

**DISEÑO DEL PLAN DIRECTOR DE CIBERSEGURIDAD PARA LAS
APLICACIONES EXPUESTAS EN INTERNET POR EL BANCO AGRARIO
DE COLOMBIA BASADO EN LA NORMA ISO/IEC 27032:2012**

**JOHANNA CAROLINA GONZÁLEZ REYES
JUAN RICARDO MÉNDEZ ROZO**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021**

**DISEÑO DEL PLAN DIRECTOR DE CIBERSEGURIDAD PARA LAS
APLICACIONES EXPUESTAS EN INTERNET POR EL BANCO AGRARIO
DE COLOMBIA BASADO EN LA NORMA ISO/IEC 27032:2012**

**JOHANNA CAROLINA GONZÁLEZ REYES
JUAN RICARDO MÉNDEZ ROZO**

**Trabajo de grado para optar por el título de
Especialista en Seguridad Informática**

**Director
Álvaro Escobar Escobar**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021**

Nota de aceptación

Presidente del jurado

Firma del jurado

Firma del jurado

Bogotá D.C. septiembre de 2021

AGRADECIMIENTOS

Agradecemos al Ingeniero Álvaro Escobar Escobar, director de nuestro trabajo de grado y director del programa, quien nos orientó y guio en la elaboración de este documento. A nuestros padres y familiares, quienes estuvieron pendientes de nuestro proceso, brindándonos su apoyo incondicional durante esta etapa. Al Banco Agrario de Colombia por permitirnos desarrollar nuestro trabajo de grado en su entorno y facilitarnos la información necesaria para llevarlo a cabo.

CONTENIDO

	pág.
GLOSARIO	18
INTRODUCCIÓN	20
1. PROBLEMA DE INVESTIGACIÓN	21
1.1 FORMULACIÓN DEL PROBLEMA	21
1.2 PLANTEAMIENTO DEL PROBLEMA	21
2. JUSTIFICACIÓN	22
3. OBJETIVOS	23
3.1 OBJETIVO GENERAL	23
3.2 OBJETIVOS ESPECÍFICOS	23
4. MARCO TEÓRICO	24
4.1 PLAN DIRECTOR DE SEGURIDAD	24
4.2 CIBERSEGURIDAD	25
4.3 ESTANDAR ISO/IEC 27032:2012	26
4.4 GESTIÓN DEL RIESGO NTC- ISO31000:2018	28
5. MARCO CONTEXTUAL	31
5.1 CREACIÓN Y OBJETO SOCIAL BANCO AGRARIO DE COLOMBIA	31
5.2 MISIÓN	31
5.3 VISIÓN	32
5.4 VALORES CORPORATIVOS	32
5.5 ORGANIGRAMA	32
5.6 PROCESOS Y PROCEDIMIENTOS	33
5.6.1 Procesos Estratégicos	34
5.6.2 Procesos Misionales	34
5.6.3 Procesos de Apoyo	35
5.6.4 Procesos de Evaluación y Control	36
5.7 GESTIÓN DE RIESGOS	36
5.8 SGSI	37
5.9 PARTES INTERESADAS	38
5.9.1 Proveedores	38
5.9.2 Clientes	39
5.10 INFRAESTRUCTURA EXPUESTA EN INTERNET	39
5.10.1 Plataformas Core	39
5.10.2 Plataformas no Core	40
5.10.3 Seguridad Perimetral	42
5.10.4 Ciberseguridad	42

5.10.5	Movilidad	43
6.	METODOLOGÍA PARA LA EVALUACIÓN DEL RIESGO DE CIBERSEGURIDAD	44
6.1	CONTEXTUALIZACIÓN E IDENTIFICACIÓN DE RIESGOS	44
6.2	MEDICIÓN DEL RIESGO	44
6.2.1	Niveles para Probabilidad	45
6.2.2	Niveles para Impacto	45
6.2.3	Cálculo del riesgo	46
6.2.4	Calificación de los riesgos	47
6.3	CONTROL DEL RIESGO	49
6.4	ETAPA DE MONITOREO	49
7.	ANÁLISIS DE RIESGOS A LAS APLICACIONES QUE SE ENCUENTRAN EXPUESTAS EN INTERNET	50
7.1	ANÁLISIS DE RIESGOS – CIBERSEGURIDAD	50
7.1.1	Forcepoint DLP.	50
7.1.2	Interpretación de los resultados del análisis de riesgos – Ciberseguridad	52
7.2	ANÁLISIS DE RIESGOS – MOVILIDAD	52
7.2.1	Almacenamiento Sharefile	52
7.2.2	Citrix Movilidad Teletrabajo	55
7.2.3	Citrix Movilidad XenMobile	57
7.2.4	Citrix Movilidad Apps	59
7.2.5	VPN Movilidad	61
7.2.6	Interpretación de los resultados del análisis de riesgos – Movilidad	63
7.3	ANALISIS DE RIESGOS – PLATAFORMAS CORE	63
7.3.1	En Línea ACH PSE	63
7.3.2	Gestión Cobranza (ICS)	65
7.3.3	Aula Financiera	67
7.3.4	Interpretación de los resultados del análisis de riesgos – Plataformas Core	69
7.4	ANÁLISIS DE RIESGOS – PLATAFORMAS NO CORE	69
7.4.1	Correo Electrónico Banco Agrario	70
7.4.2	Depósitos Judiciales	72
7.4.3	Portal Web Banco Agrario	74
7.4.4	Banca Virtual Banco Agrario	76
7.4.5	ADFS	78
7.4.6	Conéctate al Conocimiento	80
7.4.7	Portal Tu Referido	82
7.4.8	Portal Vivienda	84
7.4.9	Portal Clientes	86
7.4.10	Ingreso Solidario	88
7.4.11	Consulta Giros	90
7.4.12	Portal PAEF	92

7.4.13	Interpretación de los resultados del análisis de riesgos – Plataformas No Core	94
7.5	ANÁLISIS DE RIESGOS – SEGURIDAD PERIMETRAL	94
7.5.1	Tráfico In - Acceso Remoto Checkpoint	95
7.5.2	Tráfico Out – Navegación sin Proxy	97
7.5.3	VPN SSL DG	99
7.5.4	Consola Antivirus	101
7.5.5	VPN SSL NAOS	103
7.5.6	Interpretación de los resultados del análisis de riesgos – Seguridad Perimetral	105
8.	TRATAMIENTO DE LOS RIESGOS DE CIBERSEGURIDAD	106
8.1	CONTROLES IMPLEMENTADOS	106
8.2	CÁLCULO DE RIESGO RESIDUAL	107
8.2.1	Forcepoint DLP	107
8.2.2	Almacenamiento Sharefile	109
8.2.3	Citrix Movilidad Teletrabajo	111
8.2.4	Citrix Movilidad XenMobile	113
8.2.5	Citrix Movilidad Apps	115
8.2.6	VPN Movilidad	117
8.2.7	En Línea ACH PSE	119
8.2.8	Gestión Cobranza (ICS)	121
8.2.9	Aula Financiera	123
8.2.10	Correo Electrónico Banco Agrario	125
8.2.11	Depósitos Judiciales	127
8.2.12	Portal Web Banco Agrario	129
8.2.13	Banca Virtual Banco Agrario	131
8.2.14	ADFS	133
8.2.15	Conéctate al Conocimiento	135
8.2.16	Portal Tu Referido	137
8.2.17	Portal Vivienda	139
8.2.18	Portal Cliente	141
8.2.19	Ingreso Solidario	143
8.2.20	Consulta Giros	145
8.2.21	Portal PAEF	147
8.2.22	Tráfico In - Acceso Remoto Checkpoint	149
8.2.23	Tráfico Out – Navegación sin Proxy	151
8.2.24	VPN SSL DG	152
8.2.25	Consola Antivirus	154
8.2.26	VPN SSL NAOS	156
8.2.27	Interpretación de los resultados del tratamiento de riesgos	158
8.3	AMENAZAS A APLICACIONES DEL BANCO AGRARIO DE COLOMBIA	159
8.3.1	Mecanismos de Ataque	159
8.4	ROLES DE LAS PARTES INTERESADAS	160
8.4.1	Roles de los clientes	160

8.4.2	Roles de los proveedores	161
8.5	CONTROLES PROPUESTOS	162
8.5.1	Controles de nivel de aplicación	162
8.5.2	Protección de servidores	163
8.5.3	Controles de usuario final	163
8.5.4	Controles frente a ataques de ingeniería social	164
8.5.5	Preparación para la ciberseguridad	165
9.	LINEAMIENTOS PARA EL INTERCAMBIO DE LA INFORMACIÓN ENTRE LAS PARTES INTERESADAS.	167
9.1	POLÍTICAS	167
9.2	MÉTODOS Y PROCESOS	168
9.3	FUENTES Y ORGANIZACIONES	169
9.4	TÉCNICOS	170
10.	CONCLUSIONES	171
11.	RECOMENDACIONES	172
	BIBLIOGRAFÍA	173

LISTA DE FIGURAS

	pág.
Figura 1. Implementando un plan director de seguridad	24
Figura 2. Gestión de la ciberseguridad	26
Figura 3. Proceso de gestión de riesgos según ISO 31000	29
Figura 4. Organigrama	32
Figura 5. Gestión por procesos Banco Agrario de Colombia	33
Figura 6. Procesos estratégicos Banco Agrario de Colombia	34
Figura 7. Procesos Misionales Banco Agrario de Colombia	34
Figura 8. Procesos de Apoyo Banco Agrario de Colombia	35
Figura 9. Procesos de Evaluación y Control Banco Agrario de Colombia	36
Figura 10. Mapa de calor	47
Figura 11. Mapa de calor - Seguridad en aplicaciones - Forcepoint DLP	50
Figura 12. Mapa de calor - Seguridad en redes - Forcepoint DLP	51
Figura 13. Mapa de calor - Seguridad en aplicaciones - Almacenamiento Sharefile	53
Figura 14. Mapa de calor - Seguridad en redes - Almacenamiento Sharefile	53
Figura 15. Mapa de calor - Seguridad en internet - Almacenamiento Sharefile	54
Figura 16. Mapa de calor - Seguridad en aplicaciones - Citrix Movilidad Teletrabajo	55
Figura 17. Mapa de calor - Seguridad en redes - Citrix Movilidad Teletrabajo	56
Figura 18. Mapa de calor - Seguridad en internet - Citrix Movilidad Teletrabajo	56
Figura 19. Mapa de calor - Seguridad en aplicaciones - Citrix Movilidad XenMobile	57
Figura 20. Mapa de calor - Seguridad en redes - Citrix Movilidad XenMobile	58
Figura 21. Mapa de calor – Seguridad en internet - Citrix Movilidad XenMobile	58
Figura 22. Mapa de calor – Seguridad en aplicaciones - Citrix Movilidad Apps	59
Figura 23. Mapa de calor – Seguridad en redes - Citrix Movilidad Apps	60
Figura 24. Mapa de calor – Seguridad en internet - Citrix Movilidad Apps	60
Figura 25. Mapa de calor – Seguridad en aplicaciones – VPN Movilidad	61
Figura 26. Mapa de calor – Seguridad en redes – VPN Movilidad	62
Figura 27. Mapa de calor – Seguridad en internet – VPN Movilidad	62
Figura 28. Mapa de calor – Protección de infraestructura crítica – VPN Movilidad	63
Figura 29. Mapa de calor – Seguridad en aplicaciones – En Línea ACH PSE	64
Figura 30. Mapa de calor – Seguridad en redes – En Línea ACH PSE	64
Figura 31. Mapa de calor – Seguridad en internet – En Línea ACH PSE	65
Figura 32. Mapa de calor – Protección de infraestructura crítica – En Línea ACH PSE	65
Figura 33. Mapa de calor – Seguridad en aplicaciones – Gestión Cobranza (ICS)	66
Figura 34. Mapa de calor – Seguridad en redes – Gestión Cobranza (ICS)	66
Figura 35. Mapa de calor – Seguridad en internet – Gestión Cobranza (ICS)	67

Figura 36. Mapa de calor – Protección de infraestructura crítica – Gestión Cobranza (ICS)	67
Figura 37. Mapa de calor – Seguridad en aplicaciones – Aula Financiera	68
Figura 38. Mapa de calor – Seguridad en redes – Aula Financiera	68
Figura 39. Mapa de calor – Seguridad en internet – Aula Financiera	69
Figura 40. Mapa de calor – Seguridad en aplicaciones – Correo Electrónico	70
Figura 41. Mapa de calor – Seguridad en redes – Correo Electrónico	71
Figura 42. Mapa de calor – Seguridad en internet – Correo Electrónico	71
Figura 43. Mapa de calor – Protección de infraestructura crítica – Correo Electrónico	72
Figura 44. Mapa de calor – Seguridad en aplicaciones – Depósitos Judiciales	72
Figura 45. Mapa de calor – Seguridad en redes – Depósitos Judiciales	73
Figura 46. Mapa de calor – Seguridad en internet – Depósitos Judiciales	73
Figura 47. Mapa de calor – Protección de infraestructura crítica – Depósitos Judiciales	74
Figura 48. Mapa de calor – Seguridad en aplicaciones – Portal Web	75
Figura 49. Mapa de calor – Seguridad en redes – Portal Web	75
Figura 50. Mapa de calor – Seguridad en internet – Portal Web	76
Figura 51. Mapa de calor – Protección de infraestructura crítica – Portal Web	76
Figura 52. Mapa de calor – Seguridad en aplicaciones – Banca Virtual	77
Figura 53. Mapa de calor – Seguridad en redes – Banca Virtual	77
Figura 54. Mapa de calor – Seguridad en internet – Banca Virtual	78
Figura 55. Mapa de calor – Protección de infraestructura crítica – Banca Virtual	78
Figura 56. Mapa de calor – Seguridad en aplicaciones – ADFS	79
Figura 57. Mapa de calor – Seguridad en redes – ADFS	79
Figura 58. Mapa de calor – Seguridad en internet – ADFS	80
Figura 59. Mapa de calor – Protección de infraestructura crítica – ADFS	80
Figura 60. Mapa de calor – Seguridad en aplicaciones – Conéctate al Conocimiento	81
Figura 61. Mapa de calor – Seguridad en redes – Conéctate al Conocimiento	81
Figura 62. Mapa de calor – Seguridad en internet – Conéctate al Conocimiento	82
Figura 63. Mapa de calor – Seguridad en aplicaciones – Portal Tu Referido	83
Figura 64. Mapa de calor – Seguridad en redes – Portal Tu Referido	83
Figura 65. Mapa de calor – Seguridad en internet – Portal Tu Referido	84
Figura 66. Mapa de calor – Seguridad en aplicaciones – Portal Vivienda	85
Figura 67. Mapa de calor – Seguridad en redes – Portal Vivienda	85
Figura 68. Mapa de calor – Seguridad en internet – Portal Vivienda	86
Figura 69. Mapa de calor – Seguridad en aplicaciones – Portal Clientes	87
Figura 70. Mapa de calor – Seguridad en redes – Portal Clientes	87
Figura 71. Mapa de calor – Seguridad en internet – Portal Clientes	88
Figura 72. Mapa de calor – Seguridad en aplicaciones – Ingreso Solidario	89
Figura 73. Mapa de calor – Seguridad en redes – Ingreso Solidario	89
Figura 74. Mapa de calor – Seguridad en internet – Ingreso Solidario	90
Figura 75. Mapa de calor – Seguridad en aplicaciones – Consulta Giros	91
Figura 76. Mapa de calor – Seguridad en redes – Consulta Giros	91

Figura 77. Mapa de calor – Seguridad en internet – Consulta Giros	92
Figura 78. Mapa de calor – Seguridad en aplicaciones – Portal PAEF	93
Figura 79. Mapa de calor – Seguridad en redes – Portal PAEF	93
Figura 80. Mapa de calor – Seguridad en internet – Portal PAEF	94
Figura 81. Mapa de calor – Seguridad en aplicaciones – Acceso Remoto	95
Figura 82. Mapa de calor – Seguridad en redes – Acceso Remoto	96
Figura 83. Mapa de calor – Seguridad en internet – Acceso Remoto	96
Figura 84. Mapa de calor – Protección de infraestructura crítica – Acceso Remoto	97
Figura 85. Mapa de calor – Seguridad en redes – Navegación sin Proxy	98
Figura 86. Mapa de calor – Seguridad en aplicaciones – VPN SSL DG	99
Figura 87. Mapa de calor – Seguridad en redes – VPN SSL DG	100
Figura 88. Mapa de calor – Seguridad en internet – VPN SSL DG	100
Figura 89. Mapa de calor – Protección de infraestructura crítica – VPN SSL DG	101
Figura 90. Mapa de calor – Seguridad en aplicaciones – Consola Antivirus	101
Figura 91. Mapa de calor – Seguridad en redes – Consola Antivirus	102
Figura 92. Mapa de calor – Seguridad en aplicaciones – VPN SSL NAOS	103
Figura 93. Mapa de calor – Seguridad en redes – VPN SSL NAOS	104
Figura 94. Mapa de calor – Seguridad en internet – VPN SSL NAOS	105
Figura 95. Mapa de calor – Protección de infraestructura crítica – VPN SSL NAOS	105
Figura 96. Políticas compartir y coordinar información	168
Figura 97. Métodos y procesos para compartir y coordinar información.	169
Figura 98. Métodos y procesos para compartir y coordinar información	170
Figura 99. Lineamientos técnicos para compartir y coordinar información	170

LISTA DE CUADROS

	pág.
Cuadro 1. Infraestructura expuesta en internet por Plataformas Core	40
Cuadro 2. Infraestructura expuesta en internet por Plataformas no Core	40
Cuadro 3. Infraestructura expuesta en internet por Seguridad Perimetral	42
Cuadro 4. Infraestructura expuesta en internet por Ciberseguridad	42
Cuadro 5. Infraestructura expuesta en internet por Movilidad	43
Cuadro 6. Plantilla ejemplo análisis de riesgos	47
Cuadro 7. Seguridad en aplicaciones - Forcepoint DLP	50
Cuadro 8. Seguridad en redes - Forcepoint DLP	51
Cuadro 9. Seguridad en internet - Forcepoint DLP	51
Cuadro 10. Protección de infraestructura crítica - Forcepoint DLP	52
Cuadro 11. Seguridad en aplicaciones - Almacenamiento Sharefile	52
Cuadro 12. Seguridad en redes - Almacenamiento Sharefile	53
Cuadro 13. Seguridad en Internet - Almacenamiento Sharefile	54
Cuadro 14. Seguridad en Protección Infraestructura crítica - Almacenamiento Sharefile	54
Cuadro 15. Seguridad en aplicaciones - Citrix Movilidad Teletrabajo	55
Cuadro 16. Seguridad en redes - Citrix Movilidad Teletrabajo	55
Cuadro 17. Seguridad en internet - Citrix Movilidad Teletrabajo	56
Cuadro 18. Seguridad en Protección de infraestructura crítica - Citrix Movilidad XenMobile	56
Cuadro 19. Seguridad en aplicaciones - Citrix Movilidad XenMobile	57
Cuadro 20. Seguridad en redes - Citrix Movilidad XenMobile	57
Cuadro 21. Seguridad en internet - Citrix Movilidad XenMobile	58
Cuadro 22. Protección de infraestructura crítica - Citrix Movilidad XenMobile	58
Cuadro 23. Seguridad en aplicaciones - Citrix Movilidad Apps	59
Cuadro 24. Seguridad en redes - Citrix Movilidad Apps	59
Cuadro 25. Seguridad en internet - Citrix Movilidad Apps	60
Cuadro 26. Protección de infraestructura crítica - Citrix Movilidad Apps	60
Cuadro 27. Seguridad en aplicaciones – VPN Movilidad	61
Cuadro 28. Seguridad en redes – VPN Movilidad	61
Cuadro 29. Seguridad en internet – VPN Movilidad	62
Cuadro 30. Protección de infraestructura crítica – VPN Movilidad	62
Cuadro 31. Seguridad en aplicaciones – En Línea ACH PSE	63
Cuadro 32. Seguridad en redes – En Línea ACH PSE	64
Cuadro 33. Seguridad en redes – En Línea ACH PSE	64
Cuadro 34. Protección de infraestructura crítica – En Línea ACH PSE	65
Cuadro 35. Seguridad en aplicaciones – Gestión Cobranza (ICS)	65
Cuadro 36. Seguridad en redes – Gestión Cobranza (ICS)	66
Cuadro 37. Seguridad en internet – Gestión Cobranza (ICS)	66
Cuadro 38. Protección de infraestructura crítica – Gestión Cobranza (ICS)	67
Cuadro 39. Seguridad en aplicaciones – Aula Financiera	67

Cuadro 40. Seguridad en redes – Aula Financiera	68
Cuadro 41. Seguridad en internet – Aula Financiera	68
Cuadro 42. Protección de infraestructura crítica – Aula Financiera	69
Cuadro 43. Seguridad en aplicaciones – Correo Electrónico	70
Cuadro 44. Seguridad en redes – Correo Electrónico	70
Cuadro 45. Seguridad en internet – Correo Electrónico	71
Cuadro 46. Protección de infraestructura crítica – Correo Electrónico	71
Cuadro 47. Seguridad en aplicaciones – Depósitos Judiciales	72
Cuadro 48. Seguridad en redes – Depósitos Judiciales	73
Cuadro 49. Seguridad en internet – Depósitos Judiciales	73
Cuadro 50. Protección de infraestructura crítica – Depósitos Judiciales	74
Cuadro 51. Seguridad en aplicaciones – Portal Web	74
Cuadro 52. Seguridad en redes – Portal Web	75
Cuadro 53. Seguridad en internet – Portal Web	75
Cuadro 54. Protección de infraestructura crítica – Portal Web	76
Cuadro 55. Seguridad en aplicaciones – Banca Virtual	76
Cuadro 56. Seguridad en redes – Banca Virtual	77
Cuadro 57. Seguridad en internet – Banca Virtual	77
Cuadro 58. Protección de infraestructura crítica – Banca Virtual	78
Cuadro 59. Seguridad en aplicaciones – ADFS	78
Cuadro 60. Seguridad en redes – ADFS	79
Cuadro 61. Seguridad en internet – ADFS	79
Cuadro 62. Protección de infraestructura crítica – ADFS	80
Cuadro 63. Seguridad en aplicaciones – Conéctate al Conocimiento	80
Cuadro 64. Seguridad en aplicaciones – Conéctate al Conocimiento	81
Cuadro 65. Seguridad en internet – Conéctate al Conocimiento	81
Cuadro 66. Protección de infraestructura crítica – Conéctate al Conocimiento	82
Cuadro 67. Seguridad en aplicaciones – Portal Tu Referido	82
Cuadro 68. Seguridad en redes – Portal Tu Referido	83
Cuadro 69. Seguridad en internet – Portal Tu Referido	83
Cuadro 70. Protección de infraestructura crítica – Portal Tu Referido	84
Cuadro 71. Seguridad en aplicaciones – Portal Vivienda	84
Cuadro 72. Seguridad en redes – Portal Vivienda	85
Cuadro 73. Seguridad en internet – Portal Vivienda	85
Cuadro 74. Protección de infraestructura crítica – Portal Vivienda	86
Cuadro 75. Seguridad en aplicaciones – Portal Clientes	86
Cuadro 76. Seguridad en redes – Portal Clientes	87
Cuadro 77. Seguridad en internet – Portal Clientes	87
Cuadro 78. Protección de infraestructura crítica – Portal Clientes	88
Cuadro 79. Seguridad en aplicaciones – Ingreso Solidario	88
Cuadro 80. Seguridad en redes – Ingreso Solidario	89
Cuadro 81. Seguridad en internet – Ingreso Solidario	89
Cuadro 82. Protección de infraestructura crítica – Ingreso Solidario	90
Cuadro 83. Seguridad en aplicaciones – Consulta Giros	90
Cuadro 84. Seguridad en redes – Consulta Giros	91

Cuadro 85. Seguridad en internet – Consulta Giros	91
Cuadro 86. Protección de infraestructura crítica – Consulta Giros	92
Cuadro 87. Seguridad en aplicaciones – Portal PAEF	92
Cuadro 88. Seguridad en redes – Portal PAEF	93
Cuadro 89. Seguridad en internet – Portal PAEF	93
Cuadro 90. Protección de infraestructura crítica – Portal PAEF	94
Cuadro 91. Seguridad en aplicaciones – Acceso Remoto	95
Cuadro 92. Seguridad en redes – Acceso Remoto	95
Cuadro 93. Seguridad en internet – Acceso Remoto	96
Cuadro 94. Protección de infraestructura crítica – Acceso Remoto	96
Cuadro 95. Seguridad en aplicaciones – Navegación sin Proxy	97
Cuadro 96. Seguridad en redes – Navegación sin Proxy	97
Cuadro 97. Seguridad en internet – Navegación sin Proxy	98
Cuadro 98. Protección de infraestructura crítica – Navegación sin Proxy	98
Cuadro 99. Seguridad en aplicaciones – VPN SSL DG	99
Cuadro 100. Seguridad en redes – VPN SSL DG	99
Cuadro 101. Seguridad en internet – VPN SSL DG	100
Cuadro 102. Protección de infraestructura crítica – VPN SSL DG	100
Cuadro 103. Seguridad en aplicaciones – Consola Antivirus	101
Cuadro 104. Seguridad en redes – Consola Antivirus	102
Cuadro 105. Seguridad en internet – Consola Antivirus	102
Cuadro 106. Protección de infraestructura crítica – Consola Antivirus	103
Cuadro 107. Seguridad en aplicaciones – VPN SSL NAOS	103
Cuadro 108. Seguridad en redes – VPN SSL NAOS	104
Cuadro 109. Seguridad en internet – VPN SSL NAOS	104
Cuadro 110. Protección de infraestructura crítica – VPN SSL NAOS	105
Cuadro 111. Controles implementados por el Banco	106
Cuadro 112. Cálculo riesgo residual – Seguridad en aplicaciones Forcepoint DLP	107
Cuadro 113. Cálculo riesgo residual – Seguridad en aplicaciones Forcepoint DLP	108
Cuadro 114. Cálculo riesgo residual – Seguridad en aplicaciones Almacenamiento Sharefile	109
Cuadro 115. Cálculo riesgo residual – Seguridad en redes Almacenamiento Sharefile	110
Cuadro 116. Cálculo riesgo residual – Seguridad en internet Almacenamiento Sharefile	110
Cuadro 117. Cálculo riesgo residual – Seguridad en aplicaciones Citrix Movilidad Teletrabajo	111
Cuadro 118. Cálculo riesgo residual – Seguridad en redes Citrix Movilidad Teletrabajo	112
Cuadro 119. Cálculo riesgo residual – Seguridad en internet Almacenamiento Citrix Movilidad Teletrabajo	112
Cuadro 120. Cálculo riesgo residual – Seguridad en aplicaciones - Citrix Movilidad XenMobile	113

Cuadro 121. Cálculo riesgo residual – Seguridad en redes - Citrix Movilidad XenMobile	114
Cuadro 122. Cálculo riesgo residual – Seguridad en Internet - Citrix Movilidad XenMobile	114
Cuadro 123. Cálculo riesgo residual – Seguridad en aplicaciones - Citrix Movilidad Apps	115
Cuadro 124. Cálculo riesgo residual – Seguridad en redes - Citrix Movilidad Apps	116
Cuadro 125. Cálculo riesgo residual – Seguridad en internet - Citrix Movilidad Apps	116
Cuadro 126. Cálculo riesgo residual – Seguridad en aplicaciones - VPN Movilidad	117
Cuadro 127. Cálculo riesgo residual – Seguridad en redes - VPN Movilidad	118
Cuadro 128. Cálculo riesgo residual – Seguridad en interne - VPN Movilidad	118
Cuadro 129. Cálculo riesgo residual – Protección infraestructura crítica - VPN Movilidad	119
Cuadro 130. Cálculo riesgo residual – Seguridad en aplicaciones - En Línea ACH PSE	119
Cuadro 131. Cálculo riesgo residual – Seguridad en redes - En Línea ACH PSE	120
Cuadro 132. Cálculo riesgo residual – Seguridad en internet - En Línea ACH PSE	120
Cuadro 133. Cálculo riesgo residual – Protección infraestructura crítica - En Línea ACH PSE	121
Cuadro 134. Cálculo riesgo residual – Seguridad en aplicaciones - Gestión Cobranza (ICS)	121
Cuadro 135. Cálculo riesgo residual – Seguridad en redes - Gestión Cobranza (ICS)	122
Cuadro 136. Cálculo riesgo residual – Seguridad en internet - Gestión Cobranza (ICS)	122
Cuadro 137. Cálculo riesgo residual – Protección infraestructura crítica - Gestión Cobranza (ICS)	123
Cuadro 138. Cálculo riesgo residual – Seguridad en aplicaciones - Aula Financiera	123
Cuadro 139. Cálculo riesgo residual – Seguridad en redes - Aula Financiera	124
Cuadro 140. Cálculo riesgo residual – Seguridad en internet - Aula Financiera	124
Cuadro 141. Cálculo riesgo residual – Seguridad en aplicaciones - Correo Electrónico	125
Cuadro 142. Cálculo riesgo residual – Seguridad en redes - Correo Electrónico	126
Cuadro 143. Cálculo riesgo residual – Seguridad en internet - Correo Electrónico	126
Cuadro 144. Cálculo riesgo residual – Protección infraestructura crítica - Correo Electrónico	127
Cuadro 145. Cálculo riesgo residual – Seguridad en aplicaciones - Depósitos Judiciales	127

Cuadro 146. Cálculo riesgo residual – Seguridad en redes - Depósitos Judiciales	128
Cuadro 147. Cálculo riesgo residual – Seguridad en internet - Depósitos Judiciales	128
Cuadro 148. Cálculo riesgo residual – Protección infraestructura crítica - Depósitos Judiciales	129
Cuadro 149. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Web	129
Cuadro 150. Cálculo riesgo residual – Seguridad en redes - Portal Web	130
Cuadro 151. Cálculo riesgo residual – Seguridad en internet - Portal Web	130
Cuadro 152. Cálculo riesgo residual – Protección infraestructura crítica - Portal Web	131
Cuadro 153. Cálculo riesgo residual – Seguridad en aplicaciones - Banca Virtual	131
Cuadro 154. Cálculo riesgo residual – Seguridad en redes - Banca Virtual	132
Cuadro 155. Cálculo riesgo residual – Seguridad en internet - Banca Virtual	132
Cuadro 156. Cálculo riesgo residual – Protección infraestructura crítica - Banca Virtual	133
Cuadro 157. Cálculo riesgo residual – Protección infraestructura crítica - Banca Virtual	133
Cuadro 158. Cálculo riesgo residual – Seguridad en redes - ADFS	134
Cuadro 159. Cálculo riesgo residual – Seguridad en internet - ADFS	134
Cuadro 160. Cálculo riesgo residual – Protección infraestructura crítica - ADFS	135
Cuadro 161. Cálculo riesgo residual – Seguridad en aplicaciones - Conéctate al conocimiento	135
Cuadro 162. Cálculo riesgo residual – Seguridad en redes - Conéctate al conocimiento	136
Cuadro 163. Cálculo riesgo residual – Seguridad en internet - Conéctate al conocimiento	136
Cuadro 164. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Tu Referido	137
Cuadro 165. Cálculo riesgo residual – Seguridad en redes - Portal Tu Referido	138
Cuadro 166. Cálculo riesgo residual – Seguridad en internet - Portal Tu Referido	138
Cuadro 167. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Vivienda	139
Cuadro 168. Cálculo riesgo residual – Seguridad en redes - Portal Vivienda	140
Cuadro 169. Cálculo riesgo residual – Seguridad en internet - Portal Vivienda	140
Cuadro 170. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Cliente	141
Cuadro 171. Cálculo riesgo residual – Seguridad en redes - Portal Cliente	142
Cuadro 172. Cálculo riesgo residual – Seguridad en internet - Portal Cliente	142
Cuadro 173. Cálculo riesgo residual – Seguridad en aplicaciones - Ingreso Solidario	143
Cuadro 174. Cálculo riesgo residual – Seguridad en redes - Ingreso Solidario	144
Cuadro 175. Cálculo riesgo residual – Seguridad en internet - Ingreso Solidario	144

Cuadro 176. Cálculo riesgo residual – Seguridad en aplicaciones - Consulta Giros	145
Cuadro 177. Cálculo riesgo residual – Seguridad en redes - Consulta Giros	146
Cuadro 178. Cálculo riesgo residual – Seguridad en internet - Consulta Giros	146
Cuadro 179. Cálculo riesgo residual – Seguridad en aplicaciones - Portal PAEF	147
Cuadro 180. Cálculo riesgo residual – Seguridad en redes - Portal PAEF	148
Cuadro 181. Cálculo riesgo residual – Seguridad en internet - Portal PAEF	148
Cuadro 182. Cálculo riesgo residual – Seguridad en aplicaciones - Acceso Remoto	149
Cuadro 183. Cálculo riesgo residual – Seguridad en redes - Acceso Remoto	150
Cuadro 184. Cálculo riesgo residual – Seguridad en internet - Acceso Remoto	150
Cuadro 185. Cálculo riesgo residual – Protección infraestructura crítica - Acceso Remoto	151
Cuadro 186. Cálculo riesgo residual – Seguridad en redes - Navegación sin Proxy	151
Cuadro 187. Cálculo riesgo residual – Seguridad en aplicaciones - VPN SSL DG	152
Cuadro 188. Cálculo riesgo residual – Seguridad en redes - VPN SSL DG	153
Cuadro 189. Cálculo riesgo residual – Seguridad en internet - VPN SSL DG	153
Cuadro 190. Cálculo riesgo residual – Protección infraestructura crítica - VPN SSL DG	154
Cuadro 191. Cálculo riesgo residual – Seguridad en aplicaciones - Consola Antivirus	154
Cuadro 192. Cálculo riesgo residual – Seguridad en redes - Consola Antivirus	155
Cuadro 193. Cálculo riesgo residual – Seguridad en aplicaciones - VPN SSL NAOS	156
Cuadro 194. Cálculo riesgo residual – Seguridad en redes - VPN SSL NAOS	157
Cuadro 195. Cálculo riesgo residual – Seguridad en internet - VPN SSL NAOS	157
Cuadro 196. Cálculo riesgo residual – Protección infraestructura crítica - VPN SSL NAOS	158

GLOSARIO

ACTIVO: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.¹

AMENAZA: Causa potencial de un incidente no deseado, el cual puede resultar en el daño a un sistema, individuo u organización.²

BOTS: Programa de software automatizado empleado para realizar tareas específicas.

Nota 1: El término es a menudo usado para describir programas, usualmente ejecutados en un servidor, que automatizan tareas tales como reenvío y clasificación de correo.

Nota 2: Un bot también puede ser descrito como un programa que actúa como agente para un usuario o un programa que simula una actividad humana. En internet, los bots más ubicuos son programas que acceden sitios web y recopilan su contenido para indexadores de motores de búsqueda, también llamados spiders o crawlers.³

CIBERENTORNO: Esto incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes⁴.

HACKING: Acción de acceder intencionalmente al sistema de un equipo de cómputo sin la autorización del usuario o el propietario⁵.

IMPACTO: Cambio adverso en el nivel de los objetivos del negocio logrados.

INFRAESTRUCTURA CRÍTICA: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de

¹ DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad nacional [en línea]. [Consultado 10 de septiembre de 2020]. Disponible en <<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>>

² ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN – ISO. Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad. ISO / IEC 27032: 2012. 1 ed. Génova, Suiza ISO, 2012.

³ Ibid., p. 6.

⁴ UNIÓN INTERNACIONAL DE TELECOMUNICACIONES – UIT. Aspectos generales de la ciberseguridad [en línea]. [Consultado 30 de agosto de 2020]. Disponible en <https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-!!!PDF-E&type=items>

⁵ ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN – ISO. ISO / IEC 27032: 2012 Op. Cit., p. 7

los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.⁶

INTERESADOS: Quienes están afectados por el proyecto que se desarrolla, siendo de dos tipos: 1. usuarios: aquellos que utilizarán el sistema y 2. clientes: aquellos que requieren el sistema y son los responsables de su validación o aprobación.

INTERNET: Sistema global de redes interconectadas en el dominio público.⁷

MALWARE: Software diseñado con intención maliciosa e incluye características o capacidades que potencialmente pueden causar daño, directa o indirectamente, al usuario o sistema del equipo de cómputo del usuario.⁸

PROBABILIDAD: Posibilidad de que ocurra algo.

Nota: En la terminología de gestión de riesgos, la palabra "probabilidad" se utiliza para referirse a la posibilidad de que ocurra algo, ya sea definido, medido o determinado de manera objetiva o subjetiva, cualitativa o cuantitativa, y se describe usando términos generales o matemáticamente (como una probabilidad o una frecuencia durante un período de tiempo determinado)⁹.

RIESGO: Efecto de la incertidumbre sobre los objetivos.¹⁰

RIESGO INHERENTE: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.¹¹

RIESGO RESIDUAL: Remanente después del tratamiento del riesgo.¹²

TIC (TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES): Conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.¹³

⁶ DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad nacional [en línea]. [Consultado 10 de septiembre de 2012]. Disponible en <<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>>

⁷ ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN – ISO. ISO / IEC 27032: 2012 Op. Cit., p. 7

⁸ Ibid., p. 8.

⁹ INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Introducción. NTC-ISO 31000:2018. Bogotá D.C.: El Instituto, 2018

¹⁰ Ibid., p. 12.

¹¹ MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo Nacional de Gestión de Riesgos de Seguridad Digital [en línea]. [Consultado 25 de septiembre de 2020]. Disponible en <https://www.mintic.gov.co/portal/604/articles-61854_documento.docx>

¹² INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. NTC-ISO 31000:2018 Op. Cit., p. 14

¹³ COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1341 (30 de julio de 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Bogotá D.C. 2009. 4 p.

INTRODUCCIÓN

Hoy por hoy, las entidades deben estar a la vanguardia en cuanto a las formas para establecer contacto con sus clientes y/o usuarios con el fin de ser más competitivos en el mercado y la industria. Una de ellas es a través de la publicación de páginas y portales web en internet, los cuales permiten la interacción y conocimiento de los productos y servicios que las organizaciones ponen a disposición de estos.

Al publicar estos sitios en Internet, clientes, usuarios, *hackers*, *bots*, entre otros, pueden acceder a sus servicios con fines legítimos; sin embargo, otros no lo hacen de esta forma, aumentando la probabilidad de que se materialicen incidentes de ciberseguridad en la entidad a través de, por ejemplo, un ataque cibernético originado desde diferentes ubicaciones alrededor del mundo (*botnet*) dirigido a uno de estos sitios. Este es el caso del Banco Agrario de Colombia; entidad que en aras de facilitar la interacción con sus clientes y/o usuarios, tiene publicados varios portales y servicios en Internet, exponiéndose a los riesgos y amenazas que allí se encuentran.

Teniendo en cuenta lo anterior, y con el fin de mitigar los riesgos de ciberseguridad para los portales que el Banco Agrario pone a disposición de los consumidores financieros y demás interesados, es preciso conocer el diagnóstico que permita evaluar el estado de la ciberseguridad de estos sitios, con el fin de identificar las brechas y oportunidades de mejora en cuanto a la gestión de la ciberseguridad de la entidad.

1. PROBLEMA DE INVESTIGACIÓN

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo establecer un diagnóstico del estado de la ciberseguridad para las aplicaciones expuestas en internet por el Banco Agrario de Colombia para la definición de los planes de acción?

1.2 PLANTEAMIENTO DEL PROBLEMA

El Banco Agrario de Colombia es una institución financiera estatal enfocada a prestar sus servicios especialmente al sector rural, apoyando las directrices provenientes del Ministerio de Agricultura y Desarrollo Rural en materia de financiación de proyectos productivos en el campo.

Durante los últimos años, esta entidad ha venido exponiendo diferentes portales en internet, por medio de los cuales sus clientes y/o usuarios pueden interactuar con la entidad, gestionar sus productos o efectuar cualquier otro tipo de trámite; permitiendo un mayor acercamiento con sus clientes, atrayendo la atención de sus usuarios y aumentando la oportunidad de atención para los mismos.

De acuerdo con la Encuesta Global de Seguridad de la Información 2018-2019 de la firma EY, Colombia es el país de América Latina con mayor porcentaje de detecciones de *malware* tipo *ransomware*, así mismo, concluyen que el sector financiero es uno de los más sensibles a ciberataques en Colombia¹⁴.

Por lo anterior, existe una necesidad por parte de la entidad de conocer el estado de la ciberseguridad para las aplicaciones que expone en internet con el fin de salvaguardar estos activos de información, mitigando la probabilidad de que se materialice un incidente de ciberseguridad.

¹⁴ EY LATAM, Encuesta Global de Seguridad de la Información 2018-19 [en línea]. [Consultado el 15 de agosto de 2020]. Disponible en <[https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/\\$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf)>

2. JUSTIFICACIÓN

El sector financiero es uno de los más involucrados en el avance cibernético, teniendo en cuenta el aumento significativo del uso de la tecnología en la mayoría de sus actividades diarias y dada la necesidad de ofrecer a sus clientes soluciones virtuales para hacer más fácil el manejo de los productos financieros a través de internet.

Actualmente, el Banco Agrario de Colombia ofrece a sus clientes y/o usuarios diferentes aplicaciones a través de internet, en las cuales se pueden realizar transferencias interbancarias, pago de servicios públicos y privados, consulta de saldos de cuentas, entre otras operaciones. Teniendo en cuenta lo anterior, se establece la necesidad de garantizar un canal seguro para la ejecución de las operaciones realizadas por sus clientes.

Dada la premisa de ofrecer canales y portales seguros, se plantea el presente proyecto el cual consiste en el diseño del plan director de ciberseguridad para las aplicaciones que el Banco Agrario de Colombia tiene expuestas en internet. El desarrollo de este proyecto permitirá identificar el estado actual de la ciberseguridad de estas con el fin de identificar las brechas a las cuales están expuestas la confidencialidad, integridad y disponibilidad de estos sitios, para que la entidad pueda, posteriormente, efectuar las acciones preventivas y correctivas necesarias y de esta forma fortalecer su entorno de ciberseguridad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el plan director de ciberseguridad de las aplicaciones expuestas en internet por el Banco Agrario de Colombia basado en la norma ISO/IEC 27032:2012 con el fin de identificar el estado actual de la ciberseguridad de la entidad.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer el contexto del Banco Agrario de Colombia, incluyendo las partes interesadas y aplicaciones expuestas en internet.
- Realizar un análisis de riesgos a las aplicaciones que se encuentran expuestas en internet por el Banco Agrario de Colombia.
- Definir los roles y las directrices para las partes interesadas.
- Seleccionar los controles de ciberseguridad a implementar.
- Especificar los lineamientos para el intercambio de la información entre las partes interesadas.

4. MARCO TEÓRICO

4.1 PLAN DIRECTOR DE SEGURIDAD

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial¹⁵.

Los proyectos que componen el Plan Director de Seguridad varían en función de diversos factores relacionados como:

- El tamaño de la organización
- El nivel de madurez en tecnología
- El sector al que pertenece la empresa
- El contexto legal que regula las actividades de esta
- La naturaleza de la información que manejamos
- El alcance del proyecto
- Otros aspectos organizativos

Estos factores determinarán la magnitud y complejidad del Plan Director de Seguridad resultante. No obstante, en general, para la elaboración y puesta en marcha de un Plan Director de Seguridad se siguen las fases o etapas que muestra la figura 1¹⁶:

Figura 1. Implementando un plan director de seguridad



¹⁵ INSTITUTO NACIONAL DE CIBERSEGURIDAD - INCIBE. Plan Director de Seguridad [en línea]. [Consultado 30 de agosto 2020]. Disponible en <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf>

¹⁶ Ibid., p. 5.

Figura 1. (continúa)



Fuente: INCIBE¹⁷

A continuación, se resume en qué consisten las fases referidas en la figura 1:

- Conocer la situación actual: consiste en conocer la situación actual de nuestra empresa en materia de ciberseguridad. Para ello se llevan a cabo distintos análisis considerando aspectos técnicos, organizativos, regulatorios y normativos, entre otros.
- Conocer la estrategia de la organización: consiste en conocer la estrategia corporativa de la organización a la cual se le va a realizar la implantación del plan.
- Definir proyectos e iniciativas: A partir de la información recabada se definen las acciones, iniciativas y proyectos necesarios para alcanzar el nivel de seguridad que nuestra organización requiere.
- Clasificación y priorización: Una vez identificadas las acciones, iniciativas y proyectos, se clasifican y priorizan. El detalle y granularidad de las acciones a llevar a cabo puede ser muy variado.
- Aprobación por la dirección: En este punto, ya dispondremos de una versión preliminar del Plan Director de Seguridad. Este plan debe revisarlo y aprobarlo la Dirección.
- Implantación del Plan Director de Seguridad: Una vez aprobado por la Dirección, el Plan Director de Seguridad marca el camino a seguir para alcanzar el nivel de seguridad que nuestra organización necesita. Como si de un proyecto más se tratara, cada organización puede emplear la metodología de gestión de proyectos que considere oportuno para llevarlo a cabo.

4.2 CIBERSEGURIDAD

La Unión Internacional de Telecomunicaciones define Ciberseguridad así:

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los

¹⁷ Ibid., p. 5.

activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad¹⁸.

4.3 ESTANDAR ISO/IEC 27032:2012

El estándar ISO/IEC 27032 es un estándar de ciberseguridad, publicado en Julio de 2012 por la Organización Internacional de Normalización (ISO), la cual es una guía para la mejora del estado de la ciberseguridad (frente a otros dominios) tal como se muestra en la figura 2:

Figura 2. Gestión de la ciberseguridad



Fuente: Colombia Inteligente¹⁹

A continuación, se definen los conceptos ilustrados en la figura 2:

- Seguridad en las aplicaciones: proceso llevado a cabo para aplicar controles y medidas a las aplicaciones de la organización, con el fin de gestionar los riesgos de su uso.

¹⁸ UNIÓN INTERNACIONAL DE TELECOMUNICACIONES – UIT. Aspectos generales de la ciberseguridad [en línea]. [Consultado 30 de agosto de 2020]. Disponible en <https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items>

¹⁹ COLOMBIA INTELIGENTE. Norma ISO 27032:Gestión de la Ciberseguridad [en línea]. [Consultado 30 de agosto de 2020]. Disponible en <<https://www.colombiainteligente.org/index.php/noticias/noticias-sectoriales/2448-norma-iso-27032-gestion-de-la-ciberseguridad>>

- Seguridad de redes: diseño, implementación y operación de redes para llevar a cabo los propósitos de la seguridad de la información en redes dentro de las organizaciones y entre organizaciones y usuarios.
- Seguridad en internet: protección de servicios relacionados con Internet y TIC como una extensión de la seguridad de redes organizacionales y hogar.
- Protección de infraestructura crítica de información (CIIP): protección de sistemas que son proporcionados u operados por proveedores críticos y que son considerados como infraestructura crítica para el negocio.

Este estándar cubre prácticas de seguridad de línea base para partes interesadas en el ciberespacio:

- Visión general de la ciberseguridad.
- Explicación de las relaciones entre ciberseguridad y otros tipos de seguridad.
- Definición de partes interesadas y descripción de roles en ciberseguridad.
- Guía para atender asuntos comunes de ciberseguridad.
- Marco de referencia para facilitar la colaboración de las partes interesadas en la solución de asuntos de ciberseguridad.

La Norma ISO 27032:2012 cuenta con dos áreas de enfoque:²⁰

La primera área de enfoque de este estándar internacional es atender la seguridad en el ciberespacio o asuntos de ciberseguridad los cuales se concentran en reducir las brechas entre los diferentes dominios de ciberseguridad en el ciberespacio. En particular, este estándar provee guía técnica para atender riesgos comunes de ciberseguridad, incluyendo:

- Ataques de ingeniería social,
- *Hacking*,
- Proliferación de software malicioso (*malware*);
- *Spyware*; y
- Otros tipos de software potencialmente no deseados.

La guía técnica provee controles para atender estos riesgos, incluyendo controles para:

- Prepararse ante ataques tales como, por ejemplo, *malware*, delincuentes individuales, u organizaciones criminales en internet;
- Detectar y monitorear ataques; y
- Responder a ataques.

²⁰ INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Introducción. ISO/IEC 27032:2012. Bogotá D.C.: El Instituto, 2012

La segunda área de enfoque de este estándar internacional es la colaboración debido a que hay una necesidad de compartir y coordinar información de forma eficiente y eficaz, así como de manejo de incidentes, entre las partes interesadas en el ciberespacio. Esta colaboración debe suceder de forma segura y confiable de forma que igualmente proteja la privacidad de los individuos interesados. Muchas de estas partes interesadas pueden residir en diferentes ubicaciones geográficas y zonas horarias, y están gobernadas por diferentes requisitos regulatorios. Las partes interesadas incluyen:

- Clientes, los cuales pueden ser de diversos tipos de organizaciones e individuos; y
- Proveedores, los cuales incluyen proveedores de servicios.

Por ellos, este estándar internacional también provee un marco de referencia para:

- Compartir información;
- Coordinación; y
- Manejo de incidentes.

El marco de referencia incluye:

- Elementos clave para establecer confianza;
- Los procesos necesarios para colaboración, intercambio y el compartir información, así como
- Requisitos técnicos para la integración e interoperabilidad de sistemas entre diferentes partes interesadas.

4.4 GESTIÓN DEL RIESGO NTC- ISO31000:2018

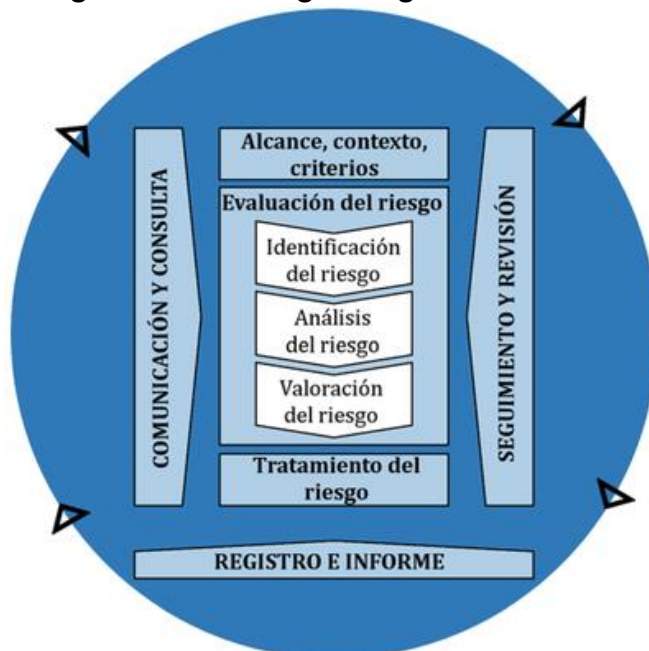
Aunque todas las organizaciones gestionan el riesgo en algún grado, la norma ISO 3100 establece un número de principios que es necesario satisfacer para hacer que la gestión del riesgo será eficaz. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos globales de gobierno, estrategia y planificación, gestión, proceso de presentación de informes, políticas, valores y cultura de la organización. La gestión del riesgo se puede aplicar a toda la organización, en todas sus muchas áreas y niveles, en cualquier momento, así como a funciones, proyectos y actividades específicos.²¹

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta,

²¹ INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Introducción. NTC-ISO 31000:2018. Bogotá D.C.: El Instituto, 2018

establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. El proceso mencionado se ilustra en la figura 3.

Figura 3. Proceso de gestión de riesgos según ISO 31000



Fuente: Organización Internacional de Normalización – ISO²²

A continuación, se resume cada paso del proceso descrito en la figura 3:

- Comunicación y consulta: La comunicación y la consulta con las partes involucradas externas e internas deberían tener lugar durante todas las etapas del proceso para la gestión del riesgo.
- Establecimiento del contexto: Al establecer el contexto, la organización articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso.
- Identificación del riesgo: La organización debería identificar las fuentes de riesgo, las áreas de impacto, los eventos (incluyendo los cambios en las circunstancias) y sus causas y consecuencias potenciales. El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Es importante identificar los riesgos asociados a la no búsqueda de una oportunidad. La identificación exhaustiva es crítica porque un riesgo que no se identifique en esta fase no será incluido en el análisis posterior.

²² ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN – ISO. ISO 31000:2018(es) Gestión del riesgo — Directrices [en línea]. [Consultado 30 de agosto de 2020] Disponible en <<https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>>

- **Análisis del riesgo:** El análisis del riesgo implica el desarrollo y la comprensión del riesgo. Este análisis brinda una entrada para la evaluación del riesgo y para las decisiones sobre si es necesario o no tratar los riesgos y sobre las estrategias y métodos más adecuados para su tratamiento. El análisis del riesgo también brinda una entrada para la toma de decisiones, en la cual se deben hacer elecciones y las opciones implican diversos tipos y niveles de riesgo.
- **Valoración del riesgo:** El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basada en los resultados de dicho análisis, a acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento.
- **Tratamiento del riesgo:** El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.
- **Seguimiento y revisión:** Tanto el seguimiento como la revisión debería ser una parte planificada del proceso para la gestión del riesgo e incluir verificación o vigilancia regulares. Pueden ser periódicos o según convenga.

5. MARCO CONTEXTUAL

5.1 CREACIÓN Y OBJETO SOCIAL BANCO AGRARIO DE COLOMBIA

El Banco es el producto de la conversión de la sociedad Leasing Colvalores - Compañía de Financiamiento Comercial-, de establecimiento de crédito del tipo de las Compañías de Financiamiento Comercial al tipo de los establecimientos de crédito de los bancos comerciales, denominado inicialmente Banco de Desarrollo Empresarial S. A. y, posteriormente, Banco Agrario de Colombia S.A.; conversión autorizada por la Superintendencia Bancaria, mediante Resolución No. 0968 del 24 de junio de 1.999.

Por su composición accionaria, el Banco es una sociedad de economía mixta del orden nacional, del tipo de las anónimas, sujeta al régimen de empresa industrial y comercial del Estado, vinculada al Ministerio de Agricultura y Desarrollo Rural.

El 28 de junio de 1999 el Banco Agrario de Colombia S.A., entidad financiera estatal, abrió sus puertas al público con el objetivo principal de prestar servicios bancarios al sector rural. Actualmente, a través de sus 749 sucursales financia actividades rurales, agrícolas, pecuarias, pesqueras, forestales y agroindustriales. Para atender las necesidades financieras del sector rural y urbano cuenta con la red de oficinas más extensa del país.

El Banco Agrario de Colombia S.A., tiene como objeto desarrollar las operaciones propias de un establecimiento bancario comercial, financiar en forma principal, pero no exclusiva, las actividades relacionadas con el sector rural, agrícola, pecuario, pesquero, forestal y agroindustrial. No menos del 70% de su saldo de cartera estará dirigido a la financiación de las actividades relacionadas con las actividades rurales, agrícolas, pecuarias, pesqueras, forestales y agroindustriales.²³

5.2 MISIÓN

Banco comercial comprometido con el desarrollo rural que ofrece soluciones financieras integrales a sus clientes, creando valor a nuestros grupos de interés dentro de límites de riesgo tolerable, soportado en procesos y tecnología de calidad, y un equipo humano competente.²⁴

²³ BANCO AGRARIO DE COLOMBIA. Acerca del Banco Agrario [en línea]. [Consultado 15 de agosto de 2020]. Disponible en <<https://www.bancoagrario.gov.co/acerca/Paginas/default.aspx>>

²⁴ BANCO AGRARIO DE COLOMBIA. Acerca del Banco Agrario [en línea]. [Consultado 15 de agosto de 2020]. Disponible en <<https://www.bancoagrario.gov.co/acerca/Paginas/Entidad.aspx>>

5.3 VISIÓN

Ser el Banco preferido de los habitantes y de las empresas que producen en la ruralidad colombiana.²⁵

5.4 VALORES CORPORATIVOS

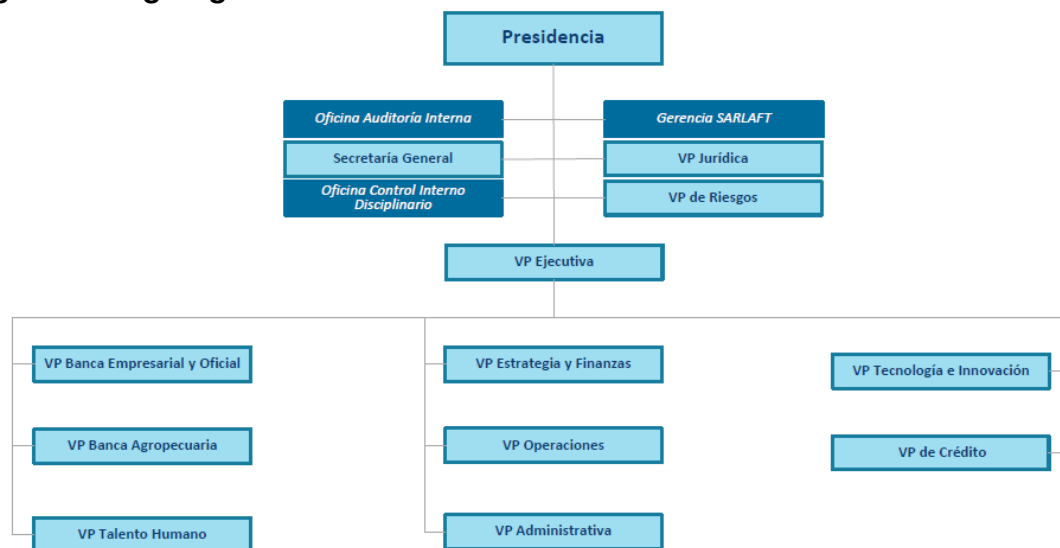
Los valores corporativos que determinan la actuación del Banco Agrario de Colombia S.A. son:

- Transparencia.
- Compromiso.
- Responsabilidad Social
- Respeto.
- Coherencia.
- Equidad.

5.5 ORGANIGRAMA

La estructura organizacional con la que se encuentra establecido el Banco Agrario de Colombia se evidencia en la figura 4:

Figura 4. Organigrama



Fuente: Banco Agrario de Colombia²⁶

²⁵ Ibid.

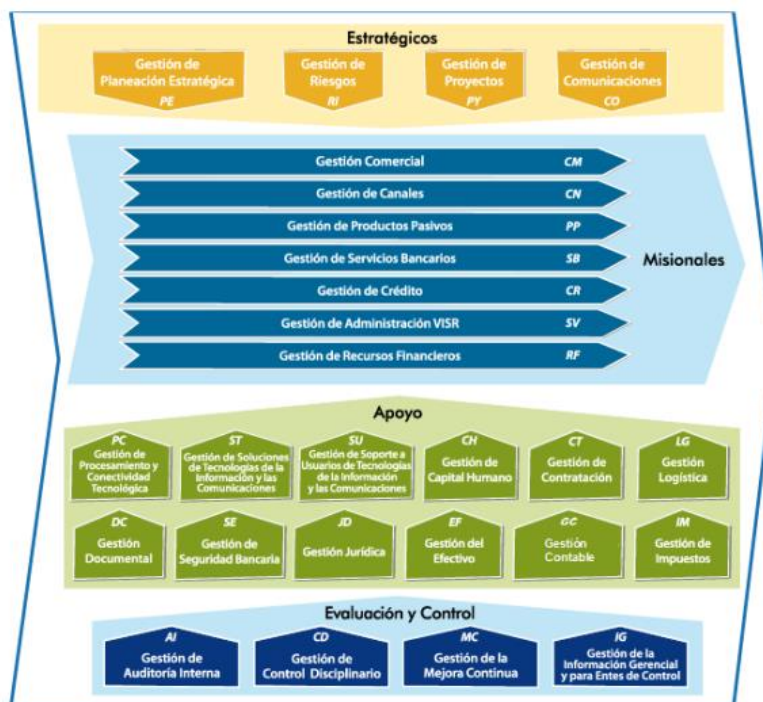
²⁶ BANCO AGRARIO DE COLOMBIA. Organigrama [en línea]. [Consultado 15 de agosto de 2020]. Disponible en <<https://www.bancoagrario.gov.co/acerca/Paginas/default.aspx>>

La Vicepresidencia de Tecnología e Innovación, bajo los lineamientos de la Vicepresidencia Ejecutiva del Banco Agrario de Colombia, tiene dentro de sus funciones liderar, coordinar, y gestionar las acciones necesarias en tecnología informática, de comunicaciones, de innovación y transformación digital del Banco para el desarrollo de nuevos productos, servicios, convenios y canales²⁷, y dentro de esta se encuentra la gestión de las aplicaciones expuestas en internet con base en los procesos y procedimientos de apoyo que serán descritos en el numeral 5.6.3.

5.6 PROCESOS Y PROCEDIMIENTOS

Entendiendo que un proceso constituye un conjunto de actividades mutuamente relacionadas o que interactúan para generar valor, las cuales transforman elementos de entrada en resultados y con esto satisfacer las necesidades del cliente, de la organización o de la ley. Los procesos del Banco se agrupan, por su naturaleza, en la siguiente clasificación buscando una mejor comunicación y cumplimiento de las estrategias de forma sistémica y disciplinada.²⁸ Esta clasificación se detalla de forma general en la figura 5 y será descrita en los siguientes numerales.

Figura 5. Gestión por procesos Banco Agrario de Colombia



Fuente: Documento Gestión por Procesos Banco Agrario de Colombia

²⁷ COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. Decreto 1341 (25 de julio de 2019). Por el cual se modifica la estructura del Banco Agrario de Colombia S.A. y se determinan las funciones de sus dependencias. Bogotá D.C. 2019. 15 p.

²⁸ BANCO AGRARIO DE COLOMBIA, Procesos y Procedimientos. Recuperado de: https://www.bancoagrario.gov.co/Documents/Gestion_por_procesos_Banco_Agrario.pdf. 2020

5.6.1 Procesos Estratégicos. Estos procesos son relativos al establecimiento de políticas y estrategias, fijación de objetivos. En la figura 6 se describen los que los componen y el objetivo de cada uno:

Figura 6. Procesos estratégicos Banco Agrario de Colombia

Gestión de Planeación Estratégica	• Brindar a la organización las herramientas necesarias para definir una ruta estratégica a largo plazo a través de la articulación de la formulación y seguimiento a la implementación de la estrategia.
Gestión de Riesgos	• Definir, orientar, divulgar, implantar, interpretar, socializar y administrar las políticas de Riesgo de Crédito, de Riesgo de Mercado, de Riesgo Operativo, Seguridad de la Información y SARLAFT, utilizando herramientas y modelos de aproximación científica para afrontar los riesgos mencionados.
Gestión de Proyectos	• Suministrar a las áreas del Banco Agrario el acompañamiento metodológico en la estructuración de iniciativas y planeación, ejecución, monitoreo, control, cierre y post-implementación de planes estratégicos, para contribuir al logro de los objetivos del Banco, optimizando el uso de los recursos a su disposición.
Gestión de Comunicaciones	• Describir los diferentes procesos y las actividades que se ejecutan desde el punto de vista del posicionamiento publicitario, comunicaciones internas, divulgación de marca y gestión de prensa. Definir los diferentes canales de comunicación del Banco Agrario de Colombia.

Fuente: Documento Gestión por Procesos Banco Agrario de Colombia

5.6.2 Procesos Misionales. Estos procesos proporcionan el resultado previsto por la entidad en el cumplimiento de su objeto social o razón de ser. En la figura 7 se describen los que los componen y el objetivo de cada uno:

Figura 7. Procesos Misionales Banco Agrario de Colombia

Gestión Comercial	• Ofrecer productos y servicios financieros, acordes con las necesidades de los diferentes segmentos objetivos del banco, a través de diversas alternativas de canales de atención y con el desarrollo de estrategias comerciales que permitan el logro de los objetivos definidos en el plan de negocios, aumentando el nivel de vinculación fidelización y satisfacción de nuestros clientes.
Gestión de Canales	• Proveer canales que permitan al Banco tener mayor cobertura y eficiencia en la prestación de servicios a los Clientes.
Gestión de Productos Pasivos	• Garantizar la operación de los diferentes Productos Pasivos que ofrece la entidad enmarcados dentro de la normatividad vigente y encaminados al cumplimiento del plan de negocios del Banco, satisfaciendo las necesidades y expectativas de clientes y usuarios.
Gestión de Servicios Bancarios	• Garantizar la operación de los diferentes servicios bancarios en moneda legal y moneda extranjera que ofrece la entidad enmarcados dentro de la normatividad vigente y encaminados al cumplimiento del plan de negocios del Banco, satisfaciendo las necesidades y expectativas de clientes y usuarios.
Gestión de Crédito	• Financiar oportunamente las actividades agrícolas, pecuarias, forestales y agroindustriales, y atender las necesidades financieras de los entes territoriales y de la banca comercial.
Gestión de Administración VISR	• Administrar los recursos asignados por el Estado para las comunidades rurales menos favorecidas contribuyendo al mejoramiento de su calidad de vida, supervisando la debida inversión de los recursos.
Gestión de Recursos Financieros	• Maximizar la rentabilidad y los recursos financieros del Banco y/o de los portafolios de terceros a través de las operaciones en moneda legal, moneda extranjera, derivados y liquidez, dentro de los parámetros legales y de riesgo definidos por la ley, la Junta Directiva y la Alta Dirección, haciendo uso de metodologías de supervisión acordes con las actividades.

Fuente: Documento Gestión por Procesos Banco Agrario de Colombia

5.6.3 Procesos de Apoyo. Estos procesos corresponden a todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos, misionales y de evaluación y control. En la figura 8 se describen los que los componen y el objetivo de cada uno:

Figura 8. Procesos de Apoyo Banco Agrario de Colombia

Gestión de Procesamiento y Conectividad Tecnológica	• Garantizar la disponibilidad de las plataformas tecnológicas para asegurar la operación del negocio y procesamiento de la información en condiciones de seguridad, administrando y realizando seguimiento y control al tráfico de las redes internas y externas.
Gestión de Soluciones de Tecnologías de la Información y de la Comunicación	• Generar e implementar Soluciones Tecnológicas que permitan cubrir las necesidades y expectativas manifestadas por los usuarios, teniendo en cuenta el proceso de priorización definido en el BAC.
Gestión de Soporte a Usuarios de Tecnologías de la Información y las Comunicaciones	• Brindar Soporte Operativo y Tecnológico prestando un servicio eficiente y oportuno en el Banco Agrario de Colombia S.A.
Gestión de Capital Humano	• Atraer, vincular, retener y desarrollar el Talento Humano requerido para cumplir la misión y objetivos estratégicos del Banco con alta efectividad y la adaptación a un medio altamente cambiante.
Gestión de Contratación	• Administrar en forma integral, eficiente, oportuna y segura el proceso de contratación, para la compra o arrendamiento de bienes o la prestación de servicios en consonancia con el marco normativo que rige al Banco.
Gestión Logística	• Administrar de forma eficiente la gestión de: Suministros, Seguros, muebles e inmuebles, Equipos Activos, Gastos de Viajes y logística de eventos, correspondencia y transporte, asegurando el adecuado desarrollo de la operación bancaria.
Gestión Documental	• Aplicar a los documentos del Banco Agrario los criterios para la administración de manera adecuada, eficiente y eficaz en cuanto a la producción, recepción, organización, recuperación y conservación de la información documental, garantizando la optimización.
Gestión de Seguridad Bancaria	• Analizar, diseñar, e implementar estrategias y planes tendientes a salvaguardar la seguridad del negocio bancario y a prevenir y detectar fraudes e ilícitos, tanto de origen interno como de agentes externos.
Gestión Jurídica	• Suministrar a las áreas que intervienen en el proceso de Gestión Legal, una herramienta de planificación, de rápida consulta y fácil comprensión, mediante procedimientos simplificados con el fin de asegurar el conocimiento y disposición de los pasos a seguir
Gestión del Efectivo	• Garantizar la disponibilidad de efectivo en los lugares de prestación de servicios bancarios mediante la adecuada planeación y coordinación en las diferentes etapas del proceso.
Gestión Contable	• Emitir Estados Financieros del Banco, conforme a la normatividad vigente en Colombia y NIIF de Información Financiera, con el fin de brindar una información financiera útil, (comparable, confiable y relevante), para la toma de decisiones de los usuarios de la información contables.
Gestión de Impuestos	• Optimizar los recursos y la interpretación y aplicación de las normas que le permitan al Banco cumplir con sus obligaciones fiscales nacionales, departamentales y municipales, así como servir de apoyo a las oficinas y dependencias de la Dirección General en las consultas y procedimientos en materia tributaria.

Fuente: Documento Gestión por Procesos Banco Agrario de Colombia

Dentro de los procesos descritos en la figura 8 se encuentran los procesos que exponen los sitios web en internet correspondientes a:

- Gestión de procesamiento
- Gestión de soluciones de TIC

En el numeral 5.10 se detallarán los sitios expuestos en internet que corresponden a las áreas que componen estos procesos.

5.6.4 Procesos de Evaluación y Control. Estos procesos corresponden a la medición, seguimiento y auditoría interna, acciones correctivas y preventivas, y son una parte integral de los procesos estratégicos, de apoyo y los misionales. En la figura 9 se describen los que los componen y el objetivo de cada uno:

Figura 9. Procesos de Evaluación y Control Banco Agrario de Colombia

Gestión de de Auditoría Interna	•Evaluar y/o asesorar con calidad, oportunidad y eficacia a los procesos, áreas y demás entes auditables del Banco para mejorar los procesos y agregar valor y contribuir al fortalecimiento del Sistema Integral de Gestión y Control.
Gestión de Control Disciplinario	•Asegurar que se acaten los principios de la administración pública adelantando investigaciones por acciones u omisiones, de los cuales puedan resultar responsables los funcionarios del Banco; lo anterior enmarcado en un propósito de prevenir y reprender las posibles conductas que puedan constituir faltas disciplinarias .
Gestión de Mejora Continua	•Establecer en la organización estructuración, análisis, rediseño e implementación de mejoras que contribuyan al cumplimiento de la planeación estratégica y de los objetivos de los procesos, a través de buenas prácticas y metodologías ágiles, con el fin de transformar procesos simples para el cliente, con calidad y oportunidad .
Gestión de la Información Gerencial y para Entes de Control	•Generar y analizar la información producida por los procesos misionales del Banco con oportunidad y calidad así como atender y gestionar los requerimientos realizados por las diferentes áreas del Banco así como de los entes de control relacionados con la información que la Gerencia de Sistemas de Información administra.

Fuente: Documento Gestión por Procesos Banco Agrario de Colombia

5.7 GESTIÓN DE RIESGOS

El Banco Agrario de Colombia. Actualmente cuenta con una Política del Sistema de Administración del Riesgo (SAR) implementado y actualizado al año 2020, la cual se establece con el propósito de fortalecer la cultura de gestión de riesgo, determinar los métodos para el tratamiento y monitoreo de los riesgos administrados, así como prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de los objetivos empresariales, o, en caso de que ello no resulte razonablemente posible, mitigar su impacto.

Para lograr este propósito, el Sistema de Administración de Riesgo (SAR) del Banco Agrario de Colombia está compuesto por los Sistemas SARC, SARM, SARL, SARO, SARLAFT y SGSI; los cuales obedecen a la normatividad vigente en materia de

riesgos establecida por la Superintendencia Financiera de Colombia y demás entidades gubernamentales.²⁹

5.8 SGSI

El Banco Agrario de Colombia cuenta con la certificación NTC ISO/IEC 27001:2013 para los subprocesos de: Operaciones de Tesorería en moneda Legal y extranjera del proceso de recursos financieros. Riesgo de Seguridad de la información del proceso de Gestión de riesgos y Gestión para el control y monitoreo de acceso y manos remotas al centro principal de procesamiento. Adicionalmente, se aplica la Política General de Seguridad de la Información, creada por el Banco, para todos los procesos mencionados en el numeral 5.6. Esta política tiene como propósito:

El BANCO AGRARIO DE COLOMBIA, consciente que en el desarrollo de su actividad como Establecimiento Financiero y Entidad del Estado, se ve expuesto a diferentes riesgos de seguridad de la información y ciberseguridad que podrían afectar los principios de la confidencialidad, integridad o disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento asociados a los sistemas de información de la Entidad o en el ciberespacio, define y establece las directrices que permiten el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información y la Ciberseguridad, a fin de promover y fortalecer la gestión de riesgos administrados en la toma de decisiones al interior de la Entidad, apoyar el cumplimiento de los objetivos estratégicos, determinar métodos de tratamiento y monitoreo de los riesgos y asegurar el cumplimiento de la normatividad relacionada con la seguridad de la información y la ciberseguridad.³⁰

Como complemento adicional y en función del cumplimiento de la Política General de Seguridad de la Información, se encuentran establecidos trece (13) Lineamientos de Seguridad de la Información y ciberseguridad en el cual se establecen “las directrices y responsabilidades que deben ser atendidas en el Banco Agrario de Colombia por sus colaboradores, proveedores y entes reguladores que consultan, procesan, transmitan y/o almacenan información en soporte físico y electrónico a cargo del Banco y para tal fin accedan y hagan uso de los sistemas de información, recursos tecnológicos del Banco ubicados en centros de procesamiento, en el ciberespacio o en servicios de computación en la nube.”³¹

²⁹ INTRANET BANCO AGRARIO DE COLOMBIA. Política Administración del Riesgo. Recuperado de: <http://bac/Normatividad/gestionProcesos/Políticas/RI-PL-001.pdf>.2020

³⁰ INTRANET BANCO AGRARIO DE COLOMBIA. Política General de Seguridad de la Información y Ciberseguridad. Recuperado de: <http://bac/Normatividad/gestionProcesos/Políticas/RI-PL-014.pdf>.2020

³¹ INTRANET BANCO AGRARIO DE COLOMBIA. Lineamientos de Seguridad de la Información y ciberseguridad. Recuperado de: <http://bac/Normatividad/gestionProcesos/MarcosContextuales/RI-LI-003.pdf>.2020

5.9 PARTES INTERESADAS

Dentro de las partes interesadas para la gestión de la ciberseguridad en los sitios de internet expuestos por el Banco Agrario de Colombia se encuentran los siguientes:

5.9.1 Proveedores. En este grupo se encuentran los diferentes proveedores de servicios en el ciberespacio, que permiten a los clientes acceder a los mismos, los cuales se dividen en dos grupos: Proveedores de internet y proveedores de aplicación.

5.9.1.1 Proveedores de Internet. Son todos aquellos proveedores que a nivel de telecomunicaciones permiten acceder al ciberespacio y a los diversos servicios disponibles en él. Para el caso del Banco Agrario de Colombia se cuentan con los siguientes proveedores:

- Canales de Telecomunicaciones
 - Claro
 - Telefónica
 - Lazu
- Servicios Administrativos
 - Password Consulting Services
 - UT Password- Nexura
 - Easy Solutions
 - Globaltek Security
 - Telefónica
 - Moviredes
 - Inetum
 - BT Latam Colombia S.A.

5.9.1.2 Proveedores de Aplicación. Los proveedores de servicios de aplicación hacen disponibles sus servicios a través de su software y/o soporte de estos. Para el caso del Banco Agrario de Colombia se cuentan con los siguientes proveedores:

- Servicios de Soporte
 - Agilitix/Citrix
 - Microsoft
 - Vmware
 - HP
 - Dell
- Servicios de desarrollo de software
 - Cobiscorp
 - Fábrica UT Intergrupo Data
 - Financial System Company

5.9.2 Clientes. El termino clientes dentro de la gestión de la ciberseguridad, hace referencia a usuarios individuales, así como organizaciones privadas y públicas, los cuales llegan a ser clientes cuando acceden al ciberespacio o a cualquiera de los servicios disponibles en el mismo.

5.9.2.1 Individuos. Personas naturales o jurídicas quienes pueden tener o no relación con el Banco y usan sus servicios.

5.9.2.2 Organizaciones. Corresponde a las organizaciones privadas y públicas. Las organizaciones privadas incluyen empresas pequeñas y medianas, así como empresas grandes. El gobierno y Entes de control públicos son referidos en general como organizaciones públicas.

- Banco Agrario de Colombia (BAC).
- Empresas del sector.
 - Entidades que conforman el Sector Financiero reguladas por la Superintendencia Financiera de Colombia (SFC).
- Entes reguladores.
 - Superintendencia de Industria y Comercio – SIC.
 - Superintendencia Financiera de Colombia – SFC.
 - Auditoría Interna.
 - Auditoría - Ernest and Young.
 - Asociación bancaria y de entidades financieras de Colombia – ASOBANCARIA.
 - Contraloría General de la Nación.
 - Procuraduría General de la Nación.
 - Ministerio de Agricultura.

5.10 INFRAESTRUCTURA EXPUESTA EN INTERNET

Actualmente el Banco Agrario de Colombia cuenta con 26 aplicaciones expuestas en internet, distribuidas entre las áreas de Ciberseguridad, Movilidad, Plataformas Core, Plataformas no Core y Seguridad Perimetral. Este proyecto está orientado a cada una de estas soluciones tecnológicas bajo la administración de las áreas mencionadas anteriormente.

A continuación, se describen de forma general, las soluciones tecnológicas que tiene a su cargo cada área:

5.10.1 Plataformas Core. Esta área tiene a su cargo el conjunto de aplicaciones que soportan a la entidad bancaria. En el cuadro 1 se encuentra la dirección IP pública, el nombre que se le da al servicio y la URL de consulta en Internet.

Cuadro 1. Infraestructura expuesta en internet por Plataformas Core

Dirección IP	Nombre del servicio	Resolución DNS
186.115.219.176	En línea ACH PSE	https://enlinea.bancoagrario.gov.co https://enlinea.bancoagrario.gov.co/depositos/ https://enlinea.bancoagrario.gov.co/PSEBanco/faces/app/pse/login.xhtml
186.115.219.175	Gestión Cobranza (ICS)	https://ics.bancoagrario.gov.co:9443
186.115.219.177	Aula Financiera	https://aulafinanciera.bancoagrario.gov.co/

Fuente: Banco Agrario de Colombia

A continuación, se realiza una descripción general de los servicios relacionados a Plataformas Core

- En Línea ACH PSE: Plataforma enlace para la realización de pagos a través de la plataforma PSE (Pagos seguros en línea).
- Gestión Cobranza (ICS): ICS (*Internet Collection System*) es una plataforma utilizada para el cargue de gestión realizada por las casas de cobranza que tienen relación contractual con el Banco.
- Aula Financiera: Aplicativo del Banco Agrario utilizado para la capacitación de sus clientes en cuanto a educación financiera y económica.

5.10.2 Plataformas no Core. Esta área tiene a su cargo las aplicaciones que sirven de apoyo al negocio bancario. En el cuadro 2 se encuentra la relacione entre la dirección IP pública, el nombre que se le da al servicio y la URL de consulta en Internet de las aplicaciones bajo esta área.

Cuadro 2. Infraestructura expuesta en internet por Plataformas no Core

Dirección IP	Nombre del servicio	Resolución DNS
186.115.19.200	Correo Electrónico Banco Agrario	https://correo.bancoagrario.gov.co/owa https://autodiscover.bancoagrario.gov.co
186.115.219.169	Depósitos Judiciales	https://depositosespeciales.bancoagrario.gov.co
52.179.117.93	Portal Web Banco Agrario	https://www.bancoagrario.gov.co
186.115.219.183	Banca virtual Banco Agrario	https://ebanking.bancoagrario.gov.co/BA.ICBanking.WebUI https://ebanking.bancoagrario.gov.co/BA.ICBanking.MobileUI
186.115.219.184	ADFS (Servicios de Federación de <i>Active Directory</i>)	https://ads.bancoagrario.gov.co/ads/ls/idpinitiatedsignon.aspx
52.186.147.190	Conéctate al conocimiento	https://conectate.bancoagrario.gov.co/ekp
186.115.219.187	Portal tu Referido	https://tureferido.bancoagrario.gov.co

Cuadro 2. (continúa)

186.115.219.190	Portal Vivienda	https://portalvivienda.bancoagrario.gov.co
186.115.219.188	Portal Clientes	https://portalclientes.bancoagrario.gov.co/portalclientes
190.242.23.70	Ingreso Solidario	https://ingresosolidario.bancoagrario.gov.co
190.242.23.73	Consulta Giros – Jóvenes en Acción	https://consultagiros.bancoagrario.gov.co
190.242.23.74	Portal PAEF – Pago Ayuda Empleo Formal	https://portalpaef.bancoagrario.gov.co

Fuente: Banco Agrario de Colombia

A continuación, se realiza una descripción general de los servicios relacionados a Plataformas No Core:

- Correo Electrónico Banco Agrario: Servicio de correo electrónico soportado en los servidores del Banco.
- Depósitos Judiciales: Aplicativo en servicio para que juzgados y entes coactivos, administren y generen órdenes de pago y administración de depósitos judiciales³².
- Portal Web Banco Agrario: Página web principal de Banco Agrario donde se realiza la publicación de contenido hacia los clientes y usuarios de la entidad.
- Banca virtual Banco Agrario: Aplicación expuesta para que sus clientes accedan a la administración de productos financieros del Banco y puedan realizar transacciones o solicitudes de acuerdo con sus necesidades.
- ADFS (Servicios de Federación de Active Directory): Solución de Microsoft para proporcionar inicio de sesión único y autenticación a los servicios de Office 365 y Azure, entre otros.
- Conéctate al conocimiento: Aplicativo del Banco Agrario utilizado para la capacitación de sus colaboradores.
- Portal tu Referido: Portal para referenciar clientes prospecto de crédito desde los corresponsales bancarios.
- Portal Vivienda: Portal para beneficiarios de créditos de vivienda rural en donde se pueden hacer consultas con el número de cédula del ciudadano.
- Portal Clientes: Permite a clientes del Banco Agrario radicar una nueva intención de crédito basada en las condiciones de un crédito anterior.
- Ingreso Solidario: Portal que apoya el programa del Gobierno Nacional para el pago de ayudas a familias vulnerables.
- Consulta Giros – Jóvenes en Acción: Portal que apoya el programa del Gobierno Nacional para el pago de Jóvenes En Acción que no cuentan con cuenta de ahorros del Banco.
- Portal PAEF – Pago Ayuda Empleo Formal: Portal que apoya el programa del Gobierno Nacional para la Ayuda al Empleo Formal.

³² Depósitos Judiciales: Corresponde al recaudo de los depósitos constituidos en un título judicial por orden de un juzgado, fiscalía o entes coactivos.

5.10.3 Seguridad Perimetral. Esta área tiene a su cargo todas soluciones tecnológicas que emplea el Banco Agrario de Colombia para la protección del perímetro, detección de intrusos y antivirus. En el cuadro 3 se encuentra la dirección IP pública, el nombre que se le da al servicio y la URL de consulta en Internet.

Cuadro 3. Infraestructura expuesta en internet por Seguridad Perimetral

Dirección IP	Nombre del servicio	Resolución DNS
186.115.219.198	<i>Traffic in</i> – Acceso remoto Checkpoint	acceso.bancoagrario.gov.co
186.118.185.194	<i>Traffic out</i> – Navegación sin proxy	N/A
186.115.219.209	Consola Antivirus	avr.bancoagrario.gov.co
200.21.86.22	VPN SSL DG	rc.bancoagrario.gov.co
190.242.23.68	VPN SSL NAOS	rca.bancoagrario.gov.co

Fuente: Banco Agrario de Colombia

A continuación, se realiza una descripción general de los servicios relacionados Seguridad Perimetral:

- *Traffic in* – Acceso remoto CHECKPOINT: Servicio de conexión remota hacia los equipos de las oficinas del Banco a través de la plataforma Checkpoint.³³
- *Traffic out* – Navegación sin proxy: Direccionamiento IP que usan los equipos del Banco para consumir servicios en internet.
- Consola Antivirus: Consola de administración de antivirus para la conexión de equipos portátiles que se encuentran fuera de la red del Banco.
- VPN Dirección General: Servicio de conexión remota hacia los equipos de las oficinas del Banco en su sede principal.
- VPN Datacenter NAOS: Servicio de conexión remota hacia los servidores del Banco (Dirección General).

5.10.4 Ciberseguridad. Esta área tiene a su cargo la solución tecnológica correspondiente a la prevención de fuga de información en los equipos del Banco. En el cuadro 4 se encuentra la dirección IP pública y el nombre que se le da al servicio.

Cuadro 4. Infraestructura expuesta en internet por Ciberseguridad

Dirección IP	Nombre del servicio	Resolución DNS
186.115.219.178	Forcepoint DLP	dlpendpoint.bancoagrario.gov.co

Fuente: Banco Agrario de Colombia

³³ Checkpoint: Acceso remoto seguro y sin limitación a redes y recursos corporativos

A continuación, se realiza una descripción general del servicio expuesto en internet por el área de ciberseguridad:

- Forcepoint DLP Endpoint³⁴ (*Data Loss Prevention*): Herramienta para la prevención de fuga de información de los equipos portátiles que se encuentran fuera de la red del Banco.

5.10.5 Movilidad. Esta área tiene a su cargo las plataformas tecnológicas que permiten a los colaboradores del Banco acceder a las aplicaciones del Core bancario e intranet, sin encontrarse directamente en la red del Banco, a través de la plataforma Citrix³⁵. En cuadro 5 se encuentra la dirección IP pública, el nombre que se le da al servicio y la URL de consulta en Internet.

Cuadro 5. Infraestructura expuesta en internet por Movilidad

Dirección IP	Nombre del servicio	Resolución DNS
186.118.185.213	Almacenamiento Sharefile	sharefile.bancoagrario.gov.co
186.115.219.179	Citrix Movilidad Teletrabajo	https://teletrabajo.bancoagrario.gov.co
186.118.185.208	Citrix Movilidad XenMobile	https://xenmobile.bancoagrario.gov.co
186.115.219.168	Citrix Movilidad Apps	https://apps.bancoagrario.gov.co
186.115.219.199	VPN Movilidad	https://movilidad.bancoagrario.gov.co

Fuente: Banco Agrario de Colombia

A continuación, se realiza una descripción general de los servicios relacionados a Movilidad:

- Almacenamiento Sharefile: Solución segura para compartir contenido, intercambio de archivos y sincronización con entidades y entes de control.
- Citrix Movilidad Teletrabajo: Plataforma en la cual se publican las herramientas del Banco a través de virtualización por Citrix StoreFront que permite el acceso a los aplicativos bancarios para los asesores en oficinas y funcionarios del Banco.
- Citrix Movilidad XenMobile: Plataforma que permite la Administración de Dispositivos Móviles (MDM) y Administración de Aplicaciones Móviles (MAM) para el enrolamiento de tabletas lo para las actividades de MovAgro (Solución para captación de créditos en lugares de difícil acceso).
- Citrix Movilidad Apps: Servicio que se utiliza para el Acceso a las aplicaciones publicadas en los dispositivos tabletas administradas por la entidad.
- VPN Movilidad: Plataforma servicio que proporciona accesos remotos seguros a aplicaciones del banco desde complemento plug-in Citrix Gateway.

³⁴ Forcepoint DLP Endpoint: Solución para la prevención de fuga de información

³⁵ CITRIX: Servicio de virtualización de escritorios y aplicaciones.

6. METODOLOGÍA PARA LA EVALUACIÓN DEL RIESGO DE CIBERSEGURIDAD

A continuación, se describirá la metodología para identificar, medir, controlar y monitorear los diferentes eventos, incidentes, vulnerabilidades o amenazas, a los que puede verse afectadas las aplicaciones expuestas en internet y descritas en el numeral 5.10 de este documento, al momento de generar, capturar, procesar, transportar, almacenar y la disposición final de la información propia del negocio en el ciberespacio de acuerdo a la norma ISO 31000, la cual es una guía general que se considera suficiente para la gestión del riesgo en el contexto del ciberespacio³⁶, para lo cual se establecen las siguientes etapas en orden, así:

1. Contextualización e identificación de riesgos.
2. Medición del riesgo.
3. Control del riesgo.
4. Etapa de monitoreo.

6.1 CONTEXTUALIZACIÓN E IDENTIFICACIÓN DE RIESGOS

En esta etapa se busca conocer más a fondo el flujo de actividades que involucran el activo evaluado mediante la identificación de entradas, salidas, responsables, activos de información y terceros que interactúan con este. Esta contextualización se logra mediante la entrevista al administrador(es) de la(s) plataforma(s) quien(es) conoce(n) a detalle cómo es el funcionamiento de este.

6.2 MEDICIÓN DEL RIESGO

Esta etapa consiste en evaluar los riesgos identificados, con el fin de determinar la probabilidad y el impacto de estos. Para ello, se deben identificar las amenazas, vulnerabilidades y riesgos de cada una de las aplicaciones mencionadas en el numeral 5.10, con el fin de generar un plan de implementación de los controles que generen un ambiente seguro en el ciberespacio, bajo los criterios de disponibilidad, confidencialidad, integridad de la información.

Para realizar la medición del riesgo se debe conocer:

- La probabilidad (posibilidad de ocurrencia) de que dicho riesgo se materialice.
- El impacto (consecuencias) que se generaría al materializarse una o más amenazas identificadas.

³⁶ ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN – ISO. Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad. ISO / IEC 27032: 2012. 1 ed. Génova, Suiza ISO, 2012. p. 23.

6.2.1 Niveles para Probabilidad. Se definen cinco niveles para medir la probabilidad relacionados así:

- **1 – Improbable:** El evento puede ocurrir solo en circunstancias excepcionales, poco comunes o anormales (No se ha presentado en los últimos 5 años).
- **2 – Remoto:** El evento puede ocurrir en algún momento (Al menos 1 vez en los últimos 5 años).
- **3 – Ocasional:** El evento puede ocurrir en algún momento (Al menos 1 vez en los últimos 2 años).
- **4 – Frecuente:** Es viable que el evento ocurra en la mayoría de las circunstancias (Al menos 1 vez en el último año).
- **5 – Inminente:** Se espera que el evento ocurra en la mayoría de las circunstancias (Más de una vez en el año).

6.2.2 Niveles para Impacto. Para el impacto se definen cuatro tipos de acuerdo con la materialización de una amenaza. El valor total del impacto será el promedio³⁷ de los valores obtenidos en la calificación de estos cuatro tipos:

- **Impacto Operacional:** Las consecuencias que, a nivel de la operación del Banco, se puedan presentar frente a la materialización de un riesgo:
 - **1 – Insignificante:** No hay interrupción de las operaciones de la entidad.
 - **2 – Leve:** Interrupción de las operaciones de la entidad por algunas horas.
 - **3 – Moderado:** Interrupción de las operaciones de la entidad por un (1) día.
 - **4 – Severo:** Interrupción de las operaciones de la entidad por más de dos (2) días.
 - **5 – Catastrófico:** Interrupción de las operaciones de la entidad por más de cinco (5) días.
- **Impacto Reputacional:** Se definen las consecuencias que, puede sufrir la imagen de la entidad frente a la materialización de un riesgo:
 - **1 – Insignificante:** No se afecta la imagen institucional de forma significativa.
 - **2 – Leve:** Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios y/o clientes.
 - **3 – Moderado:** Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios y/o clientes.
 - **4 – Severo:** Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios y/o clientes.
 - **5 – Catastrófico:** Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

³⁷ El valor resultante se aproximará al entero más bajo si el decimal es menor a 0.5 y al entero más alto si es mayor o igual a 0.5.

- **Impacto Legal:** Se establecen las consecuencias en términos legales a las que se puede enfrentar el Banco, debido a la materialización de un riesgo:
 - **1 – Insignificante:** No genera afectación legal.
 - **2 – Leve:** Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.
 - **3 – Moderado:** Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.
 - **4 – Severo:** Sanción por parte de un ente de control u otro ente regulador.
 - **5 – Catastrófico:** Intervención por parte de un ente de control u otro ente regulador.

- **Impacto Financiero:** Se definen las consecuencias en cuanto a la afectación presupuestal de la entidad por la materialización de un riesgo:
 - **1 – Insignificante:** No se generan afectaciones económicas.
 - **2 – Leve:** Efecto mínimo sobre utilidades y/o presupuesto. Afectación en un valor $\geq 5\%$ sobre utilidades y/o presupuesto.
 - **3 – Moderado:** Efecto significativo afectando en un valor $\geq 20\%$ sobre utilidades y/o presupuesto.
 - **4 – Severo:** Incumplimiento en las metas y objetivos institucionales afectando en un valor $\geq 40\%$ las utilidades y/o presupuesto.
 - **5 – Catastrófico:** Incumplimiento en las metas y objetivos institucionales afectando en un valor $\geq 60\%$ las utilidades y/o presupuesto.

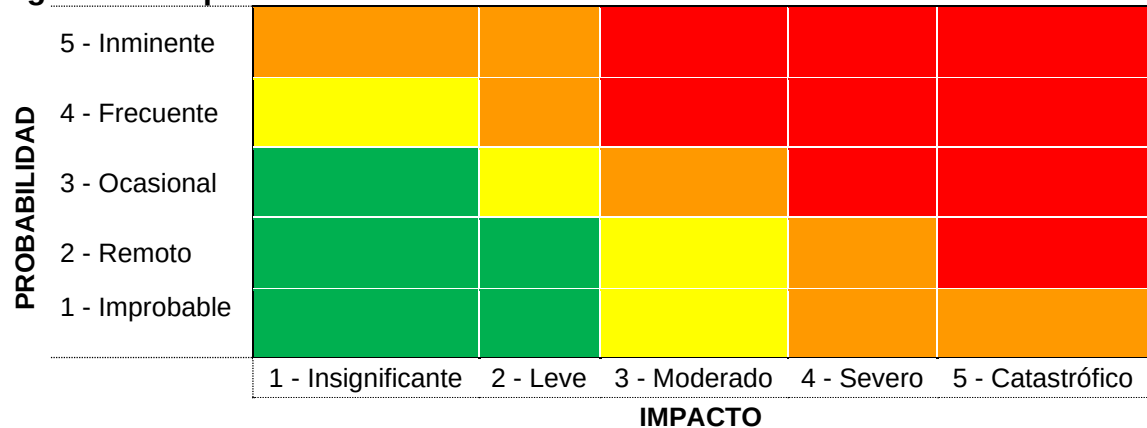
6.2.3 Cálculo del riesgo. El valor del riesgo (R) será el resultado entre el valor de la probabilidad (P) por el valor del impacto (I), así:

$$R = P * I$$

En el mapa de calor se agruparán la cantidad de riesgos en total, de acuerdo con su valor de probabilidad e impacto sin la aplicación de los controles existentes para su mitigación. El valor de cada riesgo será ubicado dentro del mapa de calor indicado en la figura 10, así:

- Bajo: casillas marcadas con color verde.
- Medio: casillas marcadas con color amarillo.
- Alto: casillas marcadas con color naranja.
- Extremo: casillas marcadas con color rojo.

Figura 10. Mapa de calor



Fuente: Autores

Se define que los riesgos a mitigar corresponden a los que se ubiquen en las casillas marcadas como “Alto” (naranja) y “Extremo” (rojo) dentro del mapa de riesgos inherente.

6.2.4 Calificación de los riesgos. Para la calificación de los riesgos se utilizará la plantilla detallada en el cuadro 6, en donde se deben calificar los riesgos para cada una de las aplicaciones en cuanto a los conceptos de la gestión de la ciberseguridad (Seguridad en aplicaciones, Seguridad en redes, Seguridad en internet y Protección de la Infraestructura crítica).

Cuadro 6. Plantilla ejemplo análisis de riesgos

Riesgo			Causa	Aplica	Probabilidad - P	Impacto - I					Valor Riesg o
C	I	D				O	R	L	F	T	
✓	x	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	1	1	3	1	2	2
x	x	x	Falta de monitoreo al tráfico de las redes	No	-	-	-	-	-	-	-

Fuente: Autores

A continuación, se detalla cómo se diligenciará la plantilla del cuadro 6 con la explicación de cada convención dentro de la misma:

- El título de cada plantilla será cada uno de los conceptos de la gestión de la ciberseguridad...Véase el numeral 4.3...
- Se evaluará el riesgo de afectación a la Confidencialidad (C), Integridad (I) y Disponibilidad (D) para cada causa evaluada: se indicará con un “✓” para el riesgo que aplique, de lo contrario se marcará con una “x”. En caso de que no exista

afectación a la confidencialidad, integridad o disponibilidad, no se evaluará la probabilidad e impacto y se rellenarán las casillas con “-”.

- El impacto se evaluará en sus cuatro tipos: Operacional (O), Reputacional (R), Legal (L) y Financiero (F) para generar el valor total (T) ...Véase el numeral 6.2.2...

Para determinar si existe una afectación a la confidencialidad, integridad o disponibilidad de acuerdo con los conceptos de la gestión de ciberseguridad ...Véase el numeral 4.3... se deben tener en cuenta las siguientes definiciones respecto a las causas evaluadas:

- Seguridad en aplicaciones
 - Afectación a la disponibilidad: Toda causa que pueda dejar fuera de línea la aplicación impidiendo que los usuarios o interesados puedan acceder a ella a nivel de software.
 - Afectación a la integridad: Toda causa que pueda alterar, modificar, manipular y/o eliminar datos de configuración, del usuario y/o del banco dentro de la aplicación.
 - Afectación a la confidencialidad: Toda causa que pueda otorgar acceso a los datos del usuario o del banco dentro de la aplicación sin consentimiento de los dueños de la información.
- Seguridad en redes
 - Afectación a la disponibilidad: Toda causa que afecte a la infraestructura que soporta el funcionamiento de la aplicación impidiendo el acceso a la misma.
 - Afectación a la integridad: Toda causa que pueda alterar, modificar, manipular y/o eliminar datos de configuración, del usuario y/o del banco en la infraestructura que soporta el funcionamiento de la aplicación.
 - Afectación a la confidencialidad: Toda causa que pueda otorgar un acceso no autorizado a los datos del usuario o del banco dentro la infraestructura que soporta el funcionamiento de la aplicación.
- Seguridad en internet
 - Afectación a la disponibilidad: Toda causa que impida el acceso a la aplicación por parte de los clientes o usuarios de esta.
 - Afectación a la integridad: Toda causa que pueda alterar, modificar, manipular y/o eliminar datos de configuración, del usuario y/o del banco debido al uso de la aplicación por parte de los clientes o usuarios.
 - Afectación a la confidencialidad: Toda causa que pueda otorgar un acceso no autorizado a los datos del usuario o del banco debido al uso de la aplicación por parte de los clientes o usuarios.
- Protección de infraestructura crítica
 - Afectación a la disponibilidad: Toda causa que impida el acceso a una aplicación crítica para el negocio y/o proporcionada u operada por un proveedor considerado crítico ...Véase el numeral 5.9.1...
 - Afectación a la integridad: Toda causa que pueda alterar, modificar, manipular y/o eliminar datos de configuración, del usuario y/o del banco de una aplicación

crítica para el negocio y/o proporcionada u operada por un proveedor considerado crítico...Véase el numeral 5.9.1...

- Afectación a la confidencialidad: Toda causa que pueda otorgar un acceso no autorizado a los datos del usuario o del banco en una aplicación crítica para el negocio y/o proporcionada u operada por un proveedor considerado crítico...Véase el numeral 5.9.1...

6.3 CONTROL DEL RIESGO

En esta etapa se identifican los controles existentes de los riesgos y causas identificadas mediante la aplicación de la metodología expuesta en el numeral 6.2. También se proponen los controles que se deberían implementar con base en la norma ISO/IEC 27032:2012 para mitigar los riesgos de ciberseguridad a los cuales se ven expuestos las aplicaciones descritas en el numeral 5.10, así como los roles y directrices que deben tener los interesados respecto a los controles sugeridos.

Se listarán los controles que se tienen actualmente implementados y se establecerá su aplicabilidad para mitigar los riesgos a la confidencialidad, integridad y/o disponibilidad de acuerdo con los conceptos de la gestión de ciberseguridad ...Véase el numeral 4.3... Se definirá si dicho control mitiga la probabilidad y/o el impacto y en qué medida, culminando con el detalle de la parte interesada responsable del control.

Para establecer el cálculo del riesgo residual (RR) por cada causa, se verificará la aplicabilidad del control que se tiene implementado de acuerdo con el inventario de controles del Banco, teniendo en cuenta si dicho control mitiga la probabilidad o el impacto de la causa evaluada. Posteriormente se sumará el valor de cada uno de los controles que mitigan probabilidad (CP) y/o impacto (CI), y este valor se restará al valor de probabilidad (PI) o impacto inherente (II) según aplique. El resultado final será la multiplicación de la probabilidad residual (PR) y el impacto residual (IR), así:

$$RR = (PI - CP)(II - CI) = PR * IR$$

6.4 ETAPA DE MONITOREO

Corresponde a la última fase del proceso de análisis de riesgos, la cual consiste en determinar los métodos de seguimiento al cumplimiento de los planes de acción definidos con respecto a los controles mencionados en la etapa detallada en el numeral 6.3 para los riesgos identificados con severidad alta y extrema.

Esta etapa estará a cargo de la organización con el fin de que continúe con la evaluación de riesgos de ciberseguridad para las aplicaciones descritas en este documento, teniendo en cuenta los controles sugeridos resultantes del análisis de riesgos realizado.

7. ANÁLISIS DE RIESGOS A LAS APLICACIONES QUE SE ENCUENTRAN EXPUESTAS EN INTERNET

En este capítulo se encuentran los análisis de riesgos realizados a las aplicaciones expuestas en internet relacionadas en el numeral 5.10 de acuerdo con la metodología detallada en el numeral 6.2, así como los mapas de riesgos generados a partir de los resultados obtenidos.

7.1 ANÁLISIS DE RIESGOS – CIBERSEGURIDAD

En los siguientes numerales se encuentra el desarrollo del análisis de riesgos para la infraestructura expuesta en internet por parte de Plataformas Core. En los cuadros 7 al10 se encuentra el detalle de este análisis, mientras que en las figuras 11 y 12 se encuentra la cantidad de riesgos en total asociados a cada causa

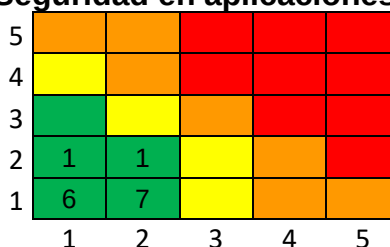
7.1.1 Forcepoint DLP.

Cuadro 7. Seguridad en aplicaciones - Forcepoint DLP

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	1	1	3	1	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	1	1	1	1	1	2
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	1	1	3	3	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	2	3	2	2
✗	✓	✓	Fallas en el control de acceso	Si	1	1	1	2	3	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	2	1	1	3	3	2	4
✓	✓	✗	Exfiltración de información	Si	1	1	4	4	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✗	✗	✗	Falta de backups de la aplicación	No	N/A	-	-	-	-	-	-
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	2	2	2
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	1	1	2	2	2	2
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	1	1	1	1
✓	✓	✗	Almacenamiento sin protección	Si	1	1	2	4	3	3	3
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 11. Mapa de calor - Seguridad en aplicaciones - Forcepoint DLP



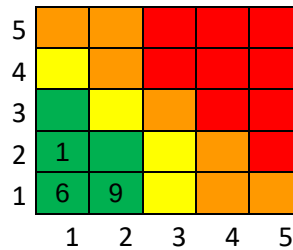
Fuente: Autores

Cuadro 8. Seguridad en redes - Forcepoint DLP

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	1	1	1	1	1	2
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	1	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	1	1	1	1	1	1
✗	✗	✓	Daños en los equipos de red	Si	1	1	1	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	1	1	4	3	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	3	2	1	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Trafico sensible sin protección	Si	1	1	1	3	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 12. Mapa de calor - Seguridad en redes - Forcepoint DLP



Fuente: Autores

Cuadro 9. Seguridad en internet - Forcepoint DLP

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-
✗	✗	✗	Suplantación de identidad en línea	No	N/A	-	-	-	-	-	-
✗	✗	✗	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✗	✗	✗	Acceso con Sistemas operativos y aplicaciones desactualizadas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ingeniería social	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en la configuración de las soluciones de seguridad del equipo	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en redes de comunicaciones	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Seguridad en Internet toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

Cuadro 10. Protección de infraestructura crítica - Forcepoint DLP

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

7.1.2 Interpretación de los resultados del análisis de riesgos – Ciberseguridad. De acuerdo con las tablas y mapas de riesgos obtenidos para la aplicación expuesta por el área de Ciberseguridad, se evidencia únicamente la aplicación de los riesgos para Seguridad en Aplicaciones y Seguridad en Redes, los cuales, en su mayoría, tienen un nivel de riesgo bajo sin la aplicación de controles. Lo anterior debido a que la aplicación evaluada no es considerada crítica para el negocio y tampoco tiene interacción alguna con los usuarios finales: no hay clientes humanos que accedan al servicio expuesto.

7.2 ANÁLISIS DE RIESGOS – MOVILIDAD

En los siguientes numerales se encuentra el desarrollo del análisis de riesgos para la infraestructura expuesta en internet por parte de Movilidad. En los cuadros 11 al 30 se encuentra el detalle de este análisis, mientras que en las figuras 13 a la 28 se encuentra la cantidad de riesgos en total asociados a cada causa.

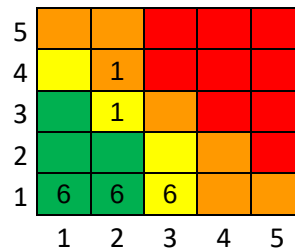
7.2.1 Almacenamiento Sharefile.

Cuadro 11. Seguridad en aplicaciones - Almacenamiento Sharefile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	2	3	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	1	2	1	2	2
✓	✓	✓	Fallas operativas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	3	2	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	3	1	2	2
✓	✓	✓	Ejecución de malware	Si	1	3	2	3	3	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	3	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	1	1	1	2	1	1	1
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	4	3	3	3	3
✓	✓	✗	Exfiltración de información	Si	1	1	4	4	2	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	3	3	3	3	3
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	1	2	1	2	2
✗	✗	✓	Ausencia de documentación	Si	1	1	1	2	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	1	1	2	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	1	2	1	2	8
✓	✓	✓	Versión del software desactualizada	Si	3	2	1	2	1	2	6
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	1	2	1	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	1	3	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 13. Mapa de calor - Seguridad en aplicaciones - Almacenamiento Sharefile



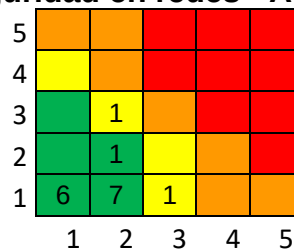
Fuente: Autores

Cuadro 12. Seguridad en redes - Almacenamiento Sharefile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	1	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	2	2	1	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	1	1	1	1	1
✗	✗	✓	Desastres naturales	Si	3	2	1	1	4	2	6
✗	✗	✓	Daños en los equipos de red	Si	1	2	1	1	1	1	1
✓	✓	✓	Abuso de privilegios	Si	1	1	1	3	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	1	2	1	1	1
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	2	1	2	1	2	2
✓	✓	✓	Uso no autorizado	Si	1	2	1	3	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	1	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	3	1	1	1	2	2
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	1	4	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 14. Mapa de calor - Seguridad en redes - Almacenamiento Sharefile



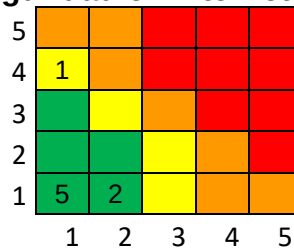
Fuente: Autores

Cuadro 13. Seguridad en Internet - Almacenamiento Sharefile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	2	1	1	1
✓	✓	✓	Suplantación de identidad en línea	Si	1	1	2	3	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	1	1	1	1	1	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	1	2	3	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 15. Mapa de calor - Seguridad en internet - Almacenamiento Sharefile



Fuente: Autores

Cuadro 14. Seguridad en Protección Infraestructura crítica - Almacenamiento Sharefile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

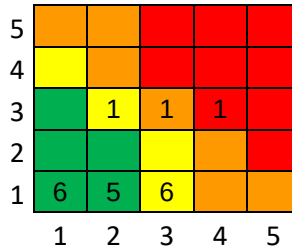
7.2.2 Citrix Movilidad Teletrabajo.

Cuadro 15. Seguridad en aplicaciones - Citrix Movilidad Teletrabajo

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	4	3	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	1	2	2
✓	✓	✓	Fallas operativas	Si	3	4	4	3	3	4	12
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	1	3	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	3	2	3	3	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	2	3	3	2	2
✗	✓	✓	Fallas en el control de acceso	Si	1	1	1	1	3	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	2	3	3	2	2
✓	✓	✗	Exfiltración de información	Si	1	1	3	3	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	2	1	1
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	3	4	4	1	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	1	2	2	6
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	3	3	3	3	3
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	3	4	3	3	3	3

Fuente: Autores

Figura 16. Mapa de calor - Seguridad en aplicaciones - Citrix Movilidad Teletrabajo



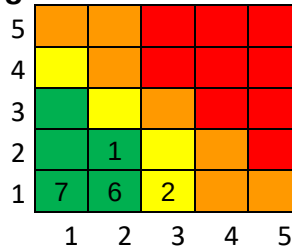
Fuente: Autores

Cuadro 16. Seguridad en redes - Citrix Movilidad Teletrabajo

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	3	1	2	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	1	2	2	2
✗	✗	✓	Desastres naturales	Si	1	2	2	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	3	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	2	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	2	3	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	1	2	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	2	1	1
✓	✓	✗	Trafico sensible sin protección	Si	1	3	3	3	3	3	3
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 17. Mapa de calor - Seguridad en redes - Citrix Movilidad Teletrabajo



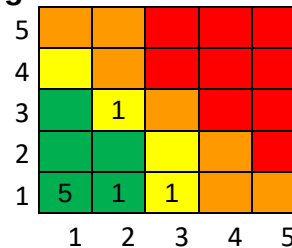
Fuente: Autores

Cuadro 17. Seguridad en internet - Citrix Movilidad Teletrabajo

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	1	1	1	1
✓	✓	✗	Suplantación de identidad en línea	Si	1	1	3	3	3	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	3	3	2	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	1	2	3	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 18. Mapa de calor - Seguridad en internet - Citrix Movilidad Teletrabajo



Fuente: Autores

Cuadro 18. Seguridad en Protección de infraestructura crítica - Citrix Movilidad XenMobile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

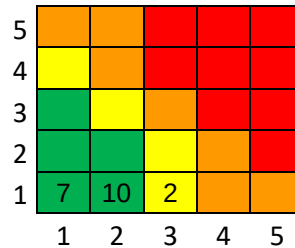
7.2.3 Citrix Movilidad XenMobile.

Cuadro 19. Seguridad en aplicaciones - Citrix Movilidad XenMobile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	3	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	1	2	3	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	1	3	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	3	3	3	2	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	3	1	3	2	2	2
✗	✓	✓	Fallas en el control de acceso	Si	1	2	1	2	1	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	3	1	2	2	2	2
✓	✓	✗	Exfiltración de información	Si	1	2	1	2	1	2	2
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	1	2	1	2	2
✗	✓	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	2	1	1	1	1	1
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	-	-	-	-	-	-	-
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	1	2	1	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	2	1	2	1	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 19. Mapa de calor - Seguridad en aplicaciones - Citrix Movilidad XenMobile



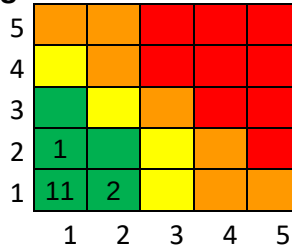
Fuente: Autores

Cuadro 20. Seguridad en redes - Citrix Movilidad XenMobile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	3	1	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	1	1	1	1	2
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	1	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	3	1	1	2	1	1
✗	✗	✓	Daños en los equipos de red	Si	1	2	1	1	2	1	1
✓	✓	✓	Abuso de privilegios	Si	1	2	1	2	1	1	1
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	1	3	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	1	2	1	2	1	1	1
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	No	-	-	-	-	-	-	-
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Tráfico sensible sin protección	No	-	-	-	-	-	-	-
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 20. Mapa de calor - Seguridad en redes - Citrix Movilidad XenMobile



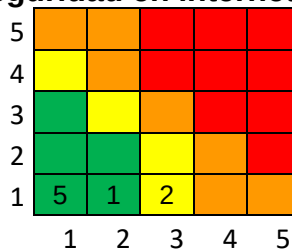
Fuente: Autores

Cuadro 21. Seguridad en internet - Citrix Movilidad XenMobile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	3	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	1	3	3	2	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	1	1	1	1	1
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	1	3	3	2	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 21. Mapa de calor – Seguridad en internet - Citrix Movilidad XenMobile



Fuente: Autores

Cuadro 22. Protección de infraestructura crítica - Citrix Movilidad XenMobile

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

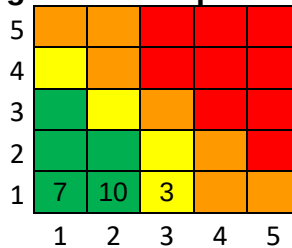
7.2.4 Citrix Movilidad Apps.

Cuadro 23. Seguridad en aplicaciones - Citrix Movilidad Apps

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	1	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	1	2	2
✓	✓	✓	Fallas operativas	Si	1	1	2	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	1	3	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	1	2	3	3	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	1	2	3	3	2	2
✗	✓	✓	Fallas en el control de acceso	Si	1	1	1	1	3	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	2	3	3	2	2
✓	✓	✗	Exfiltración de información	Si	1	1	3	3	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	2	1	1
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	1	3	1	3	2	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	1	2	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	3	3	3	3	3
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 22. Mapa de calor – Seguridad en aplicaciones - Citrix Movilidad Apps



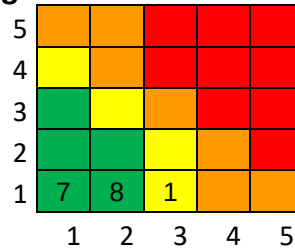
Fuente: Autores

Cuadro 24. Seguridad en redes - Citrix Movilidad Apps

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	1	2	2	1	2	2	2
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	1	2	2	2
✗	✗	✓	Desastres naturales	Si	1	2	2	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	3	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	2	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	2	3	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	1	2	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	2	1	1
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	2	3	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 23. Mapa de calor – Seguridad en redes - Citrix Movilidad Apps



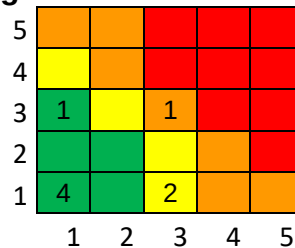
Fuente: Autores

Cuadro 25. Seguridad en internet - Citrix Movilidad Apps

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	1	1	1	1
✓	✓	✗	Suplantación de identidad en línea	Si	1	1	3	3	3	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	2	3	3	2	3	9
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	2	3	3	2	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	1	2	1	1	1	3

Fuente: Autores

Figura 24. Mapa de calor – Seguridad en internet - Citrix Movilidad Apps



Fuente: Autores

Cuadro 26. Protección de infraestructura crítica - Citrix Movilidad Apps

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

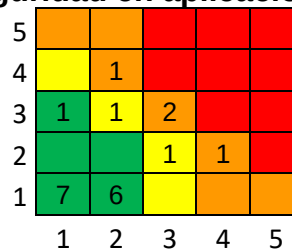
7.2.5 VPN Movilidad.

Cuadro 27. Seguridad en aplicaciones – VPN Movilidad

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Fallas operativas	Si	2	4	4	4	4	4	8
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	3	3	3	1	3	6
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	1	1	1
✓	✓	✗	Exfiltración de información	Si	1	1	1	2	1	1	1
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	3	1	2	1	1	1	3
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	3	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	2	1	2	8
✓	✓	✓	Versión del software desactualizada	Si	3	3	3	3	1	3	9
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	3	3	3	1	1	2	6
✓	✓	✗	Almacenamiento sin protección	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 25. Mapa de calor – Seguridad en aplicaciones – VPN Movilidad



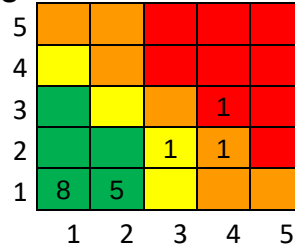
Fuente: Autores

Cuadro 28. Seguridad en redes – VPN Movilidad

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	2	4	4	4	4	4	8
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	4	4	4	4	4	12
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	1	1	1
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	2	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	2	3	3	3	1	3	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Trafico sensible sin protección	Si	1	1	2	3	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 26. Mapa de calor – Seguridad en redes – VPN Movilidad



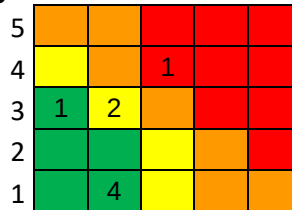
Fuente: Autores

Cuadro 29. Seguridad en internet – VPN Movilidad

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	3	1	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	2	2	2	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	3	1	1	1	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	3	3	3	3	12
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	1	1	1	1	3
✓	✓	✓	Ingeniería social	Si	1	2	2	2	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	3	1	1	2	6
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	3	3	1	1	2	2

Fuente: Autores

Figura 27. Mapa de calor – Seguridad en internet – VPN Movilidad



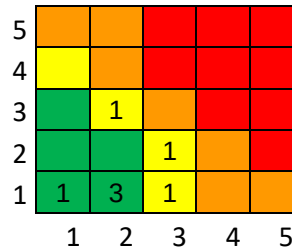
Fuente: Autores

Cuadro 30. Protección de infraestructura crítica – VPN Movilidad

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	2	2	1	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	2	3	3	3	2	3	6
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Falta de servidores redundantes	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de planes de continuidad	Si	1	2	1	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	3	3	3	3	3
✓	✓	✓	Incumplimiento Contractual	Si	1	2	2	3	2	2	2

Fuente: Autores

Figura 28. Mapa de calor – Protección de infraestructura crítica – VPN Movilidad



Fuente: Autores

7.2.6 Interpretación de los resultados del análisis de riesgos – Movilidad. De acuerdo con las tablas y mapas de riesgos obtenidos para las aplicaciones expuestas por el área de Movilidad, se evidencian varias aplicaciones que son críticas para el Banco tales como Citrix Movilidad Teletrabajo y VPN Movilidad, las cuales tienen riesgos clasificados como altos y extremos. Lo anterior corresponde a que estas aplicaciones establecen conexión directa hacia la infraestructura interna del Banco. Para las demás aplicaciones, su criticidad es media-baja toda vez que la mayoría de los riesgos están clasificados como bajos y medios.

7.3 ANALISIS DE RIESGOS – PLATAFORMAS CORE

En los siguientes numerales se encuentra el desarrollo del análisis de riesgos para la infraestructura expuesta en internet por parte de Plataformas Core. En los cuadros 31 al 42 se encuentra el detalle de este análisis, mientras que en las figuras 19 a la 39 se encuentra la cantidad de riesgos en total asociados a cada causa.

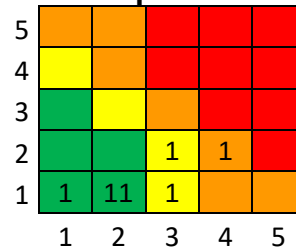
7.3.1 En Línea ACH PSE.

Cuadro 31. Seguridad en aplicaciones – En Línea ACH PSE

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	2	3	2	2	2
✓	✓	✓	Fallas operativas	Si	2	3	4	4	3	4	8
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	2	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	3	3	2	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	2	3	3	3	3	3
✓	✓	✓	Fallas en el control de acceso	Si	1	1	2	2	2	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✗	Exfiltración de información	Si	1	1	3	4	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	2	2	1	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	2	2	2	2	2
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	2	3	3	2	2	3	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	3	2	2	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✓	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	1	2	2	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	3	4	3	3	3
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	3	3	2	2

Fuente: Autores

Figura 29. Mapa de calor – Seguridad en aplicaciones – En Línea ACH PSE



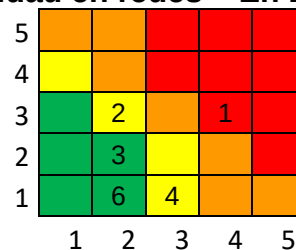
Fuente: Autores

Cuadro 32. Seguridad en redes – En Línea ACH PSE

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	3	3	4	3	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	3	2	1	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	2	1	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	2	1	2	2
✗	✗	✓	Daños en los equipos de red	Si	3	2	3	2	2	2	6
✓	✓	✓	Abuso de privilegios	Si	1	2	3	3	2	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	2	2	1	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	3	4	4	3	3	4	12
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	3	2	1	2	1	2	6
✓	✓	✓	Uso no autorizado	Si	1	1	3	3	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	2	1	1	2	2	2	4
✓	✓	✗	Tráfico sensible sin protección	Si	1	3	3	4	3	3	3
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	2	2	3	2	2	4
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	2	2	2

Fuente: Autores

Figura 30. Mapa de calor – Seguridad en redes – En Línea ACH PSE



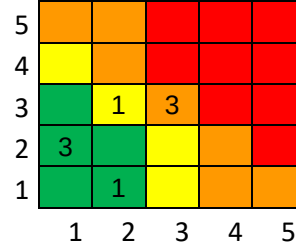
Fuente: Autores

Cuadro 33. Seguridad en redes – En Línea ACH PSE

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	3	2	1	1	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	3	3	3	4	2	3	9
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	1	1	1	1	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	3	3	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	2	1	1	1	1	1	2
✓	✓	✓	Ingeniería social	Si	3	3	3	3	2	3	9
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	1	1	1	1	2
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	1	3	3	3	3	9

Fuente: Autores

Figura 31. Mapa de calor – Seguridad en internet – En Línea ACH PSE



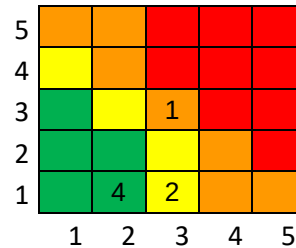
Fuente: Autores

Cuadro 34. Protección de infraestructura crítica – En Línea ACH PSE

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Fallas en las redes de comunicaciones	Si	3	2	3	3	3	3	9
✓	✓	✓	Fallas en el suministro eléctrico	Si	1	2	3	1	2	2	2
✓	✓	✓	Desastres naturales	Si	1	3	3	1	3	3	3
✓	✓	✓	Falta de servidores redundantes	Si	1	2	2	2	3	2	2
✓	✓	✓	Ausencia de planes de continuidad	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	3	2	2	2
✓	✓	✓	Incumplimiento Contractual	Si	1	4	3	3	3	3	3

Fuente: Autores

Figura 32. Mapa de calor – Protección de infraestructura crítica – En Línea ACH PSE



Fuente: Autores

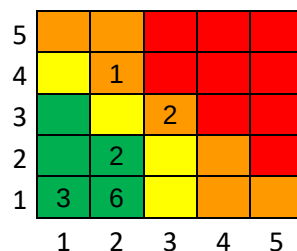
7.3.2 Gestión Cobranza (ICS).

Cuadro 35. Seguridad en aplicaciones – Gestión Cobranza (ICS)

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	4	4	3	3	3
✓	✓	✓	Fallas operativas	Si	3	2	3	3	2	3	9
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	2	1	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	3	3	2	2	3	3
✓	✓	✓	Fallas en el control de acceso	Si	1	2	2	2	1	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	3	2	3	3	3
✓	✓	✓	Exfiltración de información	Si	1	1	3	3	3	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	2	2	3	2	2
✓	✓	✓	Falta de backups de la aplicación	Si	1	1	2	2	3	2	2
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	2	1	2	2	2	2	4
✓	✓	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	2	2	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	1	1	1	1	1
✓	✓	✓	Versión del software desactualizada	Si	4	2	3	2	1	2	8
✓	✓	✓	Incumplimiento en el mantenimiento de la aplicación	Si	2	1	2	2	1	2	4
✓	✓	✓	Almacenamiento sin protección	Si	1	1	3	3	2	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 33. Mapa de calor – Seguridad en aplicaciones – Gestión Cobranza (ICS)



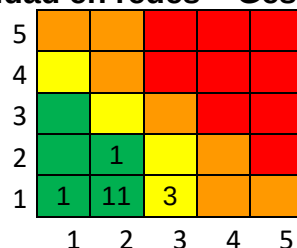
Fuente: Autores

Cuadro 36. Seguridad en redes – Gestión Cobranza (ICS)

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	3	3	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	2	2	2	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	1	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	3	1	2	3	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	1	2	1	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	2	2	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	2	1	2	2	2	2
✓	✓	✓	Uso no autorizado	Si	1	3	2	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	2	1	2	1	2	2
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	3	3	3	3	3
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	2	2	2
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 34. Mapa de calor – Seguridad en redes – Gestión Cobranza (ICS)



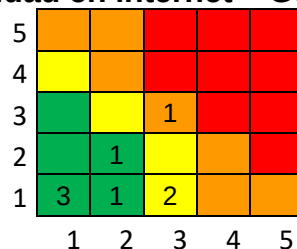
Fuente: Autores

Cuadro 37. Seguridad en internet – Gestión Cobranza (ICS)

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	3	1	2	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	3	2	3	3	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	3	3	1	2	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	3	2	3	2	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	1	3	3	3	3	9

Fuente: Autores

Figura 35. Mapa de calor – Seguridad en internet – Gestión Cobranza (ICS)



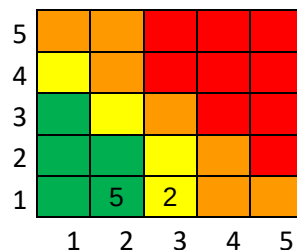
Fuente: Autores

Cuadro 38. Protección de infraestructura crítica – Gestión Cobranza (ICS)

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	1	2	3	3	3	3	3
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	2	3	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Falta de servidores redundantes	Si	1	3	2	2	2	2	2
✗	✗	✓	Ausencia de planes de continuidad	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	2	3	2	2	2
✓	✓	✓	Incumplimiento Contractual	Si	1	4	3	3	3	3	3

Fuente: Autores

Figura 36. Mapa de calor – Protección de infraestructura crítica – Gestión Cobranza (ICS)



Fuente: Autores

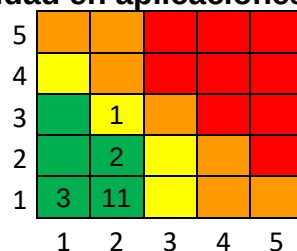
7.3.3 Aula Financiera.

Cuadro 39. Seguridad en aplicaciones – Aula Financiera

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	2	2	2	1	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	3	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	3	2	3	2	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	3	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	1	1	1	2	2	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	2	2	2
✓	✗	✗	Exfiltración de información	Si	1	1	1	3	3	2	2
✓	✗	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✗	✗	✗	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✗	✗	✗	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	2	2	2
✗	✗	✗	Ausencia de documentación	No	-	-	-	-	-	-	-
✓	✓	✓	Mal funcionamiento del software	Si	1	2	2	2	2	2	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	1	3	2	2	6
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	2	3	3	1	1	2	4
✓	✓	✓	Almacenamiento sin protección	Si	1	1	3	2	2	2	2
✗	✗	✗	Falta de monitoreo a la aplicación	No	-	-	-	-	-	-	-

Fuente: Autores

Figura 37. Mapa de calor – Seguridad en aplicaciones – Aula Financiera



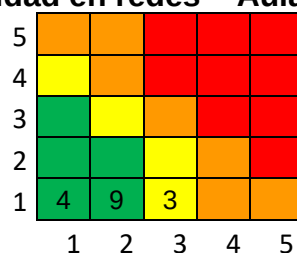
Fuente: Autores

Cuadro 40. Seguridad en redes – Aula Financiera

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	3	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	1	2	2	2	1	2	2
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	1	1	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	3	2	2	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	2	1	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	2	1	2	1	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	2	1	2	1	2	2
✓	✓	✓	Uso no autorizado	Si	1	3	2	3	2	3	3
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	1	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	2	2	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✗	✗	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 38. Mapa de calor – Seguridad en redes – Aula Financiera



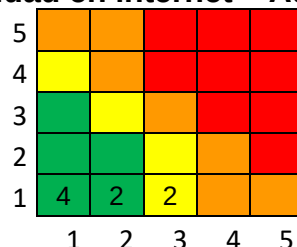
Fuente: Autores

Cuadro 41. Seguridad en internet – Aula Financiera

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	2	1	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	3	3	3	2	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	2	1	1	1	1	1
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	3	2	2	2	2	2
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	2	1	1	1	1	1
✓	✓	✓	Ingeniería social	Si	1	3	2	3	2	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	2	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 39. Mapa de calor – Seguridad en internet – Aula Financiera



Fuente: Autores

Cuadro 42. Protección de infraestructura crítica – Aula Financiera

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
×	×	×	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
×	×	×	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
×	×	×	Desastres naturales	No	N/A	-	-	-	-	-	-
×	×	×	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
×	×	×	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
×	×	×	Abuso de privilegios	No	N/A	-	-	-	-	-	-
×	×	×	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

7.3.4 Interpretación de los resultados del análisis de riesgos – Plataformas Core. De acuerdo con las tablas y mapas de riesgos obtenidos para las aplicaciones expuestas por el área de Plataformas Core, se evidencia que las aplicaciones En Línea ACH PSE y Gestión Cobranza (ICS) son críticas para el Banco teniendo en cuenta que se encontraron riesgos categorizados como altos. Esto se debe a que en la primera aplicación en cuestión se efectúan transacciones monetarias, mientras que en la segunda se gestiona la cartera vencida del Banco. La aplicación Aula Financiera no es crítica para el negocio dado que la mayoría de los riesgos encontrados tienen un nivel de riesgo bajo.

7.4 ANÁLISIS DE RIESGOS – PLATAFORMAS NO CORE

En los siguientes numerales se encuentra el desarrollo del análisis de riesgos para la infraestructura expuesta en internet por parte de Plataformas No Core. En los cuadros 43 al 90 se encuentra el detalle de este análisis, mientras que en las figuras 40 a la 80 se encuentra la cantidad de riesgos en total asociados a cada causa.

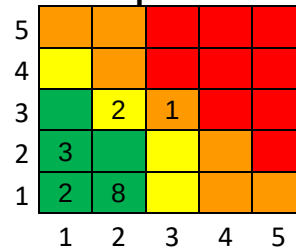
7.4.1 Correo Electrónico Banco Agrario.

Cuadro 43. Seguridad en aplicaciones – Correo Electrónico

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	3	2	3	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	3	2	2	2	2	2
✓	✓	✓	Fallas operativas	Si	3	2	2	2	2	2	6
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	3	2	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	2	1	2	2
✓	✓	✓	Ejecución de malware	Si	3	3	2	3	2	3	9
✓	✓	✓	Usuarios malintencionados	Si	1	2	2	2	1	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	2	1	1	1	1	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	1	2	2	2	2
✓	✓	✗	Exfiltración de información	Si	1	1	3	3	3	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	2	2	1	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	2	1	1	1	1
✗	✗	✗	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	No	-	-	-	-	-	-	-
✗	✗	✓	Ausencia de documentación	Si	2	1	1	1	1	1	2
✓	✓	✓	Mal funcionamiento del software	Si	3	2	2	1	1	2	6
✓	✓	✗	Falta de concientización de políticas de seguridad de la información	Si	2	1	2	1	1	1	2
✓	✓	✓	Versión del software desactualizada	Si	1	2	2	1	1	2	2
✗	✗	✗	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	3	1	2	2
✓	✓	✓	Almacenamiento sin protección	Si	1	1	2	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 40. Mapa de calor – Seguridad en aplicaciones – Correo Electrónico



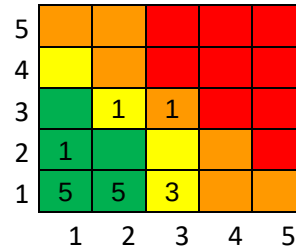
Fuente: Autores

Cuadro 44. Seguridad en redes – Correo Electrónico

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	3	3	2	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	2	2	2	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	2	3	3	3
✗	✗	✓	Daños en los equipos de red	Si	1	3	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	2	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	3	3	3	2	2	3	9
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	2	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	2	1	1	1
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	3	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	1	1	1	1	1	2
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 41. Mapa de calor – Seguridad en redes – Correo Electrónico



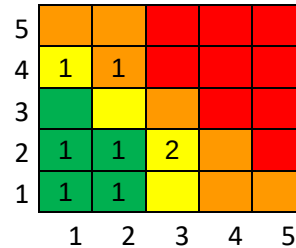
Fuente: Autores

Cuadro 45. Seguridad en internet – Correo Electrónico

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	3	2	1	1	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	2	1	3	3	3	3	6
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	1	1	1	1	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	2	2	1	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	4	1	1	1	1	1	4
✓	✓	✓	Ingeniería social	Si	2	2	4	4	2	3	6
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	1	1	1	1
✗	✗	✓	Fallas en redes de comunicaciones	Si	4	3	1	1	1	2	8

Fuente: Autores

Figura 42. Mapa de calor – Seguridad en internet – Correo Electrónico



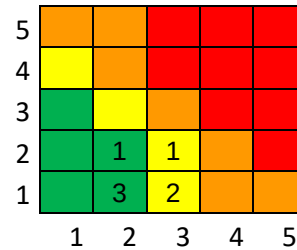
Fuente: Autores

Cuadro 46. Protección de infraestructura crítica – Correo Electrónico

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	3	3	2	2	3	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	3	3	1	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Falta de servidores redundantes	Si	2	2	2	1	2	2	4
✗	✗	✓	Ausencia de planes de continuidad	Si	1	3	3	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	3	3	2	2	3	3
✗	✗	✓	Incumplimiento contractual	Si	1	3	3	3	2	3	3

Fuente: Autores

Figura 43. Mapa de calor – Protección de infraestructura crítica – Correo Electrónico



Fuente: Autores

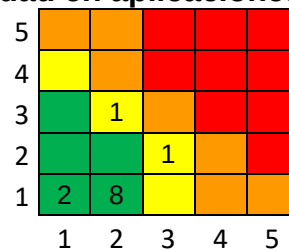
7.4.2 Depósitos Judiciales.

Cuadro 47. Seguridad en aplicaciones – Depósitos Judiciales

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	3	3	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	2	3	2	2	2
✓	✓	✓	Fallas operativas	Si	2	2	2	3	4	3	6
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	3	3	2	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	2	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	3	3	2	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	2	3	3	2	3	3
✓	✓	✓	Fallas en el control de acceso	Si	1	2	2	2	1	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	3	2	2	2	2
✓	✓	✗	Exfiltración de información	Si	1	1	3	4	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	3	1	2	2
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	3	3	2	2	1	2	6
✓	✓	✓	Mal funcionamiento del software	Si	1	2	3	3	2	3	3
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	3	4	3	3	3
✓	✓	✓	Versión del software desactualizada	Si	1	1	2	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	2	1	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	3	3	3	3	3
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	1	2	1	1

Fuente: Autores

Figura 44. Mapa de calor – Seguridad en aplicaciones – Depósitos Judiciales



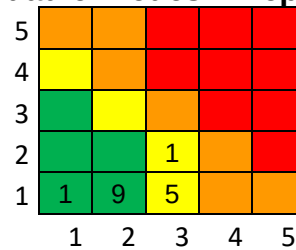
Fuente: Autores

Cuadro 48. Seguridad en redes – Depósitos Judiciales

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	3	3	2	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	3	3	2	3	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	3	2	3	3
✗	✗	✓	Desastres naturales	Si	1	3	3	3	3	3	3
✗	✗	✓	Daños en los equipos de red	Si	1	2	3	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	2	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	2	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	2	2	1	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	2	1	2	1	2	2
✓	✓	✓	Uso no autorizado	Si	1	2	2	3	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	2	1	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	2	3	2	2	2
✓	✓	✗	Trafico sensible sin protección	Si	1	1	3	3	3	3	3
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	2	2	2
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 45. Mapa de calor – Seguridad en redes – Depósitos Judiciales



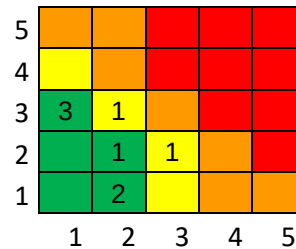
Fuente: Autores

Cuadro 49. Seguridad en internet – Depósitos Judiciales

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	2	2	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	2	1	3	3	2	2	4
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	1	1	1	1	3
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	1	2	2	2
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	1	2	1	3
✓	✓	✓	Ingeniería social	Si	2	2	3	3	2	3	6
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	1	1	1	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	2	2	1	1	2	6

Fuente: Autores

Figura 46. Mapa de calor – Seguridad en internet – Depósitos Judiciales



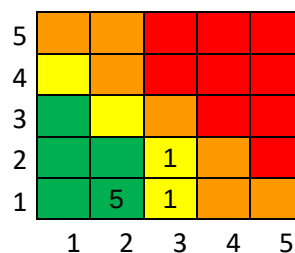
Fuente: Autores

Cuadro 50. Protección de infraestructura crítica – Depósitos Judiciales

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	3	3	3	3	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	2	3	1	3	2	2
✗	✗	✓	Falta de servidores redundantes	Si	1	2	2	2	2	2	2
✗	✗	✓	Ausencia de planes de continuidad	Si	1	1	2	3	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	3	2	2	2
✓	✓	✓	Incumplimiento contractual	Si	1	3	3	3	2	3	3

Fuente: Autores

Figura 47. Mapa de calor – Protección de infraestructura crítica – Depósitos Judiciales



Fuente: Autores

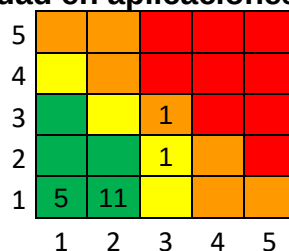
7.4.3 Portal Web Banco Agrario.

Cuadro 51. Seguridad en aplicaciones – Portal Web

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	3	3	2	2	3	6
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	3	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	2	1	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	3	2	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	1	2	2	2	1	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	4	3	3	3	3
✓	✓	✗	Exfiltración de información	Si	1	1	1	2	2	2	2
✓	✓	✗	Gestión de usuarios deficiente	Si	1	2	2	2	1	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	2	1	1
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	3	1	3	9
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✓	✓	✓	Versión del software desactualizada	Si	1	1	2	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	1	2	1	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	1	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 48. Mapa de calor – Seguridad en aplicaciones – Portal Web



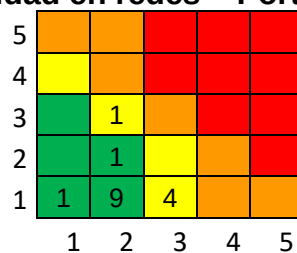
Fuente: Autores

Cuadro 52. Seguridad en redes – Portal Web

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	3	3	3	2	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	2	2	2	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	1	1	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	2	3	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	2	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	3	2	3	2	3	3
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	3	2	2	2	2
✓	✓	✓	Uso no autorizado	Si	1	2	2	3	3	3	3
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	2	2	2	2	2	2
✓	✓	✗	Trafico sensible sin protección	Si	1	1	2	2	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	3	2	1	2	2	2	6

Fuente: Autores

Figura 49. Mapa de calor – Seguridad en redes – Portal Web



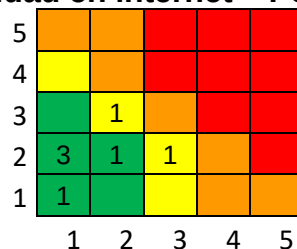
Fuente: Autores

Cuadro 53. Seguridad en internet – Portal Web

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	1	1	1	1
✗	✗	✗	Suplantación de identidad en línea	No	-	-	-	-	-	-	-
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	1	1	1	1	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	2	2	3	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	2	1	1	1	1	1	2
✓	✓	✓	Ingeniería social	Si	2	2	4	2	3	3	6
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	1	1	1	1	2
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	2	2	1	1	2	6

Fuente: Autores

Figura 50. Mapa de calor – Seguridad en internet – Portal Web



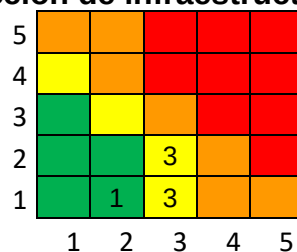
Fuente: Autores

Cuadro 54. Protección de infraestructura crítica – Portal Web

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	3	4	3	3	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	4	3	3	3
✗	✗	✓	Desastres naturales	Si	1	3	3	2	2	3	3
✗	✗	✓	Falta de servidores redundantes	Si	2	2	3	4	3	3	6
✗	✗	✓	Ausencia de planes de continuidad	Si	2	2	3	4	3	3	6
✓	✓	✓	Abuso de privilegios	Si	1	2	2	3	2	2	2
✗	✗	✓	Incumplimiento contractual	Si	1	3	3	3	2	3	3

Fuente: Autores

Figura 51. Mapa de calor – Protección de infraestructura crítica – Portal Web



Fuente: Autores

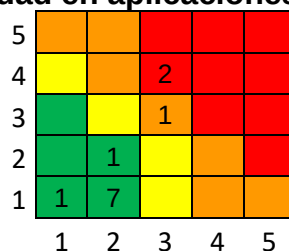
7.4.4 Banca Virtual Banco Agrario.

Cuadro 55. Seguridad en aplicaciones – Banca Virtual

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	3	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	3	4	3	3	3
✓	✓	✓	Fallas operativas	Si	4	4	3	3	3	3	12
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	4	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	2	3	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	1	3	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	3	2	3	2	3	3
✓	✓	✓	Fallas en el control de acceso	Si	3	3	3	3	2	3	9
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	3	4	3	3	3	3
✓	✓	✓	Exfiltración de información	Si	1	1	4	4	3	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	2	2	2	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	2	2	2	2	2	2
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	3	2	2	1	2	2
✗	✗	✓	Ausencia de documentación	Si	1	1	2	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	4	4	3	3	3	3	12
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	2	3	3	3	3	3
✓	✓	✓	Versión del software desactualizada	Si	1	2	2	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	2	2	2	2
✓	✓	✗	Almacenamiento sin protección	Si	1	1	3	4	3	3	3
✓	✓	✓	Falta de monitoreo a la aplicación	Si	2	2	1	2	1	2	4

Fuente: Autores

Figura 52. Mapa de calor – Seguridad en aplicaciones – Banca Virtual



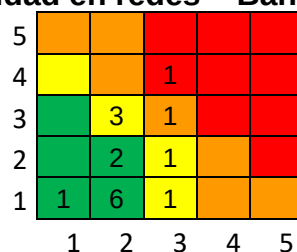
Fuente: Autores

Cuadro 56. Seguridad en redes – Banca Virtual

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	3	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	4	2	3	3	2	3	12
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	2	3	1	3	3	3	6
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	1	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	3	2	2	2	1	2	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	2	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	2	3	1	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	3	1	2	2	2	2	6
✗	✗	✓	Falta de dispositivos redundantes	Si	3	1	1	2	3	2	6
✓	✓	✗	Tráfico sensible sin protección	Si	3	2	4	3	4	3	9
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	1	2	3	2	2	4
✓	✓	✓	Ausencia de control de cambios	Si	2	1	2	2	1	2	4

Fuente: Autores

Figura 53. Mapa de calor – Seguridad en redes – Banca Virtual



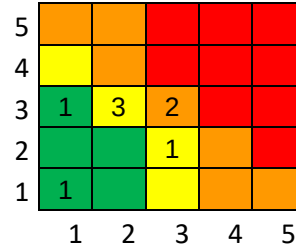
Fuente: Autores

Cuadro 57. Seguridad en internet – Banca Virtual

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	1	1	1	1
✓	✓	✓	Suplantación de identidad en línea	Si	3	2	4	4	3	3	9
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	3	1	1	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	4	3	3	3	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	2	1	2	6
✓	✓	✓	Ingeniería social	Si	3	1	4	4	3	3	9
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	2	1	1	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	3	2	2	1	2	6

Fuente: Autores

Figura 54. Mapa de calor – Seguridad en internet – Banca Virtual



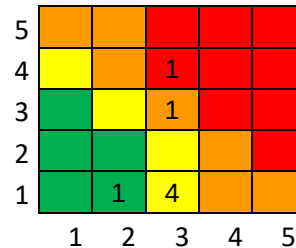
Fuente: Autores

Cuadro 58. Protección de infraestructura crítica – Banca Virtual

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	4	2	3	3	3	3	12
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	3	3	3	3
✗	✗	✓	Desastres naturales	Si	1	3	3	3	3	3	3
✗	✗	✓	Falta de servidores redundantes	Si	3	2	2	3	3	3	9
✓	✓	✓	Ausencia de planes de continuidad	Si	1	2	3	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	3	3	2	3	3
✓	✓	✓	Incumplimiento contractual	Si	1	3	3	3	2	3	3

Fuente: Autores

Figura 55. Mapa de calor – Protección de infraestructura crítica – Banca Virtual



Fuente: Autores

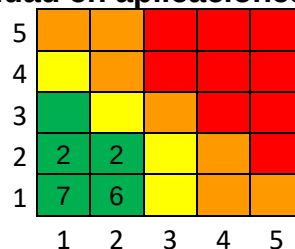
7.4.5 ADFS.

Cuadro 59. Seguridad en aplicaciones – ADFS

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	4	2	2	2	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Fallas operativas	Si	2	3	2	2	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	4	2	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	2	1	2	1	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	1	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	1	2	1	1	1	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	2	2	1	2	2
✓	✓	✓	Exfiltración de información	Si	1	3	3	3	1	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	1	1	1	1	1
✗	✗	✓	Ausencia de documentación	Si	2	1	1	1	1	1	2
✓	✓	✓	Mal funcionamiento del software	Si	2	3	3	2	1	2	4
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	1	1	1	1
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	1	1	1
✓	✓	✓	Almacenamiento sin protección	Si	1	1	3	2	1	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 56. Mapa de calor – Seguridad en aplicaciones – ADFS



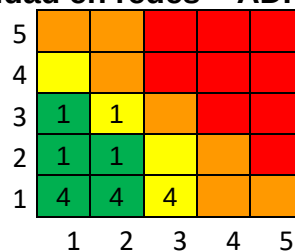
Fuente: Autores

Cuadro 60. Seguridad en redes – ADFS

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	4	2	3	2	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	2	2	2	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	2	3	3	3
✗	✗	✓	Daños en los equipos de red	Si	1	3	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	4	3	3	2	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	2	1	2	2	1	2	4
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	3	3	2	2	3	3
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	3	1	1	2	1	1	3
✓	✓	✓	Trafico sensible sin protección	Si	1	2	2	2	2	2	2
✓	✓	✓	Falta de monitoreo al tráfico de las redes	Si	2	2	1	1	1	1	2
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 57. Mapa de calor – Seguridad en redes – ADFS



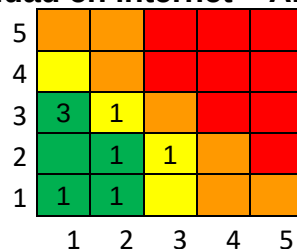
Fuente: Autores

Cuadro 61. Seguridad en internet – ADFS

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	1	1	1	1
✓	✓	✓	Suplantación de identidad en línea	Si	2	1	4	3	2	3	6
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	1	2	1	1	3
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	2	2	1	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	1	1	1	3
✓	✓	✓	Ingeniería social	Si	1	1	3	2	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	1	1	1	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	3	2	2	1	2	6

Fuente: Autores

Figura 58. Mapa de calor – Seguridad en internet – ADFS



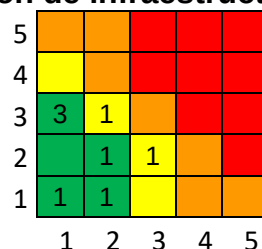
Fuente: Autores

Cuadro 62. Protección de infraestructura crítica – ADFS

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	3	2	2	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	3	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	2	2	2	2	2
✗	✗	✓	Falta de servidores redundantes	Si	2	2	2	1	2	2	4
✗	✗	✓	Ausencia de planes de continuidad	Si	1	3	3	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	3	3	2	2	3	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	3	2	2	1	2	6

Fuente: Autores

Figura 59. Mapa de calor – Protección de infraestructura crítica – ADFS



Fuente: Autores

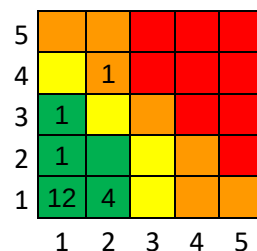
7.4.6 Conéctate al Conocimiento.

Cuadro 63. Seguridad en aplicaciones – Conéctate al Conocimiento

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	1	1	3	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✗	✗	✓	Fallas operativas	Si	3	1	1	1	1	1	3
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	1	3	3	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	1	1	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	1	1	1	1
✓	✓	✓	Fallas en el control de acceso	Si	1	1	1	1	1	1	1
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	1	1	1	1
✓	✓	✓	Exfiltración de información	Si	1	1	1	1	1	1	1
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	2	1	1	1	1
✗	✗	✓	Ausencia de documentación	Si	2	1	2	1	1	1	2
✓	✓	✓	Mal funcionamiento del software	Si	4	1	3	1	1	2	8
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	-	-	-	-	-	-	-
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	1	1	1	1
✓	✓	✓	Almacenamiento sin protección	Si	1	1	1	1	1	1	1
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 60. Mapa de calor – Seguridad en aplicaciones – Conéctate al Conocimiento



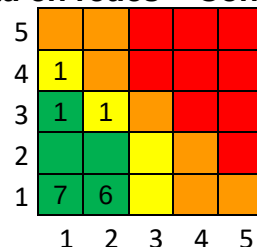
Fuente: Autores

Cuadro 64. Seguridad en aplicaciones – Conéctate al Conocimiento

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	1	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	4	1	2	1	1	1	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	1	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	1	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	1	1	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	1	1	1
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	1	1	4	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	3	1	2	2	1	2	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	3	1	1	1	1	1	3
✓	✓	✗	Trafico sensible sin protección	Si	1	1	1	3	1	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 61. Mapa de calor – Seguridad en redes – Conéctate al Conocimiento



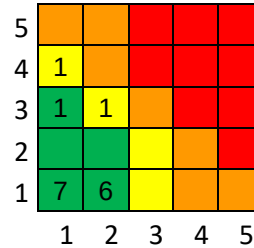
Fuente: Autores

Cuadro 65. Seguridad en internet – Conéctate al Conocimiento

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	3	2	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	1	1	1	2	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	1	1	1	1	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	1	3	2	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	1	1	3
✓	✓	✓	Ingeniería social	Si	1	1	1	3	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	1	1	1	1	2
✗	✗	✓	Fallas en redes de comunicaciones	Si	2	3	2	2	1	2	4

Fuente: Autores

Figura 62. Mapa de calor – Seguridad en internet – Conéctate al Conocimiento



Fuente: Autores

Cuadro 66. Protección de infraestructura crítica – Conéctate al Conocimiento

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en redes de comunicaciones	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

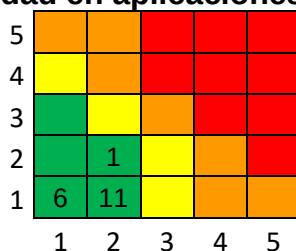
7.4.7 Portal Tu Referido.

Cuadro 67. Seguridad en aplicaciones – Portal Tu Referido

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	1	2	1	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	1	3	3	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	1	1	1	1	2	1	1
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✓	Exfiltración de información	Si	1	1	1	3	1	2	2
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	2	1	1	1
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	2	2	1	2	2
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	1	1	2	2	2	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	1	3	3	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	1	2	1	1
✓	✓	✓	Almacenamiento sin protección	Si	1	1	1	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	2	2	2

Fuente: Autores

Figura 63. Mapa de calor – Seguridad en aplicaciones – Portal Tu Referido



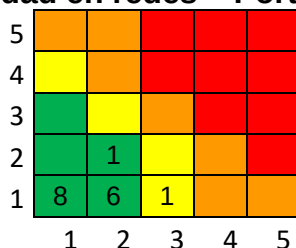
Fuente: Autores

Cuadro 68. Seguridad en redes – Portal Tu Referido

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	1	2	3	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	1	1	2	2	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	1	1	2	1	1
✗	✗	✓	Desastres naturales	Si	1	2	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	1	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	1	1	1	1	1
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✓	Trafico sensible sin protección	Si	1	1	2	3	3	2	2
✓	✓	✓	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 64. Mapa de calor – Seguridad en redes – Portal Tu Referido



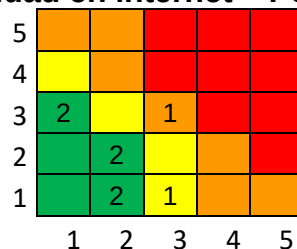
Fuente: Autores

Cuadro 69. Seguridad en internet – Portal Tu Referido

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	2	2	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	1	2	2	2	3	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	1	1	1	1	3
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	2	1	2	3	2	2	4
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	1	1	3
✓	✓	✓	Ingeniería social	Si	1	1	3	3	3	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	2	2	2	2	4
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	1	3	3	3	3	9

Fuente: Autores

Figura 65. Mapa de calor – Seguridad en internet – Portal Tu Referido



Fuente: Autores

Cuadro 70. Protección de infraestructura crítica – Portal Tu Referido

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

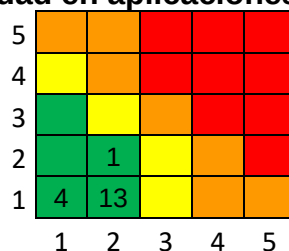
7.4.8 Portal Vivienda.

Cuadro 71. Seguridad en aplicaciones – Portal Vivienda

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	2	2	3	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	1	2	3	3	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	2	3	3	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	1	1	2	2	1	2	2
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	2	2	2	2	2
✓	✓	✓	Exfiltración de información	Si	1	2	2	3	2	2	2
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	1	1	1	2	1	1	1
✓	✓	✓	Mal funcionamiento del software	Si	1	1	2	3	2	2	2
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	2	2	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	2	2	2	2	2
✓	✓	✓	Almacenamiento sin protección	Si	1	1	2	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	2	2	1	2	2

Fuente: Autores

Figura 66. Mapa de calor – Seguridad en aplicaciones – Portal Vivienda



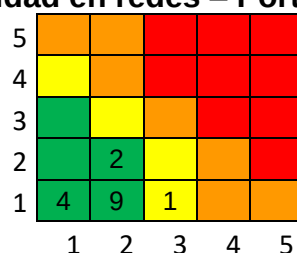
Fuente: Autores

Cuadro 72. Seguridad en redes – Portal Vivienda

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	1	3	3	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	1	2	3	1	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	1	2	1	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	1	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	2	2	2	2	1	2	4
✓	✓	✗	Trafico sensible sin protección	Si	1	2	2	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 67. Mapa de calor – Seguridad en redes – Portal Vivienda



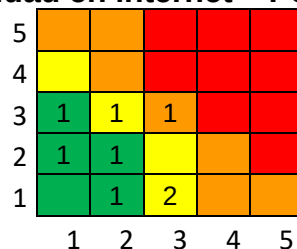
Fuente: Autores

Cuadro 73. Seguridad en internet – Portal Vivienda

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	2	4	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	1	1	2	3	4	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	2	2	2	2	4
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	3	3	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	1	1	3
✓	✓	✓	Ingeniería social	Si	1	1	3	3	3	3	3
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	1	1	2	1	2
✗	✗	✓	Fallas en redes de comunicaciones	Sí	3	1	3	3	3	3	9

Fuente: Autores

Figura 68. Mapa de calor – Seguridad en internet – Portal Vivienda



Fuente: Autores

Cuadro 74. Protección de infraestructura crítica – Portal Vivienda

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	Si	1	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

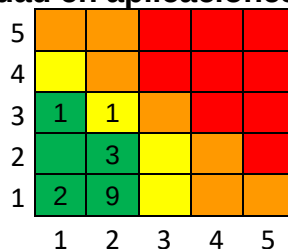
7.4.9 Portal Clientes.

Cuadro 75. Seguridad en aplicaciones – Portal Clientes

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	4	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	2	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	3	1	2	3	2	2	6
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	4	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	2	1	1	2	2	2	4
✓	✓	✓	Ejecución de malware	Si	1	2	2	4	3	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	1	1	2	2	2	4
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	2	3	2	2	2
✓	✓	✓	Exfiltración de información	Si	1	1	3	4	3	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Falta de backups de la aplicación	Si	1	1	1	2	2	2	2
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	3	1	2	2
✗	✗	✓	Ausencia de documentación	Si	3	1	1	2	1	1	3
✓	✓	✓	Mal funcionamiento del software	Si	2	1	2	3	2	2	4
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	3	3	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	3	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✓	Almacenamiento sin protección	Si	1	1	2	2	1	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 69. Mapa de calor – Seguridad en aplicaciones – Portal Clientes



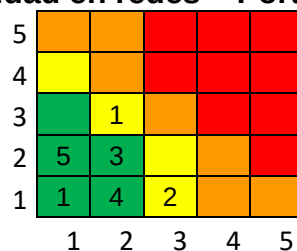
Fuente: Autores

Cuadro 76. Seguridad en redes – Portal Clientes

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	3	3	3	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	1	2	2	2	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	2	2	2	2	2	2	4
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	2	1	2	2	2	2	4
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	2	1	1	2	1	1	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	1	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	2	1	1	2	2	2	4
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	2	1	1	2	1	1	2
✗	✗	✓	Falta de dispositivos redundantes	Si	2	1	1	2	1	1	2
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	1	2	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	1	1	2	1	1	2
✓	✓	✓	Ausencia de control de cambios	Si	2	1	1	2	1	1	2

Fuente: Autores

Figura 70. Mapa de calor – Seguridad en redes – Portal Clientes



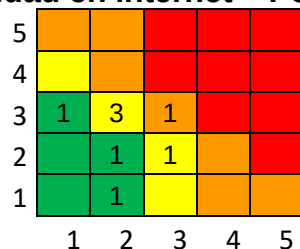
Fuente: Autores

Cuadro 77. Seguridad en internet – Portal Clientes

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	3	3	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	2	2	3	4	3	3	6
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	1	2	2	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	3	2	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	2	2	6
✓	✓	✓	Ingeniería social	Si	2	1	3	3	2	2	4
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	1	2	1	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	1	3	3	3	3	9

Fuente: Autores

Figura 71. Mapa de calor – Seguridad en internet – Portal Clientes



Fuente: Autores

Cuadro 78. Protección de infraestructura crítica – Portal Clientes

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

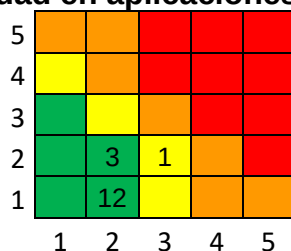
7.4.10 Ingreso Solidario.

Cuadro 79. Seguridad en aplicaciones – Ingreso Solidario

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	4	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	2	2	3	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	2	3	4	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	2	3	3	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	1	1	2	2	2	4
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	2	2	3	2	2
✓	✓	✓	Exfiltración de información	Si	1	1	2	3	4	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	2	3	2	2
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	2	2	2
✗	✗	✓	Ausencia de documentación	Si	2	1	1	2	2	2	4
✓	✓	✓	Mal funcionamiento del software	Si	2	2	2	3	3	3	3
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	3	3	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✓	Almacenamiento sin protección	Si	1	1	1	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	2	2	2

Fuente: Autores

Figura 72. Mapa de calor – Seguridad en aplicaciones – Ingreso Solidario



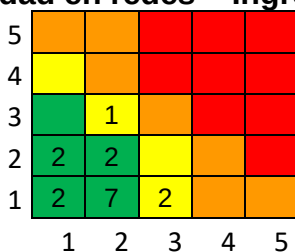
Fuente: Autores

Cuadro 80. Seguridad en redes – Ingreso Solidario

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	3	3	2	3	3
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	1	2	3	1	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	1	2	1	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	2	2	1	2	1	2	4
✗	✗	✓	Falta de dispositivos redundantes	Si	2	2	2	2	1	2	4
✓	✓	✗	Trafico sensible sin protección	Si	1	2	2	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	1	1	2	1	1	2
✓	✓	✓	Ausencia de control de cambios	Si	2	1	1	2	1	1	2

Fuente: Autores

Figura 73. Mapa de calor – Seguridad en redes – Ingreso Solidario



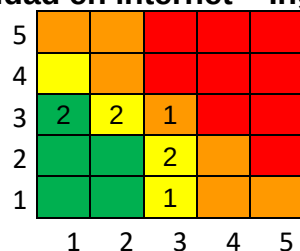
Fuente: Autores

Cuadro 81. Seguridad en internet – Ingreso Solidario

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Sí	1	2	3	2	4	3	3
✓	✓	✓	Suplantación de identidad en línea	Sí	2	1	2	3	4	3	6
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Sí	3	1	2	2	2	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Sí	3	1	2	3	3	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Sí	3	1	1	2	1	1	3
✓	✓	✓	Ingeniería social	Sí	2	1	3	3	3	3	6
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Sí	3	1	1	1	2	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Sí	3	1	3	3	3	3	9

Fuente: Autores

Figura 74. Mapa de calor – Seguridad en internet – Ingreso Solidario



Fuente: Autores

Cuadro 82. Protección de infraestructura crítica – Ingreso Solidario

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

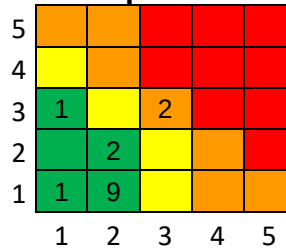
7.4.11 Consulta Giros.

Cuadro 83. Seguridad en aplicaciones – Consulta Giros

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	3	3	3	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	2	2	2	2	2
✓	✓	✓	Fallas operativas	Si	3	2	3	3	3	3	9
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	3	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	2	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	3	3	3	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	2	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	1	2	2	1	2	4
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	3	2	3	3	3
✓	✓	✓	Exfiltración de información	Si	1	2	3	2	3	3	3
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	2	2	1	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	2	2	1	2	2
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	2	2	1	2	2
✗	✗	✓	Ausencia de documentación	Si	3	1	1	1	1	1	3
✓	✓	✓	Mal funcionamiento del software	Si	3	2	3	3	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	3	3	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	2	1	1	1	1
✓	✓	✓	Almacenamiento sin protección	Si	1	1	3	3	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	2	1	2	2	1	2	4

Fuente: Autores

Figura 75. Mapa de calor – Seguridad en aplicaciones – Consulta Giros



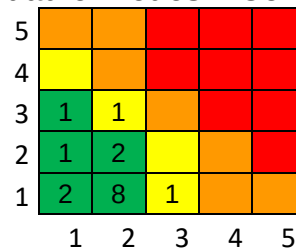
Fuente: Autores

Cuadro 84. Seguridad en redes – Consulta Giros

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	1	3	3	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	1	2	3	1	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	2	2	2	2	2	2	4
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	2	1	1	2	1	1	2
✓	✓	✓	Uso no autorizado	Si	1	2	1	2	1	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	2	2	1	2	1	2	4
✗	✗	✓	Falta de dispositivos redundantes	Si	1	2	2	2	1	2	2
✓	✓	✗	Trafico sensible sin protección	Si	1	2	2	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	3	1	1	2	1	1	3
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 76. Mapa de calor – Seguridad en redes – Consulta Giros



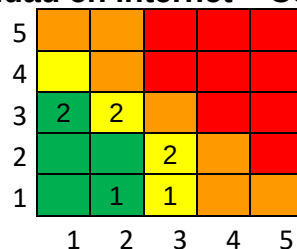
Fuente: Autores

Cuadro 85. Seguridad en internet – Consulta Giros

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	1	2	4	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	1	1	2	3	4	3	3
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	2	2	2	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	3	3	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	1	1	3
✓	✓	✓	Ingeniería social	Si	2	1	3	3	3	3	6
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	1	1	2	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	2	1	3	3	3	3	6

Fuente: Autores

Figura 77. Mapa de calor – Seguridad en internet – Consulta Giros



Fuente: Autores

Cuadro 86. Protección de infraestructura crítica – Consulta Giros

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

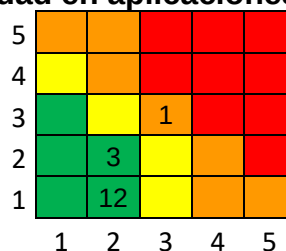
7.4.12 Portal PAEF.

Cuadro 87. Seguridad en aplicaciones – Portal PAEF

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	3	4	3	3
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2
✓	✓	✓	Fallas operativas	Si	2	2	2	3	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	3	3	3	3
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	2	2	2
✓	✓	✓	Ejecución de malware	Si	1	2	2	3	4	3	3
✓	✓	✓	Usuarios malintencionados	Si	1	1	2	3	3	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	1	1	2	2	2	4
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	2	2	2	3	2	2
✓	✓	✓	Exfiltración de información	Si	1	1	2	3	4	3	3
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	2	3	2	2
✗	✗	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	3	2	2
✗	✗	✓	Ausencia de documentación	Si	2	1	1	2	2	2	4
✓	✓	✓	Mal funcionamiento del software	Si	3	2	2	3	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	1	1	2	3	3	2	2
✓	✓	✓	Versión del software desactualizada	Si	1	1	1	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2
✓	✓	✓	Almacenamiento sin protección	Si	1	1	1	2	2	2	2
✓	✓	✗	Falta de monitoreo a la aplicación	Si	1	1	1	2	2	2	2

Fuente: Autores

Figura 78. Mapa de calor – Seguridad en aplicaciones – Portal PAEF



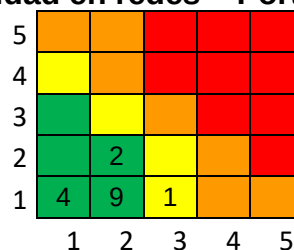
Fuente: Autores

Cuadro 88. Seguridad en redes – Portal PAEF

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	1	3	3	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	1	2	3	1	2	4
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	3	1	1	3	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	3	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	2	1	2	1	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	1	2	1	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	2	2	2	2	1	2	4
✓	✓	✗	Trafico sensible sin protección	Si	1	2	2	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	2	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 79. Mapa de calor – Seguridad en redes – Portal PAEF



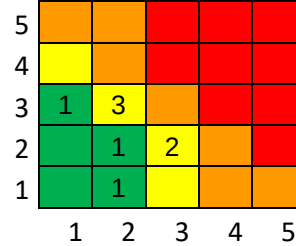
Fuente: Autores

Cuadro 89. Seguridad en internet – Portal PAEF

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✓	✓	✓	Ejecución de malware	Si	1	1	2	3	3	2	2
✓	✓	✓	Suplantación de identidad en línea	Si	2	2	3	4	3	3	6
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	1	2	2	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	3	1	2	3	2	2	6
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	1	2	2	2	6
✓	✓	✓	Ingeniería social	Si	2	1	3	3	2	2	4
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	1	2	1	1	3
✗	✗	✓	Fallas en redes de comunicaciones	Si	2	1	3	3	3	3	6

Fuente: Autores

Figura 80. Mapa de calor – Seguridad en internet – Portal PAEF



Fuente: Autores

Cuadro 90. Protección de infraestructura crítica – Portal PAEF

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
×	×	×	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
×	×	×	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
×	×	×	Desastres naturales	No	N/A	-	-	-	-	-	-
×	×	×	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
×	×	×	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
×	×	×	Abuso de privilegios	No	N/A	-	-	-	-	-	-
×	×	×	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

7.4.13 Interpretación de los resultados del análisis de riesgos – Plataformas No Core. De acuerdo con las tablas y mapas de riesgos obtenidos para las aplicaciones expuestas por el área de Plataformas No Core, se evidencia que aplicaciones como Correo Electrónico y Banca Virtual son críticos para el Banco dado que tienen riesgos de nivel alto y extremo, mientras que los riesgos para las demás aplicaciones tienen nivel medio y bajo. Varias de estas aplicaciones no son consideradas como infraestructura crítica dado que en caso de alguna afectación no se ven comprometidas las actividades propias del negocio.

7.5 ANÁLISIS DE RIESGOS – SEGURIDAD PERIMETRAL

En los siguientes numerales se encuentra el desarrollo del análisis de riesgos para la infraestructura expuesta en internet por parte de Seguridad perimetral. En los cuadros 91 al 110 se encuentra el detalle de este análisis, mientras que en las figuras 81 a la 95 se encuentra la cantidad de riesgos en total asociados a cada causa.

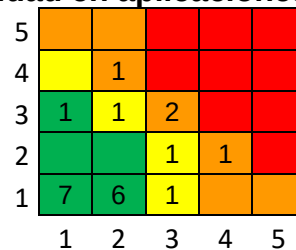
7.5.1 Traffic in - Acceso Remoto Checkpoint.

Cuadro 91. Seguridad en aplicaciones – Acceso Remoto

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2
✓	✓	✓	Fallas operativas	Si	2	4	4	4	4	4	8
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	2	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	3	3	3	1	3	6
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	1	1	1
✓	✓	✗	Exfiltración de información	Si	1	1	1	2	1	1	1
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de documentación	Si	3	1	2	1	1	1	3
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	3	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	2	1	2	8
✓	✓	✓	Versión del software desactualizada	Si	3	3	3	3	1	3	9
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	3	3	3	1	1	2	6
✓	✓	✗	Almacenamiento sin protección	Si	1	1	2	2	2	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1

Fuente: Autores

Figura 81. Mapa de calor – Seguridad en aplicaciones – Acceso Remoto



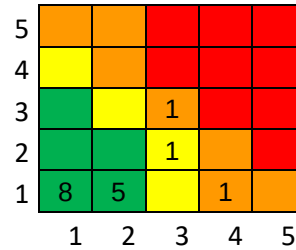
Fuente: Autores

Cuadro 92. Seguridad en redes – Acceso Remoto

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	4	4	4	4	4	4
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	3	3	3	1	3	9
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	1	1	1
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	2	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	2	3	3	3	1	3	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Trafico sensible sin protección	Si	1	1	2	3	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 82. Mapa de calor – Seguridad en redes – Acceso Remoto



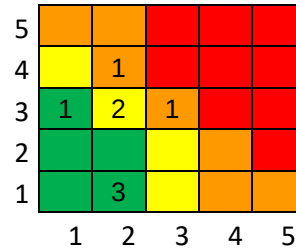
Fuente: Autores

Cuadro 93. Seguridad en internet – Acceso Remoto

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Ejecución de malware	Si	1	3	1	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	2	2	2	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	3	1	1	1	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	3	1	2	8
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	1	1	1	1	3
✓	✓	✓	Ingeniería social	Si	1	2	2	2	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	3	1	1	2	6
✗	✗	✓	Fallas en redes de comunicaciones	Si	3	3	3	2	2	3	9

Fuente: Autores

Figura 83. Mapa de calor – Seguridad en internet – Acceso Remoto



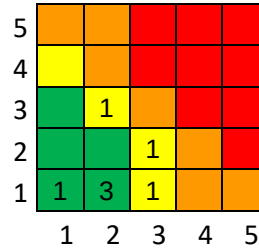
Fuente: Autores

Cuadro 94. Protección de infraestructura crítica – Acceso Remoto

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	2	2	1	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	2	3	3	3	2	3	6
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Falta de servidores redundantes	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de planes de continuidad	Si	1	2	1	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	3	3	3	3	3
✓	✓	✓	Incumplimiento Contractual	Si	1	2	2	3	2	2	2

Fuente: Autores

Figura 84. Mapa de calor – Protección de infraestructura crítica – Acceso Remoto



Fuente: Autores

7.5.2 Traffic out – Navegación sin Proxy.

Cuadro 95. Seguridad en aplicaciones – Navegación sin Proxy

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Explotación de vulnerabilidades en las aplicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas operativas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ataques informáticos internos y/o externos a la aplicación	No	N/A	-	-	-	-	-	-
✗	✗	✗	Gestión y/o uso inadecuado de contraseñas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-
✗	✗	✗	Usuarios malintencionados	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el control de acceso	No	N/A	-	-	-	-	-	-
✗	✗	✗	Modificación deliberada o accidental a la aplicación	No	N/A	-	-	-	-	-	-
✗	✗	✗	Exfiltración de información	No	N/A	-	-	-	-	-	-
✗	✗	✗	Gestión de usuarios deficiente	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de backups de la aplicación	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de documentación	No	N/A	-	-	-	-	-	-
✗	✗	✗	Mal funcionamiento del software	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✗	✗	✗	Versión del software desactualizada	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento en el mantenimiento de la aplicación	No	N/A	-	-	-	-	-	-
✗	✗	✗	Almacenamiento sin protección	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de monitoreo a la aplicación	No	N/A	-	-	-	-	-	-

Fuente: Autores

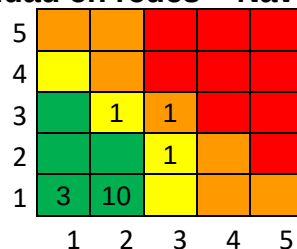
Nota: No se agrega mapa de calor de Seguridad en aplicaciones toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

Cuadro 96. Seguridad en redes – Navegación sin Proxy

Riesgo			Causa	Aplica	PI	Impacto					RI
C	I	D				O	R	L	F	II	
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	2	2	2	3	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	3	3	3	2	3	9
✗	✗	✓	Fallas en el suministro eléctrico	Si	2	2	1	1	2	2	4
✗	✗	✓	Desastres naturales	Si	1	3	1	1	4	2	2
✗	✗	✓	Daños en los equipos de red	Si	2	1	1	2	2	2	4
✓	✓	✓	Abuso de privilegios	Si	1	2	1	1	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	2	1	2	1	2	2	4
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	3	2	3	3	3
✓	✓	✓	Configuración deficiente de los equipos	Si	2	3	3	3	2	3	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	3	1	3	3	2	2	6
✓	✓	✓	Uso no autorizado	Si	1	1	1	1	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	1	1	1	1
✗	✗	✓	Falta de dispositivos redundantes	Si	2	2	1	1	2	2	4
✓	✓	✗	Trafico sensible sin protección	Si	2	2	2	2	2	2	4
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	2	1	1	1	1	2
✓	✓	✓	Ausencia de control de cambios	Si	2	2	1	1	1	1	2

Fuente: Autores

Figura 85. Mapa de calor – Seguridad en redes – Navegación sin Proxy



Fuente: Autores

Cuadro 97. Seguridad en internet – Navegación sin Proxy

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-
✗	✗	✗	Suplantación de identidad en línea	No	N/A	-	-	-	-	-	-
✗	✗	✗	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✗	✗	✗	Acceso con Sistemas operativos y aplicaciones desactualizadas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ingeniería social	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en la configuración de las soluciones de seguridad del equipo	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en redes de comunicaciones	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Seguridad en internet toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

Cuadro 98. Protección de infraestructura crítica – Navegación sin Proxy

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

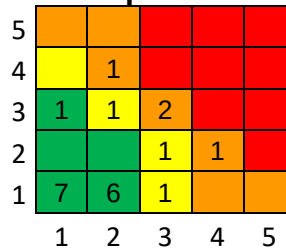
7.5.3 VPN SSL DG.

Cuadro 99. Seguridad en aplicaciones – VPN SSL DG

Riesgo			Causa	Aplica	PI	Impacto					II	RI
C	I	D				O	R	L	F			
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2	2
✓	✓	✓	Fallas operativas	Si	2	4	4	4	4	4	4	8
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	2	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	3	3	3	1	3	6	6
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	1	1	1	1
✓	✓	✗	Exfiltración de información	Si	1	1	1	2	1	1	1	1
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1	1
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1	1
✗	✗	✓	Ausencia de documentación	Si	3	1	2	1	1	1	3	3
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	3	3	3	9	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	2	1	2	8	8
✓	✓	✓	Versión del software desactualizada	Si	3	3	3	3	1	3	9	9
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	3	3	3	1	1	2	6	6
✓	✓	✗	Almacenamiento sin protección	Si	1	1	2	2	2	2	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1	1

Fuente: Autores

Figura 86. Mapa de calor – Seguridad en aplicaciones – VPN SSL DG



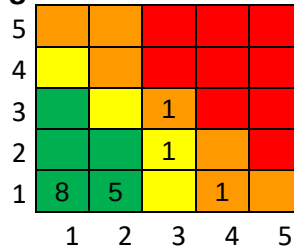
Fuente: Autores

Cuadro 100. Seguridad en redes – VPN SSL DG

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	4	4	4	4	4	4
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	3	3	3	1	3	9
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	1	1	1	1
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	1	1	1
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	2	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	2	3	3	3	1	3	6
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1
✓	✓	✗	Trafico sensible sin protección	Si	1	1	2	3	3	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1

Fuente: Autores

Figura 87. Mapa de calor – Seguridad en redes – VPN SSL DG



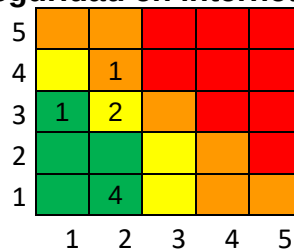
Fuente: Autores

Cuadro 101. Seguridad en internet – VPN SSL DG

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Ejecución de malware	Si	1	3	1	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	2	2	2	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	3	1	1	1	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	3	1	2	8
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	1	1	1	1	3
✓	✓	✓	Ingeniería social	Si	1	2	2	2	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	3	1	1	2	6
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	3	3	1	1	2	2

Fuente: Autores

Figura 88. Mapa de calor – Seguridad en internet – VPN SSL DG



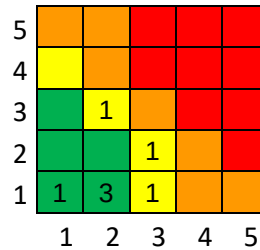
Fuente: Autores

Cuadro 102. Protección de infraestructura crítica – VPN SSL DG

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	2	2	1	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	2	3	3	3	2	3	6
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2
✗	✗	✓	Falta de servidores redundantes	Si	1	1	1	2	1	1	1
✗	✗	✓	Ausencia de planes de continuidad	Si	1	2	1	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	3	3	3	3	3
✓	✓	✓	Incumplimiento Contractual	Si	1	2	2	3	2	2	2

Fuente: Autores

Figura 89. Mapa de calor – Protección de infraestructura crítica – VPN SSL DG



Fuente: Autores

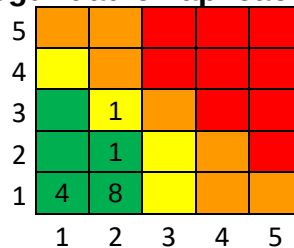
7.5.4 Consola Antivirus.

Cuadro 103. Seguridad en aplicaciones – Consola Antivirus

Riesgo			Causa	Aplica	PI	Impacto			L	F	II	RI
C	I	D				O	R					
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	1	1	3	1	2	2	
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2	
✓	✓	✓	Fallas operativas	Si	3	2	2	2	1	2	6	
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	1	1	3	3	2	2	
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1	
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-	
✓	✓	✓	Usuarios malintencionados	Si	1	1	1	2	3	2	2	
✗	✓	✓	Fallas en el control de acceso	Si	1	2	2	2	3	2	2	
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	2	1	1	3	3	2	4	
✓	✓	✗	Exfiltración de información	Si	1	1	1	4	3	2	2	
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1	
✗	✗	✓	Falta de backups de la aplicación	Si	1	2	1	2	1	2	2	
✗	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	2	2	2	
✗	✗	✓	Ausencia de documentación	Si	1	1	1	1	1	1	1	
✓	✓	✓	Mal funcionamiento del software	Si	1	3	3	2	2	3	3	
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-	
✓	✓	✓	Versión del software desactualizada	Si	1	3	3	3	3	3	3	
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	1	1	1	1	
✓	✓	✗	Almacenamiento sin protección	Si	1	2	1	4	3	3	3	

Fuente: Autores

Figura 90. Mapa de calor – Seguridad en aplicaciones – Consola Antivirus



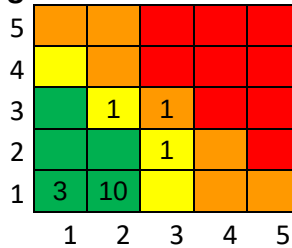
Fuente: Autores

Cuadro 104. Seguridad en redes – Consola Antivirus

Riesgo			Causa	Aplica	PI	Impacto					II	RI
C	I	D				O	R	L	F			
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	1	1	2	2	2	2	2
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	2	3	1	2	2	2	6
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	2	2	2	2	2
✗	✗	✓	Desastres naturales	Si	1	1	1	1	3	2	2	2
✗	✗	✓	Daños en los equipos de red	Si	2	3	3	2	2	3	3	6
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	2	2	2	2
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	2	2	2	2
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	1	1	4	3	2	2	2
✓	✓	✓	Configuración deficiente de los equipos	Si	3	3	3	3	1	3	3	9
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	1	1	1	1	1
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	2	2	2	2
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2	2
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1	1
✓	✓	✗	Tráfico sensible sin protección	Si	1	1	1	3	3	2	2	2
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	2	2	2	1	2	2	2
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1	1

Fuente: Autores

Figura 91. Mapa de calor – Seguridad en redes – Consola Antivirus



Fuente: Autores

Cuadro 105. Seguridad en internet – Consola Antivirus

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Ejecución de malware	No	N/A	-	-	-	-	-	-
✗	✗	✗	Suplantación de identidad en línea	No	N/A	-	-	-	-	-	-
✗	✗	✗	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-
✗	✗	✗	Acceso con Sistemas operativos y aplicaciones desactualizadas	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ingeniería social	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en la configuración de las soluciones de seguridad del equipo	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en redes de comunicaciones	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Seguridad en internet toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

Cuadro 106. Protección de infraestructura crítica – Consola Antivirus

Riesgo			Causa	Aplica	Probabilidad	Impacto					Valor Riesgo
C	I	D				O	R	L	F	T	
✗	✗	✗	Fallas en las redes de comunicaciones	No	N/A	-	-	-	-	-	-
✗	✗	✗	Fallas en el suministro eléctrico	No	N/A	-	-	-	-	-	-
✗	✗	✗	Desastres naturales	No	N/A	-	-	-	-	-	-
✗	✗	✗	Falta de servidores redundantes	No	N/A	-	-	-	-	-	-
✗	✗	✗	Ausencia de planes de continuidad	No	N/A	-	-	-	-	-	-
✗	✗	✗	Abuso de privilegios	No	N/A	-	-	-	-	-	-
✗	✗	✗	Incumplimiento Contractual	No	N/A	-	-	-	-	-	-

Fuente: Autores

Nota: No se agrega mapa de calor de Protección de infraestructura crítica toda vez que no hay riesgos inherentes a este concepto de la gestión de Ciberseguridad para esta aplicación.

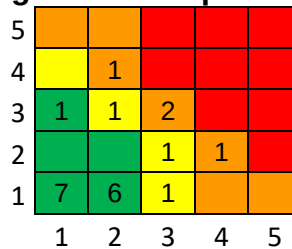
7.5.5 VPN SSL NAOS.

Cuadro 107. Seguridad en aplicaciones – VPN SSL NAOS

Riesgo			Causa	Aplica	PI	Impacto					II	RI
C	I	D				O	R	L	F	T		
✓	✓	✓	Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Abuso de privilegios	Si	1	2	2	2	1	2	2	2
✓	✓	✓	Fallas operativas	Si	2	4	4	4	4	4	4	8
✓	✓	✓	Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1	1
✓	✓	✓	Ejecución de malware	Si	1	2	2	2	2	2	2	2
✓	✓	✓	Usuarios malintencionados	Si	1	2	1	2	2	2	2	2
✓	✓	✓	Fallas en el control de acceso	Si	2	3	3	3	1	3	3	6
✓	✓	✓	Modificación deliberada o accidental a la aplicación	Si	1	1	1	2	1	1	1	1
✓	✓	✗	Exfiltración de información	Si	1	1	1	2	1	1	1	1
✓	✓	✗	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1	1
✗	✗	✓	Falta de backups de la aplicación	Si	1	1	1	1	1	1	1	1
✓	✓	✓	Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1	1
✗	✗	✓	Ausencia de documentación	Si	3	1	2	1	1	1	1	3
✓	✓	✓	Mal funcionamiento del software	Si	3	3	3	3	3	3	3	9
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	2	1	2	2	8
✓	✓	✓	Versión del software desactualizada	Si	3	3	3	3	1	3	3	9
✗	✗	✓	Incumplimiento en el mantenimiento de la aplicación	Si	3	3	3	1	1	2	2	6
✓	✓	✗	Almacenamiento sin protección	Si	1	1	2	2	2	2	2	2
✓	✓	✓	Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1	1

Fuente: Autores

Figura 92. Mapa de calor – Seguridad en aplicaciones – VPN SSL NAOS



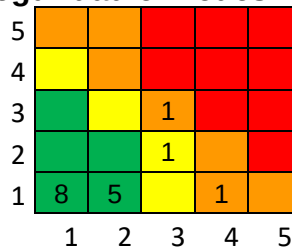
Fuente: Autores

Cuadro 108. Seguridad en redes – VPN SSL NAOS

Riesgo			Causa	Aplica	PI	Impacto					II	RI
C	I	D				O	R	L	F			
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	4	4	4	4	4	4	
✗	✗	✓	Fallas en las redes de comunicaciones	Si	3	3	3	3	1	3	9	
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	1	2	1	1	1	1	
✗	✗	✓	Desastres naturales	Si	1	3	2	1	2	2	2	
✗	✗	✓	Daños en los equipos de red	Si	1	2	2	1	2	2	2	
✓	✓	✓	Abuso de privilegios	Si	1	1	1	2	1	1	1	
✓	✓	✓	Gestión de usuarios deficiente	Si	1	1	1	2	1	1	1	
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	2	2	2	2	
✓	✓	✓	Configuración deficiente de los equipos	Si	2	3	3	3	1	3	6	
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	1	1	1	2	1	1	1	
✓	✓	✓	Uso no autorizado	Si	1	1	1	2	1	1	1	
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	2	2	2	2	
✗	✗	✓	Falta de dispositivos redundantes	Si	1	1	1	1	1	1	1	
✓	✓	✗	Trafico sensible sin protección	Si	1	1	2	3	3	2	2	
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	1	1	1	1	1	1	1	
✓	✓	✓	Ausencia de control de cambios	Si	1	1	1	2	1	1	1	

Fuente: Autores

Figura 93. Mapa de calor – Seguridad en redes – VPN SSL NAOS



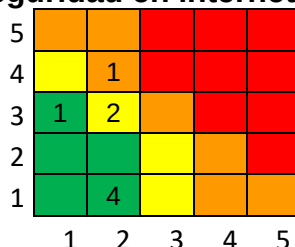
Fuente: Autores

Cuadro 109. Seguridad en internet – VPN SSL NAOS

Riesgo			Causa	Aplica	PI	Impacto				II	RI
C	I	D				O	R	L	F		
✓	✓	✓	Ejecución de malware	Si	1	3	1	1	2	2	2
✓	✓	✗	Suplantación de identidad en línea	Si	1	2	2	2	2	2	2
✓	✓	✓	Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	3	1	1	1	2	6
✓	✓	✓	Falta de concientización de políticas de seguridad de la información	Si	4	2	2	3	1	2	8
✓	✓	✓	Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	1	1	1	1	3
✓	✓	✓	Ingeniería social	Si	1	2	2	2	2	2	2
✓	✓	✓	Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	3	1	1	2	6
✗	✗	✓	Fallas en redes de comunicaciones	Si	1	3	3	1	1	2	2

Fuente: Autores

Figura 94. Mapa de calor – Seguridad en internet – VPN SSL NAOS



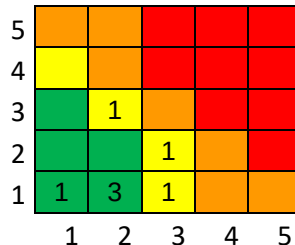
Fuente: Autores

Cuadro 110. Protección de infraestructura crítica – VPN SSL NAOS

Riesgo			Causa	Aplica	PI	Impacto						RI
C	I	D				O	R	L	F	II		
✖	✖	✔	Fallas en las redes de comunicaciones	Si	3	2	2	2	1	2	6	
✖	✖	✔	Fallas en el suministro eléctrico	Si	2	3	3	3	2	3	6	
✖	✖	✔	Desastres naturales	Si	1	3	2	1	2	2	2	
✖	✖	✔	Falta de servidores redundantes	Si	1	1	1	2	1	1	1	
✖	✖	✔	Ausencia de planes de continuidad	Si	1	2	1	2	2	2	2	
✔	✔	✔	Abuso de privilegios	Si	1	2	3	3	3	3	3	
✔	✔	✔	Incumplimiento Contractual	Si	1	2	2	3	2	2	2	

Fuente: Autores

Figura 95. Mapa de calor – Protección de infraestructura crítica – VPN SSL NAOS



Fuente: Autores

7.5.6 Interpretación de los resultados del análisis de riesgos – Seguridad Perimetral. De acuerdo con las tablas y mapas de riesgos obtenidos para las aplicaciones expuestas en internet por el área de Seguridad perimetral, se evidencia que las aplicaciones relacionadas con las VPN (Acceso Remoto Checkpoint, SSL DG y SSL NAOS) dieron como resultado riesgos de nivel alto toda vez que permiten el acceso a la infraestructura interna del Banco, tanto a empleados como proveedores de servicio. Los riesgos de las aplicaciones restantes son en su mayoría bajos y algunos medios indicando que su criticidad para el Banco es media – baja.

8. TRATAMIENTO DE LOS RIESGOS DE CIBERSEGURIDAD

8.1 CONTROLES IMPLEMENTADOS

En esta sección se detallan en el cuadro 111, los controles que el Banco ya tiene implementados para las aplicaciones expuestas en internet detalladas en el numeral 5.10 y usando la metodología expuesta en el numeral 6.3.

Cuadro 111. Controles implementados por el Banco

Controles Implementados	Seguridad en Aplicaciones			Seguridad en Redes			Seguridad en Internet			Protección Infraestructura Crítica			Mitiga Probabilidad	Valor reducción Probabilidad	Mitiga Impacto	Valor reducción Impacto	Parte(s) interesada(s) responsable(s)
	C	I	D	C	I	D	C	I	D	C	I	D					
1 Actualización de Parches	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Si	1	No	-	Proveedores, Empresas del sector, Clientes
2 Web Application Firewall - WAF	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	Si	1	No	-	Banco
3 Security Information and Event Management - SIEM	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	Si	1	No	-	Proveedores de internet, Banco
4 Firewall perimetral	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	Si	1	No	-	Proveedores de internet, Banco
5 Security Operation Center - SOC	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	Si	1	No	-	Proveedores de internet, Banco
6 Hardening	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	Si	1	No	-	Proveedores, Empresas del sector
7 Gestión de Vulnerabilidades Técnicas	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	Si	2	No	-	Proveedores, Banco
8 Gestión de Identidades	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	Si	1	No	-	Banco
9 Pruebas <i>Ethical Hacking</i>	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	Si	2	No	-	Proveedores de aplicación, Banco
10 Separación de ambientes	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	Si	1	No	-	Banco
11 Antivirus	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	Si	1	No	-	Banco, Clientes
12 Data Loss Prevention - DLP	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	Si	1	No	-	Proveedores de internet, Banco
13 Capacitaciones en Seguridad de la Información	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Si	2	No	-	Proveedores, Empresas del sector, Clientes
14 Segmentación de Redes	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	Si	1	No	-	Banco
15 Monitoreo servicios web	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	Si	1	No	-	Proveedores de internet, Banco
16 Plataforma correo seguro	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	Si	1	No	-	Proveedores de aplicación, Banco
17 Hiperconvergencia Servidores	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	Si	1	No	-	Banco
18 Pruebas de Continuidad de Negocio	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	No	-	Si	1	Proveedores de internet, Empresas del sector
19 Alta Disponibilidad (Datacenter)	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	No	-	Si	1	Proveedores de internet, Empresas del sector
20 Alta Disponibilidad (Canales de Internet)	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	No	-	Si	1	Proveedores de internet, Empresas del sector
21 Replica Bases de Datos	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	No	-	Si	1	Proveedores de aplicación, Empresas del sector
22 Acuerdos de nivel de servicio - ANS	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	No	-	Si	1	Banco
23 Balanceador de cargas	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	No	-	Si	1	Banco

Fuente: Autores

8.2 CÁLCULO DE RIESGO RESIDUAL

En los siguientes numerales y en los cuadros 112 al 196 se detalla el proceso para el cálculo del riesgo residual para las aplicaciones expuestas en internet detalladas en el numeral 5.10 y los conceptos de gestión de Ciberseguridad aplicables a cada una. La metodología para este cálculo se detalla en el numeral 6.3.

8.2.1 Forcepoint DLP.

Cuadro 112. Cálculo riesgo residual – Seguridad en aplicaciones Forcepoint DLP

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RI
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	1	2	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1				
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Ejecución de malware	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-				
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	1	2	2				
Modificación deliberada o accidental a la aplicación	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1				
Exfiltración de información	Si	1	3	3	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de backups de la aplicación	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-				
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Mal funcionamiento del software	Si	1	2	2	✓	✗	✓	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	1	1	1				
Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-				
Versión del software desactualizada	Si	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	1	1	1				
Almacenamiento sin protección	Si	1	3	3	✓	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2				
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				

Fuente: Autores

Cuadro 113. Cálculo riesgo residual – Seguridad en redes Forcepoint DLP

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1

Fuente: Autores

8.2.2 Almacenamiento Sharefile.

Cuadro 114. Cálculo riesgo residual – Seguridad en aplicaciones Almacenamiento Sharefile

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto					PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23				
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1	
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1	
Fallas operativas	Si	2	4	8	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1	
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1	
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Fallas en el control de acceso	Si	2	3	6	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	3	3	
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1	
Exfiltración de información	Si	1	1	1	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1	
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1	
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6	
Versión del software desactualizada	Si	3	3	9	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	2	2	
Incumplimiento en el mantenimiento de la aplicación	Si	3	2	6	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	1	1	1	
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1	

Fuente: Autores

Cuadro 115. Cálculo riesgo residual – Seguridad en redes Almacenamiento Sharefile

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto					PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23				
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1	
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1	
Fallas operativas	Si	1	1	1	1	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1	
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3	
Usuarios malintencionados	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Fallas en el control de acceso	Si	1	1	1	1	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1	
Modificación deliberada o accidental a la aplicación	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1	
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1	
Gestión de usuarios deficiente	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	1	2	2	
Falta de backups de la aplicación	Si	1	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	1	1	1	
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Ausencia de documentación	Si	1	1	1	1	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1	
Mal funcionamiento del software	Si	1	1	1	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6	
Versión del software desactualizada	Si	3	2	6	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1	
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	1	1	1	
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1	
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1	

Fuente: Autores

Cuadro 116. Cálculo riesgo residual – Seguridad en internet Almacenamiento Sharefile

Causa	Aplica	PI	II	RI	Controles Probabilidad							CI	PR	IR	RR
					1	7	11	12	13	15	16	20			
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	4	1	4	✗	✗	✗	✗	✓	✗	✗	✗	2	1	2
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1
Fallas en redes de comunicaciones	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1

Fuente: Autores

8.2.3 Citrix Movilidad Teletrabajo.

Cuadro 117.Cálculo riesgo residual – Seguridad en aplicaciones Citrix Movilidad Teletrabajo

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	3	4	12	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	3	3	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	2	2	4			
Versión del software desactualizada	Si	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	3	3	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2			
Falta de monitoreo a la aplicación	Si	1	3	3	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	2	2			

Fuente: Autores

Cuadro 118. Cálculo riesgo residual – Seguridad en redes Citrix Movilidad Teletrabajo

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	1	1	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Tráfico sensible sin protección	Si	1	3	3	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1

Fuente: Autores

Cuadro 119. Cálculo riesgo residual – Seguridad en internet Almacenamiento Citrix Movilidad Teletrabajo

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1	1
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	2
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	2
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Fallas en redes de comunicaciones	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	1

Fuente: Autores

8.2.4 Citrix Movilidad XenMobile.

Cuadro 120. Cálculo riesgo residual – Seguridad en aplicaciones - Citrix Movilidad XenMobile

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1		
Fallas operativas	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	2	2	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Mal funcionamiento del software	Si	1	1	1	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			
Versión del software desactualizada	Si	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1			

Fuente: Autores

Cuadro 121. Cálculo riesgo residual – Seguridad en redes - Citrix Movilidad XenMobile

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	1	1	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	1	1	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Trafico sensible sin protección	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	1	1	1

Fuente: Autores

Cuadro 122. Cálculo riesgo residual – Seguridad en Internet - Citrix Movilidad XenMobile

Causa	Aplica	PI	II	RI	Controles Probabilidad							CI	PR	IR	RR
					1	7	11	12	13	15	16	20			
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	1	1	1	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1
Ingeniería social	Si	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1
Fallas en redes de comunicaciones	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1

Fuente: Autores

8.2.5 Citrix Movilidad Apps.

Cuadro 123. Cálculo riesgo residual – Seguridad en aplicaciones - Citrix Movilidad Apps

Causa	Aplica	PI	II							RI	Controles Probabilidad															Controles Impacto						PR	IR	RR
											1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23					
Explotación de vulnerabilidades en las aplicaciones	Si	1	1	2	2	2	2	2	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	1	1	1	
Abuso de privilegios	Si	1	1	2	2	1	2	2	2	2	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1	
Fallas operativas	Si	1	1	2	2	2	2	2	2	2	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✗	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	1	3	3	3	3	3	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	2	1	1	1	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Ejecución de malware	Si	1	1	2	3	3	2	2	2	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Usuarios malintencionados	Si	1	1	2	3	3	2	2	2	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Fallas en el control de acceso	Si	1	1	1	1	3	2	2	2	2	2	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Modificación deliberada o accidental a la aplicación	Si	1	1	2	3	3	2	2	2	2	2	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	1	1	1		
Exfiltración de información	Si	1	1	3	3	3	3	3	3	3	3	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1		
Gestión de usuarios deficiente	Si	1	1	1	1	1	1	1	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Falta de backups de la aplicación	Si	1	1	1	1	2	1	1	1	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	2	1	1	1	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Ausencia de documentación	Si	1	1	1	1	1	1	1	1	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	1	1	1		
Mal funcionamiento del software	Si	1	1	3	1	3	2	2	2	2	2	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Falta de concientización de políticas de seguridad de la información	Si	1	1	2	1	2	1	2	2	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Versión del software desactualizada	Si	1	1	1	1	1	1	1	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1		
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	2	2	2	2	2	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1		
Almacenamiento sin protección	Si	1	1	3	3	3	3	3	3	3	3	✓	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Falta de monitoreo a la aplicación	Si	1	1	1	1	1	1	1	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1		

Fuente: Autores

Cuadro 124. Cálculo riesgo residual – Seguridad en redes - Citrix Movilidad Apps

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	1	1	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	1	1	1

Fuente: Autores

Cuadro 125. Cálculo riesgo residual – Seguridad en internet - Citrix Movilidad Apps

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1	1
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	3	3	9	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Ingeniería social	Si	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	3
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Fallas en redes de comunicaciones	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✓	2	1	2	2

Fuente: Autores

8.2.6 VPN Movilidad.

Cuadro 126. Cálculo riesgo residual – Seguridad en aplicaciones - VPN Movilidad

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	4	8	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	2	3	6	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	1	1	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6			
Versión del software desactualizada	Si	3	3	9	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2			
Incumplimiento en el mantenimiento de la aplicación	Si	3	2	6	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 127. Cálculo riesgo residual – Seguridad en redes - VPN Movilidad

Explotación de vulnerabilidades en los equipos	Si	2	4	8	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	2	2
Fallas en las redes de comunicaciones	Si	3	4	12	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	✓	
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1	
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1	
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1	
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	2	3	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	1	1	1	
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1	
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1	
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1	
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1	
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	✓	

Fuente: Autores

Cuadro 128. Cálculo riesgo residual – Seguridad en internet - VPN Movilidad

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	4	3	12	✗	✗	✗	✗	✓	✗	✗	✗	2	3	6	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Fallas en redes de comunicaciones	Si	1	2	2	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	

Fuente: Autores

Cuadro 129. Cálculo riesgo residual – Protección infraestructura crítica - VPN Movilidad

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	3	2	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	2	3	6	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1
Falta de servidores redundantes	Si	1	1	1	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗		1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Incumplimiento Contractual	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.7 En Línea ACH PSE.

Cuadro 130. Cálculo riesgo residual – Seguridad en aplicaciones - En Línea ACH PSE

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto				PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23			
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Fallas operativas	Si	2	4	8	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	1	1	1
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	2	2
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3
Usuarios malintencionados	Si	1	3	3	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	2	2
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✗	✗	1	1	1
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	1	1	1
Ausencia de documentación	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1
Mal funcionamiento del software	Si	2	3	6	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Almacenamiento sin protección	Si	1	3	3	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2
Falta de monitoreo a la aplicación	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1

Fuente: Autores

Cuadro 131. Cálculo riesgo residual – Seguridad en redes - En Línea ACH PSE

Riesgo			Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
C	I	D						1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
✓	✓	✓	Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1					
✗	✗	✓	Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1					
✗	✗	✓	Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1					
✗	✗	✓	Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1					
✗	✗	✓	Daños en los equipos de red	Si	3	2	6	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1					
✓	✓	✓	Abuso de privilegios	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3					
✓	✓	✓	Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2					
✓	✓	✓	Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓	1	1	1					
✓	✓	✓	Configuración deficiente de los equipos	Si	3	4	12	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	3	3					
✓	✓	✓	Falta de actualización del firmware de los dispositivos	Si	3	2	6	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					
✓	✓	✓	Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✓	1	1	1					
✗	✗	✓	Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1					
✗	✗	✓	Falta de dispositivos redundantes	Si	2	2	4	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓	1	1	1					
✓	✓	✗	Trafico sensible sin protección	Si	1	3	3	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	1	2	2					
✓	✓	✗	Falta de monitoreo al tráfico de las redes	Si	2	2	4	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	1	1	1					
✓	✓	✓	Ausencia de control de cambios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	1	1	1					

Fuente: Autores

Cuadro 132. Cálculo riesgo residual – Seguridad en internet - En Línea ACH PSE

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	3	3	9	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	2	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	3	3	9	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Sí	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

Cuadro 133. Cálculo riesgo residual – Protección infraestructura crítica - En Línea ACH PSE

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	3	3	9	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	2	2	4
Falta de servidores redundantes	Si	1	2	2	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Incumplimiento Contractual	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.8 Gestión Cobranza (ICS).

Cuadro 134. Cálculo riesgo residual – Seguridad en aplicaciones - Gestión Cobranza (ICS)

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	3	3	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas operativas	Si	3	3	9	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Usuarios malintencionados	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	3	3	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	2	2	4	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✓	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Versión del software desactualizada	Si	4	2	8	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	2	2	4	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 135. Cálculo riesgo residual – Seguridad en redes - Gestión Cobranza (ICS)

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	3	3	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2				
Falta de monitoreo al tráfico de las redes	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 136. Cálculo riesgo residual – Seguridad en internet - Gestión Cobranza (ICS)

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

Cuadro 137. Cálculo riesgo residual – Protección infraestructura crítica - Gestión Cobranza (ICS)

Causa	Aplica	PI	II	RI											Controles Impacto				PR	IR	RR																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
					3	4	5	10	13	14	15	17	18	19	20	22																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
Fallas en las redes de comunicaciones	Si	1	3	3	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Fuente: Autores

8.2.9 Aula Financiera.

Cuadro 138. Cálculo riesgo residual – Seguridad en aplicaciones - Aula Financiera

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	2	4	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	1	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	2	2	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			
Mal funcionamiento del software	Si	1	2	2	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	2	2	4			
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	2	2	4	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Falta de monitoreo a la aplicación	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			

Fuente: Autores

Cuadro 139. Cálculo riesgo residual – Seguridad en redes - Aula Financiera

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	3	3	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	3	3	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	2	2				
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1				
Tráfico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 140. Cálculo riesgo residual – Seguridad en internet - Aula Financiera

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	1	1	1	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	

Fuente: Autores

8.2.10 Correo Electrónico Banco Agrario.

Cuadro 141. Cálculo riesgo residual – Seguridad en aplicaciones - Correo Electrónico

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto					PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23				
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1	
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	1	1	1		
Fallas operativas	Si	3	2	6	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	1	1	1		
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2		
Ejecución de malware	Si	3	3	9	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	3	3		
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Fallas en el control de acceso	Si	2	1	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1		
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1		
Exfiltración de información	Si	1	3	3	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	1	1	1		
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	1	1	1		
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	1	1	1		
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		
Ausencia de documentación	Si	2	1	2	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Mal funcionamiento del software	Si	3	2	6	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Falta de concientización de políticas de seguridad de la información	Si	2	1	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1		
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1		

Fuente: Autores

Cuadro 142. Cálculo riesgo residual – Seguridad en redes - Correo Electrónico

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	3	3	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	3	3	9	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 143. Cálculo riesgo residual – Seguridad en internet - Correo Electrónico

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	2	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	4	1	4	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	2	3	6	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	4	2	8	✗	✗	✗	✗	✗	✓	✗	✓	3	1	3	

Fuente: Autores

Cuadro 144. Cálculo riesgo residual – Protección infraestructura crítica - Correo Electrónico

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	2	3	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1
Falta de servidores redundantes	Si	2	2	4	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Incumplimiento contractual	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.11 Depósitos Judiciales.

Cuadro 145. Cálculo riesgo residual – Seguridad en aplicaciones - Depósitos Judiciales

Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1
Fallas operativas	Si	2	3	6	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	1	1	1
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	1	1	1
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3
Usuarios malintencionados	Si	1	3	3	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3
Fallas en el control de acceso	Si	1	2	2	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	2	2
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	1	1	1
Exfiltración de información	Si	1	3	3	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	1	1	1
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	1	1	1
Ausencia de documentación	Si	3	2	6	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	1	1	1
Mal funcionamiento del software	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	1	1	1
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1
Almacenamiento sin protección	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1

Fuente: Autores

Cuadro 146. Cálculo riesgo residual – Seguridad en redes - Depósitos Judiciales

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	2	3	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	3	3	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	3	3	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	3	3	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2				
Falta de monitoreo al tráfico de las redes	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 147. Cálculo riesgo residual – Seguridad en internet - Depósitos Judiciales

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	3	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	2	3	6	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	3	2	6	✗	✗	✗	✗	✗	✓	✗	✓	2	1	2	

Fuente: Autores

Cuadro 148. Cálculo riesgo residual – Protección infraestructura crítica - Depósitos Judiciales

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	2	3	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	2	1	2
Falta de servidores redundantes	Si	1	2	2	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Incumplimiento contractual	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.12 Portal Web Banco Agrario.

Cuadro 149. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Web

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	3	6	✗	✗	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	2	2	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			
Versión del software desactualizada	Si	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 150. Cálculo riesgo residual – Seguridad en redes - Portal Web

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	3	3	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	3	3	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	2	2
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	2	2	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	3	2	6	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 151. Cálculo riesgo residual – Seguridad en internet - Portal Web

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1	1
Suplantación de identidad en línea	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	2	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	2
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Ingeniería social	Si	2	3	6	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	3
Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Fallas en redes de comunicaciones	Si	3	2	6	✗	✗	✗	✗	✗	✓	✗	✓	2	1	2	2

Fuente: Autores

Cuadro 152. Cálculo riesgo residual – Protección infraestructura crítica - Portal Web

Causa	Aplica	PI	II	RI	Controles Probabilidad									Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22				
Fallas en las redes de comunicaciones	Si	2	3	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	1	3	3	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1	
Desastres naturales	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Falta de servidores redundantes	Si	2	3	6	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1	
Ausencia de planes de continuidad	Si	2	3	6	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1	
Abuso de privilegios	Si	1	2	2	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2	
Incumplimiento contractual	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1	

Fuente: Autores

8.2.13 Banca Virtual Banco Agrario.

Cuadro 153. Cálculo riesgo residual – Seguridad en aplicaciones - Banca Virtual

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto					PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23				
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1	
Abuso de privilegios	Si	1	3	3	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	1	2	2		
Fallas operativas	Si	4	3	12	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1	
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Usuarios malintencionados	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	3	3		
Fallas en el control de acceso	Si	3	3	9	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	3	3		
Modificación deliberada o accidental a la aplicación	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	1	1	1		
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	1	1	1		
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	1	1	1		
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	1	1	1		
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Ausencia de documentación	Si	1	1	1	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Mal funcionamiento del software	Si	4	3	12	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Falta de concientización de políticas de seguridad de la información	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3		
Versión del software desactualizada	Si	1	2	2	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1		
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Almacenamiento sin protección	Si	1	3	3	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2		
Falta de monitoreo a la aplicación	Si	2	2	4	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1		

Fuente: Autores

Cuadro 154. Cálculo riesgo residual – Seguridad en redes - Banca Virtual

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	4	3	12	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	2	1	2
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	2	3	6	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	3	2	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	3	2	6	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	3	2	6	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	3	3	9	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	1	2	2
Falta de monitoreo al tráfico de las redes	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	2	2	4	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 155. Cálculo riesgo residual – Seguridad en internet - Banca Virtual

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1	1
Suplantación de identidad en línea	Si	3	3	9	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	2
Falta de concientización de políticas de seguridad de la información	Si	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	2
Ingeniería social	Si	3	3	9	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	3
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Fallas en redes de comunicaciones	Si	3	2	6	✗	✗	✗	✗	✗	✓	✗	✓	2	1	2	2

Fuente: Autores

Cuadro 156. Cálculo riesgo residual – Protección infraestructura crítica - Banca Virtual

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	4	3	12	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	3	3	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	3	3	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	2	2	4
Falta de servidores redundantes	Si	3	3	9	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2	2
Incumplimiento contractual	Si	1	3	3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.14 ADFS.

Cuadro 157. Cálculo riesgo residual – Protección infraestructura crítica - Banca Virtual

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	1	1	1				
Fallas operativas	Si	2	2	4	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	1	1	1				
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Fallas en el control de acceso	Si	2	1	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	1	1	1				
Exfiltración de información	Si	1	3	3	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	1	1	1				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1				
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Ausencia de documentación	Si	2	1	2	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Mal funcionamiento del software	Si	2	2	4	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1				
Falta de concientización de políticas de seguridad de la información	Si	1	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Versión del software desactualizada	Si	1	1	1	1	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1				
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Falta de monitoreo a la aplicación	Si	1	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1				

Fuente: Autores

Cuadro 158. Cálculo riesgo residual – Seguridad en redes - ADFS

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	3	3	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	2	2	4	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	3	3	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	2	2
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	3	1	3	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 159. Cálculo riesgo residual – Seguridad en internet - ADFS

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	1	1	✗	✗	✓	✗	✓	✗	✓	✗	1	1	1	1
Suplantación de identidad en línea	Si	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	3
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	1	3	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	1
Falta de concientización de políticas de seguridad de la información	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	2
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	2
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	1
Fallas en redes de comunicaciones	Si	3	2	6	✗	✗	✗	✗	✗	✓	✗	✓	2	1	2	2

Fuente: Autores

Cuadro 160. Cálculo riesgo residual – Protección infraestructura crítica - ADFS

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	3	2	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1
Falta de servidores redundantes	Si	2	2	4	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Fallas en redes de comunicaciones	Si	3	2	6	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.15 Conéctate al Conocimiento.

Cuadro 161. Cálculo riesgo residual – Seguridad en aplicaciones - Conéctate al conocimiento

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Fallas operativas	Si	3	1	3	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	1	1	1				
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Usuarios malintencionados	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Fallas en el control de acceso	Si	1	1	1	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1				
Exfiltración de información	Si	1	1	1	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✗	1	1	1				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	1	1	1				
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1				
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Ausencia de documentación	Si	2	1	2	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Mal funcionamiento del software	Si	4	2	8	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	1	1	1				
Falta de concientización de políticas de seguridad de la información	No	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-				
Versión del software desactualizada	Si	1	1	1	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1				
Almacenamiento sin protección	Si	1	1	1	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1				
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1				

Fuente: Autores

Cuadro 162. Cálculo riesgo residual – Seguridad en redes - Conéctate al conocimiento

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	4	1	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	2	1	2
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	3	2	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	3	1	3	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 163. Cálculo riesgo residual – Seguridad en internet - Conéctate al conocimiento

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	1	2	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	2	2	4	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	

Fuente: Autores

8.2.16 Portal Tu Referido.

Cuadro 164. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Tu Referido

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	2	4	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	1	1	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	2	2	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	1	2	2	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Versión del software desactualizada	Si	1	1	1	1	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	1	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 165. Cálculo riesgo residual – Seguridad en redes - Portal Tu Referido

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	1	1	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 166. Cálculo riesgo residual – Seguridad en internet - Portal Tu Referido

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Sí	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Sí	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Sí	3	1	3	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1	
Falta de concientización de políticas de seguridad de la información	Sí	2	2	4	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Sí	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Sí	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Sí	2	2	4	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Fallas en redes de comunicaciones	Sí	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

8.2.17 Portal Vivienda.

Cuadro 167. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Vivienda

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	2	4	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	2	2	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	1	2	2	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 168. Cálculo riesgo residual – Seguridad en redes - Portal Vivienda

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	2	2	4	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	1	1	1

Fuente: Autores

Cuadro 169. Cálculo riesgo residual – Seguridad en internet - Portal Vivienda

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	2	2	4	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	3	3	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	2	1	2	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

8.2.18 Portal Cliente.

Cuadro 170. Cálculo riesgo residual – Seguridad en aplicaciones - Portal Cliente

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto					PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23				
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1	
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1	
Fallas operativas	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	1	1	1		
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1	
Gestión y/o uso inadecuado de contraseñas	Si	2	2	4	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3	
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Fallas en el control de acceso	Si	2	2	4	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1	
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1	
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Mal funcionamiento del software	Si	2	2	4	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1	
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2	
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1	
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1	
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1	

Fuente: Autores

Cuadro 171. Cálculo riesgo residual – Seguridad en redes - Portal Cliente

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	2	2	4	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	2	1	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de actualización del firmware de los dispositivos	Si	2	2	4	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	2	1	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	2	1	2	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Ausencia de control de cambios	Si	2	1	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1

Fuente: Autores

Cuadro 172. Cálculo riesgo residual – Seguridad en internet - Portal Cliente

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Ingeniería social	Si	2	2	4	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Sí	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

8.2.19 Ingreso Solidario.

Cuadro 173. Cálculo riesgo residual – Seguridad en aplicaciones - Ingreso Solidario

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	2	4	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	2	2	4	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	2	2	4	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	2	3	3	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 174. Cálculo riesgo residual – Seguridad en redes - Ingreso Solidario

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	2	2	4	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	2	2	4	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de monitoreo al tráfico de las redes	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	2	1	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 175. Cálculo riesgo residual – Seguridad en internet - Ingreso Solidario

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Sí	1	3	3	✗	✗	✓	✗	✓	✗	✓	✗	1	3	3	
Suplantación de identidad en línea	Sí	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Sí	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Sí	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Sí	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Sí	2	3	6	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Sí	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Sí	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

8.2.20 Consulta Giros.

Cuadro 176. Cálculo riesgo residual – Seguridad en aplicaciones - Consulta Giros

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	3	3	9	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	2	2	4	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	3	3	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1			
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1				
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	2	2	4	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 177. Cálculo riesgo residual – Seguridad en redes - Consulta Giros

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	2	2	4	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	2	1	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	2	2	4	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	1	2	2	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de monitoreo al tráfico de las redes	Si	3	1	3	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 178. Cálculo riesgo residual – Seguridad en internet - Consulta Giros

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	3	3	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	2	3	6	✗	✗	✗	✗	✓	✗	✓	✗	1	3	3	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	2	3	6	✗	✗	✗	✗	✗	✓	✗	✓	1	2	2	

Fuente: Autores

8.2.21 Portal PAEF.

Cuadro 179. Cálculo riesgo residual – Seguridad en aplicaciones - Portal PAEF

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	2	4	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	3	3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Ejecución de malware	Si	1	3	3	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	2	2	4	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Modificación deliberada o accidental a la aplicación	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	3	3	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1			
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	2	2	4	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Versión del software desactualizada	Si	1	2	2	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Incumplimiento en el mantenimiento de la aplicación	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	2	2	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 180. Cálculo riesgo residual – Seguridad en redes - Portal PAEF

Causa	Aplica	PI	II	RI	Controles Probabilidad																	Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22							
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1				
Fallas en las redes de comunicaciones	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1				
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1				
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1				
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1				
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1				
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1				
Configuración deficiente de los equipos	Si	1	2	2	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	1	1				
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1				
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de dispositivos redundantes	Si	2	2	4	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1				
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1				
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1				
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1					

Fuente: Autores

Cuadro 181. Cálculo riesgo residual – Seguridad en internet - Portal PAEF

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	2	3	6	✗	✗	✗	✗	✓	✗	✗	✗	1	3	3	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	3	2	6	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Ingeniería social	Si	2	2	4	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Fallas en redes de comunicaciones	Si	2	3	6	✗	✗	✗	✗	✗	✓	✗	✓	1	2	2	

Fuente: Autores

8.2.22 Traffic in - Acceso Remoto Checkpoint.

Cuadro 182. Cálculo riesgo residual – Seguridad en aplicaciones - Acceso Remoto

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Fallas operativas	Si	2	4	8	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✓	1	1	1		
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1		
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2		
Fallas en el control de acceso	Si	2	3	6	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	3	3		
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	1	1	1		
Exfiltración de información	Si	1	1	1	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	1	1	1		
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1		
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	1	1	1		
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1		
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1		
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1		
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6		
Versión del software desactualizada	Si	3	3	9	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	2	2		
Incumplimiento en el mantenimiento de la aplicación	Si	3	2	6	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	1	1	1		
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	1	1		
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	1	1	1		

Fuente: Autores

Cuadro 183. Cálculo riesgo residual – Seguridad en redes - Acceso Remoto

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	4	4	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	2	2
Fallas en las redes de comunicaciones	Si	3	3	9	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	2	3	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓	1	1	1
Tráfico sensible sin protección	Si	1	2	2	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	1	1	1

Fuente: Autores

Cuadro 184. Cálculo riesgo residual – Seguridad en internet - Acceso Remoto

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✓	✗	✗	✗	2	2	4	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Fallas en redes de comunicaciones	Si	3	3	9	✗	✗	✗	✗	✗	✓	✗	✓	2	2	4	

Fuente: Autores

Cuadro 185. Cálculo riesgo residual – Protección infraestructura crítica - Acceso Remoto

Causa	Aplica	PI	II	RI	Controles Probabilidad								Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22			
Fallas en las redes de comunicaciones	Si	3	2	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	2	3	6	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1
Falta de servidores redundantes	Si	1	1	1	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Incumplimiento Contractual	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1

Fuente: Autores

8.2.23 Traffic out – Navegación sin Proxy.

Cuadro 186. Cálculo riesgo residual – Seguridad en redes - Navegación sin Proxy

Causa	Aplica	PI	II	RI	Controles Probabilidad														Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22				
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1	
Fallas en las redes de comunicaciones	Si	3	3	9	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	2	2	4	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1	
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1	
Daños en los equipos de red	Si	2	2	4	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	1	1	1	
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2	
Gestión de usuarios deficiente	Si	2	2	4	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2	
Ataques informáticos internos y/o externos a los dispositivos	Si	1	3	3	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1	
Configuración deficiente de los equipos	Si	2	3	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2	
Falta de actualización del firmware de los dispositivos	Si	3	2	6	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1	
Incumplimiento en el mantenimiento de los equipos	Si	1	1	1	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1	
Falta de dispositivos redundantes	Si	2	2	4	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	1	1	1	
Trafico sensible sin protección	Si	2	2	4	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Falta de monitoreo al tráfico de las redes	Si	2	1	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1	
Ausencia de control de cambios	Si	2	1	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1		

Fuente: Autores

8.2.24 VPN SSL DG.

Cuadro 187. Cálculo riesgo residual – Seguridad en aplicaciones - VPN SSL DG

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	1	1	1		
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Fallas operativas	Si	2	4	8	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	1	1	1			
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	1	1	1			
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2			
Fallas en el control de acceso	Si	2	3	6	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	3	3			
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✗	1	1	1			
Exfiltración de información	Si	1	1	1	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1			
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	1	1	1			
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1			
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	1	1			
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6			
Versión del software desactualizada	Si	3	3	9	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2			
Incumplimiento en el mantenimiento de la aplicación	Si	3	2	6	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1			
Almacenamiento sin protección	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1			
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1			

Fuente: Autores

Cuadro 188. Cálculo riesgo residual – Seguridad en redes - VPN SSL DG

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	4	4	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	2	2
Fallas en las redes de comunicaciones	Si	3	3	9	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	2	3	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1	

Fuente: Autores

Cuadro 189. Cálculo riesgo residual – Seguridad en internet - VPN SSL DG

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✓	✗	✗	✗	2	2	4	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Fallas en redes de comunicaciones	Si	1	2	2	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	

Fuente: Autores

Cuadro 190. Cálculo riesgo residual – Protección infraestructura crítica - VPN SSL DG

Causa	Aplica	PI	II	RI	Controles Probabilidad									Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22				
Fallas en las redes de comunicaciones	Si	3	2	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	2	3	6	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1	
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1	
Falta de servidores redundantes	Si	1	1	1	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1	
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1	
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Incumplimiento Contractual	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1	

Fuente: Autores

8.2.25 Consola Antivirus.

Cuadro 191. Cálculo riesgo residual – Seguridad en aplicaciones - Consola Antivirus

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto				PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23			
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	1	1	1
Fallas operativas	Si	3	2	6	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	1	1	1
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	1	1	1
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1
Ejecución de malware	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2
Fallas en el control de acceso	Si	1	2	2	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	1	2	2
Modificación deliberada o accidental a la aplicación	Si	2	2	4	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	1	1
Exfiltración de información	Si	1	2	2	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	1	1	1
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1
Falta de backups de la aplicación	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1
Ausencia de documentación	Si	1	1	1	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	1	1	1
Mal funcionamiento del software	Si	1	3	3	✓	✗	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	1	1	1
Falta de concientización de políticas de seguridad de la información	No	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Versión del software desactualizada	Si	1	3	3	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	2	2
Incumplimiento en el mantenimiento de la aplicación	Si	1	1	1	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	1	1	1
Almacenamiento sin protección	Si	1	3	3	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	1	2	2

Fuente: Autores

Cuadro 192. Cálculo riesgo residual – Seguridad en redes - Consola Antivirus

Causa	Aplica	PI	II	RI	Controles Probabilidad													Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22			
Explotación de vulnerabilidades en los equipos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	1	1
Fallas en las redes de comunicaciones	Si	3	2	6	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1
Fallas en el suministro eléctrico	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1
Daños en los equipos de red	Si	2	3	6	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1
Abuso de privilegios	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Gestión de usuarios deficiente	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	2	2
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1
Configuración deficiente de los equipos	Si	3	3	9	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1
Uso no autorizado	Si	1	2	2	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	1	1	1
Tráfico sensible sin protección	Si	1	2	2	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓	1	1	1
Falta de monitoreo al tráfico de las redes	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	1	1	1

Fuente: Autores

8.2.26 VPN SSL NAOS.

Cuadro 193. Cálculo riesgo residual – Seguridad en aplicaciones - VPN SSL NAOS

Causa	Aplica	PI	II	RI	Controles Probabilidad															Controles Impacto							PR	IR	RR
					1	2	3	4	5	6	7	8	9	10	13	14	15	18	19	20	21	22	23						
Explotación de vulnerabilidades en las aplicaciones	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	1	1	1			
Abuso de privilegios	Si	1	2	2	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	1	1	1				
Fallas operativas	Si	2	4	8	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1				
Ataques informáticos internos y/o externos a la aplicación	Si	1	2	2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	1	1	1				
Gestión y/o uso inadecuado de contraseñas	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1	1	1				
Ejecución de malware	Si	1	2	2	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Usuarios malintencionados	Si	1	2	2	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	1	2	2				
Fallas en el control de acceso	Si	2	3	6	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	1	3	3				
Modificación deliberada o accidental a la aplicación	Si	1	1	1	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	1	1	1				
Exfiltración de información	Si	1	1	1	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	1	1	1				
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Falta de backups de la aplicación	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	1	1	1				
Incumplimiento en la entrega y/o buenas prácticas en las aplicaciones desarrolladas	Si	1	1	1	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Ausencia de documentación	Si	3	1	3	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Mal funcionamiento del software	Si	3	3	9	✓	✗	✓	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	1	1	1				
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	3	2	6				
Versión del software desactualizada	Si	3	3	9	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	2	2				
Incumplimiento en el mantenimiento de la aplicación	Si	3	2	6	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	1	1	1				
Almacenamiento sin protección	Si	1	2	2	✓	✓	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	1	1	1				
Falta de monitoreo a la aplicación	Si	1	1	1	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	1	1	1				

Fuente: Autores

Cuadro 194. Cálculo riesgo residual – Seguridad en redes - VPN SSL NAOS

Causa	Aplica	PI	II	RI	Controles Probabilidad														Controles Impacto				PR	IR	RR
					1	3	4	5	6	7	8	9	10	11	13	14	17	18	19	20	22				
Explotación de vulnerabilidades en los equipos	Si	1	4	4	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	1	2	2	
Fallas en las redes de comunicaciones	Si	3	3	9	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	1	1	1	
Desastres naturales	Si	1	2	2	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	1	1	1	
Daños en los equipos de red	Si	1	2	2	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	1	1	1	
Abuso de privilegios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1	
Gestión de usuarios deficiente	Si	1	1	1	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1	1	1	
Ataques informáticos internos y/o externos a los dispositivos	Si	1	2	2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	1	1	1	
Configuración deficiente de los equipos	Si	2	3	6	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	1	2	2	
Falta de actualización del firmware de los dispositivos	Si	1	1	1	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Uso no autorizado	Si	1	1	1	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	1	1	1	
Incumplimiento en el mantenimiento de los equipos	Si	1	2	2	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	1	1	1		
Falta de dispositivos redundantes	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	1	1	1	
Trafico sensible sin protección	Si	1	2	2	✓	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Falta de monitoreo al tráfico de las redes	Si	1	1	1	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	1	1	1	
Ausencia de control de cambios	Si	1	1	1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	1	1	1		

Fuente: Autores

Cuadro 195. Cálculo riesgo residual – Seguridad en internet - VPN SSL NAOS

Causa	Aplica	PI	II	RI	Controles Probabilidad								CI	PR	IR	RR
					1	7	11	12	13	15	16	20				
Ejecución de malware	Si	1	2	2	✗	✗	✓	✗	✓	✗	✓	✗	1	2	2	
Suplantación de identidad en línea	Si	1	2	2	✗	✗	✗	✗	✓	✗	✗	✗	1	2	2	
Bases de datos de soluciones de seguridad desactualizadas o inexistentes	Si	3	2	6	✓	✓	✓	✗	✓	✗	✗	✗	1	2	2	
Falta de concientización de políticas de seguridad de la información	Si	4	2	8	✗	✗	✗	✗	✓	✗	✗	✗	2	2	4	
Acceso con Sistemas operativos y aplicaciones desactualizadas	Si	3	1	3	✓	✓	✓	✓	✓	✗	✗	✗	1	1	1	
Ingeniería social	Si	1	2	2	✗	✗	✗	✗	✓	✗	✓	✗	1	2	2	
Fallas en la configuración de las soluciones de seguridad del equipo	Si	3	2	6	✓	✓	✓	✓	✓	✗	✗	✗	1	2	2	
Fallas en redes de comunicaciones	Si	1	2	2	✗	✗	✗	✗	✗	✓	✗	✓	1	1	1	

Fuente: Autores

Cuadro 196. Cálculo riesgo residual – Protección infraestructura crítica - VPN SSL NAOS

Causa	Aplica	PI	II	RI	Controles Probabilidad									Controles Impacto				PR	IR	RR
					3	4	5	10	13	14	15	17	18	19	20	22				
Fallas en las redes de comunicaciones	Si	3	2	6	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	1	1	1	
Fallas en el suministro eléctrico	Si	2	3	6	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	1	1	1	
Desastres naturales	Si	1	2	2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	1	1	1	
Falta de servidores redundantes	Si	1	1	1	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	1	1	1	
Ausencia de planes de continuidad	Si	1	2	2	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	1	1	1	
Abuso de privilegios	Si	1	3	3	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	1	1	
Incumplimiento Contractual	Si	1	2	2	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	1	1	1	

Fuente: Autores

8.2.27 Interpretación de los resultados del tratamiento de riesgos. Después de la aplicación de la metodología para el tratamiento del riesgo detallado en el numeral 6.3, se evidencia que el riesgo más alto después de la aplicación de los controles que se tienen implementados en el Banco tiene nivel medio, mitigando los riesgos altos y extremos que se encontraron en el análisis de riesgos detallado en el numeral 7 para las aplicaciones que están expuestas en internet y de acuerdo con los conceptos de la gestión de Ciberseguridad que le aplican a cada una.

8.3 AMENAZAS A APLICACIONES DEL BANCO AGRARIO DE COLOMBIA

En esta sección se detallarán algunas de las amenazas a las que se pueden ver expuestas las aplicaciones del Banco en el ciberespacio, de acuerdo con lo establecido en la norma ISO 27032:2012 en su numeral 9. “Amenazas contra la seguridad en el ciberespacio”

Las amenazas en el ciberespacio se relacionan con los activos en el ciberespacio, en este caso a los servicios expuestos en internet por el Banco. Dichas amenazas se dividen en dos áreas clave. Amenazas a activos personales y amenazas a activos organizacionales, las cuales pueden ser aprovechadas por un agente de amenaza (un individuo o grupo de individuos que tienen un rol en la ejecución o soporte de un ataque).

En referencia a amenazas a activos personales se encuentran:

- Robo o suplantación de la identidad en línea de los clientes y/o usuarios.
- Compromiso del dispositivo del usuario final para ser parte de una *botnet* (Red de robots informáticos).

Para las amenazas a activos organizacionales están:

- *Defacement* (Desfiguración de sitios web)
- Robo de nombres de dominio.
- Afectación a la infraestructura que soporta los sitios web del Banco.

Actualmente el Banco cuenta con procedimientos para la gestión de vulnerabilidades técnicas para la infraestructura y las aplicaciones que se ejecutan en esta, sin embargo, no es posible detallar las vulnerabilidades identificadas, teniendo en cuenta que esta información puede causar daño al derecho sobre los secretos comerciales, industriales y profesionales de acuerdo con el artículo 18 de la Ley 1712 de 2014 por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.

8.3.1 Mecanismos de Ataque. En su mayoría, los ataques en el ciberespacio se realizan usando software malicioso, tales como spyware, gusanos y virus. La información es recolectada generalmente a través de técnicas de *phishing*. Los ataques pueden provenir desde dos categorías: Ataques dentro de la red privada y ataques de fuera de la red privada.

A continuación, se mencionan algunos de los ataques que se podrían ejecutar dentro de la red privada sin los controles detallados en el numeral 8.5:

- Abuso de privilegios.
- Infección por malware.

- Ataque *man-in-the-middle* (Hombre en el medio).
- Suplantación de *Access point* legítimos.
- Uso de *Keyloggers* (Captura de pulsaciones de teclado).

Algunos de los ataques desde fuera de la red privada (internet), se mencionan a continuación:

- Escaneo de puertos.
- Ataques de DDoS (Denegación de servicio Distribuido).
- Envío de archivos con código malicioso.
- Desbordamiento de búfer.
- IP *spoofing* (Manipulación de direcciones IP).

8.4 ROLES DE LAS PARTES INTERESADAS

Es importante que las partes interesadas en el ciberespacio desempeñen diferentes roles, los cuales permiten mejorar el estado de la ciberseguridad en general. Estos roles pueden, a veces, superponerse con roles individuales y organizacionales dentro de redes personales u organizacionales, tal como se expone en el estándar ISO/IEC27032:2012 en su numeral 10. Roles de las partes interesadas en ciberseguridad”.

Cuando se habla de una red organizacional, se hace referencia a la combinación de redes privadas de cada organización (típicamente intranet), extranet y redes públicamente visibles. Para los propósitos de cumplimiento del estándar ISO/IEC 27032:2012, las redes públicamente visibles son aquellas redes expuestas en internet.

Por lo anterior, estos roles pueden parecer tener un beneficio insignificante o no directo para los individuos u organizaciones. Sin embargo, son significativos para mejorar la ciberseguridad cuando los involucrados actúan en consecuencia.

8.4.1 Roles de los clientes. Los clientes pueden ver o recolectar información, así como proveer información dentro de un espacio de aplicación del ciberespacio. Las acciones tomadas por los clientes en esos roles pueden ser pasivas o activas, y pueden contribuir, directa o indirectamente, al estado de la ciberseguridad.

8.4.1.1 Roles de los individuos. Los clientes individuales del ciberespacio pueden asumir diferentes roles en diversos contextos y aplicaciones.

Los roles de los clientes pueden incluir, sin limitarse, los siguientes:

- Usuarios de aplicaciones expuestas en internet por el Banco.
- Funcionarios del Banco Agrario de Colombia.

- Otros roles. Es posible que se pueda asignar un rol a un usuario de forma no intencional o sin su consentimiento.

8.4.1.2 Roles de las organizaciones. Las organizaciones usan el ciberespacio para divulgar la compañía y su información relacionada, para este caso, el Banco Agrario de Colombia usa el ciberespacio como parte de su red para prestar diferentes servicios como, por ejemplo, el correo electrónico, portal web, entre otros, por tanto, se deben extender las responsabilidades corporativas al ciberespacio al asegurar proactivamente que sus prácticas y acciones no introduzcan riesgos adicionales de seguridad en el ciberespacio. Algunas medidas proactivas incluyen:

- Adecuada gestión de seguridad de la información al implementar y operar un sistema eficaz de gestión de seguridad de la información (SGSI), como, por ejemplo, la implementación del estándar ISO/IEC 27001:2013.
- Apropiado monitoreo y respuesta a incidentes de seguridad de la información.
- Educación regular en seguridad de la información a los funcionarios a través de actualizaciones continuas en tecnología, entendimiento y uso adecuado de los canales de comunicación.

En cuanto al Gobierno y Entes reguladores, los cuales en esencia son agencias de aseguramiento del cumplimiento de las leyes bajo las cuales se debe regir el Banco Agrario de Colombia, pueden tener los siguientes roles importantes:

- Informar a las organizaciones sobre su roles y responsabilidades en el ciberespacio.
- Compartir información con otras partes interesadas sobre las últimas tendencias y desarrollos en tecnología.
- Compartir información con otras partes interesadas sobre las últimas tendencias en riesgos sobresalientes de seguridad de la información.
- Ser conducto para recibir información, sea de forma cerrada o abierta, respecto a riesgos en el ciberespacio.
- Ser el coordinador primario para diseminación de información e instrumentación de los recursos requeridos, tanto a nivel nacional como corporativo, en momentos de crisis surgida por un ciberataque masivo.

8.4.2 Roles de los proveedores. Teniendo en cuenta que los proveedores están clasificados en dos grupos: Proveedores de aplicación y Proveedores de internet, dichos proveedores son también organizaciones clientes; se espera que ellos cumplan los mismos roles y responsabilidades que las organizaciones clientes.

Como proveedores de servicios para el Banco Agrario de Colombia, tienen responsabilidades adicionales en mantener e incluso mejorar la seguridad del ciberespacio a:

- Proveedores de productos y servicios seguros.
- Proveer guías de seguridad para usuarios finales.
- Proveer entradas de seguridad a otros proveedores y clientes en cuanto a tendencias y observaciones sobre el tráfico en sus redes y servicios.

8.5 CONTROLES PROPUESTOS

Una vez los riesgos correspondientes a ciberseguridad para las aplicaciones expuestas en internet por el Banco Agrario de Colombia son identificados, es necesario seleccionar y proponer diferentes controles de ciberseguridad, adicionales a los que ya tiene implementados, para soportar los requisitos de seguridad que se mencionan en la norma ISO/IEC 27032:2012. A continuación, se proporciona una visión general de los controles claves de ciberseguridad extraídos de la norma ISO/IEC 27032:2012 en su numera 12. “Controles de ciberseguridad”. Estos controles están divididos en los siguientes grupos:

- Controles de nivel de aplicación.
- Protección de servidores.
- Controles de usuario final.
- Controles frente a ataques de ingeniería social.
- Preparación para la ciberseguridad

8.5.1 Controles de nivel de aplicación

- Visualización de avisos breves, los cuales proveen resúmenes claros y concisos de una página usando lenguaje simple de las políticas en línea esenciales de la entidad. Con esto, los usuarios podrán tomar decisiones informadas sobre compartir su información en línea. Los avisos deberán estar ajustados a todos los requisitos regulatorios y proveer enlaces al cuerpo informativo completo, así como información adicional relevante, de forma que los clientes que desean más detalle puedan fácilmente navegar para conocer la versión completa. Dado lo anterior, los avisos deberán ser implementados por el Banco Agrario de Colombia y sus proveedores de aplicaciones a cada una de las aplicaciones expuestas en internet.
- Validación y manejo seguro de captura de datos para prevenir ataques comunes tales como inyección SQL. Teniendo en cuenta que los sitios web considerados de confianza son cada vez más usados para la distribución de código malicioso, se debería realizar una validación de entrada y salida tanto para contenido activo como para contenido dinámico. Dichos controles deberán ser implementados por el Banco y proveedores de aplicaciones.
- Los proveedores de aplicaciones deberán asegurar los scripts de los sitios web para prevenir ataques comunes tales como *Cross-site Scripting*.
- Realizar revisiones y pruebas de la seguridad del código por entidades idóneas apropiadas, solicitadas por el Banco.
- Los proveedores de aplicaciones podrían usar subdominios del dominio oficial del Banco, así como el uso de credenciales HTTPS registradas para la entidad. El

servicio debería evitar el uso de métodos engañosos donde el cliente puede tener dificultades para determinar con quien está tratando.

8.5.2 Protección de servidores. Los siguientes controles pueden ser usados para proteger servidores contra acceso no autorizado y el almacenamiento de contenido malicioso en los mismos, los cuales deberían ser implementados por el Banco Agrario de Colombia.

- Monitorear el desempeño de seguridad de los servidores mediante revisiones regulares del registro de auditoría.
- Revisar la configuración de la seguridad.
- Ejecutar controles de software anti malicioso (tales como antivirus, antispyware o EDR – *Endpoint Detection and Response*) en los servidores. En el mercado se pueden encontrar productos especializados en este tipo de soluciones como Trend Micro, Palo alto Networks, Symantec, Microsoft, entre otros.

8.5.3 Controles de usuario final. Se mencionan los controles que los usuarios finales (en general, todas las partes interesadas) pueden usar para proteger sus sistemas frente a aprovechamientos y ataques.

- Uso de sistemas operativos con soporte, teniendo instalados los más actualizados parches de seguridad. Los clientes del Banco tienen la responsabilidad de tener el conocimiento de los sistemas operativos soportados. Los clientes individuales deben ser conscientes al usar los sistemas operativos recomendados por el Banco y proveedores. En todos los casos, los sistemas operativos deben mantenerse al día respecto a los parches de seguridad.
- Uso de aplicaciones de software actuales y soportadas. En todos los casos, el software de aplicación deberá mantenerse al día respecto a actualizaciones de seguridad.
- Usar herramientas antivirus y antispyware. Usuarios de la entidad y clientes individuales deberían usar herramientas de seguridad y mantenerlos al día en parches de seguridad y bases de datos de firmas.
- Implementar salvaguardas adecuados. Los navegadores y barras de herramientas comunes han incorporados capacidades tales como bloqueadores emergentes, los cuales evitan que sitios web maliciosos exhiban ventanas que contengan spyware o software engañoso que podría aprovechar debilidades del sistema o del navegador, o usar ingeniería social para engañar a usuarios para descargar o instalarlos en sus sistemas, por ello:
 - El Banco debería establecer políticas para permitir el uso de tales herramientas.
 - Los proveedores de servicios deberían organizar una lista de herramientas recomendadas donde su uso debería ser propuesto para los usuarios finales, incluyendo guías sobre su habilitación.
- Permitir la activación de bloqueadores de scripts, para asegurar que solo se ejecuten scripts de fuentes de confianza en equipos de cómputo.

- Usar filtros de phishing. Los actuales navegadores web y barras de herramientas en los navegadores incorporan esta capacidad, la cual podría determinar si el sitio que el usuario desea visitar se encuentra dentro de la base de datos de sitios web conocidos con problemas de phishing o que contiene patrones similares.
- Usar otras características de seguridad que incluyen los navegadores web, pues con el tiempo, emergen nuevos riesgos de ciberseguridad frente a lo cual los proveedores de los navegadores web y barras de herramientas añaden nuevas capacidades de seguridad.
- Activar firewall personales y HIDS (*Host-based Intrusion Detection System*) son herramientas importantes para controlar servicios en red con acceso a los sistemas del usuario. Los nuevos sistemas operativos incluyen firewall personales y HIDS y en su mayoría vienen activados por defecto, los usuarios o aplicaciones podrían deshabilitarlos resultando en exposición no deseada de la seguridad de la red.
- Permitir las actualizaciones automáticas para prevenir aprovechamiento de vulnerabilidades que existan en los sistemas operativos y demás productos de aplicación. Esto debería asegurar que los sistemas están actualizados con los últimos parches de seguridad una vez se hacen disponibles disminuyendo la brecha de tiempo de aprovechamiento de vulnerabilidades.

8.5.4 Controles frente a ataques de ingeniería social. Controles aplicables para gestionar y minimizar los riesgos de ciberseguridad en relación con los ataques de ingeniería social basados en el concepto en el cual, la única forma eficaz de mitigar la amenaza es a través de la combinación de tecnologías de seguridad, políticas de seguridad que fijan líneas base para el comportamiento personal, tanto como individuo, como funcionarios y educación y entrenamiento apropiado.

- Políticas
 - Se deberían determinar y documentar políticas básicas que direccionen la creación, colección, almacenamiento, transmisión, compartir, procesamiento y uso general de información organizacional y personal, así como la propiedad intelectual en internet y en el ciberespacio.
 - Relacionarlas a aplicaciones tales como mensajería instantánea, *blogging*, redes para compartir archivos P2P (*peer to peer*) y redes sociales, las cuales normalmente están más allá del alcance de la seguridad de redes empresariales y de información.
 - Como parte de las políticas, declaraciones y sanciones corporativas relacionadas con el mal uso de aplicaciones en el ciberespacio, se debería incorporar lineamientos contra prácticas de mal uso por parte de los funcionarios y terceras personas en redes corporativas o sistemas que accedan al ciberespacio.
 - Desarrollar y promulgar políticas administrativas que promuevan conciencia y entendimiento de los riesgos de ciberseguridad para el aprendizaje y desarrollo de destrezas contra ataques en ciberseguridad, en particular ataques de ingeniería social.

- Conciencia y entrenamiento

Dentro del actual programa de conciencia y entrenamiento en seguridad de la información con el que cuenta el Banco Agrario de Colombia se propone incluir contenido en las últimas amenazas y formas de ataque de ingeniería social, por ejemplo, cómo el phishing ha evolucionado desde sitios web falsos a la combinación de ataques de correo no deseado, *Cross Site Scripting* e inyección SQL (*SQL Injection*).

- Técnico

Además de establecer políticas y prácticas contra ataques de ingeniería social, se deberían considerar también controles técnicos para minimizar la exposición y el potencial aprovechamiento por parte de cibercriminales.

- Implementación el uso de dos o más factores adicionales para la verificación de identidad (MFA), pueden ser provistos usando tarjetas inteligentes, biometría o mediante otros dispositivos de seguridad portátil.

- Para servicios basados en la web, el Banco y sus proveedores de aplicaciones deberían considerar el uso de un certificado de alto nivel de aseguramiento (*High Assurance Certificate*) para proveer seguridad adicional a los usuarios en línea.

8.5.5 Preparación para la ciberseguridad. A continuación, se describen controles técnicos adicionales que son aplicables para mejorar de la preparación del Banco en el área de detección de eventos a través de monitoreo de la red oscura (*Darknet*), investigación a través de *Traceback* y respuesta mediante técnicas *Sinkhole Operation*.

- Monitoreo *Darknet*: La *Darknet* son un conjunto de direcciones IP que no están en uso en las organizaciones. Las direcciones en *Darknet* no están asignadas a sistemas operacionales, servidores o equipos de cómputo alguno. Existen tres métodos comúnmente utilizados en *Darknet* para observar actividades maliciosas relacionadas con tráfico en internet, denominadas: Monitoreo de agujero negro (*Black Hole Monitoring*) y el monitoreo de interacción alto y bajo (*Low and High Interaction Monitoring*).

- Monitoreo de agujero negro (*Black Hole Monitoring*): Se refiere al monitoreo de sistemas que no responden contra paquetes de entrada que se encuentran dentro de los dominios IP *Darknet*. Este monitoreo es usado para observar de forma silenciosa el escaneo de puertos realizado por malware, el comportamiento de infecciones mediante malware (UDP con carga útil incluyendo código *Shell*). El escaneo de puertos de red es a menudo el paso inicial realizado por los atacantes para buscar sistemas vulnerables a aprovechar.

- Monitoreo de baja interacción: Sistema de monitoreo ante paquetes IP *Darknet* responde intentando conectarse al sistema sospechoso. El propósito del intento de conexión es obtener más información sobre el sistema que está atacando, las rutas de red de ataque e información relacionada.

- Monitoreo de alta interacción: También denominado *honeypot* de alta interacción, es también un sistema de monitoreo *Darknet* que responde a paquetes detectados

al intentar conexión a los sistemas sospechosos e interactuar con ellos lo máximo posible. El propósito de la interacción es obtener información mucho más profunda incluyendo la estrategia de explotación de vulnerabilidades.

- Operación *Sinkhole*: Se define como un método para redirigir tráfico IP específico a un dispositivo *sinkhole* para análisis de tráfico, desviación de ataques y detección de comportamiento anómalos en la red. Por ejemplo, si la operación del Banco es perturbada por medio de un ataque de denegación de servicio, una de las posibles soluciones eficaces es iniciar una operación *sinkhole* al inyectar una ruta alterna al blanco y redirigir el tráfico.
- Seguimiento (*Traceback*): Se usa con el fin de automatizar o acelerar el seguimiento manual contra ataques maliciosos donde se falsifica el host de origen. Las técnicas de seguimiento se reconocen como técnicas que reconstruyen la ruta de ataque y ubican los nodos de atacante corrigiendo el tráfico de ataque, la información de enrutamiento, los paquetes marcados o el registro de auditoría del tráfico de ataque.

9. LINEAMIENTOS PARA EL INTERCAMBIO DE LA INFORMACIÓN ENTRE LAS PARTES INTERESADAS.

Para la gestión de la ciberseguridad, es necesario establecer un sistema para compartir y coordinar información con el fin de ayudar en la preparación y respuesta ante eventos y/o incidentes de ciberseguridad, tal como se describe en la norma ISO 27032:2012 en su numeral 13. “Marco de referencia para compartir y coordinar información. El Banco Agrario de Colombia debería añadir a sus controles de ciberseguridad, los lineamientos para el intercambio de información entre las partes interesadas. Este sistema debería ser seguro, eficaz, confiable y eficiente con el fin de compartir y coordinar información entre las partes.

Se incluyen cuatro áreas para consideración: 1. Políticas, 2. Métodos y procesos, 3. Personas y 4. Elementos técnicos, con el fin de que se evalúen los lineamientos que se deben implementar. En este capítulo se detallarán las áreas definidas anteriormente.

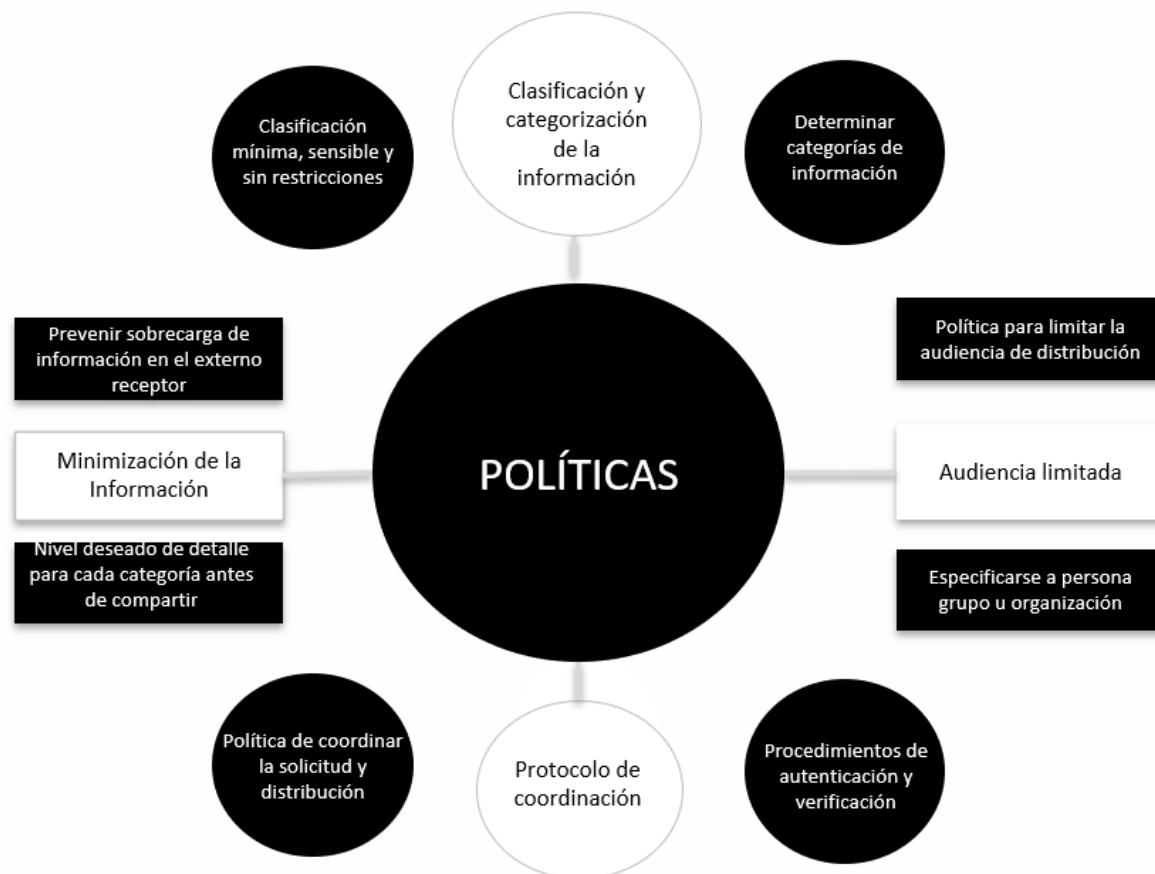
9.1 POLÍTICAS

Dentro de la definición de políticas para compartir y coordinar información, se introducen dos tipos de organización que comparten información:

- IPO (*Information Providing Organization*): Quien envía la información.
- IRO (*Information Receiving Organization*): Quien recibe la información.

Como IPO. se deberían determinar las políticas respecto a la clasificación y categorización de la información. Como externo receptor, el IRO debería acordar reforzar la protección de la seguridad con procedimientos relevantes al recibir información del IPO, tal como se referencia en la figura 96.

Figura 96. Políticas compartir y coordinar información



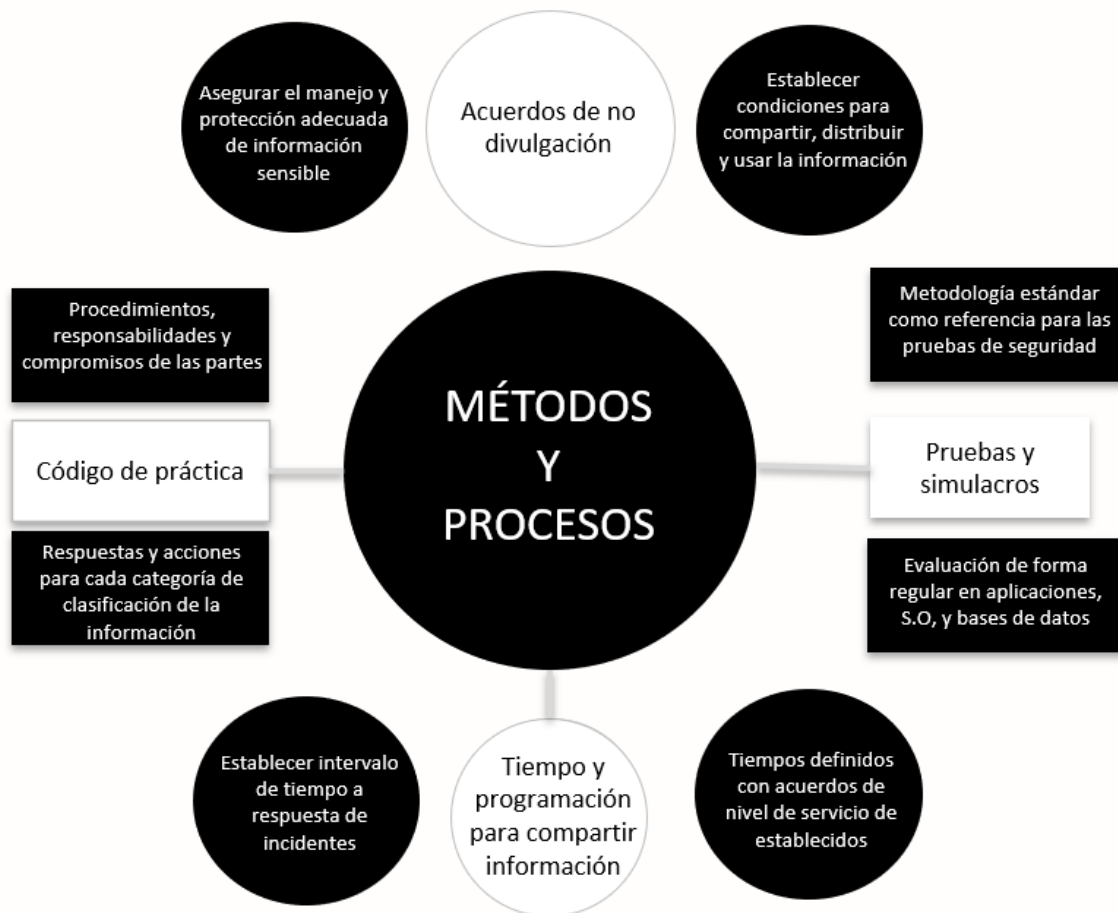
Fuente: Autores

9.2 MÉTODOS Y PROCESOS

Para aplicar las políticas para compartir información y asegurar consistencia de práctica, eficacia, eficiencia y confiabilidad de ejecución se deberían desarrollar e implementar métodos y procesos relacionados. Tales métodos deberían estar basados en estándares disponibles.

En la figura 97, se evidencia una guía sobre los métodos y procesos usados comúnmente en la industria para lograr objetivos y políticas con el fin de compartir y coordinar información en el contexto de la ciberseguridad.

Figura 97. Métodos y procesos para compartir y coordinar información.



Fuente: Autores

9.3 FUENTES Y ORGANIZACIONES

Las personas y organizaciones son determinantes claves en el éxito de la ciberseguridad. Las personas hacen referencia a individuos involucrados en la ejecución de los métodos y procesos para compartir y coordinar información. Las organizaciones refieren a grupos dentro de la entidad hasta la entidad entera involucrados en tales actividades.

En la figura 98 se describen los lineamientos propuestos para personas y organizaciones.

Figura 98. Métodos y procesos para compartir y coordinar información



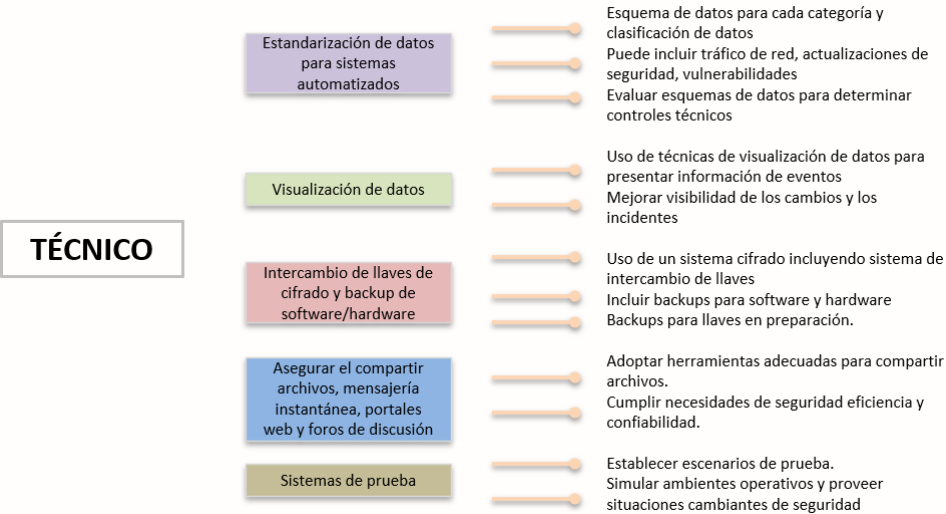
Fuente: Autores

9.4 TÉCNICOS

Los controles técnicos y de estandarización pueden ser usados para mejorar la eficiencia, reducir el error humano y mejorar la seguridad involucrada en los procesos para compartir y coordinar información. Se pueden diseñar, desarrollar e implementar varios sistemas y soluciones técnicas.

En la figura 99, se proveen algunos de los enfoques y técnicas más comunes y que pueden adaptarse para mejorar las necesidades y procesos para compartir y coordinar información.

Figura 99. Lineamientos técnicos para compartir y coordinar información



Fuente: Autores

10. CONCLUSIONES

- De acuerdo con los resultados de los análisis de riesgos realizados a las aplicaciones expuestas en internet por el Banco Agrario de Colombia, se puede evidenciar que el concepto de gestión de Ciberseguridad más sensible es el de Seguridad en Internet.
- Los controles que se tienen establecidos para los conceptos de la gestión de Ciberseguridad 1. Seguridad en aplicaciones, 2. Seguridad en redes, 3. Seguridad en internet y 4. Protección de infraestructura crítica, detallados en este documento, mitigan la probabilidad e impacto de los riesgos de forma efectiva, toda vez que se evidencia la mitigación de estos.
- Dados los resultados del análisis de riesgos realizado en este documento se evidencia que el estado de ciberseguridad de las aplicaciones expuestas en internet por el Banco Agrario de Colombia es bueno teniendo en cuenta que después del tratamiento del riesgo (aplicación de controles), el riesgo residual de la mayoría de estos es bajo y muy pocos, medio.
- La implementación de los lineamientos para el intercambio de información entre las partes interesadas le ayudará al Banco Agrario de Colombia a estar preparado para responder ante eventos e incidentes de ciberseguridad con el apoyo de las partes interesadas, permitiéndole ser más efectivo en caso de que se presenten situaciones que pongan en riesgo las aplicaciones que se exponen en internet.
- Luego de llevar a cabo las actividades propuestas en los objetivos específicos de este proyecto, es posible establecer el diagnóstico del estado de la ciberseguridad para las aplicaciones expuestas en internet por el Banco Agrario de Colombia, el cual apoyará la definición de los planes de acción para mejorar su postura de ciberseguridad.

11. RECOMENDACIONES

- El Banco Agrario de Colombia debería evaluar los controles detallados en el numeral 8.4 dado que, de acuerdo con el análisis de riesgos realizado, no se evidencia su implementación. De igual forma, debería informar a las partes interesadas sobre el rol que deben cumplir de acuerdo con lo expuesto en el numeral 8.3 con el fin de mejorar la postura de ciberseguridad para las aplicaciones que expone en internet.
- El proceso de análisis de riesgos a las aplicaciones expuestas en internet por el Banco Agrario de Colombia debería realizarse de forma periódica (mínimo una vez al año), para todas las aplicaciones que se implementen a futuro con el fin de garantizar la seguridad para los interesados.
- Se deberá llevar un monitoreo de forma periódica al menos una vez al año, a los controles que ya se encuentran implementados por el Banco Agrario de Colombia, con el fin de validar su eficacia y así mantener el estado actual de ciberseguridad evidenciado en este documento.
- El Banco Agrario de Colombia debería implementar una política de intercambio seguro de información con todas las partes interesadas de acuerdo con los organigramas detallados en el numeral 9.
- Teniendo en cuenta que para el concepto de gestión de la ciberseguridad: Seguridad en Internet, se evidenciaron la mayoría de los riesgos medios posterior al tratamiento del riesgo, el Banco Agrario de Colombia debería enfocar sus esfuerzos por establecer controles adicionales que permitan aumentar los niveles de seguridad para los clientes que hacen uso de las aplicaciones que exponen en internet.

BIBLIOGRAFÍA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en entidades públicas [en línea]. [Bogotá D.C., Colombia]: DAFP [citado en septiembre de 2020]. Disponible en Internet: <https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499>

DEPARTAMENTO NACIONAL DE PLANEACION. Conpes 3701 [en línea]. [Bogotá D.C., Colombia]: DNP [citado en 10 septiembre de 2020]. Disponible en Internet: <<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>>

EY LATAM. Encuesta Global de Seguridad de la Información 2018-19 [en línea]. 1º edición. [Ciudad de México, México]: Mancera S.C. [citado en 4 abril de 2020]. Disponible en Internet: < [https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/\\$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf)>

INCIBE. Plan Director de Seguridad [en línea]. [Madrid, España]: INCIBE. [citado en 19 agosto de 2020]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS, Gestión del Riesgo. Directrices. Bogotá D.C.: ICONTEC, 2018. 20p. NTC 31000.

INTERNATIONAL STANDARDS ORGANIZATION. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Geneva.: ISO, 2012. 50p. ISO/IEC 27032

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo Nacional de Gestión de Riesgos de Seguridad Digital [en línea]. [Consultado 25 de septiembre de 2020]. Disponible en <https://www.mintic.gov.co/portal/604/articles-61854_documento.docx>