estricto de todos los lineamientos de seguridad establecidos. Lo que actualmente no ocurre.
- La existencia de un SGSI obligaría a que ningún proyecto de incorporación o actualización tecnológica se lleve a cabo sin la consideración de los lineamientos establecidos en tal documento. Lo que evitaría poner en riesgo la funcionalidad de los sistemas y aplicaciones actualmente existentes.
- La existencia de un SGSI por tratarse de un sistema de gestión podrá y deberá ser evaluado periódicamente por el departamento o área de control interno de la entidad. Quien emitirá observaciones acerca del buen o mal funcionamiento del SGSI, así como recomendaciones de ajuste que deberán ser observadas y aplicadas por el departamento de informática. Lo que por defecto deberá llevar a un proceso de mejora continua.

4.2.2 Construcción de diseño SGSI

4.2.2.1 Plan de tratamiento de riesgos

Escala para calificación de riesgos

La escala para la calificación de riesgos será la siguiente:

Figura 235. Esquema calificación de riesgos

Fuente Centro Criptologico Nacional (ccn-cert)

Escala para tratamiento de riesgos

La escala para el tratamiento de riesgos será la siguiente:

* Se acepta
* Se trata
  - Se evita
  - Se mitiga
  - Se comparte
* Se estudia mejor

Cuadro 6. Plan de tratamiento de riesgos

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
Disponibilidad	Autenticación de usuarios	Critico	Se trata - Se evita La SNR deberá considerar la funcionalidad, implementación y estandarización de mecanismo de autenticación fuerte aplicados a todos los sistemas y	Administradores de aplicaciones, administradores de sistemas, administradores de bases de datos, dirección oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			aplicaciones	
	Directorio activo	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del servicio y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador del servicio de directorio activo
	Servicio de nombres de dominio (DNS)	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del servicio y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador del servicio de DNS
	DHCP	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del servicio y velar por su funcionalidad. Se diseñaran e implementaran procesos de	Administrador del servicio de DHCP

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	BIOMETRICO	Alto	Se trata - Se comparte La SNR en conjunto con proveedor de la solución serán responsables por la funcionalidad del servicio. Sera responsabilidad de la SNR llevar a cabo monitoreo, mientras proveedor valorara y solucionara inconvenientes. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador primer nivel por parte de SNR, Administrador segundo nivel por parte de proveedor
	Sistema de información notarial (SIN)	Muy alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación	Administrador de aplicación SIN

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			en la disponibilidad de servicios y aplicaciones	
	Sistema de personal y nomina	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador de aplicación de personal y nomina
	IRIS documental	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador de aplicación IRIS documental
	Sistema de procesos judiciales	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de	Administrador aplicación sistema de procesos judiciales

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	Hoja de vida de notarios	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador aplicación hoja de vida de notarios
	Sistema de control interno disciplinario	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de	Administrador aplicación sistema de control interno disciplinario

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			servicios y aplicaciones	
	Sistema de control interno disciplinarios notarias	Muy alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador aplicación sistema de control interno disciplinarios notarias
	Sistema integrado web	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador aplicación sistema integrado web
	Interrelación registro-catastro	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su	Administrador aplicación registro - catastro

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	Botón de pago	Muy alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador aplicación botón de pago
	Ventanilla única de registro	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema de información y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador aplicación ventanilla única de registro

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
	Netbackup	Bajo	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente de herramienta y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador bases de datos
	Oracle virtual machine	Bajo	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente de herramienta y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador bases de datos
	Endpointsecurity	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente de aplicación y velar por su funcionalidad. Se diseñaran e implementaran procesos de control de	Administrador sistema antivirus

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	EXADATA	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador de bases de datos
	EXALOGIC	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para	Administrador de bases de datos

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			evitar afectación en la disponibilidad de servicios y aplicaciones	
	Servidores	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Responsable de cada servidor
	Computadores	Alto	Se trata - Se evita Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo	Mesa de ayuda
	Portátiles	Alto	Se trata - Se evita Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo	Mesa de ayuda
	Impresoras	Bajo	Se trata - Se evita	Mesa de ayuda

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo	
	Switch	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador de comunicaciones
	Firewall	Critico	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran	Administrador de comunicaciones

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	Red LAN	Critico	Se trata - Se evita La SNR será responsable de la operatividad y funcionalidad de la red LAN. Deberá establecer los lineamientos necesarios para su correcta administración y controles pertinentes para el acceso a la misma, que permitan salvaguardar su seguridad y evitar indisponibilidad	Administrador de comunicaciones
	Internet	Muy alto	Se trata - Se comparte La SNR deberá velar por la disponibilidad y correcto funcionamiento del servicio de Internet. Para lo cual deberá supervisar la prestación del servicio ofrecido por el proveedor de comunicaciones. Aplicando sanciones económicas a proveedor de ser necesario	Administrador de comunicaciones, dirección oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
	Sistema de alimentación ininterrumpida (UPS)	Bajo	Se trata - Se mitiga La SNR será responsable de diseñar e implementar plan de mantenimiento preventivo y correctivo sobre UPS, que evite problemas de alimentación eléctrica que interrumpa la prestación de servicios y aplicaciones	Responsable operativo sobre equipos de energía eléctrica al interior de la entidad
	Fuentes de alimentación	Alto	Se trata - Se comparte La SNR será responsable de establecer convenio con empresa responsable del suministro eléctrico. De manera que se establezca tratado preferencial en la prestación del servicio eléctrico a la entidad, de tal manera que se preserve la integridad de los equipos y no se altere la prestación de servicios y aplicaciones por perdida de fluido eléctrico.	Responsable operativo sobre equipos de energía eléctrica al interior de la entidad, oficina de servicios administrativos
	Aire acondicionado	Medio	Se trata - Se evita La SNR deberá llevar a cabo monitoreo	Asistencia técnica

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	Arreglo de discos	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	Administrador de bases de datos
	Librería de cintas	Alto	Se trata - Se evita La SNR deberá llevar a cabo monitoreo permanente del	Administrador de bases de datos

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			sistema y velar por su funcionalidad. Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo. Se diseñaran e implementaran procesos de control de cambios para evitar afectación en la disponibilidad de servicios y aplicaciones	
	Unidad de DVD	Bajo	Se trata - Se evita Se deberá crear plan de mantenimiento preventivo y correctivo de los equipos de computo	Mesa de ayuda
	Correo electrónico	Alto	Se trata - Se comparte La SNR deberá velar por la disponibilidad y correcto funcionamiento del servicio de correo electrónico. Para lo cual deberá supervisar la prestación del servicio ofrecido por el proveedor de comunicaciones. Aplicando sanciones económicas a proveedor de ser	Administrador de comunicaciones, dirección oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			necesario	
	Portal	Alto	Se trata - Se comparte La SNR deberá velar por la disponibilidad y correcto funcionamiento del servicio de portal. Para lo cual deberá supervisar la prestación del servicio ofrecido por el proveedor Aplicando sanciones económicas a proveedor de ser necesario	Administrador de comunicaciones, dirección oficina de tecnologías de la información
	Hosting y administración	Critico	Se trata - Se comparte La SNR deberá velar por la disponibilidad y correcto funcionamiento del servicio de hosting y administración. Para lo cual deberá supervisar la prestación del servicio ofrecido por el proveedor de comunicaciones. Aplicando sanciones económicas a proveedor de ser necesario	Administrador de comunicaciones, dirección oficina de tecnologías de la información
	Centro de datos	Critico	Se trata - Se evita La SNR será responsable de velar por la preservación y seguridad de las	Oficina de servicios administrativos, oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			instalaciones físicas del centro de datos. Llevando a cabo labores periódicas de revisión y adecuaciones físicas, eléctricas, ducterias, etc. que sean necesarias. con el propósito de que no se afecte la disponibilidad de servicios y aplicaciones	
	Administradores de sistemas	Alto	Se trata - Se mitiga La SNR será responsable de la incorporación del recurso humano para la administración de sus recursos tecnológicos. Deberá asegurarse mediante un sistema de registro de actividades que las actividades pertinentes se llevan a cabo. Sera su responsabilidad la asignación de responsabilidades y evaluar carga de trabajo que permita la asignación y reasignación de funciones que garantice la administración y monitorización permanente de	Dirección oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			los servicios, aplicaciones y recursos tecnológicos en general.	
	Administradores de comunicaciones	Muy alto	Se trata - Se mitiga La SNR será responsable de la incorporación del recurso humano para la administración de sus recursos tecnológicos. Deberá asegurarse mediante un sistema de registro de actividades que las actividades pertinentes se llevan a cabo. Sera su responsabilidad la asignación de responsabilidades y evaluar carga de trabajo que permita la asignación y reasignación de funciones que garantice la administración y monitorización permanente de los servicios, aplicaciones y recursos tecnológicos en general.	Dirección oficina de tecnologías de la información
	Administradores de bases de datos	Muy alto	Se trata - Se mitiga La SNR será responsable de la incorporación del recurso humano	Dirección oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			para la administración de sus recursos tecnológicos. Deberá asegurarse mediante un sistema de registro de actividades que las actividades pertinentes se llevan a cabo. Sera su responsabilidad la asignación de responsabilidades y evaluar carga de trabajo que permita la asignación y reasignación de funciones que garantice la administración y monitorización permanente de los servicios, aplicaciones y recursos tecnológicos en general.	
Integridad de los datos	Formato administración cuentas de usuarios	Critico	Se trata - Se comparte. El formato de administración de cuentas de usuarios será diligenciado exclusivamente por Mesa de Ayuda, quien será responsable de la veracidad de la información que allí se consigne.	Mesa de ayuda, administradores de aplicaciones
	Registros de recurso (DNS)	Despreciable	Se acepta	Administrador servicio DNS
	Sistema de información	Critico	Se trata - Se mitiga	Administrador de aplicación SIN,

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
	notarial (SIN)		La SNR diseñara e implementara mecanismos de control, filtro y supervisión de la información que recibe de las notarias de todo el país y sobre la información que se ingresa al sistema.	Oficina Dirección de Gestión Notarial, Oficina Delegada de Notariado
	Sistema de personal y nomina	Critico	Integridad sobre los datos	Administrador de aplicación Sistema de Personal y Nomina, Oficina de Talento Humano
	Sistema de procesos judiciales	Critico	Se trata - Se mitiga La SNR diseñara e implementara mecanismos de control, filtro y supervisión de la información que se recibe en relación a los procesos judiciales en contra de la entidad y las ORIPs, así como de las denuncias de la entidad en contra de terceros y sobre la información que se ingresa al sistema.	Administrador de aplicación Sistema de Procesos Judiciales, Oficina Jurídica
	Hoja de vida de notarios	Muy alto	Se trata - Se mitiga La SNR diseñara e implementara mecanismos de control, filtro y	Administrador de la aplicación Hoja de Vida de Notarios, Oficina Dirección de Gestión Notarial

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			supervisión de la información que recibe de las notarias. específicamente la relacionada con los notarios de todo el país y sobre la información que se ingresa al sistema.	
	Sistema de control interno disciplinario	Muy alto	Se trata - Se evita La SNR diseñara e implementara los mecanismos necesarios para el recaudo, manejo y custodia de pruebas. Así como los procedimientos formales para la construcción, alimentación y administración de los expedientes.	Administrador de la aplicación Sistema de Control Interno Disciplinario, Oficina de Control Interno Disciplinario
	Sistema de control interno disciplinario notarias	Muy alto	Se trata - Se evita La SNR diseñara e implementara los mecanismos necesarios para el recaudo, manejo y custodia de pruebas. Así como los procedimientos formales para la construcción, alimentación y administración de los expedientes.	Administrador de la aplicación Sistema de Control Interno Disciplinario Notarias, Oficina Delegada Notariado
	Interrelación registro - catastro	Muy alto	Se trata - Se comparte La SNR y el IGAT deberán establecer los	Administrador de aplicación Interrelación Registro-Catastro, Oficina Delegada de

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			mecanismos óptimos de intercambio y valoración de información que garanticen la correcta identificación de los predios mediante la relación directa de los folios de matrícula y las matriculas catastrales	Registro
Confidencialidad de los datos	Sistema de procesos judiciales	Critico	Se trata - Se mitiga La SNR será responsable de diseñar y establecer mecanismos de control que permitan mantener la confidencialidad de la información. Definiendo por ejemplo procedimientos para la asignación de permisos, seguimiento sobre el uso de permisos, auditorias para el control de privilegios, pactos de confidencialidad, etc.	Administrador de aplicación, oficina de tecnologías de la información
	Sistema de control interno disciplinario	Alto	Se trata - Se mitiga La SNR será responsable de diseñar y establecer mecanismos de	Administrador de aplicación, oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			control que permitan mantener la confidencialidad de la información. Definiendo por ejemplo procedimientos para la asignación de permisos, seguimiento sobre el uso de permisos, auditorias para el control de privilegios, pactos de confidencialidad, etc.	
	Sistema de control interno disciplinario notarias	Alto	Se trata - Se mitiga La SNR será responsable de diseñar y establecer mecanismos de control que permitan mantener la confidencialidad de la información. Definiendo por ejemplo procedimientos para la asignación de permisos, seguimiento sobre el uso de permisos, auditorias para el control de privilegios, pactos de confidencialidad, etc.	Administrador de aplicación, oficina de tecnologías de la información
	Botón de pago	Muy alto	Se trata - Se mitiga	Administrador de aplicación, oficina de tecnologías

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			La SNR será responsable de diseñar y establecer mecanismos de control que permitan mantener la confidencialidad de la información. Definiendo por ejemplo procedimientos para la asignación de permisos, seguimiento sobre el uso de permisos, auditorias para el control de privilegios, pactos de confidencialidad, etc.	de la información
Autenticidad	Formato administración cuentas de usuarios	Critico	Se trata - Se mitiga La SNR será responsable de asegurar la legitimidad de la información contenida en los formatos de administración de cuentas de usuarios, mediante la definición de directrices en donde se determine que tales formatos serán firmados exclusivamente por la dirección de cada área, deberán obedecer a la versión oficial,	Mesa de Ayuda, oficina de tecnologías de la información, oficina de planeación, oficina de control interno

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			deberán ser entregados formalmente a la Mesa de Ayuda para su entrega final a los administradores de aplicaciones	
	Autenticación de usuarios	Critico	Se trata - Se evita La SNR deberá establecer mediante política de seguridad la forma en que los usuarios se autenticaran en los distintas aplicaciones, deberá estandarizarse un solo mecanismo de autenticación aplicable a todas las aplicaciones que se manejan al interior de la entidad, deberán definirse políticas relacionadas con el manejo de las credenciales por parte de los usuarios.	oficina de tecnologías de la información
	Directorio activo	Critico	Se trata - Se evita Como presente mecanismo actual de autenticación la SNR deberá velar por el correcto funcionamiento del servicio así como establecer los lineamientos necesarios para la correcta administración de las credenciales de los usuarios,	oficina de tecnologías de la información

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			para la creación, administración y eliminación de cuentas de usuarios, validación del estado de las cuentas de usuarios, deberá definir los medios formales para la entrega de credenciales , etc.	
Trazabilidad	Biométrico	Alto	Se trata - Se evita La SNR será responsable de asegurar la funcionalidad del servicio, con el propósito fundamental de llevar a cabo el registro de ingreso de personas a la entidad. Deberán diseñarse reportes que permitan realizar seguimiento sobre el ingreso y salida de funcionarios y contratistas con el propósito de establecer el cumplimiento de obligaciones contractuales en lo relacionado con el cumplimiento de horarios, así como llevar un control por razones de seguridad sobre personal ajeno a la entidad que ingresa con	Administrador de servicio biométrico, oficina de tecnologías de la información, oficina de gestión humana, oficina de servicios administrativos

Riesgo	Activo	Calificación	Decisión y Tratamiento	Responsable
			propósitos varios	
	IRIS documental	Bajo	Se trata - Se evita La SNR será responsable de garantizar la gestión de la correspondencia, circulares, oficios, etc. que se genera y que ingresa a la entidad. mediante la implementación de la aplicación IRIS. mediante directriz se exigirá la aplicación de la norma de gestión documental establecida por el gobierno colombiano, definiendo acciones de almacenamiento de información física conforme a la norma, mediante capacitación permanente se orientara a los usuarios en el uso obligatorio de la aplicación que permitirá llevar un registro y seguimiento de la documentación que se genera en la entidad	Administrador aplicación IRIS, dirección oficina de tecnologías de la información

Fuente El autor

4.2.2.2 Declaración de aplicabilidad SOA

Razones de la selección

LR - Requerimientos Legales

CO - Obligaciones Contractuales

BR/BP - Requerimientos de Negocio/Adoptar las Mejores Practicas

RRA - Resultados de la Evaluación de Riesgos

Cuadro 7. Declaración de aplicabilidad SOA

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
Dominio	***5. Políticas de seguridad de la información***					
Objetivo de control	5.1. Directrices establecidas por la dirección para la seguridad de la información					
Control	5.1.1. Políticas para la seguridad de la información	NO			Existe	Se han definido políticas de seguridad según consta en documento "Políticas de Seguridad en los Sistemas de Información". Sin embargo no se lleva ningún control de su aplicación y no existe ningún tipo de divulgación de las mismas
Control	5.1.2. Revisión de las políticas para la seguridad de la información	SI	BR/BP	NO		Si bien existen políticas de seguridad definidas según consta en documento "Políticas de Seguridad en los Sistemas de Información". No se lleva ningún control de su aplicación, no se realiza la revisión y evaluación formal de las políticas de seguridad
Dominio	***6. Organización de la seguridad de la información***					
Objetivo de control	6.1. Organización interna					
Control	6.1.1. Roles y	SI	BR/BP	NO		Acción

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
	responsabilidades para la seguridad de la información					fundamental para salvaguardar la seguridad de los equipos
Control	6.1.2. Segregación de funciones	SI	BR/BP	NO		Deberán definirse responsabilidades claramente definidas que evitaran conflictos
Control	6.1.3. Contacto con las autoridades	SI	BR/BP	NO		Permitirá identificar los entes externos a los que se puede acudir ante emergencias
Control	6.1.4. Contacto con grupos de interés especial				Existe	Deberá ajustarse y reforzarse, existe pero precariamente
Control	6.1.5. Seguridad de la información en la gestión de proyectos	SI	BR/BP	NO		Todo tipo de proyecto deberá considerar los lineamientos de seguridad que se encuentren establecidos
Objetivo de control	6.2. Dispositivos móviles y teletrabajo					
Control	6.2.1. Política para dispositivos móviles	SI	BR/BP	NO		Evitará la exposición de la información propiedad de la entidad contenida en tales dispositivos
Control	6.2.2. Teletrabajo	NO			Existe	Si bien existe política de seguridad definida sobre el tema no se lleva control de su aplicación
Dominio	***7. Seguridad del recurso humano***					
Objetivo de control	7.1. Antes de asumir el empleo					
Control	7.1.1. Selección	SI	RRA	NO		Deberá ajustarse a Oficina Tecnologías de la Información según alcance proyecto. Permitirá verificar antecedentes y cualidades éticas, morales y profesionales sobre personal seleccionado
Control	7.1.2. Términos y condiciones del empleo	SI	BR/BP	NO		Permitirá la inducción sobre los lineamientos de seguridad de la información en la entidad a toda

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						persona vinculada directa o indirectamente
Objetivo de control	7.2. Durante la ejecución del empleo					
Control	7.2.1. Responsabilidades de la dirección	SI	BR/BP	NO		Deberá contarse con el compromiso de la dirección para el éxito de políticas de seguridad y el SGSI en general.
Control	7.2.2. Toma de conciencia, educación y formación en la seguridad de la información	SI	BR/BP	NO		Deberá implementarse programa de capacitación en seguridad de la información a los miembros de la entidad para desarrollar conciencia en el manejo seguro de la información
Control	7.2.3. Proceso disciplinario	SI	BR/BP	NO		Deberán implementarse sanciones para aquellos miembros de la entidad que violan los lineamientos de seguridad establecidos. Esto ayudaría a tomar conciencia sobre la necesidad de preservar la seguridad de la información
Objetivo de control	7.3. Terminación y cambio de empleo					
Control	7.3.1. Responsabilidades en la terminación o cambio del empleo	SI	BR/BP	NO		Deberán especificarse las responsabilidades que se siguen teniendo una vez termine contrato de trabajo, haya renuncia o cambio de empleo. Esto ayudara a preservar compromisos de confidencialidad y reasignación de responsabilidades
Dominio	***8. Gestión de activos***					
Objetivo de control	8.1. Responsabilidad por los activos					
Control	8.1.1. Inventario de	SI	BR/BP	NO		Deberá llevarse un

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
	activos					inventario de los activos de la entidad. Esto ayudara a saber con que se cuenta y que se debe proteger
Control	8.1.2. Propiedad de los activos	SI	BR/BP	NO		Deberá asignarse un responsable por cada activo. Esto ayudara a la administración controlada de los mismos
Control	8.1.3. Uso aceptable de los activos	SI	BR/BP	NO		Deberán establecerse directrices para el manejo optimo de activos propiedad de la entidad por parte de empleados y de usuarios externos. Esto ayudara a que los activos se manejen bajo lineamientos aceptables de control
Control	8.1.4. Devolución de activos	SI	BR/BP	NO		Deberá determinarse directriz para la devolución formal de activos propios de la entidad por parte de empleados y usuarios externos. Esto ayudara a preservar la organización e información del activo de inventarios
Objetivo de control	8.2. Clasificación de la información					
Control	8.2.1. Clasificación de la información	SI	RRA	NO		Deberá establecerse esquema de clasificación de la información. Esto ayudara a comprender el valor de la información y de los activos que la administran y su nivel de criticidad
Control	8.2.2. Etiquetado de la información	SI	BR/BP	NO		Tanto la información como los activos sobre la que se administra deberán

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						etiquetarse. Esto ayudara a preservar la organización e información del inventario de activos
Control	8.2.3. Manejo de activos	SI	BR/BP	NO		Permitirá que los activos sean manipulados correctamente, evitando cualquier daño sobre los mismos
Objetivo de control	8.3. Manejo de medios					
Control	8.3.1. Gestión de medios removibles	SI	RRA	NO		Deberán establecerse las orientaciones necesarias. Lo que ayudara a preservar de manera segura la información contenida en tales medios. Existe política de seguridad sobre este tema en la entidad solo orientada a usuarios y no hay control de su aplicación
Control	8.3.2. Disposición de los medios	SI	RRA	NO		Deberán establecerse las orientaciones necesarias en cuanto a la forma en que deben disponerse o albergarse los medios de la entidad. Lo que ayudara a preservar de manera segura la información contenida en tales medios
Control	8.3.3. Transferencia de medios físicos	SI	RRA	NO		La información relevante de la entidad deberá transportarse y salvaguardarse de manera segura y responsable por empresa especializada en la protección de valores. Lo que permitirá garantizar la seguridad de la

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						información y su disposición
Dominio	***9. Control de acceso***					
Objetivo de control	9.1. Requisitos del negocio para control de acceso					
Control	9.1.1. Política de control de acceso	SI	RRA	NO		Deberá protegerse la información definiendo el acceso a la misma y a las instalaciones físicas donde se procese información vital de la entidad mediante lineamientos estrictos de control de acceso. Lo que ayudara a evitar los accesos no autorizados
Control	9.1.2. Acceso a redes y servicios en red	SI	RRA	NO		Se deberán especificar los lineamientos de seguridad para el control de acceso a la red y a los servicios. Actualmente existe una política de seguridad muy escueta sobre el tema pero solo limitada a contraseñas en router y switches
Objetivo de control	9.2. Gestión de acceso de usuarios					
Control	9.2.1. Registro y cancelación del registro de usuarios	NO			Existe	Deberá llevarse un registro formal de la creación y eliminación de las cuentas de usuarios. Lo que ayudaría a evitar entre otras cosas la suplantación de identidad. Actualmente existe política de seguridad relacionada con el tema pero no hay control de su aplicación
Control	9.2.2. Suministro de acceso de usuarios	SI	RRA	NO		Permitirá que los permisos y derechos asignados a los usuarios se asignen de

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						acuerdo a solicitudes formales y autorizadas según nivel jerárquico
Control	9.2.3. Gestión de derechos de acceso privilegiado	SI	RRA	NO		Permitirá que los permisos y derechos de acceso de carácter privilegiado asignados a los usuarios se asignen de acuerdo a solicitudes formales y autorizadas según nivel jerárquico
Control	9.2.4. Gestión de información secreta para la autenticación de usuarios (Management of Secret Authentication Information of Users)	SI	RRA	NO		Permitirá definir responsabilidad de los usuarios frente al uso de su cuenta de usuario y contraseña
Control	9.2.5. Revisión de los derechos de acceso de usuarios	SI	RRA	NO		Permitirá revisar de forma periódica por parte de los responsables de los activos derechos asignados a los usuarios. Lo que ayudara a controlar estrictamente los niveles de acceso y los usuarios a quienes se conceden
Control	9.2.6. Retiro o ajuste de los derechos de acceso	SI	RRA	NO		Deberá disponerse de lineamiento de seguridad que permita retirar derechos de acceso o reasignarlos según circunstancias laborales de cada usuario. Lo que ayudara a controlar estrictamente los niveles de acceso a la información y aplicaciones de la entidad
Objetivo de control	9.3. Responsabilidades de los usuarios					
Control	9.3.1. Uso de información secreta para la autenticación	NO			Existe	Orientara a los usuarios en correcto uso de sus credenciales. Actualmente existe política de

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						seguridad relacionada con el tema pero no se lleva control de su aplicación
Objetivo de control	9.4. Control de acceso a sistemas y aplicaciones					
Control	9.4.1. Restricción de acceso a la información	NO			Existe	Las acciones de los usuarios sobre las aplicaciones está determinado por los privilegios de acceso y las interfaces para la interacción con las mismas corresponde al diseño de cada aplicación
Control	9.4.2. Procedimiento de ingreso (Log-On) seguro	NO			No existe	Existe procedimiento de ingreso a equipos de escritorio. Pero no existe estandarización para el ingreso a las aplicaciones lo que esta fuera del alcance del SGSI
Control	9.4.3. Sistema de gestión de contraseñas	NO			Existe	Existe implementado servicio de A.D. , que desempeña esta labor para el ingreso de los usuarios a los equipos y a algunos servidores. Actualmente existe política de seguridad relacionada con el tema pero no se lleva control de su aplicación
Control	9.4.4. Uso de programas utilitarios privilegiados	SI	RRA	NO		Permitirá regular la utilización de programas o herramientas utilitarias que puedan alterar el correcto funcionamiento de las aplicaciones y servicios en la entidad
Control	9.4.5. Control de acceso a códigos fuente de programas	SI	RRA	NO		Permitirá establecer mecanismo para la estricta administración y manejo del código

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						fuente de las diferentes aplicaciones que funcionan en la entidad. Lo que evitara la manipulación de las aplicaciones
Dominio	***10. Criptografía***					
Objetivo de control	10.1. Controles criptográfico	NO			No existe	Fuera del alcance del SGSI
Control	10.1.1. Política sobre el uso de controles criptográficos	NO			No existe	Fuera del alcance del SGSI
Control	10.1.2. Gestión de llaves	NO			No existe	Fuera del alcance del SGSI
Dominio	***11. Seguridad física y del entorno***					
Objetivo de control	11.1. Áreas seguras					
Control	11.1.1. Perímetro de seguridad física	NO			Existe	Actualmente existe política de seguridad muy básica relacionada con el tema y no hay control sobre su aplicación
Control	11.1.2. Controles de acceso físicos	NO			Existe	Actualmente este control se ejecuta
Control	11.1.3. Seguridad de oficinas, recintos e instalaciones	NO			Existe	Actualmente este control se ejecuta
Control	11.1.4. Protección contra amenazas externas y ambientales	NO			No existe	Fuera del alcance del SGSI
Control	11.1.5. Trabajo en áreas seguras	NO			Existe	Actualmente este control se ejecuta
Control	11.1.6. Áreas de despacho y carga	NO			No existe	Fuera del alcance del SGSI
Objetivo de control	11.2. Equipos					
Control	11.2.1. Ubicación y protección de los equipos	NO			Existe	Actualmente este control se ejecuta. Específicamente para el centro de datos de la entidad
Control	11.2.2. Servicios de suministro	NO			Existe	Actualmente este control se ejecuta. Específicamente para el centro de datos de la entidad
Control	11.2.3. Seguridad del cableado	NO			Existe	Actualmente este control se ejecuta. Específicamente para el centro de datos de la entidad
Control	11.2.4. Mantenimiento de equipos	SI	RRA	NO		Deberá definirse lineamiento para el mantenimiento preventivo y correctivo de los

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						equipos. Lo que permitirá preservar la funcionalidad y estabilidad de los equipos
Control	11.2.5. Retiro de activos	NO	RRA		Existe	Actualmente este control se ejecuta.
Control	11.2.6. Seguridad de equipos y activos fuera de las instalaciones	SI	RRA	NO		Se garantizara el tratamiento seguro y adecuado de los equipos y activos de la entidad que por alguna razón se deban utilizar fuera de las instalaciones físicas por defecto
Control	11.2.7. Disposición segura o reutilización de equipos	SI	RRA	NO		Permitirá que los equipos puedan ser reutilizados una vez sea garantizada la eliminación de la información contenida en los mismos
Control	11.2.8. Equipos de usuario desatendidos	NO			Existe	Actualmente este control se ejecuta
Control	11.2.9. Política de escritorio limpio y pantalla limpia	SI	BR/BP	NO		Permitirá en lo posible que la información manejada por usuarios legítimos permanezca a salvo de personas ajenas
Dominio	***12. Seguridad de las operaciones***					
Objetivo de control	12.1. Procedimientos operacionales y responsabilidades					
Control	12.1.1. Procedimientos de operación documentados	SI	BR/BP	NO		La documentación permitirá que las tareas de operación y administración de sistemas y aplicaciones sean ejecutadas de manera organizada. Fuera del alcance del SGSI.
Control	12.1.2. Gestión de cambios	SI	BR/BP	NO		Permitirá que todos los cambios que se vayan a realizar sean estrictamente documentados y planeada su ejecución. Fuera del alcance del SGSI.
Control	12.1.3. Gestión de	NO			No existe	Fuera del alcance

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
	capacidad					del SGSI
Control	12.1.4. Separación de los ambientes de desarrollo, pruebas y producción	NO			Existe	Actualmente este control se ejecuta
Objetivo de control	12.2. Protección contra códigos maliciosos					
Control	12.2.1. Controles contra códigos maliciosos	SI	RRA	NO		Permitirá proteger los activos de la entidad contra todo tipo de código malicioso que pudiera poner en riesgo la funcionalidad de los mismos
Objetivo de control	12.3. Copias de respaldo					
Control	12.3.1. Respaldo de la información	NO			Existe	Actualmente se trabaja en el diseño e implementación total de un esquema de respaldo de la información, específicamente para el centro de datos de la entidad. Actualmente existe una política de seguridad muy básica relacionada con el tema. No se lleva control de su aplicación
Objetivo de control	12.4. Registro (Logging) y Seguimiento					
Control	12.4.1. Registro de eventos	SI	RRA	NO		Permitirá llevar a cabo el registro y almacenamiento de los eventos sobre servidores y aplicaciones de la entidad
Control	12.4.2. Protección de la información de registro (log information)	SI	RRA	NO		Deberán establecerse los mecanismos de protección para los registros de eventos. Lo que permitirá establecer cierto nivel de protección sobre los registros de eventos consolidados
Control	12.4.3. Registros (Logs) del	SI	RRA	NO		Permitirá llevar a cabo el registro y

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
	administrador y del operador					almacenamiento de los eventos sobre servidores y aplicaciones de la entidad
Control	12.4.4. Sincronización de relojes	SI	BR/BP	NO		Permitirá que todos los equipos de computo de la entidad permanezcan sincronizados alrededor de una única fuente formal de tiempo
Objetivo de control	12.5. Control de software operacional					
Control	12.5.1.Instalacion de software en sistemas operativos (Operational Systems)	SI	RRA	NO		Permitirá mantener actualizados los equipos de computo desde el punto de vista de las actualizaciones de seguridad de los sistemas operativos
Objetivo de control	12.6. Gestión de la vulnerabilidad técnica					
Control	12.6.1. Gestión de las vulnerabilidades técnicas	NO			No existe	Se requeriría una labor de auditoría de sistemas y test de penetración que detecte vulnerabilidades sobre los sistemas de información. Lo cual está fuera del alcance del SGSI
Control	12.6.2. Restricciones sobre la instalación de software	NO			Existe	Actualmente existe política de seguridad relacionada con el tema
Objetivo de control	12.7. Consideraciones sobre auditorias de sistemas de información					
Control	12.7.1. Controles sobre auditorias de sistemas de información	NO			No existe	Implicaría vinculación de especialistas en auditoria de sistemas lo cual obedece a decisiones administrativas de la alta dirección. Fuera del alcance del SGSI
Dominio	***13. Seguridad de las comunicaciones***					
Objetivo de control	13.1. Gestión de la seguridad de las redes					

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
Control	13.1.1. Controles de redes	SI	RRA	NO		Permitirá definir todos los controles que deberán implementarse para proteger las aplicaciones y servicios que operan a través de la red LAN de la entidad
Control	13.1.2. Seguridad de los servicios de red	NO			Existe	Los niveles de servicio son decisiones propias de la alta dirección de acuerdo a modelos de contratación. Fuera del alcance del SGSI
Control	13.1.3. Separación en las redes	NO			Existe	Actualmente este control se aplica. La red LAN de la entidad esta segmentada en distintas VLANs
Objetivo de control	13.2. Transferencia de información					
Control	13.2.1. Políticas y procedimientos de transferencia de información	SI	RRA	NO		Permitirá establecer las pautas necesarias que deberán considerar los usuarios en lo que respecta al manejo, uso y transferencia externa o interna de información propia de la entidad
Control	13.2.2. Acuerdos sobre transferencia de información	NO			No existe	La transferencia de información con terceros obedecerá a acuerdos interadministrativos que dependen de la alta dirección de la entidad. Fuera del alcance del SGSI
Control	13.2.3. Mensajería electrónica	NO			Existe	Actualmente este control se aplica. A través de proveedor quien administra tal servicio
Control	13.2.4. Acuerdos de confidencialidad o de no divulgación	NO			Existe	Los acuerdos de confidencialidad o de no divulgación serán generados y definidos por la alta dirección de la entidad junto con

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						su área jurídica. fuera del alcance del SGSI
Dominio	***14. Adquisición, desarrollo y mantenimiento de sistemas***					
Objetivo de control	14.1. Requisitos de seguridad de los sistemas de información					
Control	14.1.1. Análisis y especificación de requisitos de seguridad de la información	NO			No existe	Involucra tareas de auditoría de sistemas e ingeniería de software. Fuera del alcance de SGSI
Control	14.1.2. Seguridad de servicios de las aplicaciones en redes publicas	NO			No existe	Involucra la aplicación de controles de tipo criptográficos. Fuera del alcance de SGSI
Control	14.1.3. Protección de los servicios de las aplicaciones (Application Services)	NO			No Existe	Involucra la aplicación de controles de tipo criptográficos. Fuera del alcance de SGSI
Objetivo de control	14.2. Seguridad en los procesos de desarrollo y de soporte					
Control	14.2.1. Política de desarrollo seguro	NO			No existe	Las políticas para desarrollo de software involucran la consideración de conceptos y lineamientos de ingeniería de software. Fuera del alcance de SGSI
Control	14.2.2. Procedimientos de control de cambios de sistemas	NO			No existe	Los procedimientos de control de cambios para los sistemas y sistemas de información involucran consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Control	14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	NO			No existe	La revisión técnica de las aplicaciones después de cambios en plataformas involucra consideración de conceptos y lineamientos de

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						ingeniería de software, así como de auditoría de sistemas. Debe considerarse el plan de continuidad del negocio que no existe en la entidad. Fuera del alcance de SGSI
Control	14.2.4. Restricciones en los cambios a los paquetes de software	NO			No existe	Involucra consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Control	14.2.5. Principios de construcción de sistemas seguros	NO			No existe	La construcción de sistemas de información seguros involucra consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Control	14.2.6. Ambiente de desarrollo seguro	SI			No existe	Permitiría especificar los lineamientos sobre el ambiente físico (condiciones de lugar), donde se realizaran las tareas propias de desarrollo de software.
Control	14.2.7. Desarrollo contratado externamente	NO			No existe	Involucra consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Control	14.2.8. Pruebas de seguridad de sistemas	NO			No existe	El diseño de pruebas de seguridad de los sistemas de información involucra consideración de conceptos y lineamientos de ingeniería de

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Control	14.2.9. Prueba de aceptación de sistemas	NO			No existe	El diseño de pruebas de aceptación de los sistemas de información involucra consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Objetivo de control	14.3. Datos de prueba					
Control	14.3.1. Protección de datos de prueba	NO			No existe	La protección de datos de prueba para sistemas de información involucra consideración de conceptos y lineamientos de ingeniería de software, así como de auditoría de sistemas. Fuera del alcance de SGSI
Dominio	***15. Relaciones con los proveedores***					
Objetivo de control	15.1. Seguridad de la información en las relaciones con los proveedores					
Control	15.1.1. Política de seguridad de la información para las relaciones con proveedores	NO			No existe	Sujeto a disposiciones contractuales y jurídicas establecidas por la alta dirección de la entidad. Fuera del alcance del SGSI
Control	15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	NO			No existe	Sujeto a disposiciones contractuales y jurídicas establecidas por la alta dirección de la entidad. Fuera del alcance del SGSI
Control	15.1.3. Cadena de suministro de tecnología de información y comunicación	NO			No existe	Sujeto a disposiciones contractuales y jurídicas establecidas por la alta dirección de la

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						entidad. Fuera del alcance del SGSI
Objetivo de control	15.2. Gestión de la prestación de servicios de proveedores					
Control	15.2.1. Seguimiento y revisión de los servicios de los proveedores	NO			No existe	Sujeto a disposiciones contractuales y jurídicas establecidas por la alta dirección de la entidad. Fuera del alcance del SGSI
Control	15.2.2. Gestión de cambios en los servicios de los proveedores	NO			No existe	Sujeto a disposiciones contractuales y jurídicas establecidas por la alta dirección de la entidad. Fuera del alcance del SGSI
Dominio	***16. Gestión de incidentes de seguridad de la información***					
Objetivo de control	16.1. Gestión de incidentes y mejoras en la seguridad de la información					
Control	16.1.1. Responsabilidades y procedimientos	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Control	16.1.2. Reporte de eventos de seguridad de la información	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						entidad. Fuera del alcance de SGSI
Control	16.1.3. Reporte de debilidades de seguridad de la información	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Control	16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Control	16.1.5. Respuesta a incidentes de seguridad de la información	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Control	16.1.6. Aprendizaje obtenido de los	NO			No existe	Los lineamientos relacionados con

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
	incidentes de seguridad de la información					responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Control	16.1.7. Recolección de evidencia	NO			No existe	Los lineamientos relacionados con responsabilidades, procedimientos, reportes, decisiones sobre eventos de seguridad implica la organización de un grupo de seguridad encargado de formalizar la administración y gestión sobre los incidentes de seguridad que se presenten en la entidad. Fuera del alcance de SGSI
Dominio	***17. Aspectos de seguridad de la información de la gestión de continuidad de negocio***					
Objetivo de control	17.1. Continuidad de seguridad de la información					
Control	17.1.1. Planificación de la continuidad de la seguridad de la información	NO			No existe	Plan de continuidad de negocio. Fuera del alcance de SGSI
Control	17.1.2. Implementación de la continuidad de la seguridad de la información	NO			No existe	Plan de continuidad de negocio. Fuera del alcance de SGSI
Control	17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	NO			No existe	Plan de continuidad de negocio. Fuera del alcance de SGSI
Objetivo de control	17.2. Redundancias					
Control	17.2.1. Disponibilidad de instalaciones de procesamiento de información	NO			Existe	Algunos sistemas de información se encuentran ubicados en centro de datos de proveedor, que

		Control Seleccionado	Razón de la Selección	Control Implementado	Justificación Exclusión	Observación
						funciona como centro de datos alterno. Sin embargo no se consideran otros sistemas de información de importancia crítica.
Dominio	***18. Cumplimiento***					
Objetivo de control	18.1. Cumplimiento de requisitos legales y contractuales					
Control	18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	NO			No existe	Las disposiciones y obligaciones legales. Fuera del alcance de SGSI
Control	18.1.2. Derechos de propiedad intelectual	NO			No existe	Consideraciones sobre derecho de propiedad intelectual. Fuera del alcance de SGSI
Control	18.1.3. Protección de registros	NO			No existe	Fuera del alcance de SGSI
Control	18.1.4. Privacidad y protección de información de datos personales	NO			No existe	Fuera del alcance de SGSI
Control	18.1.5. Reglamentación de controles criptográficos	NO			No existe	Fuera del alcance de SGSI
Objetivo de control	18.2. Revisiones de seguridad de la información					
Control	18.2.1. Revisión independiente de la seguridad de la información	NO			No existe	Las políticas de seguridad definidas actualmente no son revisadas, evaluadas, ni controladas. Definir lineamiento para revisión de las políticas consignadas en el SGSI sería necesario si SGSI se implementara. Fuera del alcance de SGSI
Control	18.2.2. Cumplimiento con las políticas y normas de seguridad	NO			No existe	Definir lineamiento para revisión de las políticas consignadas en el SGSI sería necesario si SGSI se implementara. Fuera del alcance de SGSI
Control	18.2.3. Revisión del cumplimiento técnico	NO			No existe	Fuera del alcance de SGSI

Fuente El autor

4.2.2.3 Políticas de seguridad

A pesar de que al interior de la Superintendencia de Notariado y Registro existe un documento oficial denominado "Políticas de Seguridad en los Sistemas de Información", en donde se especifican y describen una serie de políticas orientadas a la seguridad de la información. También es cierto que desde su promulgación en el año 2008 tales políticas no han sido revisadas y actualizadas de manera formal.

El análisis de riesgo llevado a cabo evidencia además la necesidad de diseñar e implementar políticas de seguridad que contribuyan a disminuir las amenazas y los niveles de riesgo sobre la información y en general los activos de la organización que se encuentran bajo la responsabilidad del departamento de informática.

Como parte fundamental del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el departamento de informática de la Superintendencia de Notariado y Registro se proponen las siguientes políticas de seguridad:

Dominio - Políticas de seguridad de la información

Política 001: Las políticas de seguridad de la información deberán ser revisadas de forma continua y periódicamente con el objetivo fundamental de asegurar su eficacia frente a las nuevas necesidades de seguridad que vayan surgiendo.

La dirección general de la Superintendencia de Notariado y Registro (SNR), designara al departamento de informática u oficina de tecnologías de la información como responsable directo de diseñar, implementar, verificar y controlar la aplicación de las políticas de seguridad de la entidad.

El departamento de informática en cabeza de su director será responsable de la emisión periódica de informes en donde se indique a la dirección general el compromiso de las distintas áreas en la aplicabilidad de las políticas de seguridad.

Las actualizaciones a las políticas de seguridad a las que haya lugar deberán ser finalmente revisadas y aprobadas por la dirección general de la entidad y divulgadas a todos los usuarios por el medio de comunicación que se considere pertinente.

Dominio - Organización de la seguridad de la información

Política 002: La dirección del departamento de informática en cabeza de su director y por disposición legitima de la dirección general de la Superintendencia de Notariado y Registro, designara a los respectivos responsables de cada uno de los activos presentes y bajo la responsabilidad del departamento de informática.

En concreto cada individuo encargado de la administración de cualquier sistema será legitimo responsable por la seguridad del activo y por los procesos de seguridad alrededor del mismo.

Sera responsabilidad suprema de la dirección del departamento de sistemas velar por la capacitación permanente de los administradores de los distintos sistemas en temas de seguridad de la información.

Política 003: Deberán documentarse de forma detallada y precisa las responsabilidades que asumirán los responsables de los activos y procesos de seguridad asignados al departamento de informática.

Política 004: Bajo ninguna circunstancia, motivo o justificación una persona podrá hacer uso de un activo sin contar previamente con la debida y legitima autorización del responsable del activo. De lo contrario deberá someterse a las sanciones disciplinarias dispuestas para el caso.

Política 005: Sera responsabilidad de la Superintendencia de Notariado y Registro en conjunto con la dirección del departamento de informática establecer los mecanismos de colaboración y reporte con los organismos judiciales y de control ante la materialización de incidentes de seguridad propiciados por agentes externos e internos a la entidad y que pongan en riesgo latente la integridad de la información y el desempeño de las labores diarias de la entidad. Deberán diseñarse protocolos de comunicación que determinen de forma clara y detallada los momentos y circunstancias en que se acudirá a los organismos judiciales y de control por ocurrencia de incidentes de seguridad que pongan en riesgo la misión de la organización.

Política 006: Sera responsabilidad de la Superintendencia de Notariado y Registro en conjunto con la dirección del departamento de informática propiciar convenios y/o acuerdos de cooperación con otras entidades públicas y empresas privadas que propicien la colaboración y el intercambio permanente de experiencias en el campo de la seguridad de la información. Se deberá disponer y promover los escenarios necesarios para que el personal adscrito al departamento de informática tenga la posibilidad de acceder a fuentes de información que complementen o fortalezcan los conceptos y conocimientos en seguridad de la información. Por ejemplo, mediante la organización de seminarios, foros, etc., que podrán ser organizados por la oficina de capacitación de la entidad.

Política 007: Ningún proyecto de incorporación tecnológica podrá implementarse en la entidad sin que previamente sean considerados los lineamientos de seguridad dispuestos para la seguridad de la información. Sera responsabilidad del departamento de informática evaluar estrictamente los riesgos a nivel de seguridad de la información que implicaría la ejecución e implementación de los distintos proyectos de incorporación tecnológica, así mismo será responsable junto

con los proveedores de soluciones del diseño de planes de incorporación y montaje que eviten poner en riesgo la continuidad del negocio.

Política 008: En relación al uso de dispositivos móviles se establecen las siguientes consideraciones formales:

a). Los dispositivos móviles (memorias USB, discos duros extraíbles, portátiles, etc.) de propiedad de la Superintendencia de Notariado y Registro deberán estar estrictamente inventariados.
b). El departamento de informática deberá llevar registro documentado de la asignación que haga de tales dispositivos. Consignando los nombres de los responsable de cada dispositivo.
c). La dirección del departamento de informática será responsable de autorizar mediante oficio la salida de los dispositivos móviles fuera de las instalaciones de la Superintendencia de Notariado y Registro.
d). Salvo excepciones especiales ningún dispositivo del que se autorice su utilización por fuera de la entidad podrá contener información relevante del departamento de informática y la entidad.
e). En los casos en los que sea necesario la utilización de dispositivos móviles y la información contenida en ellos fuera del departamento de informática y fuera de las instalaciones de la entidad. La información contenida en tales dispositivos deberá codificarse con el propósito de evitar que tal información pueda ser robada o extraída ilegalmente.
f). En el caso de los equipos portátiles, estos deberán estar unidos al dominio privado de la entidad y deberán ser operados al interior del departamento de informática con una cuenta de usuario de dominio.
g). En el caso de que se permita la salida de los equipos portátiles del departamento de informática y de las instalaciones de la Superintendencia de Notariado y Registro. En cada portátil deberá configurarse una cuenta estándar de carácter local conservando los requerimientos de complejidad para contraseñas. esa contraseña de usuario deberá cambiarse de forma periódica.
h). Los equipos portátiles deberán tener instalado el sistema antivirus oficial de la entidad.
i). Todo dispositivo móvil que se utilice al interior del departamento de informática deberá ser vacunado con el sistema antivirus de la entidad antes de su utilización. De ser omitido tal lineamiento podrá ser considerada como una conducta inaceptable sujeta a sanciones de tipo disciplinarias.
j). Aquellos dispositivos móviles que por necesidad deban contener información relevante, deberán estar sujetos a la realización de copias de seguridad periódicamente. Esta operación será responsabilidad de la persona encargada del dispositivo móvil.

Dominio - Seguridad del recurso humano

Política 009: Sera responsabilidad de la Superintendencia de Notariado y Registro disponer de los mecanismos necesarios para la verificación de antecedentes disciplinarios y judiciales tanto de las personas que aspiran a ser nombradas en la entidad, así como de personas contratistas.

Deberán verificarse estrictamente con las instituciones académicas los títulos académicos dados a conocer por los aspirantes en su hoja de vida, así como la experiencia laboral reportada en la misma.

Política 010: Sera responsabilidad de la dirección del departamento de informática proponer ante la dirección general de la Superintendencia de Notariado y Registro documento en donde se consignen los términos para los acuerdos de confidencialidad para los funcionarios y contratistas incorporados al departamento de informática. Deberá velar por su aprobación, aplicación, actualización y vigencia permanente.

Política 011: El documento oficial de acuerdos de confidencialidad, deberá ser presentado a las personas incorporadas como funcionarios o contratistas al departamento de informática. Así como a empresas contratadas para desempeñar cualquier labor al interior del departamento de informática. Los acuerdos de confidencialidad deberán ser firmados antes de la asignación de cualquier labor o responsabilidades al interior del departamento de informática.

Política 012: Sera responsabilidad del departamento de informática llevar a cabo inducción sobre las políticas de seguridad de la información a personas (funcionarios y contratistas) que se incorporen al departamento, así como a personal de las empresas contratistas contratadas para desempeñar cualquier labor al interior del departamento de informática. En tal exposición deberá hacerse énfasis en las sanciones de tipo disciplinario en las que se puede incurrir por no atender o violar las políticas de seguridad de la información establecidas.

Política 013: Sera responsabilidad del departamento de informática diseñar un esquema de asignación de roles y responsabilidades sobre los activos. Antes de asignar a cualquier persona o empresa determinado activo, estas deberán ser informadas de la responsabilidad que asumen en relación a la administración propia del activo y la seguridad del mismo.

Política 014: Sera responsabilidad del departamento de informática llevar estricto control y supervisión sobre las personas responsables de la administración de los activos asignados al departamento de informática. Así mismo los administradores de los sistemas de información serán directamente responsables de la asignación de permisos a los usuarios y deberán llevar control documentado de la asignación de privilegios de acceso suministrados, también serán responsables de la

actualización y deshabilitar los permisos cuando los usuarios hayan sido reubicados o reasignadas sus funciones.

Política 015: Sera responsabilidad de la dirección del departamento de informática diseñar jornadas de capacitación permanente sobre la seguridad de la información. En donde especialmente se recuerde a los funcionarios y contratistas las políticas de seguridad existentes en la organización y la obligación de su observación y aplicación en las actividades diarias del departamento. Así mismo deberán establecerse medios de divulgación como correo electrónico, cartelera, etc., para la divulgación permanente de las políticas de seguridad de la información.

Dominio - Gestión de activos

Política 016: Sera responsabilidad del departamento de informática llevar de forma estricta inventario de todos los activos bajo su responsabilidad. En tal inventario cada activo deberá estar rigurosamente clasificado y por cada activo deberá estar definida la persona responsable de su estado y administración. Los responsables de los activos deberán responder por:

a). Estado de los activos.
b). Reportar y verificar la inclusión del activo en el inventario de activos.
c). Verificar que el activo este correctamente clasificado.
d). En caso de que el activo deba ser eliminado o destruido, deberá responderse por la correcta aplicación del procedimiento a seguir en tal situación.
e). Velar por la seguridad del activo.
f). La correcta disposición y almacenamiento del activo.
g). Velar por la disponibilidad del activo.

Política 017: Sera responsabilidad del departamento de informática establecer los lineamientos de seguridad y responsabilidad a los que deberán ajustarse las personas externas a la organización y que representan otras entidades con las cuales se mantienen convenios interadministrativos a través de los cuales se les habilita para tener acceso a ciertos activos o empresas contratistas que provean servicios a la entidad. En tales lineamientos se establecerá el manejo que deberá dársele a la información contenida en los activos y el compromiso que se asume por su utilización, estos lineamiento deberán considerar también para las instalaciones de proceso de información. Tales lineamientos serán una directriz institucional aplicada a cualquier usuario externo a la organización.

Política 018: En el momento en que una persona ya sea funcionaria o contratista se retire de la entidad y se encuentre adscrita al departamento de informática deberá hacer entrega formal del activo que se encontraba bajo su responsabilidad. Tal entrega implicara los siguientes pasos:

a). Dirigir oficio formalmente diligenciado y firmado al director del departamento de informática en donde describe el estado actual del activo que se está entregando.
b). Deberá realizarse la entrega formal a la persona que designe la dirección del departamento de informática, persona ultima que asumirá la responsabilidad temporal del activo hasta tanto sea designado por la dirección del departamento el nuevo titular del activo. Esta persona a la que se realiza la entrega del activo deberá dar su visto bueno en relación al estado en que se recibe el activo para que el director del departamento de informática pueda firmar el recibido al antiguo titular del activo.

Este mismo procedimiento aplica para el caso de empresas que por alguna razón administren o tengan a cargo activos de la entidad.

Política 019: Sera responsabilidad del departamento de informática diseñar y establecer un esquema de clasificación de la información y de los activos basados en el valor que estos representan para la organización. Las personas responsables de cada activo deben responder por la correcta clasificación de su activo dentro del esquema de clasificación.

Deberá considerarse un esquema de etiquetado que identifique de manera única cada activo y que de su lectura pueda establecerse que obedece a un activo ubicado en el departamento de informática de la entidad.

El principal aspecto a considerar dentro del proceso de clasificación de los activos del departamento de informática será su nivel de criticidad dentro de las labores propias de la entidad y el nivel de confidencialidad de la información.

El esquema de clasificación que se establezca deberá estar sujeta a revisión con el propósito de mantener un sistema de clasificación optimo y acorde con las necesidades y condiciones del departamento de informática.

El esquema de clasificación deberá ser producto del trabajo colectivo e integrado de todas las personas responsables de activos al interior del departamento de informática.

Política 020: Con el fin de evitar robo y/o fuga de información los puertos USB y las unidades de CD/DVD de los computadores, portátiles, servidores e impresoras deberán deshabilitarse mediante la aplicación de políticas de grupo GPOs a través de la herramienta Active Directory. Esta política se aplicara por defecto en todos los equipos del departamento de informática. De no ser posible la aplicación de la política de grupo GPOs tales puertos deberán deshabilitarse manualmente.

Solo en los casos en que sea estrictamente necesario se habilitaran los puertos USB o unidades de CD/DVD para la utilización de medios extraíbles, lo que

deberá ser argumentado por el solicitante mediante oficio dirigido a la dirección del departamento de informática.

Política 021: Las personas a las que se haya aprobado la utilización de medios extraíbles serán responsables de mantener vacunados y libre de todo tipo de contaminación (Virus, Malware, Troyanos, etc.), dichos dispositivos. En el caso en que se compruebe que tal disposición sea ignorada por las personas que emplean tales medios serán sancionadas por incumplir las políticas de seguridad de la organización y se les aplicara las sanciones a que haya lugar.

De manera periódica una persona designada por la dirección del departamento de informática y afín con los temas de seguridad de la información evaluara el estado de los medios removibles y se asegurara que tales medios estén libres de cualquier tipo de contaminación y que la información contenida en ellas corresponda a información propia de las funciones y responsabilidades de la persona que posee el respectivo medio.

Política 022: Las personas que utilicen medios extraíbles de su propiedad o de propiedad de la entidad, que se les haya aprobado la utilización de tales medios al interior del departamento de informática y que regularmente almacenen información relevante sobre activos e información que se encuentren bajo su responsabilidad, deberán crear una carpeta genérica en la que será almacenada toda la información relacionada con los activos e información relacionada con sus funciones y responsabilidades dentro del departamento de informática.
Tal carpeta deberá ser codificada para su debida protección.

Política 023: En el caso de información relevante de la entidad, como por ejemplo copias de seguridad y cuyo almacenamiento se haya dispuesto hacerlo en medios extraíbles. Se establece lo siguiente:

Las copias de seguridad solo deberán guardarse en dispositivos como CD/DVD o Discos Duros.

El responsable de tal copia de seguridad asumirá la responsabilidad por la salvaguarda de tal copia de seguridad y por su almacenamiento en lugar físico dispuesto formalmente por el departamento de informática. Así como entregar una copia a quien se designe por parte de la dirección del departamento de informática para que esta persona a su vez realice entrega formal de tal copia a la empresa de custodia de valores en caso de existir tal contrato de custodia.

Política 024: Cuando por alguna razón la información contenida en los medios extraíbles deba borrarse deberá procederse de la siguiente manera:

a). La persona que posee el medio, deberá acudir a la persona designada para evaluar el estado periódico de los medios extraíbles para que realice la eliminación

segura de la información relacionada con sus funciones y responsabilidades dentro del departamento de informática. En los siguientes casos:

- Información obsoleta.
- Daños en la información que impidan su lectura.
- Reasignación de funciones por parte de la persona que posee el medio.
- Traslado a otra área de la persona que posee el medio.
- Renuncia o terminación de contrato.

b). En el caso de aquellos dispositivos que sean propiedad del departamento de informática y que dejen de operar. Deberá procederse con la destrucción del dispositivos de acuerdo a las mejores prácticas dispuestas para tal efecto, deberá quedar registrado tal hecho para efectos de control de inventario de activos y auditoria.

Dominio – Control de acceso

Control de acceso físico

Política 025: Sera responsabilidad del departamento de informática determinar y señalizar correctamente las áreas de acceso restringido. Las señalizaciones deberán ubicarse de tal manera que sean fácilmente visibles y los mensajes deberán ser claros y precisos.

Política 026: Ningún equipo que se considere critico para las operaciones habituales de la entidad (servidores, equipos activos de comunicaciones, librerías, etc.), podrán ubicarse fuera de los lugares de procesamiento de información formalmente definidos y establecidos (centro de datos).

Política 027: El ingreso a los sitios de procesamiento de datos (centro de datos) estará condicionado de la siguiente manera:

- A los sitios de procesamiento de información (centro de datos) solo tendrán acceso personal previamente autorizado y específicamente personal encargado de la administración de activos (administradores de sistemas, administradores de bases de datos, administradores de comunicaciones).
- A los sitios de procesamiento de información se tendrá acceso solo hasta que se diligencie y firme documento de registro de ingreso. En el que deberá incluirse la siguiente información: Nombres y apellidos de quien ingresa, razón por la cual desea ingresar, hora de ingreso y hora de salida, firma de quien ingresa.
- En el caso de que empleados de empresas contratistas o de empresas proveedoras de servicios deban ingresar al sitio (s) de procesamiento de información, estos deberán estar acompañados por el responsable del activo que se vaya a revisar.

Control de acceso lógico

Política 028: Sera responsabilidad del departamento de informática diseñar formato para la solicitud de derechos de acceso por parte de los usuarios a los activos del departamento de informática. Esto no aplicara para la solicitud de creación de cuentas de usuarios de dominio, ni para las cuentas de correo electrónico.

Política 029: Las solicitudes de acceso a los activos por parte de usuarios deberá implicar el diligenciamiento del formato oficial que se establezca al interior del departamento de informática para solicitudes de acceso. Tal formato lo diligenciara la persona interesada y deberá firmarse por el director del departamento de informática o en su defecto por los coordinadores de grupo de ese mismo departamento. Tal solicitud deberá ser remitida a la Mesa de Ayuda para que esta la envié mediante ticket al responsable del activo y este proceda a conceder los derechos de acceso pertinentes. Sera la persona responsable del activo quien finalmente evalué la conveniencia de asignar los derechos de acceso que se solicitan, en caso de no considerar pertinente la asignación de determinados derechos de acceso a usuarios deberá comunicar por el medio que considere necesario tal decisión a la dirección del departamento de informática.

Política 030: Los responsables de los activos serán responsables de llevar un registro en el que se consigne la información de las personas a las que se asignen derechos de acceso (No aplica para las cuentas de usuarios de dominio y cuentas de correo electrónico). Tal registro deberá contener a grandes rasgos la siguiente información:

- Nombres y apellidos de las personas a quienes se han asignado derechos de acceso.
- Identificación (Cedula de Ciudadanía).
- Cuenta de usuario de la persona a la que se asignan derechos de acceso.
- Razones para la asignación de derechos de acceso.
- Grupo al que se encuentra asignada la persona a la que se asignan derechos de acceso al interior del departamento de informática.

Política 031: Ningún usuario o contratista podrá modificar su forma de acceso a la red LAN de la organización. Solo personal técnico de Mesa de Ayuda o en su defecto los administradores de comunicaciones podrán modificar la configuración IP de los equipos (computadores, portátiles, impresoras).

Política 032: A nivel de equipos servidores, La asignación y configuración IP será responsabilidad de los administradores de los activos relacionados. Coordinados y orientados por los administradores de comunicaciones.

Política 033: Los puertos físicos de red que no se estén utilizando deberán deshabilitarse para evitar que cualquier persona no vinculada al departamento de informática pueda conectarse directamente a la red LAN de la entidad.

Política 034: Sera responsabilidad del departamento de informática diseñar los lineamientos mediante los cuales se permitirá el establecimiento de comunicaciones entre entidades públicas o privadas a través de VPN.

Política 035: Cuando una persona sea incorporada al departamento de informática, esta deberá diligenciar el documento denominado “Formulario para la administración de usuarios nuevos, activos e inactivos”. Para que se pueda proceder por defecto con la creación de la cuenta de usuario de dominio y correo electrónico. Tal formulario deberá enviarse a la Mesa de Ayuda para que estos generen ticket que enviaran a los responsables para proceder con la creación de las cuentas mencionadas.

Política 036: Sera obligación por parte de quienes administran activos que impliquen la creación y eliminación de cuentas de usuarios de dominio y correo electrónico almacenar adecuadamente los formatos denominados “Formulario para la administración de usuarios nuevos, activos e inactivos”. Que serán recibidos a partir de la creación de ticket por parte de Mesa de Ayuda para la creación y/o eliminación de cuentas de usuarios. Tales formatos deberán ser almacenados en carpetas de acuerdo a la ley nacional de administración de documentos (Gestión Documental).
Política 037: Los administradores y responsables de activos, específicamente de quienes tienen que ver con la creación de cuentas de usuarios y asignación de derechos de acceso deberán ser informados de manera oportuna y mediante la generación de ticket acerca de la reasignación, traslado, renuncia o terminación de contrato de los usuarios. Para que los responsables de activos lleven a cabo la actualización de sus registros en relación al estado actual de los usuarios.

Política 038: Sera responsabilidad del departamento de informática el diseño y establecimiento de un sistema de nomenclatura estándar para la creación de las cuentas de usuarios. Así como la observación de las mejores prácticas para la configuración y uso de contraseñas.

Política 039: Los usuarios serán responsables por el uso que cada uno haga de las cuentas de usuarios y los derechos de acceso que se les asignen. Los usuarios deberán considerar las siguientes recomendaciones:

- El uso de las cuentas de usuarios es de carácter privado, por lo tanto queda determinante prohibido compartir el uso de cuentas de usuarios.
- Sera responsabilidad de cada uno de los usuarios conservar la privacidad de las cuentas de usuarios y contraseñas. Las mismas no deberán estar escritas o dispuestas en ningún sitio visible a terceras personas.

- Sera responsabilidad de los usuarios observar las mejores prácticas a la hora de configurar sus contraseñas.
- En el caso de ausencias por motivos de vacaciones, licencias, etc., cada usuario deberá solicitar a través de la mesa de ayuda el bloqueo temporal de su cuenta de usuario.
- En ningún caso se podrá entregar a otra persona el uso de la cuenta de usuario de una persona que se encuentre ausente del departamento de informática.

Política 040. Sera responsabilidad del departamento de informática llevar el registro y conservación del código fuente de cada uno de los aplicativos y sistemas de información existentes en la entidad, dicha información deberá consignarse en el inventario de activos del departamento de informática. Tal información deberá conservarse de forma segura a la que solo tengan acceso el director del departamento de informática o en su defecto a quien este delegue.

La modificación del código fuente de cualquier aplicativo o sistema de información solo podrá ser autorizado por el director del departamento de informática para lo cual deberá generarse documento formal en el que se exponga la necesidad o motivo de la modificación.

Política 041. Ninguna persona responsable de activos podrá tomar la decisión autónoma de utilizar programas de tipo utilitarios. Por el contrario tendrá la obligación de informar por el medio que considere pertinente al responsable de seguridad o quien haga sus veces acerca del uso de herramientas que se proponga utilizar como complementarias para la administración del activo o activos bajo su responsabilidad. Solo hasta que el responsable de seguridad evalué y dictamine la pertinencia de utilizar tales programas complementarios podrá hacerse uso de los mismos. En el caso en que se utilicen programas complementarios sin la evaluación y permiso del responsable de seguridad se podrá incurrir en el incumplimiento de las políticas de seguridad de la organización lo que acarreara sanciones disciplinarias.

Dominio - Seguridad física y del entorno

Política 042: Sera responsabilidad del departamento de informática y específicamente de la coordinación del grupo de asistencia técnica diseñar, implementar y supervisar la ejecución de un plan de mantenimiento preventivo y correctivo de los activos asignados al departamento de informática. Deberán tenerse en cuenta las siguientes consideraciones:

- El plan de mantenimiento preventivo y correctivo de los activos debe llevarse a cabo de forma periódica. Tal periodicidad será establecida en conjunto por el director del departamento de informática y los coordinadores

de grupo (coordinador de asistencia técnica, coordinador centro de computo, coordinador de desarrollo informático).

- La empresa a cargo de los mantenimientos preventivos y correctivos deberá demostrar experiencia comprobada en el tema.
- El responsable de cada activo deberá acompañar a la persona encargada de realizar el mantenimiento preventivo y correctivo. Así como comprobar la funcionalidad del activo una vez se haya realizado la actividad.
- Se deberá generar por parte de las personas encargadas de realizar las labores de mantenimiento reporte documentado de las actividades de mantenimiento llevadas a cabo en el que se indique el estado del activo. Tal reporte deberá ser firmado por el responsable de cada activo. La recopilación de los reportes deberá entregarse a la coordinación de asistencia técnica para la aprobación formal de cumplimiento.

Política 043: Ningún activo propiedad de la entidad y bajo control del departamento de informática podrá salir de las instalaciones sin la respectiva autorización del director del departamento de informática.

En el momento en que el activo salga de las instalaciones de la entidad, el estado del mismo será responsabilidad de la persona o empresa a la que se autorizo su utilización. Se deberán tener en cuenta las siguientes consideraciones:

- En el caso en que los equipos deban ser utilizados en lugares públicos, estos deberán estar bajo permanente vigilancia.
- En el caso de que los equipos deban ser utilizados en lugares públicos. Los equipos deberán accederse mediante la utilización de credenciales previamente definidas.
- En el caso de que los equipos deban ser utilizados en lugares públicos. Los equipos deben conservarse y mantenerse bajo las condiciones sugeridas por el fabricante.

Política 044: Antes de poder reutilizar cualquier equipo en caso de ser necesario. deberá asegurarse que la información contenida actualmente en el equipo sea borrada adecuadamente con las herramientas y técnicas dispuestas para tal propósito. solo hasta que esta operación sea efectuada se podrá asignar al equipo en cuestión el nuevo rol para el que ha sido dispuesto.

Política 045: Sera responsabilidad de los usuarios salvaguardar la información que se encuentra bajo su control. Deberán tenerse en cuenta las siguientes consideraciones:

- La información critica que se maneje representada en documentos deberá almacenarse en sitio seguro como por ejemplo caja fuerte, gabinete bajo llave, etc.

- La información critica almacenada en medios de almacenamiento extraíbles como USB o discos duros extraíbles deberán almacenarse en sitio seguro como por ejemplo caja fuerte, gabinete bajo llave, etc.
- En el momento en que el usuario no se encuentre frente a su equipo de trabajo deberá bloquear la sesión.
- En ningún caso los archivos y carpetas de trabajo podrán almacenarse en el escritorio del equipo. Por el contrario deberán almacenarse en cualquier ubicación dentro del disco duro del equipo.
- Por defecto en el fondo del escritorio de los equipos de los usuarios deberá prevalecer la imagen institucional de la entidad.
- Ningún usuario podrá modificar el fondo de escritorio de los equipos, para lo cual deberá aplicarse política de seguridad que impida tal cambio.

5. CONCLUSIONES

A partir de todo el levantamiento de información realizado y su posterior lectura y análisis, la observación directa y los resultados obtenidos como consecuencia del estudio de análisis de riesgo. Se puede concluir que la información y la infraestructura tecnológica a través de la cual se administra la misma, en el departamento de informática de la Superintendencia de Notariado y Registro requiere y exige la consideración de manera pronta y oportuna de la construcción y establecimiento estricto de medidas y lineamientos de seguridad para la información que sean aplicables, eficientes, efectivos, evaluables y que puedan garantizar la integridad, confidencialidad y disponibilidad de la información.

A pesar de la inversión constante en recursos de tecnología con el propósito principal de administrar más eficientemente la información y ofrecer tiempos de respuesta óptimos a los requerimientos de los usuarios. La seguridad de la información es un tema en general desconocido por la dirección del departamento de informática y cada uno de sus miembros. Situación que por demás se haya extendida a toda la entidad.

Al interior del departamento de informática al tema de la seguridad de la información no se le trata con la debida importancia y ello es producto de la generalizada ignorancia alrededor del tema. Lo que genera que los responsables y administradores de los sistemas y aplicaciones solo centren su atención en la funcionalidad y disponibilidad de los mismos perdiendo de vista la imperiosa necesidad de construir e implementar escenarios óptimos que permitan contrarrestar las amenazas que se ciernen sobre la información.

Las actuales practicas de administración de tecnología de la información por parte de la mayoría de los miembros del departamento de informática ignora todas las recomendaciones de buenas prácticas conocidas actualmente. Lo que genera situaciones riesgosas que podrían poner en serio riesgo la seguridad de la información y los recursos tecnológicos sobre la que esta se administra.

Desafortunadamente los pocos controles de seguridad que fueron diseñados en su momento no están sujetos a ningún tipo de revisión y evaluación que permitan establecer su cumplimiento por parte de todos los miembros directos o indirectos del departamento de informática. Así mismo como consecuencia de la falta de evaluación periódica de los controles de seguridad no se puede determinar la efectividad de tales controles de seguridad.

La información es el activo más importante para cualquier organización y como tal debe garantizarse por todos los medios posibles su seguridad. El departamento de informática tiene a su cargo la enorme responsabilidad no solo de administrar de forma correcta y eficiente la información de la entidad sino que también le asiste la

obligación indelegable de diseñar y establecer un marco de seguridad que permita mantener siempre segura la información y la infraestructura a través de la cual se administra.

Un Sistema de Gestión de Seguridad de la Información (SGSI), se constituye en una excelente alternativa para contribuir efectivamente a la seguridad de la información. A través del SGSI el departamento de informática podrá tener un conocimiento claro y preciso de los activos bajo su responsabilidad, la correlación existente entre ellos y su nivel de importancia dentro de la operación habitual de la organización. Lo que traerá como consecuencia que se distinga claramente cuáles son los activos que exigen mayor atención y protección, De acuerdo a ello se podrán establecer las medidas de seguridad pertinentes y ajustadas completamente a la realidad actual de departamento de informática.

La presencia de un SGSI exigirá la aplicación estricta de las medidas y lineamientos de seguridad contenidos en él y la reorganización de los procedimientos que actualmente existen en el departamento de informática. Su sola consideración exigirá una reorganización interna en donde el tema de seguridad de la información será protagonista dentro de las actividades habituales del departamento, el diseño e implementación de cualquier proyecto tecnológico deberá obligadamente considerar imperativamente los lineamientos establecidos en el SGSI. Su cumplimiento deberá ser observado por cualquier miembro del departamento de informática así como por cualquier proveedor de servicios ya que en caso contrario podrían incurrir en conductas irresponsables de acuerdo a los lineamientos establecidos por la entidad. Lo que motivara la aplicación de sanciones enmarcadas dentro de un marco sancionatorio que operara de la mano con el SGSI.

En definitiva la consideración de un Sistema de Gestión de Seguridad de la Información (SGSI) para el departamento de informática de la Superintendencia de Notariado y Registro traerá valiosos beneficios, que se traducirán en un manejo responsable y seguro de la información y los recursos tecnológicos alrededor de la misma, mediante la fijación de políticas de control claramente definidas y de estricto cumplimiento se evitara que tanto los administradores y responsables de los sistemas y aplicaciones, así como los usuarios en general actúen autónomamente y de manera irresponsable frente a las obligaciones que les asisten en cuanto al buen uso de la información y los recursos tecnológicos. El diseño y futura implementación de un SGSI permitirá establecer y afianzar el tema de la seguridad de la información al interior del departamento de informática y definir como compromiso entre sus miembros que la seguridad de la información es una responsabilidad de todos.

BIBLIOGRAFIA

Buenaño, J., & Granda, M. (2009). Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 – 27002 (tesis pregrado). Universidad Politécnica Salesiana, Guayaquil, Ecuador.

Congreso de Colombia. (2009). LEY 1273. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Chang, A., & Enrique, C. (2011). Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de seguros (tesis pregrado). Pontificia Universidad Católica del Perú, Lima, Perú.

De La Cruz, C., & Vásquez, J. (2008). Elaboración y aplicación de un sistema de gestión de la seguridad de la información (SGSI) para la realidad tecnológica de la USAT (tesis pregrado). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.

Ferrer, R. Sistema de Gestión de Seguridad de la Información SGSI. Recuperado de: http://www.sisteseg.com/files/Microsoft_PowerPoint_-_Estrategias_de_seguridad_v52.pdf

Gómez, A. (2011). Enciclopedia de la Seguridad Informática, Madrid, España: ALFAOMEGA – RAMA.

Instituto Nacional de Tecnologías de la Comunicación. Normativa. Recuperado de: http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

ISO 27000.ES. EL PORTAL DE ISO 27001 EN ESPAÑOL. Recuperado de: http: //www.iso27000.es/sgsi.html.

León, M., Mora, E., & Navarrete, J. (2011). Implementación de un Sistema de Gestión de Seguridad de la Información usando la norma ISO27000 sobre un sitio de comercio electrónico para una nueva institución bancaria aplicando los dominios de control ISO27002:2005 y utilizando la metodología Magerit (tesis de pregrado). Escuela Superior Politécnica Del Litoral (ESPOL), Ecuador.

Ministerio de Hacienda y Administraciones Públicas. MAGERIT v. 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VWxs71KTqig

Oficina de Seguridad para las Redes Informáticas. Metodología para la gestión de la seguridad informática. Recuperado de: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico (tesis maestría). Universidad de la República. Montevideo, Uruguay.

Presidencia de la República. (2014). Decreto 2723. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/decreto_2723_2014.html

Universidad de Vigo. Estándares y Normas de Seguridad. Recuperado de: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

Las fuentes de información que se utilizaran en el desarrollo del proyecto de grado serán en su gran mayoría fuentes secundarias y alguna fuente primaria documental.

ANEXOS

ANEXO A
(Circular No. 77 de 2008 - Superintendencia de Notariado y Registro)

Libertad y Orden

Superintendencia de Notariado y Registro
Ministerio del Interior y de Justicia
República de Colombia

CIRCULAR N° **77**

Bogotá, D.C., **30 de mayo de 2008**

PARA: Directivos, Registradores de Instrumentos Públicos, Coordinadores de Grupo y Funcionarios

DE: Superintendente de Notariado y Registro

ASUNTO: Políticas de Seguridad en los Sistemas de Información

Reciban un atento saludo:

Con el fin de preservar los activos institucionales como son la información, la plataforma tecnológica y los sistemas de información, se hace necesario, reglamentar e institucionalizar políticas para el correcto uso de estos, garantizando el acceso, la seguridad y confiabilidad que, por su misma naturaleza, la Superintendencia de Notariado y Registro debe proveer a sus usuarios.

A partir de la fecha y dada la reglamentación que se acoge con la presente disposición, se dispondrá de un mecanismo regulado para el uso de la información y la plataforma tecnológica.

Se abarcan aspectos como el uso de Internet, el correo electrónico, claves de acceso, cuentas de usuario, seguridad de los servidores y de los medios removibles y extraíbles.

Así mismo, el manejo de licencias de software y hardware, la implementación de planes de contingencia y backup y la reglamentación para el acceso a los centros de cómputo e instalaciones físicas en general.

Este propósito sólo es posible con el compromiso de cada uno de ustedes y con el permanente apoyo de la Oficina de Informática, dependencia encargada de liderar el cumplimiento y revisiones posteriores de estas políticas y a la cual se pueden dirigir en el teléfono 3282121 Ext. 217.

Superintendencia de Notariado y Registro
La guarda de la fe pública
Calle 26 No.13-49 Interior 201 Bogotá, D.C. Tel. 3282121
Email: computosnr@supernotariado.gov.co
www.supernotariado.gov.co

Libertad y Orden

La presente circular deja sin efectos todas las disposiciones anteriores relacionadas con las Políticas de Seguridad en los Sistemas de Información.

Cordialmente,

LIDA BEATRIZ SALAZAR MORENO
Superintendente de Notariado y Registro

Proyectó: Víctor Chitiva Acosta
Profesional Especializado-Centro de Computo

Revisó: William Fernando Albarracin Barreto
Jefe Oficina Informática

Anexo: Políticas de seguridad en los sistemas de información (18 folios)

POLITICAS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACION

El siguiente documento contiene las políticas de seguridad de la Superintendencia de Notariado y Registro, las cuales tienen como objetivo establecer un mecanismo regulado para el uso de la información, infraestructura de sistemas de cómputo y gerencia de redes de la entidad.

Los sistemas de cómputo, de gestión, equipos e infraestructura de comunicaciones están contemplados en el presente documento.

Igualmente, se pretende la protección de los activos de SNR representados tanto en la información como en los equipos y sistemas de cómputo que se utilicen.

Cada funcionario o tercero al cual se le permita acceso a los sistemas de cómputo de la entidad debe certificar el conocimiento del presente documento, como su respectiva aplicación de las prácticas y políticas que se exponen, así como las versiones posteriores que sean publicadas.

1. POLITICAS DE SEGURIDAD LOGICA

POLÍTICA 1: SEGURIDAD EN LA UTILIZACIÓN DEL CORREO ELECTRÓNICO

Objetivo: Prevenir la perdida de la buena imagen y honorabilidad de la entidad. Cuando un correo electrónico es enviado a una entidad o a personas externas se entenderá como un pronunciamiento oficial de SNR, teniendo en cuenta la ley 527 de agosto 18 de 1999, artículo 10. Que enuncia: A*dmisibilidad y fuerza probatoria de los mensajes de datos*. Los mensajes de datos serán admisibles como medio de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.
Alcance: Esta política contempla el apropiado uso del correo electrónico enviado desde una dirección de correo perteneciente al correo institucional de SNR y aplica a todos los funcionarios.
Descripción: La asignación de cuentas de correo electrónico institucional se debe hacer mediante una solicitud enviada por el jefe inmediato al correo: computosnr@supernotariado.gov.co y justificada de acuerdo con las necesidades del área y a su cargo, dirigida al jefe de Informática. Igualmente los usuarios finales deberán ser orientados en el uso de esta tecnología.

a. Se prohíbe la utilización del correo electrónico institucional para la creación o envio de mensajes ofensivos acerca de la raza, orientación sexual, edad, pornografía, creencias y prácticas de tipo religioso, terrorismo, creencias políticas o de cualquier otra índole.
Si un funcionario recibe un correo electrónico con alguno o varios de los contenidos anteriores desde una dirección institucional de SNR, debe reportar esta anomalía a su jefe inmediato.

b. El envio de correos electrónicos en los cuales se invita a hacer cadenas de correos para ser enviadas a otros usuarios desde una cuenta de correo institucional de SNR está prohibido. Las alertas acerca de nuevos virus y el envió de correos masivos desde el correo institucional deben ser aprobados por la Oficina de Informática antes de su remisión para no incurrir en prácticas de spam. Estas restricciones también aplican al reenvio de correos externos recibidos por los funcionarios de SNR en sus cuentas de correo institucional.

c. Todo funcionario que reciba un correo electrónico y que sospeche que no es confiable o es de una fuente desconocida debe inmediatamente eliminarlo.

d. La SNR, por intermedio de la oficina de informática no está obligada a monitorear los mensajes de correo electrónico, pero por razones de exceso de tráfico en la red o cualquier otra anomalía puede hacer un monitoreo sin una notificación previa por intermedio del centro de computo o de un tercero.

DEFINICIONES:

Política: Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la entidad.

SNR: Superintendencia de Notariado y Registro.

Spam (Junk-Mail): Envió de correos electrónicos basura, que puede llenar el buzón de un usuario. Por lo general esta práctica la efectúan marcas comerciales para promocionar indiscriminadamente sus productos por toda la red de Internet.

POLÍTICA 2: SEGURIDAD EN LA UTILIZACIÓN DE INTERNET

Objetivo: Definir aspectos de seguridad a ser aplicados por la SNR en cuanto a la navegación por Internet.
Alcance: Esta política contempla cualquier tipo de comunicación que se establezca a través de la Red Internet por parte de los funcionarios de SNR desde equipos pertenecientes a la red interna en el desempeño de labores operativas.
Descripción: El acceso a Internet deberá ser habilitado a los funcionarios que requieran el uso de esta herramienta en el desarrollo de procesos validos dentro de SNR. Este requerimiento se hace mediante una solicitud firmada por el Jefe inmediato y justificada de acuerdo con las necesidades del área a su cargo, dirigida al Jefe de Informática. Así mismo los usuarios finales deberán ser orientados en el uso de esta tecnología.

a. El acceso a Internet será controlado teniendo en cuenta los sitios visitados y la cantidad de recursos utilizados.

b. Toda conexión a Internet deberá pasar a través de un Firewall que controle la totalidad del tráfico entrante y saliente de la red interna. Prohibiendo el paso de todo tráfico que no se encuentre expresamente autorizado.

c. La configuración del Firewall implementado deberá revisarse periódicamente y cada vez que se produzcan cambios sobre los sistemas relacionados con Internet.

d. Toda conexión entre sistemas de comunicación de SNR e Internet o cualquier Red pública de datos debe hacerse a través de un Firewall y mecanismos de control de acceso y detección de intrusos.

e. Toda conexión VPN que se realice con otras entidades públicas o privadas debe ser solicitada al Jefe de la Oficina de Informática por el respectivo jefe de área o coordinador, indicando la dirección a la cual necesita establecer la conexión, tipo de tráfico y puertos utilizados, además del usuario que utilizara este servicio.

f. La conexión directa entre un computador de SNR y otra organización vía redes públicas de datos como Internet requieren de la aprobación del administrador de la seguridad de SNR o quien lo represente, quien estipulará los mecanismos de seguridad apropiados como Firewalls, Autenticación, encripción, etc.

g. Cuando un funcionario de SNR publique un mensaje en un grupo de discusión de Internet, foro, boletín electrónico, o cualquier otro sistema de información publico, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de SNR, dichas frases son requeridas aun cuando el nombre de SNR no aparezca en el texto del mensaje y/o cuando una afiliación con la entidad no ha sido establecida explícitamente.

h. Los funcionarios de SNR no deben anunciar, promover, presentar o hacer afirmaciones acerca de los productos y servicios de la entidad en foros de Internet, sesiones de charla (Chat), sin la previa aprobación del Grupo Divulgación de SNR.

i. Se debe acceder únicamente a sitios de confianza, si se presenta alguna duda en cuanto a la autenticidad de determinado sitio o portal de Internet se debe hacer la respectiva consulta a la Oficina de Informática o al encargado de la seguridad.

j. Los funcionarios no deben utilizar los computadores asignados para el desarrollo de su trabajo para la exploración ociosa.

k. No está permitido:

- Descargar, instalar y utilizar el programa Messenger en los equipos de SNR pues éste es una puerta abierta para el ingreso de virus y

software malicioso además carga considerablemente el tráfico en la red ocasionando lentitud en el uso de los aplicativos misionales.

- Descargar videos que no tengan relación con la actividad laboral.
- Descargar música ya que esto ocasiona que la red se congestione.
- Sintonizar emisoras de radio desde Internet.
- Descargar contenidos de tipo sexual, racista, terrorista o de tipo ofensivo
- Utilizar el acceso a Internet para promover actividades ilegales.
- Hacer solicitudes comerciales (no relacionadas con la entidad).
- Descargar o o instalar programas sin conocer su procedencia y sin consultar con la Oficina de Informática y el centro de cómputo.

l. Está prohibido navegar a través de páginas o portales de Internet que muestren contenidos sexuales, racistas, terroristas o que contengan cualquier otro tipo de material ofensivo. La posibilidad de conectarse a una página específica por si mismo no implica que el funcionario de SNR tenga el permiso para visitar dichos sitios.

m. Se prohíbe el uso de redes informáticas P2P (en ingles peer-to-peer).

DEFINICIONES:

Firewall: Sistema de defensa que puede estar compuesto de hardware y software o de sólo software que funciona como una barrera entre la red local e Internet, permitiendo o denegando transmisiones desde una red a la otra. Por lo general estos dispositivos se instalan entre la red local y de Internet para evitar que los intrusos accedan a información confidencial.

VPN (Virtual Private Network): Redes privadas virtuales con tecnología que permiten la transmisión de información privada sobre redes de uso público de manera segura, utilizando conexiones virtuales.

P2P: Se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red. Este tipo de redes se suelen utilizar para el intercambio de todo tipo de archivos, preferiblemente canciones, películas y juegos, entre usuarios particulares que necesitan para ello haber instalado un software en su computador, por ejemplo: programas como emule, edonkey, overnet, bittorrent, ares, kazaa, etc.

POLÍTICA 3: SEGURIDAD EN LAS CLAVES DE ACCESO Ó PASSWORD Y CUENTAS DE USUARIO

Objetivo: Establecer el mecanismo de creación y eliminación de cuentas de acceso. Igualmente determinar un estándar para la creación de claves de acceso fuertes, la protección de dichas claves y la frecuencia de cambio. El objetivo final es asegurar que un usuario es quien dice ser, cuando acceda a los sistemas de cómputo de SNR.
Alcance: Esta política incluye a todos los funcionarios que tienen o son responsables de una cuenta de usuario (o cualquier forma de acceso que requiera un password) para acceder a un sistema que esté almacenado en los servidores o sistemas de

computo de SNR o para tener acceso a la red de la entidad o para almacenar información privada que solo pertenece a la entidad.
Descripción: La asignación de cuentas de usuario las debe efectuar el centro de cómputo de SNR, pero las claves de acceso son privadas y las define cada usuario teniendo en cuenta las normas de seguridad correspondientes.

a. Las cuentas de acceso a los sistemas de SNR se clasifican así:

   - Usuarios: Tienen únicamente el derecho de usar los sistemas y recursos.
   - Operadores: Tienen derecho de uso, monitoreo y administración limitada de los sistemas y equipos.
   - Administradores: Tienen control total de los sistemas y equipos.

b. Todos los computadores de SNR, deben estar integrados dentro del Directorio Activo para la aplicación de políticas de seguridad y no deben ser deshabilitados de este por ningún motivo por parte de los usuarios.

c. Se debe realizar una auditoria periódica y aleatoria en el proceso de creación y eliminación de cuentas.
   Todos los funcionarios adquieren los siguientes compromisos con la entidad cuando se les asigna una cuenta de acceso: ética, confidencialidad y uso responsable de los recursos de cómputo.

d. Todas las claves de acceso deben ser cambiadas al menos cada 90 días.

e. La contraseña suministrada por primera vez al usuario, deberá ser cambiada en el primer acceso al sistema. Está prohibido el re-uso de las últimas diez (10) contraseñas usadas.

f. Las claves de acceso no deben ser insertadas dentro de mensajes de correos electrónicos u otras formas electrónicas de comunicación, no deben ser enviadas por teléfono a nadie, no se debe hablar de su clave de acceso en frente de otras personas o funcionarios de SNR, no escriba su clave de acceso en cuestionarios o formularios que se diligencien por Internet, no comparta su clave de acceso con familia o amigos. Las claves de acceso son personales e intransferibles es decir estrictamente confidenciales.

g. Cuando un usuario sea trasladado de oficina, grupo o se encuentre en período de vacaciones no debe suministrar su clave a ningún otro usuario. Si es estrictamente necesario se debe solicitar al centro de cómputo el cambio de clave para que otro funcionario pueda consultar los archivos del funcionario que se encuentre ausente.

   Cuando se efectúe un traslado de un funcionario debe ser informado al Coordinador del Centro de Cómputo para realizar las actualizaciones en el software administrativo.

h. Las claves de acceso no deben basarse en información personal como nombres de la familia, mascotas, aficiones, hijos, números de teléfono,

direcciones, números consecutivos como: 123456, letras consecutivas como: aaaabbbb, etc.

i. Las claves de acceso deben contener al menos: un carácter en minúscula, un carácter en mayúscula, un digito del 0 al 9 y un carácter especial por ejemplo cualquiera de los siguientes: @#+=[&!$%}<>/.,):-

j. Las claves de acceso deben ser de una longitud mínima de seis (6) caracteres y deben ser creadas teniendo en cuenta el numeral anterior.

k. Las claves de acceso deben ser de fácil recordación. Una forma sencilla es que el usuario cree las claves de acceso basadas por ejemplo en una frase o en el título de una canción, por ejemplo la frase puede ser "Esta Puede Ser Una Forma Para Recordar" y la clave de acceso para esta frase podría ser: EpS1f2R! ó Eps1F>R-% o cualquier otra combinación.
Nota: no use este ejemplo como clave de acceso.

l. No se debe utilizar la opción de "Recordar contraseña" en aplicaciones como el correo de Hotmail, Yahoo o cualquier otra aplicación de Internet que lo solicite.

m. Para recordar su clave de acceso no se debe escribir en lugares como el escritorio, al lado del computador, pegada en papelitos al lado del monitor, debajo del teclado o en cualquier lugar que pueda ser fácilmente observada por alguien.

n. Si un funcionario de SNR sospecha que su clave de acceso ha sido descubierta o está seriamente comprometida, debe reportar este incidente a la Oficina de Informática o al encargado de seguridad y se debe proceder a cambiar inmediatamente su clave de acceso.

o. Todos los usuarios de los sistemas de cómputo de SNR son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y su clave de acceso personales.

p. Se debe llevar un sistema de control en donde se registrará todos los accesos o intentos de acceso realizados por cada uno de los usuarios de los sistemas de cómputo de SNR, los cuales podrán ser consultados para efectos de auditorias de seguridad.

Se limitará los intentos fallidos a tres (3) intentos, después del tercer intento se bloqueará la cuenta y se almacenará en el registro de logs, con el fin de identificar el usuario que está realizando estos intentos de acceso y así mismo evitar ataques sistemáticos.

POLÍTICA 4: SEGURIDAD EN LOS ACCESOS REMOTOS

Objetivo: Definir estándares para la conectividad de la red de SNR con cualquier otra entidad u organización. Estos estándares son diseñados para minimizar la potencial exposición de SNR a daños que puedan resultar de un uso no autorizado de recursos de la entidad. Los daños incluyen la perdida de información sensible o

datos confidenciales, propiedad intelectual, daños a la imagen pública, daños a los sistemas críticos internos de la entidad, etc.
Alcance: Esta política incluye a todos los funcionarios, contratistas, proveedores y en general a quienes estén autorizados para conectarse a la red de SNR por medio de un computador o estación de trabajo. Esta política aplica a todas las conexiones de acceso remoto usadas para trabajar sobre sistemas internos de la entidad, incluyendo la lectura y el envio de correo electrónico y la consulta de la intranet. Las implementaciones de acceso remoto cubiertas por esta política incluyen: VPN, SSH, frame relay, etc.
Descripción: Los accesos remotos a la red de SNR deben ser autorizados por la oficina de Informática de acuerdo a las normas y protocolos de comunicación que establezca la entidad.

a. Es responsabilidad de los funcionarios, contratistas, proveedores con privilegios de acceso remoto a la red de SNR asegurarse que su conexión de acceso remoto esta dada en las mismas condiciones de seguridad como si dicho usuario estuviera dentro de las instalaciones de la entidad.

b. El acceso remoto seguro debe ser estrictamente controlado por la Oficina de Informática de SNR. El acceso será forzado a una autenticación por medio de una clave de acceso o una llave publica/privada.

c. El acceso remoto deber ser hecho a través de una solución que incluya mecanismos de encripciòn y autenticación a través de llave única. Todo acceso que sea hecho remotamente a recursos internos o internamente a recursos externos de la entidad debe ser efectuado a través de sistemas de protección de la red de SNR.

d. El acceso remoto únicamente debe ser hecho a través de: clientes de software certificado y autorizado, IPSEC, criptografía y uso de cuentas de usuario.

e. Los funcionarios, contratistas y proveedores con privilegios de acceso remoto deben asegurarse que sus computadores personales o estaciones de trabajo, los cuales están conectados remotamente a la red de SNR, NO estén conectados al mismo tiempo a cualquier otra red, con excepción del personal de la Oficina de Informática que pueden tener un control total del usuario.

f. Todos los host que sean conectados a la red interna de SNR por la tecnología de acceso remoto deben usar un software antivirus actualizado, esto incluye computadores personales.

g. Los funcionarios u organizaciones que deseen implementar soluciones de acceso remoto a red de SNR deben obtener una aprobación de la Oficina de Informática y del funcionario encargado de seguridad.

h. No está permitido el uso de tarjetas de FAX/MODEM para ingresar a la infraestructura de red de SNR.

DEFINICIONES:

SSH: Protocolo que permite conectarse con equipos remotos a través de una red.

Frame Relay: Tecnología de conmutación rápida de paquetes orientada a conexión cuya principal aplicación es la interconexión de redes de área local. Actualmente están en desuso por la aparición de tecnologías como Gigabit Ethernet.

IPSEC: Conjunto de protocolos que permiten asegurar las comunicaciones sobre Internet autenticando y cifrando los flujos de datos.

Host: Cualquier equipo conectado a una red, que proporciona servicios a equipos o usuarios remotos.

POLÍTICA 5: SEGURIDAD EN LOS SERVIDORES

Objetivo: El propósito de esta política es establecer estándares para la configuración inicial de los servidores internos que son propiedad y/o son operados por la SNR. La implementación de esta política minimizará el acceso no autorizado a la información de propiedad de SNR y a su tecnología.
Alcance: Esta política es específica para los equipos que están en la red interna de SNR.
Descripción: Los servidores de SNR son los equipos en donde están instaladas las aplicaciones internas con sus respectivas bases de datos, además permiten la autenticación de usuarios en el Directorio Activo para la aplicación de políticas de seguridad, por lo tanto su protección y seguridad es fundamental en la operatividad diaria de SNR.

a. Todos los servidores internos de SNR deben ser operados y serán responsables por su administración los funcionarios del centro de cómputo. Las guías aprobadas de configuración deben ser establecidas y mantenidas por los mismos funcionarios, basados en las necesidades de SNR. Se debe establecer una guía para cualquier cambio de configuración, la cual debe ser revisada y aprobada por el Coordinador del Centro de Cómputo.

b. Los servidores deben ser registrados con la siguiente información para poder tener un control:
   - Localización
   - Hardware y versión del sistema operativo
   - Función principal y aplicaciones instaladas

   Esta información debe mantenerse al día.

c. Los cambios en la configuración para los servidores en producción de SNR deben seguir los procedimientos apropiados.

d. La configuración del sistema operativo de los servidores de SNR deben estar de acuerdo con la guías suministradas por el fabricante.

e. Los servicios y aplicaciones que no estén siendo usados deben ser deshabilitados.

f. El acceso a los servicios deben ser protegidos por medio de métodos de controles de acceso.

g. Los más recientes parches de seguridad deben ser instalados en los servidores tan pronto como sea posible, la única excepción cuando la aplicación inmediata de dichos parches interfieran con los requerimientos operativos de SNR.

h. No se debe utilizar el usuario ROOT para acceder los servidores de SNR, se debe utilizar una cuenta que tenga menos privilegios.

i. Los servidores de SNR deben estar físicamente localizados en un ambiente controlado de acceso.

j. Los servidores de SNR no deben ser operados desde áreas que estén fuera del centro de cómputo.

k. Todos los eventos sobre los servidores de SNR que manejen información crítica deben ser auditados.

l. Todos los eventos relacionados con la seguridad deben ser reportados y revisados (revisión de logs) por el responsable de la seguridad o por los funcionarios del centro de cómputo. Estos incluyen: el escaneo de puertos, evidencia de acceso no autorizado a cuentas privilegiadas y ocurrencia de sucesos anormales que no estén relacionados con aplicaciones específicas ubicadas en los servidores de SNR.

m. Se deben efectuar auditarías sobre el funcionamiento y operación de los servidores de SNR, para prevenir fallas en la operación normal de la entidad o interrupciones en el servicio.

n. Todos los servidores de SNR deben tener una aplicación anti-virus que ofrezca en tiempo real protección a los archivos y aplicaciones que estén corriendo sobre el sistema.

POLÍTICA 6: SEGURIDAD EN LOS MEDIOS REMOVIBLES O EXTRAIBLES

Objetivo: Minimizar el riesgo de pérdida de información o exposición de información sensible mantenida por la SNR y reducir el riesgo de adquirir infecciones por malware sobre los computadores de propiedad de la entidad.
Alcance: Esta política cubre todos los computadores y servidores que están en operación en SNR y a todos los funcionarios que los utilicen.
Descripción : Los medios extraíbles son una fuente potencial de infecciones de malware y han sido directamente relacionados con la pérdida de información sensible en muchas entidades.

a. Los medios removibles deben ser utilizados por los funcionarios únicamente en los computadores asignados para el desempeño de su trabajo y dentro de las instalaciones de SNR. Si por algún motivo se utilizan dichos medios en otro lugar deben ser revisados por el sistema antivirus antes de ser usados en la SNR.

b. La información sensible de SNR debe ser almacenada en medios removibles únicamente cuando es una función impresindible en el desempeño de la labores de un funcionario.

c. Cuando se almacene información sensible de SNR en un medio removible, esta debe ser encriptada.

d. Si un usuario sospecha que hay infección, por virus en su computador, debe informar inmediatamente al Centro de Computo, desconectarlo físicamente de la red y no utilizarlo hasta que sea revisado por el funcionario encargado de la seguridad o el delegado para tal efecto.

DEFINICIONES:

Medio removible: Dispositivo o medio que puede ser de lectura y /o escritura y el cual el usuario puede mover desde un computador a otro sin modificación del computador. Entre éstos se incluyen dispositivos de memorias flash para cámaras, reproductores de MP3 y PDAs; discos duros removibles, discos ópticos como CD y DVD, diskettes y cualquier disco comercial y de software no suministrado por la SNR.

Encripción: Procedimiento para convertir datos desde su forma original a un formato que no puede ser leído y/o usado por cualquiera sin la utilización de herramientas necesarias para efectuar la reversión del proceso de encripción.

Información Sensible: Datos que por alguna causa podrían estar disponibles a personas no autorizadas, pueden causar efectos adversos tanto a los programas como a los usuarios que los utilizan. Por ejemplo, una persona no autorizada obtiene acceso a la información financiera de la entidad.

Malware: Software malicioso que causa un gran impacto como virus, gusanos y Spyware, que pueden dañar el computador de un usuario.

Spyware: Son programas espías que se instalan sin el consentimiento del usuario, con el objetivo de recopilar información y enviarla a empresas publicitarias o a personas inescrupulosas para tratar de realizar algún fraude de tipo electrónico. Pueden recolectar información acerca de páginas que visita el usuario y con qué frecuencia, qué software tiene instalado, información de tarjetas de crédito y cuentas bancarias.

Gusanos: Este tipo de programas son similares a los virus, pero tiene la capacidad de difundirse sin la ayuda de un usuario. Por su efecto de replicación un computador puede enviar miles de copias del mismo.

POLÍTICA 7: SEGURIDAD EN LOS ROUTERS Y SWITCHES

Objetivo: Establecer los requerimientos mínimos de seguridad en la configuración de todos los routers y switches conectados a la red de SNR.
Alcance: Todos los routers y switches conectados a la SNR que estén en producción.
Descripción : Todos los routers y switches que pertenezcan y estén operando en la red de SNR deben ser debidamente administrados y controlados para su normal funcionamiento.

a. Los Router deben poseer un sistema de autenticación para su administración y configuración. La administración de este tipo de dispositivos será exclusiva de la Oficina de Informática de la entidad.

b. La habilitación del password en el router debe mantenerse en forma encriptada.

c. Se debe deshabilitar: el envío de broadcasts a direcciones IP y el ingreso de paquetes al router con direcciones invalidas.

d. Las reglas de acceso serán adicionadas de acuerdo a las necesidades de SNR.

e. Cada router debe tener la siguiente leyenda colocada en un lugar visible: "EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTÀ PROHIBIDO". Únicamente los funcionarios del centro de cómputo de SNR están autorizados para acceder y administrar dichos dispositivos.

f. El protocolo telnet nunca debe ser usado a través de la red para administrar un router si no existe un canal seguro protegiendo la comunicación.

DEFINICIONES:

Router: Dispositivo de hardware que permite el enrutamiento de paquetes entre diferentes redes. Igualmente permite determinar la ruta adecuada que deben tomar los paquetes de datos transmitidos.

Switch: Dispositivo de hardware que permite interconectar dos o más segmentos de red, transmiten datos de un segmento a otro de la misma red.

POLÍTICA 8: SEGURIDAD EN LAS COMUNICACIONES WIRELESS (INALAMBRICAS)

Objetivo: Asegurar y proteger la información de SNR teniendo en cuenta que este tipo de comunicaciones son inseguras ya que su medio de transporte es el aire.
Alcance: Todos los funcionarios, contratistas, proveedores que posean un dispositivo o utilicen un dispositivo gíreles para comunicarse con la red de SNR.
Descripción: Esta política especifica las condiciones que los dispositivos de la infraestructura wireless (inalámbrica) deben cumplir para conectarse a la red de SNR. Únicamente los dispositivos que cumplan con los estándares especificados en

esta política serán autorizados para conectarse a la red de SNR.

a. Todos los dispositivos que soporten la infraestructura wireless dentro de SNR y que estén conectados a la red, o suministren acceso a información confidencial o restringida deben cumplir:

   - Ser administrados y mantenidos por un equipo de soporte del centro de cómputo de SNR.
   - Utilizar un sistema de autenticación aprobado por el centro de computo de SNR
   - Utilizar un sistema de encripción aprobado por el centro de cómputo de SNR.
   - No interferir con otros accesos wireless mantenidos por otras entidades u organizaciones.

b. Se deben cumplir los estándares existentes para las comunicaciones wireless que serán aprobados por el centro de cómputo de SNR.

DEFINICIONES:

Wireless: Sistema de comunicaciones que transmite y recibe datos utilizando las ondas electromagnéticas, en lugar de cables como el coaxial, la fibra óptica utilizados en las redes de área local convencionales.

POLÍTICA 9: SEGURIDAD EN LA INFORMACION SENSIBLE

Objetivo: **Ayudar** a los funcionarios de SNR a determinar que información puede ser publica, así como determinar que información puede salir de la entidad sin una autorización.
Alcance: Todos los funcionarios que manejen información de la entidad.
Descripción : Esta política especifica que la información se puede dividir en dos clases pública y confidencial.

a. Todo funcionario que utilice recursos informáticos en la SNR tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que esté a su cargo, especialmente si tal información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

b. La información de SNR de acuerdo a su contenido se clasificará así:

   - Confidencial: Solamente tendrán acceso un grupo restringido de funcionarios. Ningún documento e información de este tipo puede ser compartido con otro funcionario o tercero que no se encuentre explícitamente autorizado.
   - Propietario: Puede ser de libre circulación dentro de la entidad siendo limitado el envío de esta información a terceros que no se encuentren debidamente autorizados. La información o documentos que no se identifiquen explícitamente se clasificarán como propietarios.

- Libre Distribución: Información de libre circulación y que puede ser enviada a cualquier destinatario. Todo documento que se encuentre en esta clasificación debe indicarlo de manera explícita, estipulando el departamento o funcionario responsable de la liberación del documento.

c. El funcionario que detecte un mal uso de la información está en la obligación de reportar este hecho al grupo de control disciplinario.

d. La información de políticas, normas y procedimientos de seguridad se deben dar a conocer únicamente a los funcionarios y entidades externas que lo requieran, de acuerdo con su competencia y las actividades que vayan a desarrollar.

DEFINICIONES:

Integridad: Hace referencia a que la información no sea modificada por personas no autorizadas.

Confidencialidad: Se refiere a que la información solo puede ser conocida por los usuarios autorizados para tal fin.

Disponibilidad: Hace referencia a que la información esté disponible para el usuario que la requiera, que pueda ser recuperada en el momento en que se necesite.

Confiabilidad: Se refiere a que la información que se genere para un usuario sea verídica y exacta.

POLÍTICA 10: SEGURIDAD EN EL SOFTWARE UTILIZADO

Objetivo: Dar cumplimiento a la ley de derechos de autor en cuanto a la utilización de software legal debidamente licenciado. Minimizar los riesgos de perdida de funcionalidad de los programas de propiedad de SNR, la exposición de la información sensible que se encuentra dentro de la red de cómputo de SNR, el riesgo de introducción de malware, y los riesgos legales por utilización de software no licenciado.
Alcance: Todos los funcionarios que utilicen software en sus computadores asignados para sus labores. Igualmente para todos los computadores, servidores, y demás dispositivos de cómputo que operen dentro de SNR.
Descripción: Esta política define las normas del buen uso de los programas de computador que utilicen todos los funcionarios usuarios de sistemas de cómputo. Permitir que los funcionarios no autorizados instalen software en los dispositivos de cómputo de la entidad genera la posibilidad de una exposición innecesaria de la información de SNR. Igualmente se pueden presentar conflictos en las versiones de los programas, los no autorizados pueden ocasionar que la red de la entidad sea atacada por hackers.

a. El software que utilice la SNR deberá ser adquirido cumpliendo las normas vigentes en cuanto a derechos de autor y siguiendo los procedimientos que la entidad tenga para tal efecto.

b. Está prohibido a los funcionarios de SNR utilizar software que no tenga la respectiva licencia de uso.

c. Deberá existir un inventario de licencias para el software instalado con el objetivo de permitir su fácil administración y evitar sanciones de los Órganos de Control por instalarlo sin el respectivo licenciamiento.

d. Todo cambio al software de propiedad de SNR (creación y modificación de programas, pantallas y reportes) debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes éstos formalmente deleguen.

e. Todo cambio relacionado con el mantenimiento de software debe realizarse de tal forma que no disminuya la seguridad existente y debe quedar formalmente documentado desde su solicitud hasta su implantación.

f. Ningún cambio al software de propiedad de la entidad puede ser aprobado, realizado e implantado por la misma persona o área.

g. Está prohibido que los funcionarios instalen software sobre cualquier equipo de cómputo que este dentro de la red de SNR, la instalación de software únicamente la deben efectuar las personas autorizadas que pertenezcan a la oficina de informática de la entidad.

h. Los requerimientos de software deben ser primero aprobados por la oficina de Informática de la entidad.

i. El centro de cómputo de la entidad será el único autorizado para obtener las licencias correspondientes para la instalación de nuevo software.

j. La oficina de informática es la única autorizada para efectuar pruebas de nuevo software con el fin de evitar conflictos de versiones e incompatibilidades en la instalación.

DEFINICIONES:

Hacker: Persona con grandes conocimientos de informática y telecomunicaciones que utiliza dichos conocimientos para actividades por lo general ilegales. La acción de usar dichos conocimientos se llama hacking o hackeo.

POLÍTICA 11: PLANES DE CONTINGENCIA Y BACKUP

Objetivo: Establecer un plan que permita el funcionamiento normal de SNR en caso de un hecho fortuito o calamidad natural.
Alcance: Todos los funcionarios y equipos de computo utilizados por la SNR

Descripción : Los planes de contingencia para dar un servicio ininterrumpido en todas las áreas que utilicen recursos informáticos.

a. La SNR de acuerdo con la oficina de informática debe establecer un plan de contingencia para asegurar el normal funcionamiento de todos los sistemas de cómputo y comunicaciones en caso de de un evento natural como terremoto, inundación, etc. o para casos de explosión, terrorismo, vandalismo, etc.

b. El plan de contingencia debe ser probado antes de que ocurra algún caso fortuito o de fuerza mayor que obligue la suspensión de los servicios informáticos prestados por la SNR.

c. La frecuencia de la realización de los backups dependerá de la criticidad de los sistemas y la cantidad de información que estos procesan, y se procederá de acuerdo con las normas establecidas por el centro de cómputo de la entidad.

d. Todos los backups de las bases de datos de SNR o de los sistemas operativos deben ser almacenados en medios magnéticos, los cuales deben ser entregados al coordinador del centro de cómputo para su respectivo almacenamiento y custodia.

POLÍTICA 12: ADQUISICION Y ADMINISTRACION DE HARDWARE

Objetivo: Establecer responsabilidades en cuanto a la adquisición de equipos de hardware para la SNR, y definir los requerimientos mínimos de seguridad para asegurar su adquisición.
Alcance: Esta política aplica a los proveedores de todos los computadores, redes, switches y en general que suministren Hardware a la SNR.
Descripción: La adquisición confiable de hardware permite asegurar que lo que se está adquiriendo no representa un riesgo para la red de SNR, sus sistemas internos y/o su información confidencial.

a. Todo tipo de hardware que sea adquirido por la SNR deberá cumplir con las respectivas garantías de funcionamiento y calidad que el fabricante se compromete a cumplir a cabalidad.

b. Todos los computadores y servidores requieren que la SNR por intermedio de la Oficina de Informática suministren una protección antivirus y antispam a dichos equipos antes de ser conectados a la red.

c. Todos los servidores en producción que no puedan ser reemplazados deberán ser auditados por el centro de cómputo de SNR para garantizar su normal funcionamiento o su repotenciaciòn.

d. Cualquier cambio a los equipos de cómputo de SNR como cambios de memoria, disco duro, procesador, etc., deberá tener previamente una revisión técnica y una autorización por parte del área de informática.

e. La reparación técnica de los equipos de cómputo, que implique la apertura de los mismos, únicamente deberá ser realizada por el personal de la oficina de informática autorizado.

f. Los equipos de computadores (PC, servidores, redes, switches, etc.,) no deben moverse o reubicarse sin la respectiva autorización previa.

g. La asignación de clave para el SETUP de los computadores únicamente la debe efectuar los funcionarios de la Oficina de Informática.

2. POLITICAS DE SEGURIDAD FISICA

POLÍTICA 1: SEGURIDAD EN LOS CENTROS DE CÓMPUTO

Objetivo: Prevenir accesos no autorizados a áreas restringidas
Alcance: Todos los funcionarios de SNR y visitantes de la entidad
***Descripción*:** Los centros de cómputo de SNR deben contar con ciertos requisitos mínimos para su acceso físico de los funcionarios autorizados.

a. Los centros de cómputo deben ser lugares de acceso restringido y cualquier funcionario o persona externa que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañado permanentemente de quien lo atenderá en el centro de cómputo.

b. En los centros de cómputo y demás áreas que la SNR considere deberán existir elementos de control de incendio, aire acondicionado, inundación y alarmas.

c. Los centros de cómputo y áreas que la SNR considere deberán estar demarcadas con zonas de circulación y zonas restringidas.

d. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitaciones y controles de acceso por medio de puertas y tarjetas inteligentes.

e. Todos los computadores portátiles, módems y equipos en general se deben registrar en la recepción de SNR tanto a su ingreso como a su salida, y no deben ser retirados sin que tengan la respectiva autorización de la Oficina de Informática.

f. Los centros de cómputo deben ser lugares de acceso restringido y cualquier funcionario o persona externa que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente de la persona que lo atenderá.

g. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitaciones y controles de acceso por medio de puertas y tarjetas inteligentes.

h. El centro de cómputo de la SNR deberá contar con pisos falsos para evitar riesgos de cortos circuitos o exceso de cables fluctuando a la vista.

i. El centro de cómputo debe contar con una fuente de corriente ininterrumpida UPS para posibles caídas de luz o fluctuaciones de corriente y así evitar posibles daños en los sistemas de Bases de Datos o en los sistemas operativos y aplicaciones.

POLÍTICA 2: SEGURIDAD EN LAS DEMAS AREAS DE LA ENTIDAD

Objetivo: Prevenir accesos no autorizados a áreas restringidas
Alcance: Todos los funcionarios de SNR y visitantes de la entidad
***Descripción*:** Para tener un control de visitantes a la entidad se deben suministrar todos los mecanismos necesarios para tal fin.

a. La SNR deberá contar con mecanismos de acceso como puertas de seguridad, sistemas de tarjeta inteligentes, alarmas y circuito cerrado de televisión en las áreas que se consideren demasiado críticas.

b. Los visitantes de las oficinas de SNR deberán ser escoltados en lo posible durante todo el tiempo que permanezcan en la entidad por un funcionario de la misma.

c. Cuando un funcionario se percate de que un visitante no escoltado se encuentra en áreas restringidas deberá informar dicha anormalidad a los responsables de la seguridad del edificio de SNR.

d. Toda persona que se encuentre dentro del edificio de SNR deberá portar su identificación en un lugar visible.

e. Todos los visitantes deberán mostrar su identificación con fotografía y firmar antes de tener acceso a las áreas restringidas y controladas por la SNR.

f. Todos los funcionarios de SNR se comprometen a NO utilizar la red regulada para conectar equipos eléctricos diferentes a su computador como cargadores de celulares, grabadoras, electrodomésticos y en general cualquier equipo que genere caídas de energía.

g. Las personas particulares en general, entre ellos los familiares de los funcionarios de SNR, NO están autorizados para utilizar los recursos informáticos de la entidad.

CUMPLIMIENTO:

Cualquier violación a cualquiera de las anteriores políticas podrá generar un llamado de atención con copia a la hoja de vida o un proceso disciplinario, según la actuación del funcionario.

Corresponderá a la Oficina de Informática dar a conocer al superior inmediato el incumplimiento de las políticas de seguridad de la información para que proceda de acuerdo con la gravedad de los hechos.

Las sanciones pueden ser desde una recomendación técnica, llamada de atención o una comunicación a la oficina de Control Interno Disciplinario.

APROBADO,

LIDA BEATRIZ SALAZAR MORENO
SUPERINTENDENTE DE NOTARIADO Y REGISTRO

Proyectó: Víctor Chitiva Acosta
Profesional Especializado-Centro de Computo

Revisó: Mario Perdomo Devia
Coordinador Centro De Cómputo

VoBo: William Fernando Albarracin Barreto
Jefe Oficina Informática

ANEXO B
(Circular No. 230 de 2009 - Superintendencia de Notariado y Registro))

Libertad y Orden

Superintendencia de Notariado y Registro
Ministerio del Interior y de Justicia
República de Colombia

CIRCULAR Nº 230

PARA: Directivos, Registradores de Instrumentos Públicos, Coordinadores de Grupo y Funcionarios

DE: Superintendente de Notariado y Registro

Fecha: 6 de octubre de 2009

ASUNTO: Políticas de Seguridad en los Sistemas de Información

Reciban un atento saludo:

Teniendo en cuenta que la Superintendencia de Notariado y Registro está llevando a cabo el proceso de modernización de la plataforma tecnológica que apoya los procesos misionales y administrativos, dentro de los cuales se contempla la integración y consolidación de la información registral, al interior y exterior de la entidad, así como los servicios de internet y correo electrónico, se hace necesario garantizar la seguridad de la información, proteger la red de contenidos no deseado de internet, reducción de los riesgos que representan amenazas a la información, a la seguridad y a la productividad de los sistemas de la Entidad.

Por lo anterior, y complementando las políticas de seguridad en los sistemas de información de la SNR reglamentadas mediante la circular No 77 de mayo 30 de 2008, se emiten las siguientes disposiciones:

1. Garantizar el correcto funcionamiento de los equipos de computo, deshabilitando de los equipos de cómputo los puertos USB, que permiten el uso de las memorias las cuales se han identificado como focos de alta contaminación de virus, malware y gusanos entre otros, que dañan la configuración de los equipos y los perfiles de usuario. Por lo anterior, se recomienda que para realizar la transferencia de archivos y documentos entre usuarios y oficinas se utilice el correo electrónico institucional, en las Oficinas o grupos donde se requieran la transferencia de archivos que no lo permita el correo electrónico, se haga uso de carpetas compartidas en uno de los equipos del grupo de trabajo.

2. Minimizar el tráfico de la red de datos de la SNR, de servicios que no cumplen funciones netamente institucionales, para lo cual se controlará el acceso a las páginas de internet no autorizando para fines institucionales.

3. Se limitará el acceso a los servicios de Messenger, de las descargas de música, videos y el acceso a emisoras de radio.

Las anteriores políticas serán implementadas por la Oficina de Informática de la Superintendencia de Notariado y Registro.

Cordialmente,

ORLANDO GARCIA-HERREROS SALCEDO
Superintendente de Notariado y Registro

Proyectó: Mario Perdomo Devia
Profesional Universitario-Centro de Computo

Revisó: Antonio Peña Fajardo
Coordinador centro de Computo

Aprobó: William Albarracín
Jefe Oficina Informática

Superintendencia de Notariado y Registro
La guarda de la fe pública
Calle 26 No.13-49 Interior 201 Bogotá, D.C. Tel. 3282121

ANEXO C
(Comunicado 003 de 2010 - Superintendencia de Notariado y Registro)

Ministerio del Interior y de Justicia
República de Colombia

Libertad y Orden

BICENTENARIO
1810-2010

COMUNICADO No. 003

Bogotá, D.C., Octubre 11 de 2010.

Señores:
REGISTRADORES DE INSTRUMENTOS PÚBLICOS
Superintendencia de Notariado y Registro
E. S. D.

ASUNTO: Servicio de Internet.

Respetados señores Registradores.

La Superintendencia a través del contrato interadministrativo 217 de 2009, adquirió un equipo de seguridad perimetral con funcionalidad de filtrados de contenido, el cual controla el servicio de ingreso a las diferentes páginas de Internet.

La Oficina de Informática, con el fin de mejorar los servicios que sobre las redes de la Entidad operan y para optimizar la administración y el control de uso de servicios de Internet, solicita de la manera atenta y respetuosa, la información descrita continuación, donde se reporta a los funcionarios autorizados actualmente para utilizar el servicio mencionado, la cual deberá remitirse al correo enrique.quintero@supernotariado.gov.co.

Funcionario	Cargo	Nombre de Equipo	Dirección IP	Permitir S/N
Ricardo Jorge	Profesional Universitario 2044-10	SONSESTO9	10.10.40.26	N

Reciban un cordial Saludo,

WILLIAM FERNANDO ALBARRACIN BARRETO
Jefe Oficina Informática
Superintendencia de Not[illegible]