



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



DESARROLLO DE SISTEMAS DE INFORMACIÓN

CURSO: AUDITORIA DE INFORMACION

PROFESOR: ING. TEODORO MIGUEL VERA PALOMINO

TEMA: AUDITORÍA A LOS SISTEMAS DE PRODUCCIÓN

INTEGRANTES:

FRANKLIN HUAYTALLA ALDANA

SARI SUERE KEVIN YOSETH

SEMESTRE VI

2024 -1



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

ÍNDICE

2	EMPRESA DE CONSTRURA: CEFOISA INGENIERÍA Y CONSTRUCCIÓN S.A.C.....	11
3	MISIÓN Y VISIÓN.....	11
3.1	MISIÓN.....	11
3.2	VISIÓN.....	11
4	OBJETIVOS ESTRATÉGICOS	12
5	ORGANIGRAMA DE LA EMPRESA CEFOISA	12
6	MAPA DE PROCESOS DE LA EMPRESA CEFOISA.....	14
7	SOCIOS ESTRATÉGICOS DE LA EMPRESA CEFOISA	15
8	IDENTIFICACIÓN DE RIESGOS EN EL ÁREA DE TI EMPRESA CEFOISA.....	16
8.1	MATRIZ DE RIESGOS.....	16
8.2	EVENTOS CON SU EVALUACIÓN DE PROBABILIDAD E IMPACTO	17
8.3	MATRIZ DE INCIDENCIAS	21
9	REGISTRO DE INCIDENCIAS ÁREA DE TI Y OTROS - EMPRESA CEFOISA	23
9.1	REGISTRO DE USUARIOS.....	23
9.2	REGISTRO DE PROBABILIDAD IMPACTO nivel de RIESGO.....	26
9.3	REGISTRO DE CATEGORIZACIÓN Y RESPONSABLES	29
10	KEY PERFORMANCE INDICATOR.....	31
10.1	KPIS CALCULADOS	31
10.1.1	NÚMERO TOTAL DE INCIDENCIAS POR CATEGORÍA.....	31
10.1.2	PROMEDIO DE RESOLUCIÓN (HORAS)	31
	32
10.1.3	INCIDENCIAS POR NIVEL DE RIESGO.....	32
10.1.4	Incidenias Detectadas por Área	32
11	POPUESTA DE MITIGACIONES Y COSTO DE MITIGACIÓN	33
11.1	RE001 - Mantenimiento Eléctrico y Actualización de Cableado	33
11.2	RE002 - Adquisición de Licencias y Control de Inventario	34
11.3	RE003 - Políticas de Actualización de Software	35
11.4	RE004 - Políticas de Backup y Mejora de Infraestructura	36
11.5	RE005 - Gestión de Contraseñas y Seguridad de Acceso.....	37
11.6	RE006 - Configuración Segura de Red	38
11.7	RE007 - Desarrollo de Planes de Contingencia en TI.....	39
11.8	RE008 - Política BYOD y Control de Endpoints	40
11.9	RE009 - Capacitación Continua en TI.....	41



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.10	RE010 - Monitoreo y Optimización de Servidores Críticos.....	42
11.11	RE011 - Actualización de Equipos de Red	43
11.12	RE012 - Definición de SLAs y Evaluación de Proveedores	44
11.13	RE013 - Implementación de Herramientas de Monitoreo de Red.....	45
11.14	RE014 - Plan de Actualización de Software	46
11.15	RE015 - Implementación de Cifrado en Transmisión de Datos.....	47
11.16	RE016 - Fortalecimiento de Seguridad Física y Control de Accesos.....	48
11.17	RE017 - Asesoría Legal para Cumplimiento Normativo.....	49
11.18	RE018 - Pruebas de Recuperación en Caso de Desastres	50
11.19	RE019 - Implementación de Segmentación de Red.....	51
11.20	RE020 - Diversificación de Proveedores Críticos	52
11.21	RE021 - Plan de Mantenimiento Preventivo de Equipos de Obra.....	53
12	ELABORACIÓN PLANES DE RESPUESTAS A INCIDENTES CON MEDIDAS DE CONTENCIÓN Y MITIGACIÓN RECOMENDADAS.	54
12.1	PLAN DE RESPUESTA AL INCIDENTE RE001 - CÓDIGO: PDA001 - "FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA"	54
12.1.1	INCIDENCIA:.....	54
12.1.2	ENCARGADO:.....	54
12.1.3	MATERIALES O RECURSOS:.....	54
12.1.4	COMENTARIO:.....	54
12.1.5	TIEMPO:	54
12.1.6	ACTIVIDADES PASO A PASO – FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA:	54
12.2	PLAN DE RESPUESTA AL INCIDENTE RE002 - CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"	57
12.2.1	INCIDENCIA:.....	57
12.2.2	ENCARGADO:.....	57
12.2.3	MATERIALES O RECURSOS:.....	57
12.2.4	COMENTARIO:.....	57
12.2.5	TIEMPO:	57
12.2.6	ACTIVIDADES PASO A PASO – REGULARIZACIÓN DE LICENCIAS DE SOFTWARE:	57
12.3	PLAN DE RESPUESTA AL INCIDENTE RE002 - CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"	58
12.4	PLAN DE RESPUESTA AL INCIDENTE RE003 - CÓDIGO: PDA003 - "VULNERABILIDAD EN SEGURIDAD DE SOFTWARE"	60
12.4.1	INCIDENCIA:.....	60
12.4.2	ENCARGADO:.....	60



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

12.4.3	MATERIALES O RECURSOS:	60
12.4.4	COMENTARIO:	60
12.4.5	TIEMPO:	60
12.4.6	ACTIVIDADES PASO A PASO – VULNERABILIDAD EN SEGURIDAD DE SOFTWARE:	60
12.5	PLAN DE RESPUESTA AL INCIDENTE RE004 - CÓDIGO: PDA004 - "PÉRDIDA DE DATOS CRÍTICOS"	63
12.5.1	INCIDENCIA:	63
12.5.2	ENCARGADO:	63
12.5.3	MATERIALES O RECURSOS:	63
12.5.4	COMENTARIO:	63
12.5.5	TIEMPO:	63
12.5.6	ACTIVIDADES PASO A PASO – PÉRDIDA DE DATOS CRÍTICOS:	63
12.6	PLAN DE RESPUESTA AL INCIDENTE RE005 - CÓDIGO: PDA005 - "COMPROMISO DE ACCESO NO AUTORIZADO"	66
12.6.1	INCIDENCIA:	66
12.6.2	ENCARGADO:	66
12.6.3	MATERIALES O RECURSOS:	66
12.6.4	COMENTARIO:	66
12.6.5	TIEMPO:	66
12.6.6	ACTIVIDADES PASO A PASO – COMPROMISO DE ACCESO NO AUTORIZADO:	66
12.7	PLAN DE RESPUESTA AL INCIDENTE RE006-CÓDIGO: PDA006 - "ACCESO NO AUTORIZADO A LA RED"	69
12.7.1	INCIDENCIA:	69
12.7.2	ENCARGADO:	69
12.7.3	MATERIALES O RECURSOS:	69
12.7.4	COMENTARIO:	69
12.7.5	TIEMPO:	69
12.7.6	ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A LA RED:	69
12.8	PLAN DE RESPUESTA AL INCIDENTE RE007-CÓDIGO: PDA007 - "TIEMPO DE INACTIVIDAD POR FALLAS EN TI"	72
12.8.1	INCIDENCIA:	72
12.8.2	ENCARGADO:	72
12.8.3	MATERIALES O RECURSOS:	72
12.8.4	COMENTARIO:	72
12.8.5	TIEMPO:	72



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

12.8.6	ACTIVIDADES PASO A PASO – TIEMPO DE INACTIVIDAD POR FALLAS EN TI:	72
12.9	PLAN DE RESPUESTA AL INCIDENTE RE008-CÓDIGO: PDA008 - "FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES"	75
12.9.1	INCIDENCIA:.....	75
12.9.2	ENCARGADO:	75
12.9.3	MATERIALES O RECURSOS:.....	75
12.9.4	COMENTARIO:.....	75
12.9.5	TIEMPO:	75
12.9.6	ACTIVIDADES PASO A PASO – FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES:	75
12.10	PLAN DE RESPUESTA AL INCIDENTE RE009-CÓDIGO: PDA009 - "ERRORES HUMANOS EN TI"	78
12.10.1	INCIDENCIA:.....	78
12.10.2	ENCARGADO:	78
12.10.3	MATERIALES O RECURSOS:.....	78
12.10.4	COMENTARIO:.....	78
12.10.5	TIEMPO:	78
12.10.6	ACTIVIDADES PASO A PASO – ERRORES HUMANOS EN TI:.....	78
12.11	PLAN DE RESPUESTA AL INCIDENTE RE010-CÓDIGO: PDA010 - "INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA"	81
12.11.1	INCIDENCIA:.....	81
12.11.2	ENCARGADO:	81
12.11.3	MATERIALES O RECURSOS:.....	81
12.11.4	COMENTARIO:.....	81
12.11.5	TIEMPO:	81
12.11.6	ACTIVIDADES PASO A PASO – INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA:	81
12.12	PLAN DE RESPUESTA AL INCIDENTE RE011- CÓDIGO: PDA011 - "DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS"	84
12.12.1	INCIDENCIA:.....	84
12.12.2	ENCARGADO:	84
12.12.3	MATERIALES O RECURSOS:.....	84
12.12.4	COMENTARIO:.....	84
12.12.5	TIEMPO:	84
12.12.6	ACTIVIDADES PASO A PASO – DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS:.....	84
12.13	PLAN DE RESPUESTA AL INCIDENTE RE012-CÓDIGO: PDA012 - "FALLOS DE SOPORTE TÉCNICO"	87



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

12.13.1	INCIDENCIA:.....	87
12.13.2	ENCARGADO:	87
12.13.3	MATERIALES O RECURSOS:.....	87
12.13.4	COMENTARIO:.....	87
12.13.5	TIEMPO:	87
12.13.6	ACTIVIDADES PASO A PASO – FALLOS DE SOPORTE TÉCNICO:.....	87
12.14	PLAN DE RESPUESTA AL INCIDENTE RE013-CÓDIGO: PDA013 - "CAÍDAS INESPERADAS DE LA RED"	90
12.14.1	INCIDENCIA:.....	90
12.14.2	ENCARGADO:	90
12.14.3	MATERIALES O RECURSOS:.....	90
12.14.4	COMENTARIO:.....	90
12.14.5	TIEMPO:	90
12.14.6	ACTIVIDADES PASO A PASO – CAÍDAS INESPERADAS DE LA RED: 90	
12.15	PLAN DE RESPUESTA AL INCIDENTE RE014-CÓDIGO: PDA014 - "INCOMPATIBILIDAD CON NUEVOS SISTEMAS"	93
12.15.1	INCIDENCIA:.....	93
12.15.2	ENCARGADO:	93
12.15.3	MATERIALES O RECURSOS:.....	93
12.15.4	COMENTARIO:.....	93
12.15.5	TIEMPO:	93
12.15.6	ACTIVIDADES PASO A PASO – INCOMPATIBILIDAD CON NUEVOS SISTEMAS:	93
12.16	PLAN DE RESPUESTA AL INCIDENTE RE015-CÓDIGO: PDA015 - "ROBO DE INFORMACIÓN EN TRANSMISIÓN"	96
12.16.1	INCIDENCIA:.....	96
12.16.2	ENCARGADO:	96
12.16.3	MATERIALES O RECURSOS:.....	96
12.16.4	COMENTARIO:.....	96
12.16.5	TIEMPO:	96
12.16.6	ACTIVIDADES PASO A PASO – ROBO DE INFORMACIÓN EN TRANSMISIÓN:.....	96
12.17	PLAN DE RESPUESTA AL INCIDENTE RE016-CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"	99
12.17.1	INCIDENCIA:.....	99
12.17.2	ENCARGADO:	99
12.17.3	MATERIALES O RECURSOS:.....	99



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

12.17.4	COMENTARIO:.....	99
12.17.5	TIEMPO:	99
12.17.6	ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS:.....	99
12.18	PLAN DE RESPUESTA AL INCIDENTE RE016 - CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"	102
12.18.1	INCIDENCIA:.....	102
12.18.2	ENCARGADO:	102
12.18.3	MATERIALES O RECURSOS:.....	102
12.18.4	COMENTARIO:.....	102
12.18.5	TIEMPO:	102
12.18.6	ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS:.....	102
12.19	PLAN DE RESPUESTA AL INCIDENTE RE017 - CÓDIGO: PDA017 - "SANCIONES POR INCUMPLIMIENTO NORMATIVO"	105
12.19.1	INCIDENCIA:.....	105
12.19.2	ENCARGADO:	105
12.19.3	MATERIALES O RECURSOS:.....	105
12.19.4	COMENTARIO:.....	105
12.19.5	TIEMPO:	105
12.19.6	ACTIVIDADES PASO A PASO – SANCIONES POR INCUMPLIMIENTO NORMATIVO:	105
12.20	PLAN DE RESPUESTA AL INCIDENTE RE018 - CÓDIGO: PDA018 - "FALLOS EN RECUPERACIÓN DE DESASTRES"	108
12.20.1	INCIDENCIA:.....	108
12.20.2	ENCARGADO:	108
12.20.3	MATERIALES O RECURSOS:.....	108
12.20.4	COMENTARIO:.....	108
12.20.5	TIEMPO:	108
12.20.6	ACTIVIDADES PASO A PASO – FALLOS EN RECUPERACIÓN DE DESASTRES:	108
12.21	PLAN DE RESPUESTA AL INCIDENTE RE019 - CÓDIGO: PDA019 - "PROPAGACIÓN DE ATAQUES EN RED"	111
12.21.1	INCIDENCIA:.....	111
12.21.2	ENCARGADO:	111
12.22	MATERIALES O RECURSOS:	111
12.22.1	COMENTARIO:.....	111
12.22.2	TIEMPO:	111



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

12.22.3 ACTIVIDADES PASO A PASO – PROPAGACIÓN DE ATAQUES EN
RED: 111

12.23 PLAN DE RESPUESTA AL INCIDENTE RE020 - CÓDIGO: PDA020 -
"FALLO DE PROVEEDOR CRÍTICO" 114

12.23.1 INCIDENCIA:..... 114

12.23.2 ENCARGADO: 114

12.23.3 MATERIALES O RECURSOS:..... 114

12.23.4 COMENTARIO:..... 114

12.23.5 TIEMPO: 114

12.23.6 ACTIVIDADES PASO A PASO – FALLO DE PROVEEDOR CRÍTICO:..... 114

12.24 PLAN DE RESPUESTA AL INCIDENTE RE021 - CÓDIGO: PDA021 -
"FALLO DE EQUIPOS DE OBRA" 117

12.24.1 INCIDENCIA:..... 117

12.24.2 ENCARGADO: 117

12.24.3 MATERIALES O RECURSOS:..... 117

12.24.4 COMENTARIO:..... 117

12.24.5 TIEMPO: 117

12.24.6 ACTIVIDADES PASO A PASO – FALLO DE EQUIPOS DE OBRA: 117

13 GALERÍA DE FOTOGRAFÍAS – CEFOÍSA 120



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

TABLAS

TABLA 1: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO – PARTE1	17
TABLA 2: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 2	18
TABLA 3: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 3	19
TABLA 4: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 4	20
TABLA 5: MATRIZ DE INCIDENCIA - PARTE 1	21
TABLA 6: MATRIZ DE INCIDENCIA - PARTE 2	22
TABLA 7: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 1	23
TABLA 8: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 2	24
TABLA 9: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 3	25
TABLA 10: REGISTRO DE PROBABILIDAD, IMPACTO, NIVEL DE RIESGO	26
TABLA 11: REGISTRO DE CATEGORIZACIÓN Y RESPONSABLES	29
TABLA 12: CÓDIGO: PDA001 - FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA	55
TABLA 13: CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"	58
TABLA 14: CÓDIGO: PDA003 - "VULNERABILIDAD EN SEGURIDAD DE SOFTWARE"	61
TABLA 15: CÓDIGO: PDA004 - "PÉRDIDA DE DATOS CRÍTICOS"	64
TABLA 16: CÓDIGO: PDA005 - "COMPROMISO DE ACCESO NO AUTORIZADO"	67
TABLA 17: CÓDIGO: PDA006 - "ACCESO NO AUTORIZADO A LA RED"	70
TABLA 18: CÓDIGO: PDA007 - "TIEMPO DE INACTIVIDAD POR FALLAS EN TI"	73
TABLA 19: CÓDIGO: PDA008 - "FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES"	76
TABLA 20: CÓDIGO: PDA009 - "ERRORES HUMANOS EN TI"	79
TABLA 21: CÓDIGO: PDA010 - "INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA"	82
TABLA 22: CÓDIGO: PDA011 - "DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS"	85
TABLA 23: CÓDIGO: PDA012 - "FALLOS DE SOPORTE TÉCNICO"	88
TABLA 24: CÓDIGO: PDA013 - "CAÍDAS INESPERADAS DE LA RED"	91
TABLA 25: CÓDIGO: PDA014 - "INCOMPATIBILIDAD CON NUEVOS SISTEMAS"	94
TABLA 26: CÓDIGO: PDA015 - "ROBO DE INFORMACIÓN EN TRANSMISIÓN"	97
TABLA 27: CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"	100
TABLA 28: CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"	103
TABLA 29: - CÓDIGO: PDA017 - "SANCIONES POR INCUMPLIMIENTO NORMATIVO"	106
TABLA 30: CÓDIGO: PDA018 - "FALLOS EN RECUPERACIÓN DE DESASTRES"	109
TABLA 31: CÓDIGO: PDA019 - "PROPAGACIÓN DE ATAQUES EN RED"	112
TABLA 32: CÓDIGO: PDA020 - "FALLO DE PROVEEDOR CRÍTICO"	115



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

ILUSTRACIONES

ILUSTRACIÓN 1: ORGANIGRAMA CEFOISA SAC	13
ILUSTRACIÓN 2: MAPA DE PROCESOS CEFOISA	14
ILUSTRACIÓN 3: SOCIOS ESTRATÉGICOS - CEFOISA.....	15
ILUSTRACIÓN 4: MATRIZ DE RIESGO CEFOISA.....	16
ILUSTRACIÓN 5: NÚMERO DE INCIDENCIAS POR TIPO	31
ILUSTRACIÓN 6: TIEMPO DE RESOLUCIÓN DE INCIDENCIAS.....	31
ILUSTRACIÓN 7: NÚMERO DE INCIDENCIAS POR NIVEL DE RIESGO.....	32
ILUSTRACIÓN 8: INCIDENCIAS POR ÁREA.....	32
ILUSTRACIÓN 9: CAPACITACIÓN DE CIBERSEGURIDAD CEFOISA -OBRA.....	120
ILUSTRACIÓN 10: INCIDENTE - TOMACORRIENTE NO ES DE TIPO CIRCULAR, MALA ADAPTACIÓN PARA CONECTAR ROUTER.....	120



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

1 EMPRESA DE CONSTRURA: CEFOISA INGENIERÍA Y CONSTRUCCIÓN S.A.C

- Es una empresa que se constituyó en Perú en marzo de 1965 con el objetivo de desarrollar proyectos especializados en infraestructura portuaria. Su domicilio legal y sede social se encuentra en la avenida Benavides 2345, Miraflores, Lima. ha logrado consolidar su presencia en el mercado nacional en los años 70, destacándose como un referente en la construcción y desarrollo de proyectos portuarios y de infraestructura marítima.
- El grupo CEFOISA es un conglomerado de empresas cuyas operaciones abarcan diferentes sectores; entre las más relevantes se encuentran la construcción y mantenimiento de muelles, proyectos de infraestructura portuaria, negocios inmobiliarios en zonas costeras, y servicios especializados de logística y transporte marítimo

2 MISIÓN Y VISIÓN

2.1 MISIÓN

- Es desarrollar proyectos de infraestructura portuaria y marítima con los más altos estándares de calidad, seguridad y sostenibilidad, contribuyendo al crecimiento económico y social del Perú. Nos comprometemos a ofrecer soluciones innovadoras y eficientes que generen valor a nuestros clientes, colaboradores y comunidades, liderando el mercado de construcción en el sector portuario con responsabilidad y excelencia operativa

2.2 VISIÓN

- Ser reconocidos como el principal referente en la construcción y operación de infraestructura portuaria en América Latina, impulsando el desarrollo sostenible mediante proyectos innovadores que contribuyan al progreso de los sectores marítimos y logísticos, y manteniendo una reputación de confianza, calidad y compromiso con el medio ambiente



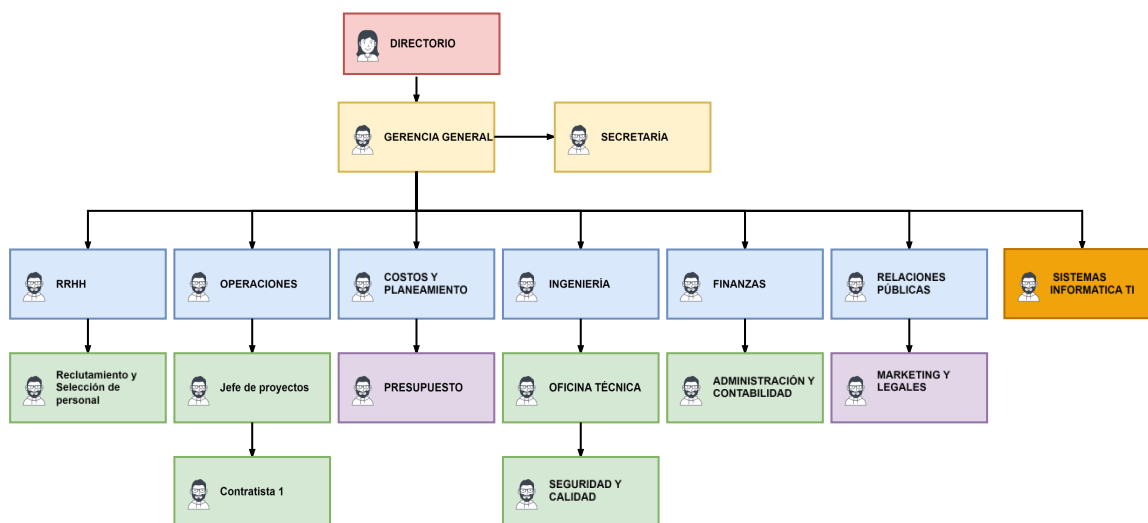
“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO “MISIONEROS MONFORTIANOS”

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

3 OBJETIVOS ESTRATÉGICOS

- Expandir nuestra presencia en América Latina, ingresando a al menos tres nuevos países de la región. Con este crecimiento, buscamos no solo aumentar nuestra participación en el mercado, sino también crear alianzas estratégicas con empresas locales para garantizar una entrada exitosa. El objetivo es alcanzar esta expansión para 2026, consolidando nuestra posición como líderes en infraestructura portuaria.
- Optimizar la eficiencia operativa reduciendo los tiempos de entrega de proyectos en un 15% y los costos operativos en un 10% en los próximos dos años. Esto se logrará mediante la implementación de nuevas tecnologías y la capacitación continua del equipo, garantizando una mayor competitividad y satisfacción de nuestros clientes.
- Certificar todos los proyectos de CEFOISA bajo la norma ISO 14001 de gestión ambiental antes de diciembre de 2025. Esta certificación asegurará que nuestras operaciones sean respetuosas con el medio ambiente, fortaleciendo nuestro compromiso con la sostenibilidad y el desarrollo responsable.
- Aumentar en un 10% la satisfacción de nuestros clientes a través de un mejor servicio y atención personalizada. Estableceremos un equipo de seguimiento post-venta y realizaremos encuestas periódicas para asegurarnos de que nuestras soluciones cumplan y superen las expectativas de quienes confían en nosotros.
- Incorporar prácticas sostenibles en al menos el 30% de nuestros proyectos en los próximos tres años. Esto implicará integrar materiales y tecnologías respetuosas con el medio ambiente en nuestras obras, con el fin de liderar en sostenibilidad y ofrecer a nuestros clientes proyectos alineados con los más altos estándares ecológicos.

4 ORGANIGRAMA DE LA EMPRESA CEFOISA





**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

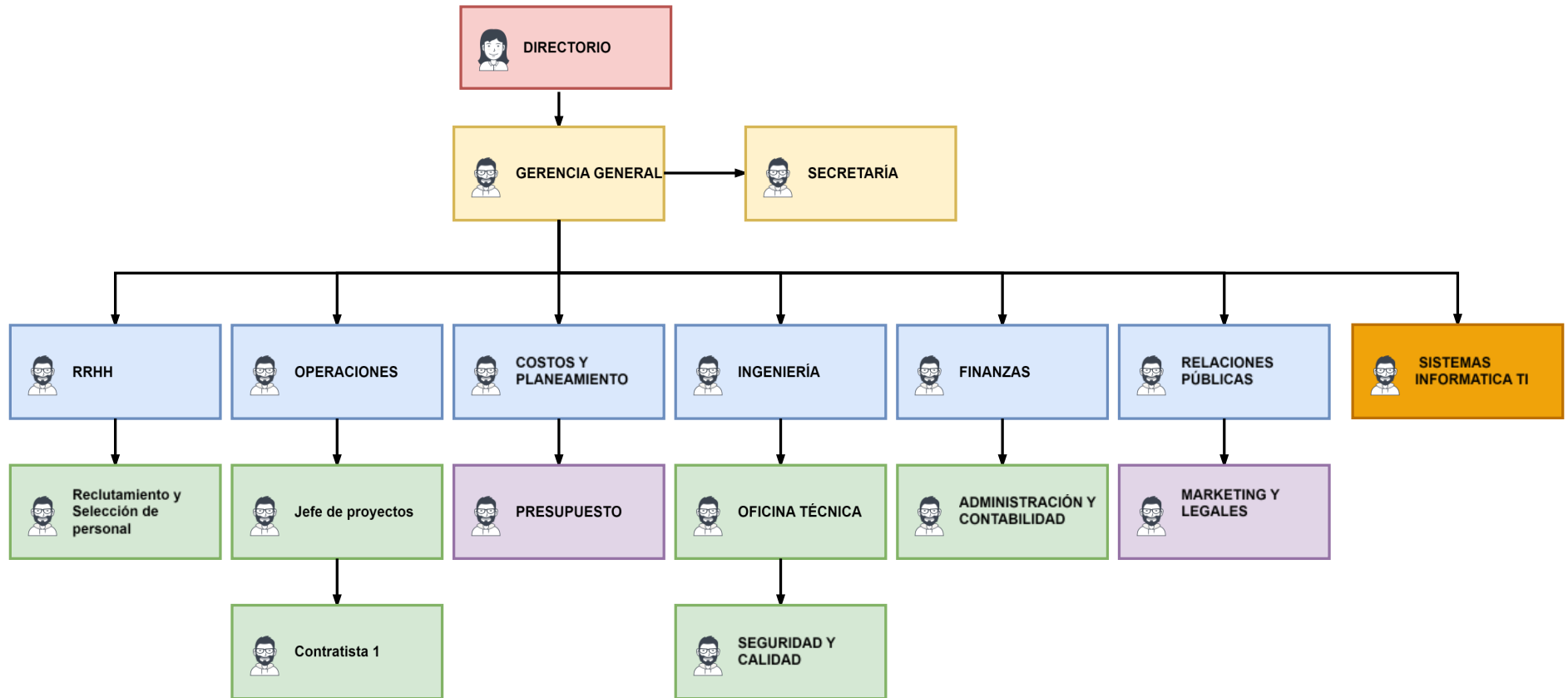


Ilustración 1: Organigrama CEFOISA SAC



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

5 MAPA DE PROCESOS DE LA EMPRESA CEFOISA



Ilustración 2: Mapa de Procesos CEFOISA



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

6 SOCIOS ESTRATÉGICOS DE LA EMPRESA CEFOISA



Nuestro clientes confían en nosotros



Ilustración 3: Socios Estratégicos - CEFOISA



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

7 IDENTIFICACIÓN DE RIESGOS EN EL ÁREA DE TI EMPRESA CEFOISA

7.1 MATRIZ DE RIESGOS

MATRIZ DE RIESGOS						
IMPACTO						
		Mínima (1)	Menor (2)	Moderada (4)	Mayor (8)	Máxima (16)
PROBABILIDAD		1	2	4	8	16
Muy Alta (5)	5	5	10	20	40	80
Alta (4)	4	4	8	16	32	64
Media (3)	3	3	6	12	24	48
Baja (2)	2	2	4	8	16	32
Muy Baja (1)	1	1	2	4	8	16

NIVEL DE RIESGO
Riesgo Aceptable
Riesgo Tolerable
Riesgo alto
Riesgo Extremo

Ilustración 4: Matriz de Riesgo CEFOISA



“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO “MISIONEROS MONFORTIANOS”

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

7.2 EVENTOS CON SU EVALUACIÓN DE PROBABILIDAD E IMPACTO

Tabla 1: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO – PARTE1

CÓDIGO	TIPO RIESGO	CAUSA	EVENTO	DESCRIPCION	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE001	Costos	1. Falta mantenimiento de cableado eléctrico por aumento de equipos en oficina. 2. Carga maxima de demanda sobrepasa el diseño de distribución eléctrica para los equipos. 3. Instalaciones eléctricas obsoletas	Tiempo muerto de servicio	Pérdida de funcionamiento de servidores, internet y equipos	Muy Alta (5)	Máxima (16)	Riesgo Extremo 80
RE002	Legal y TI	1. Software sin licencias 2. Falta de presupuesto 3. Sin inventario de licencias	Detectado en Auditorías inesperadas	Sanciones legales y administrativas	Baja (2)	Mayor (8)	Riesgo Alto 16
RE003	TI	1. Falta actualización software. 2. Sin políticas de actualización 3. Recursos insuficientes	Vulnerabilidad a ciberataques	Exposición a amenazas de seguridad	Alta (4)	Máxima (16)	Riesgo Extremo 64
RE004	Costo y TI	1. Falta respaldo de datos 2. Sin políticas backup 3. Infraestructura inadecuada	Pérdida de datos críticos de proyectos	Pérdida información crucial proyectos	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE005	Seguridad	1. Mal manejo contraseñas 2. Sin políticas seguridad 3. Sin capacitación	Acceso no autorizado	Compromiso sistemas críticos	Media (3)	Mayor (8)	Riesgo Alto 24
RE006	Seguridad y TI	1. Conexiones inseguras 2. Configuración inadecuada 3. Sin monitoreo	Acceso no autorizado a la red	Vulnerabilidad infraestructura	Media (3)	Mayor (8)	Riesgo Alto 24



“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO “MISIONEROS MONFORTIANOS”

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 2: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 2

CÓDIGO	TIPO RIESGO	CAUSA	EVENTO	DESCRIPCION	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE007	TI	1. Sin planes contingencia 2. Sin procedimientos DR/BC 3. Sin pruebas recuperación	Tiempo de inactividad por fallas en TI	Incapacidad recuperación crítica	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE008	Seguridad	1. Dispositivos personales inseguros 2. Sin políticas BYOD 3. Sin control endpoints	Fugas de información	Compromiso datos corporativos	Media (3)	Mayor (8)	Riesgo Alto 24
RE009	Costo y TI	1. Sin capacitación personal 2. Sin programas entrenamiento 3. Alta rotación	Errores humanos en TI	Incidentes por desconocimiento	Alta (4)	Moderada (4)	Riesgo Alto 16
RE010	Continuidad de Negocio y TI	1. Sobrecarga servidores 2. Capacidad inadecuada 3. Sin monitoreo recursos	Interrupción del servicio	Caída sistemas críticos	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE011	Costo y TI	1. Equipos red antiguos 2. Sin presupuesto renovación 3. Sin plan actualización	Lentitud o pérdida de conexión	Degradación servicio red	Alta (4)	Moderada (4)	Riesgo Alto 16
RE012	Continuidad de Negocio, Costos, TI	1. Proveedores poco confiables 2. Sin SLAs definidos 3. Sin evaluación proveedores	Fallos de soporte técnico	Respuesta inadecuada incidentes	Media (3)	Máxima (16)	Riesgo Extremo 48



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 3: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 3

CÓDIGO	TIPO RIESGO	CAUSA	EVENTO	DESCRIPCION	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE013	Continuidad de Negocio y TI	1. Sin monitoreo red 2. Sin herramientas monitoreo 3. Personal insuficiente	Caídas inesperadas de la red	Interrupciones no detectadas	Media (3)	Máxima (16)	Riesgo Extremo 48
RE014	Costo y TI	1. Software obsoleto 2. Resistencia cambio 3. Sin plan actualizaciones	Incompatibilidad con nuevos sistemas	Problemas integración	Alta (4)	Mayor (8)	Riesgo Extremo 32
RE015	Seguridad	1. Sin cifrado 2. Configuraciones inseguras 3. Sin políticas seguridad	Robo de información durante la transmisión	Intercepción datos sensibles	Media (3)	Máxima (16)	Riesgo Extremo 48
RE016	Seguridad	1. Fallos control acceso 2. Sistema obsoleto 3. Configuración incorrecta	Acceso no autorizado a áreas restringidas	Compromiso seguridad física	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE017	Legal	1. Incumplimiento normativas 2. Desconocimiento legal 3. Sin asesoría	Sanciones legales	Penalizaciones normativas	Baja (2)	Mayor (8)	Riesgo Alto 16
RE018	Continuidad de Negocio	1. Sin pruebas recuperación 2. Sin procedimientos 3. Sin ambiente pruebas	Fallos en la recuperación de desastres	Incapacidad restaurar servicios	Media (3)	Máxima (16)	Riesgo Extremo 48



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 4: EVALUACIÓN PROBABILIDAD E IMPACTO POR EVENTO - PARTE 4

CÓDIGO	TIPO DE RIESGO	CAUSA	EVENTO	DESCRIPCION	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE019	Seguridad Informática y TI	1. Red no segmentada 2. Diseño inadecuado 3. Sin políticas segmentación	Propagación de ataques a toda la red	Compromiso general sistemas	Media (3)	Máxima (16)	Riesgo Extremo 48
RE020	Continuidad de Negocio y Costos	1. Dependencia proveedor único 2. Sin alternativas 3. Contratos restrictivos	Fallo del proveedor	Interrupción servicios críticos	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE021	Costo y TI	1. Sin mantenimiento equipos obra 2. Condiciones adversas 3. Personal no capacitado	Fallo de equipos en campo	Interrupciones operativas sitios	Media (3)	Mayor (8)	Riesgo Alto 24



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

7.3 MATRIZ DE INCIDENCIAS

Tabla 5: MATRIZ DE INCIDENCIA - PARTE 1

Código de Incidencia	Tipo de Riesgo	Descripción de la Incidencia	Causas	Probabilidad	Impacto	Nivel de Riesgo
RE001	Costo y TI	Pérdida de funcionamiento de servidores, internet y equipos por falta de mantenimiento eléctrico.	Falta de mantenimiento de cableado, demanda que sobrepasa el diseño eléctrico, instalaciones obsoletas.	Muy Alta	Máxima	Riesgo Extremo
RE002	Legal y TI	Sanciones legales y administrativas debido a software sin licencias y falta de presupuesto.	Software sin licencias, falta de presupuesto, sin inventario de licencias.	Baja	Mayor	Riesgo Alto
RE003	TI	Exposición a amenazas de seguridad debido a falta de actualizaciones de software.	Falta de actualización de software, sin políticas de actualización, recursos insuficientes.	Alta	Máxima	Riesgo Extremo
RE004	Costo y TI	Pérdida de información crucial por falta de respaldo y políticas de backup.	Falta de respaldo de datos, sin políticas de backup, infraestructura inadecuada.	Baja	Máxima	Riesgo Extremo
RE005	Seguridad y TI	Acceso no autorizado y compromiso de sistemas críticos por mal manejo de contraseñas.	Mal manejo de contraseñas, sin políticas de seguridad, sin capacitación.	Media	Mayor	Riesgo Alto
RE006	Seguridad y TI	Vulnerabilidad de infraestructura por conexiones inseguras y configuración inadecuada.	Conexiones inseguras, configuración inadecuada, sin monitoreo.	Media	Mayor	Riesgo Alto
RE007	TI	Inactividad operativa por ausencia de planes de contingencia.	Sin planes de contingencia, sin procedimientos DR/BC, sin pruebas de recuperación.	Baja	Máxima	Riesgo Extremo
RE008	Seguridad y TI	Compromiso de datos corporativos por dispositivos personales inseguros.	Dispositivos personales inseguros, sin políticas BYOD, sin control de endpoints.	Media	Mayor	Riesgo Alto
RE009	Costo y TI	Errores humanos en TI por falta de capacitación y alta rotación de personal.	Sin capacitación del personal, sin programas de entrenamiento, alta rotación.	Alta	Moderada	Riesgo Alto
RE010	Continuidad de Negocio y TI	Interrupciones de sistemas críticos por sobrecarga de servidores.	Sobrecarga de servidores, capacidad inadecuada, sin monitoreo de recursos.	Baja	Máxima	Riesgo Extremo
RE011	Costo y TI	Degradación del servicio de red por equipos antiguos sin actualización.	Equipos de red antiguos, sin presupuesto de renovación, sin plan de actualización.	Alta	Moderada	Riesgo Alto
RE012	Continuidad de Negocio, Costos y TI	Fallos en respuesta técnica debido a proveedores poco confiables.	Proveedores poco confiables, sin SLAs definidos, sin evaluación de proveedores.	Media	Máxima	Riesgo Extremo
RE013	Continuidad de Negocio y TI	Caidas inesperadas de la red por falta de monitoreo y herramientas adecuadas.	Sin monitoreo de red, sin herramientas de monitoreo, personal insuficiente.	Media	Máxima	Riesgo Extremo
RE014	Costo y TI	Problemas de integración por uso de software obsoleto.	Software obsoleto, resistencia al cambio, sin plan de actualizaciones.	Alta	Mayor	Riesgo Extremo



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 6: MATRIZ DE INCIDENCIA - PARTE 2

Código de Incidencia	Tipo de Riesgo	Descripción de la Incidencia	Causas	Probabilidad	Impacto	Nivel de Riesgo
RE015	Seguridad TI	Intercepción de datos sensibles debido a falta de cifrado.	Sin cifrado, configuraciones inseguras, sin políticas de seguridad.	Media	Máxima	Riesgo Extremo
RE016	Seguridad	Compromiso de seguridad física debido a fallos en control de acceso.	Fallos en control de acceso, sistema obsoleto, configuración incorrecta.	Baja	Máxima	Riesgo Extremo
RE018	Continuidad de Negocio	Incapacidad de restaurar servicios por fallos en recuperación de desastres.	Sin pruebas de recuperación, sin procedimientos, sin ambiente de pruebas.	Media	Máxima	Riesgo Extremo
RE019	Seguridad, Informática y TI	Compromiso general del sistema por falta de segmentación de red.	Red no segmentada, diseño inadecuado, sin políticas de segmentación.	Media	Máxima	Riesgo Extremo
RE020	Continuidad de Negocio y Costos	Interrupción de servicios críticos por fallo del proveedor único.	Dependencia de un proveedor único, sin alternativas, contratos restrictivos.	Baja	Máxima	Riesgo Extremo
RE021	Costo y TI	Interrupciones operativas en sitios por falta de mantenimiento y condiciones adversas.	Sin mantenimiento de equipos, condiciones adversas, personal no capacitado.	Media	Mayor	Riesgo Alto



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

8 REGISTRO DE INCIDENCIAS ÁREA DE TI Y OTROS - EMPRESA CEFOSA

8.1 REGISTRO DE USUARIOS

Tabla 7: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 1

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS
RE001	Ana Pérez Cornejo	Ingeniería	11/17/2024 8:30	Insuficiencias de respuestas de servidores, del sitio web, insuficiencias del hardware por falta de distribución eléctrica para los equipos, delimitaciones en los sistemas de gestión de procesos, respuestas deficientes en del sitio web de Cefoisa.
RE002	Luis Ramírez Cornejo	Finanzas	11/16/2024 10:15	Presencia de inconsistencia y desactualizaciones, limitaciones deficientes en su utilidad funcional.
RE003	Sofía Gómez Cornejo	Ingeniería	11/15/2024 9:00	Presencia de inconsistencia en parches y desactualizaciones, recursos insuficientes.
RE004	Carlos Sánchez Cornejo	Costos y Presupuestos	11/14/2024 11:45	Gestión ineficiente en respaldo y Backus de datos, exposiciones a vulnerabilidades frecuentes.
RE005	Laura Fernández Cornejo	Seguridad	11/13/2024 14:20	Cambios informáticos leves a bruscos, en los procesos de cada actividad del sistema.
RE006	Rodrigo Vargas Cornejo	Seguridad	11/13/2024 10:00	Configuraciones o gestiones inadecuadas, conexiones o direcciones desconocidas entrantes conectadas, para su gestión.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 8: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 2

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS
RE007	Paula Navarro Cornejo	Ingeniería	11/12/2024 9:30	Limitaciones de actividades o gestiones diarias, incapacidades o reducciones de los equipos informáticos.
RE008	Daniel Lozano Cornejo	Seguridad	11/11/2024 16:00	Dispositivos personales inseguros, pésimas respuestas de asistencia contra servicios de ciberseguridad.
RE009	Clara Jiménez Cornejo	Ingeniería	11/10/2024 14:45	Respuestas no aptas ante problemas sistémicos, software no seguros para la continuidad de las actividades, accesos no autorizados.
RE010	Álvaro Méndez Cornejo	Oficina Técnica	11/9/2024 12:00	Síntoma de deficiencias sistémicas no planificadas, malas configuraciones, cambios informáticos planificados leves a bruscos, en los procesos de cada actividad del sistema.
RE011	Gabriela Herrera Cornejo	Costos y Presupuestos	11/8/2024 11:30	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por intrusos en la red.
RE012	Enrique Molina Cornejo	Oficina Técnica	11/7/2024 10:45	Presencia de insuficiencias de rendimiento, seguridad o confiabilidad, proveedores con poca confiabilidad.
RE013	Alicia Morales Cornejo	Oficina Técnica	11/6/2024 14:00	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por pérdidas o intrusos en la red.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Tabla 9: REGISTRO DE SÍNTOMAS DE USUARIOS - PARTE 3

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS
RE014	Santiago Peña Cornejo	Costos y Presupuestos	11/5/2024 13:30	Limitaciones de uso de nuevos sistemas o incompatibilidades a nuevos modelos de arquitectura.
RE015	Esteban Ríos Cornejo	Seguridad	11/4/2024 9:00	Malas configuraciones, malas prácticas humanas o exposiciones a ciberataques intencionales.
RE016	Beatriz Cruz Cornejo	Seguridad	11/3/2024 15:15	La falta de controles de acceso basados en roles, monitoreo y detecciones inadecuadas de actividades sospechosas.
RE017	Marcos Hidalgo Cornejo	Finanzas	11/2/2024 11:00	Posibles incumplimientos de normativas, exposiciones y sanciones ante las violaciones de políticas de datos confidenciales.
RE018	Lucía Varela Cornejo	Oficina Técnica	11/1/2024 13:00	Datos sin ningún respaldo ante las pérdidas o caídas, falta de prioridad con el plan con nuevas tecnologías o integraciones sistemas.
RE019	Martina Salinas Cornejo	Seguridad	10/31/2024 12:45	Sistemas de configuración de infraestructura de red inadecuados, accesos sospechosos, infiltraciones o comportamientos inadecuados.
RE020	Elena Rivas Cornejo	Oficina Técnica	10/30/2024 9:30	Interrupciones de servicio, gestión inadecuada al soporte.
RE021	Víctor Muñoz Cornejo	Costos y Planeamiento	10/29/2024 10:30	Interrupciones operativas, paulatinas o con frecuencias, condiciones defectuosas notorias en su funcionamiento.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

8.2 REGISTRO DE PROBABILIDAD IMPACTO NIVEL DE RIESGO

Tabla 10: REGISTRO DE PROBABILIDAD, IMPACTO, NIVEL DE RIESGO

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE001	Ana Pérez Cornejo	Ingeniería	11/17/2024 8:30	Insuficiencias de respuestas de servidores, del sitio web, insuficiencias del hardware por falta de distribución eléctrica para los equipos, delimitaciones en los sistemas de gestión de procesos, respuestas deficientes en del sitio web de Cefoisa.	Muy Alta (5)	Máxima (16)	Riesgo Extremo 80
RE002	Luis Ramírez Cornejo	Finanzas	11/16/2024 10:15	Presencia de inconsistencia y desactualizaciones, limitaciones deficientes en su utilidad funcional.	Baja (2)	Mayor (8)	Riesgo Alto 16
RE003	Sofía Gómez Cornejo	Ingeniería	11/15/2024 9:00	Presencia de inconsistencia en parches y desactualizaciones, recursos insuficientes.	Alta (4)	Máxima (16)	Riesgo Extremo 64
RE004	Carlos Sánchez Cornejo	Costos y Presupuestos	11/14/2024 11:45	Gestión ineficiente en respaldo y Backus de datos, exposiciones a vulnerabilidades frecuentes.	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE005	Laura Fernández Cornejo	Seguridad	11/13/2024 14:20	Cambios informáticos leves a bruscos, en los procesos de cada actividad del sistema.	Media (3)	Mayor (8)	Riesgo Alto 24
RE006	Rodrigo Vargas Cornejo	Seguridad	11/13/2024 10:00	Configuraciones o gestiones inadecuadas, conexiones o direcciones desconocidas entrantes conectadas, para su gestión.	Media (3)	Mayor (8)	Riesgo Alto 24



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE007	Paula Navarro Cornejo	Ingeniería	11/12/2024 9:30	Limitaciones de actividades o gestiones diarias, incapacidades o reducciones de los equipos informáticos.	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE008	Daniel Lozano Cornejo	Seguridad	11/11/2024 16:00	Dispositivos personales inseguros, pésimas respuestas de asistencia contra servicios de ciberseguridad.	Media (3)	Mayor (8)	Riesgo Alto 24
RE009	Clara Jiménez Cornejo	Ingeniería	11/10/2024 14:45	Respuestas no aptas ante problemas sistémicos, software no seguros para la continuidad de las actividades, accesos no autorizados.	Alta (4)	Moderada (4)	Riesgo Alto 16
RE010	Álvaro Méndez Cornejo	Oficina Técnica	11/9/2024 12:00	Síntoma de deficiencias sistémicas no planificadas, malas configuraciones, cambios informáticos planificados leves a bruscos, en los procesos de cada actividad del sistema.	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE011	Gabriela Herrera Cornejo	Costos y Presupuestos	11/8/2024 11:30	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por intrusos en la red.	Alta (4)	Moderada (4)	Riesgo Alto 16
RE012	Enrique Molina Cornejo	Oficina Técnica	11/7/2024 10:45	Presencia de insuficiencias de rendimiento, seguridad o confiabilidad, proveedores con poca confiabilidad.	Media (3)	Máxima (16)	Riesgo Extremo 48
RE013	Alicia Morales Cornejo	Oficina Técnica	11/6/2024 14:00	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por pérdidas o intrusos en la red.	Media (3)	Máxima (16)	Riesgo Extremo 48



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
RE014	Santiago Peña Cornejo	Costos y Presupuestos	11/5/2024 13:30	Limitaciones de uso de nuevos sistemas o incompatibilidades a nuevos modelos de arquitectura.	Alta (4)	Mayor (8)	Riesgo Extremo 32
RE015	Esteban Ríos Cornejo	Seguridad	11/4/2024 9:00	Malas configuraciones, malas prácticas humanas o exposiciones a ciberataques intencionales.	Media (3)	Máxima (16)	Riesgo Extremo 48
RE016	Beatriz Cruz Cornejo	Seguridad	11/3/2024 15:15	La falta de controles de acceso basados en roles, monitoreo y detecciones inadecuadas de actividades sospechosas.	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE017	Marcos Hidalgo Cornejo	Finanzas	11/2/2024 11:00	Posibles incumplimientos de normativas, exposiciones y sanciones ante las violaciones de políticas de datos confidenciales.	Baja (2)	Mayor (8)	Riesgo Alto 16
RE018	Lucía Varela Cornejo	Oficina Técnica	11/1/2024 13:00	Datos sin ningún respaldo ante las pérdidas o caídas, falta de prioridad con el plan con nuevas tecnologías o integraciones sistemas.	Media (3)	Máxima (16)	Riesgo Extremo 48
RE019	Martina Salinas Cornejo	Seguridad	10/31/2024 12:45	Sistemas de configuración de infraestructura de red inadecuados, accesos sospechosos, infiltraciones o comportamientos inadecuados.	Media (3)	Máxima (16)	Riesgo Extremo 48
RE020	Elena Rivas Cornejo	Oficina Técnica	10/30/2024 9:30	Interrupciones de servicio, gestión inadecuada al soporte.	Baja (2)	Máxima (16)	Riesgo Extremo 32
RE021	Víctor Muñoz Cornejo	Costos y Planeamiento	10/29/2024 10:30	Interrupciones operativas, paulatinas o con frecuencias, condiciones defectuosas notorias en su funcionamiento.	Media (3)	Mayor (8)	Riesgo Alto 24



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

8.3 REGISTRO DE CATEGORIZACIÓN Y RESPONSABLES

Tabla 11: REGISTRO DE CATEGORIZACIÓN Y RESPONSABLES

CÓDIGO	USUARIO	AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS	CATEGORIA	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	RESPONSABLE	FECHA Y HORA DE RESOLUCION	ACTIVIDAD DE RESOLUCION	FECHA Y HORA DE CIERRE
RE001	Ana Pérez Cornejo	Ingeniería	11/17/2024 8:30	Insuficiencias de respuestas de servidores, del sitio web, insuficiencias del hardware por falta de distribución eléctrica para los equipos, delimitaciones en los sistemas de gestión de procesos, respuestas deficientes en el sitio web de Cefoisa.	Hardware	Muy Alta (5)	Máxima (16)	Riesgo Extremo 80	Juan López Marín, Jefe de TI	11/17/2024 14:00	Reparación de cableado eléctrico y redistribución	11/17/2024 14:30
RE002	Luis Ramírez Cornejo	Finanzas	11/16/2024 10:15	Presencia de inconsistencia y desactualizaciones, limitaciones deficientes en su utilidad funcional.	Software	Baja (2)	Mayor (8)	Riesgo Alto 16	Claudia Torres Velarde, Legal	11/16/2024 16:00	Compra de licencias y creación de inventario	11/16/2024 16:30
RE003	Sofía Gómez Cornejo	Ingeniería	11/15/2024 9:00	Presencia de inconsistencia en parches y desactualizaciones, recursos insuficientes.	Seguridad	Alta (4)	Máxima (16)	Riesgo Extremo 64	Pedro Cáceres Lujan, Seguridad	11/15/2024 12:30	Implementación de actualizaciones y capacitación	11/15/2024 13:00
RE004	Carlos Sánchez Cornejo	Costos y Presupuestos	11/14/2024 11:45	Gestión ineficiente en respaldo y Backus de datos, exposiciones a vulnerabilidades frecuentes.	Seguridad	Baja (2)	Máxima (16)	Riesgo Extremo 32	María Valverde Rojas, TI	11/14/2024 15:30	Configuración de políticas backup	11/14/2024 16:00
RE005	Laura Fernández Cornejo	Seguridad	11/13/2024 14:20	Cambios informáticos leves a bruscos, en los procesos de cada actividad del sistema.	Seguridad	Media (3)	Mayor (8)	Riesgo Alto 24	Francisco Ruiz Luna, Seguridad	11/13/2024 17:00	Implementación de políticas de seguridad	11/13/2024 17:30
RE006	Rodrigo Vargas Cornejo	Seguridad	11/13/2024 10:00	Configuraciones o gestiones inadecuadas, conexiones o direcciones desconocidas entrantes conectadas, para su gestión.	Redes	Media (3)	Mayor (8)	Riesgo Alto 24	Elena Moreno Guerra, Redes	11/13/2024 15:00	Revisión y configuración adecuada de conexiones	11/13/2024 15:30
RE007	Paula Navarro Cornejo	Ingeniería	11/12/2024 9:30	Limitaciones de actividades o gestiones diarias, incapacidades o reducciones de los equipos informáticos.	Hardware	Baja (2)	Máxima (16)	Riesgo Extremo 32	Marco Torres Mayta, Infraestructura	11/12/2024 13:00	Creación de planes de contingencia y recuperación	11/12/2024 13:30
RE008	Daniel Lozano Cornejo	Seguridad	11/11/2024 16:00	Dispositivos personales inseguros, pésimas respuestas de asistencia contra servicios de ciberseguridad.	Seguridad	Media (3)	Mayor (8)	Riesgo Alto 24	Sofía Vega Cañón, Ciberseguridad	11/11/2024 20:00	Implementación de políticas BYOD y control de endpoints	11/11/2024 20:30
RE009	Clara Jiménez Cornejo	Ingeniería	11/10/2024 14:45	Respuestas no aptas ante problemas sistémicos, software no seguros para la continuidad de las actividades, accesos no autorizados.	Seguridad	Alta (4)	Moderada (4)	Riesgo Alto 16	Adrián Torres Luna, Capacitación	11/10/2024 18:00	Programa de capacitación intensivo	11/10/2024 18:30
RE010	Álvaro Méndez Cornejo	Oficina Técnica	11/9/2024 12:00	Síntoma de deficiencias sistémicas no planificadas, malas configuraciones, cambios informáticos planificados leves a bruscos, en los procesos de cada actividad del sistema.	Redes	Baja (2)	Máxima (16)	Riesgo Extremo 32	Diego Rosales Arnao, Operaciones	11/9/2024 16:30	Optimización de recursos y monitoreo de servidores	11/9/2024 17:00
RE011	Gabriela Herrera Cornejo	Costos y Presupuestos	11/8/2024 11:30	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por intrusos en la red.	Redes	Alta (4)	Moderada (4)	Riesgo Alto 16	Natalia Reyes Marín, Redes	11/8/2024 15:00	Renovación de equipos y revisión de red	11/8/2024 15:30



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

AREA	FECHA Y HORA DE INCIDENCIA	SINTOMAS	CATEGORIA	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	RESPONSABLE	FECHA Y HORA DE RESOLUCION	ACTIVIDAD DE RESOLUCION	FECHA Y HORA DE CIERRE
Oficina Técnica	11/7/2024 10:45	Presencia de insuficiencias de rendimiento, seguridad o confiabilidad, proveedores con poca confiabilidad.	Servicio	Media (3)	Máxima (16)	Riesgo Extremo 48	Fernanda López García, Proveedores	11/7/2024 15:30	Definición de SLAs y evaluación de proveedores	11/7/2024 16:00
Oficina Técnica	11/6/2024 14:00	Incapacidad de respuestas en gestiones de actividades, alteraciones en las cargas por pérdidas o intrusos en la red.	Redes	Media (3)	Máxima (16)	Riesgo Extremo 48	Jorge Navarro Ramirez, Redes	11/6/2024 18:00	Instalación de herramientas de monitoreo	11/6/2024 18:30
Costos y Presupuestos	11/5/2024 13:30	Limitaciones de uso de nuevos sistemas o incompatibilidades a nuevos modelos de arquitectura.	Software	Alta (4)	Mayor (8)	Riesgo Extremo 32	Valeria Ortiz Cocco, TI	11/5/2024 16:00	Planificación de actualizaciones y capacitaciones	11/5/2024 16:30
Seguridad	11/4/2024 9:00	Malas configuraciones, malas prácticas humanas o exposiciones a ciberataques intencionales.	Seguridad	Media (3)	Máxima (16)	Riesgo Extremo 48	Rafael Pérez Vila, Seguridad	11/4/2024 13:00	Implementación de políticas de cifrado	11/4/2024 13:30
Seguridad	11/3/2024 15:15	La falta de controles de acceso basados en roles, monitoreo y detecciones inadecuadas de actividades sospechosas.	Seguridad	Baja (2)	Máxima (16)	Riesgo Extremo 32	Alejandro Castillo Vega, Seguridad	11/3/2024 18:30	Configuración de controles basados en roles	11/3/2024 19:00
Finanzas	11/2/2024 11:00	Posibles incumplimientos de normativas, exposiciones y sanciones ante las violaciones de políticas de datos confidenciales.	Servicio	Baja (2)	Mayor (8)	Riesgo Alto 16	Andrea Méndez Huayta, Legal	11/2/2024 15:00	Revisión normativa y asesoría especializada	11/2/2024 15:30
Oficina Técnica	11/1/2024 13:00	Datos sin ningún respaldo ante las pérdidas o caídas, falta de prioridad con el plan con nuevas tecnologías o integraciones sistemas.	Redes	Media (3)	Máxima (16)	Riesgo Extremo 48	Antonio Díaz Pena, TI	11/1/2024 17:00	Implementación de procedimientos DR/BC	11/1/2024 17:30
Seguridad	10/31/2024 12:45	Sistemas de configuración de infraestructura de red inadecuados, accesos sospechosos, infiltraciones o comportamientos inadecuados.	Seguridad	Media (3)	Máxima (16)	Riesgo Extremo 48	Manuel Serrano Tulio, Infraestructura	10/31/2024 16:30	Segmentación de red y fortalecimiento de seguridad	10/31/2024 17:00
Oficina Técnica	10/30/2024 9:30	Interrupciones de servicio, gestión inadecuada al soporte.	Servicio	Baja (2)	Máxima (16)	Riesgo Extremo 32	Felipe Ruiz Vega, Proveedores	10/30/2024 13:00	Definición de alternativas con nuevos proveedores	10/30/2024 13:30
Costos y Planeamiento	10/29/2024 10:30	Interrupciones operativas, paulatinas o con frecuencias, condiciones defectuosas notorias en su funcionamiento.	Hardware	Media (3)	Mayor (8)	Riesgo Alto 24	Laura Medina Rojas, Operaciones	10/29/2024 14:30	Mantenimiento de equipos y actualización de sistemas	10/29/2024 15:00



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

9 KEY PERFORMANCE INDICATOR

9.1 KPIS CALCULADOS

9.1.1 NÚMERO TOTAL DE INCIDENCIAS POR CATEGORÍA

Mide la cantidad de incidencias en cada categoría para identificar áreas críticas.

Resultados:

Hardware: 4

Software: 2

Redes: 5

Seguridad: 7

Servicio: 3

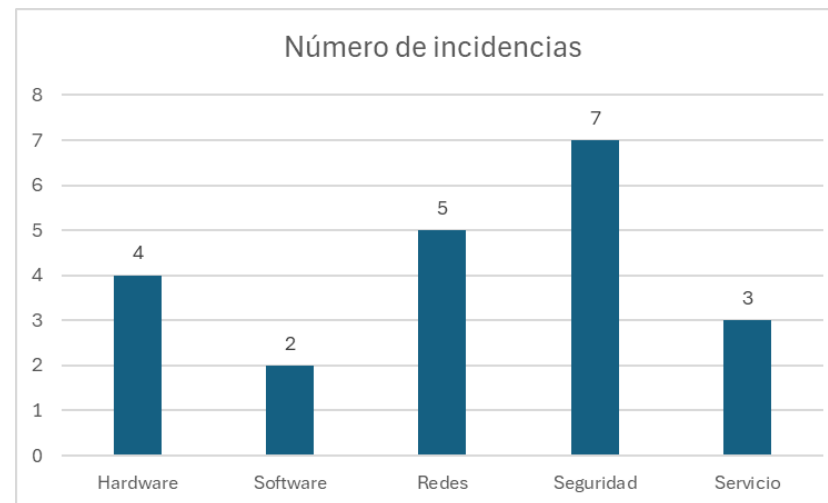


Ilustración 5: NÚMERO DE INCIDENCIAS POR TIPO

9.1.2 PROMEDIO DE RESOLUCIÓN (HORAS)

Mide el tiempo promedio requerido para resolver incidencias.

Cálculo: (Resolución - Incidencia) para cada caso.

Resultado: 4.25 horas (promedio general).

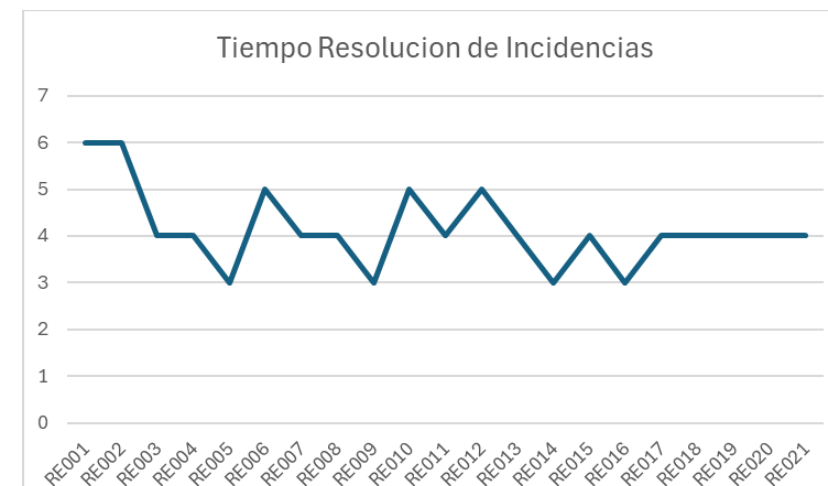


Ilustración 6: TIEMPO DE RESOLUCIÓN DE INCIDENCIAS



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

9.1.3 INCIDENCIAS POR NIVEL DE RIESGO

Ayuda a priorizar las acciones basadas en el nivel de riesgo.

Resultados:

Riesgo Extremo: 11

Riesgo Alto: 10

Riesgo Moderado o Bajo: 0

9.1.4 INCIDENCIAS DETECTADAS POR ÁREA

Mide la cantidad de incidencias asignadas a diferentes áreas.

Resultados:

Ingeniería: 8

Finanzas: 5

Costos y Presupuestos: 4

Seguridad: 2

Oficina Técnica: 2



Ilustración 7: NÚMERO DE INCIDENCIAS POR NIVEL DE RIESGO

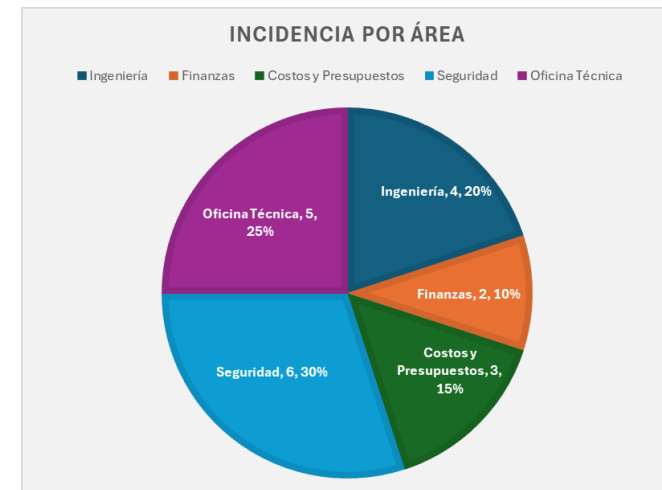


Ilustración 8: INCIDENCIAS POR ÁREA



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**


“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10 POPUSTA DE MITIGACIONES Y COSTO DE MITIGACIÓN

10.1 RE001 - MANTENIMIENTO ELÉCTRICO Y ACTUALIZACIÓN DE CABLEADO

Se decide implementar un plan de mantenimiento eléctrico preventivo y monitoreo de carga para evitar fallos en el funcionamiento de servidores y equipos críticos debido a sobrecargas y cableado obsoleto.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE001	<p>Pérdida de funcionamiento de servidores y equipos por falta de mantenimiento eléctrico</p> 	50,000 (debido a pérdida de productividad y reparación de equipos)	15,000 (mantenimiento y actualización del cableado eléctrico)	<p>Implementar un plan de mantenimiento eléctrico preventivo y monitoreo regular de la carga.</p> <p>Observación: El encargado indica que este trabajo no estuvo contemplado porque no se vió problemas.</p> <p>Recuperación de Inversión: El gasto en realizar el mantenimiento es menor que las perdidas, por lo tanto es recuperable desde el primer mes la inversión.</p>

RE001 - Mantenimiento Eléctrico y Actualización de Cableado

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Mano de obra (5 técnicos electricistas)	Jornada	5	S/ 500.00	S/ 2,500.00
Materiales (cableado eléctrico, herramientas)	global	1	S/ 3,000.00	S/ 3,000.00
Pruebas de carga y certificación	Servicio	1	S/ 1,500.00	S/ 1,500.00
Supervisión y monitoreo	Jornada	2	S/ 400.00	S/ 800.00
Subtotal				S/ 7,800.00
IGV (18%)				S/ 1,404.00
Total Mitigación RE002				S/ 9,204.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.2 RE002 - ADQUISICIÓN DE LICENCIAS Y CONTROL DE INVENTARIO

Para prevenir sanciones legales y asegurar el uso adecuado de software, se adquieren las licencias necesarias y se establece un control de inventario de software, evitando problemas de cumplimiento normativo y riesgos de auditorías.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE002	<p>Sanciones legales por uso de software sin licencias</p> 	25,000 (Sanciones y multas por auditorías)	8,024 (Adquisición de licencias y control de inventario)	Adquirir licencias de software y establecer un inventario controlado. Observación: Falta de inventario impidió cumplimiento normativo. Recuperación: Recuperable evitando multas y mejorando la gestión.

RE002 - Adquisición de Licencias y Control de Inventario

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Licencias de software (paquete anual)	Paquete	1	S/ 5,000.00	S/ 5,000.00
Implementación y configuración del inventario	Servicio	1	S/ 1,200.00	S/ 1,200.00
Capacitación del personal en gestión de licencias	Jornada	2	S/ 300.00	S/ 600.00
Subtotal				S/ 6,800.00
IGV (18%)				S/ 1,224.00
Total Mitigación RE002				S/ 8,024.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.3 RE003 - POLÍTICAS DE ACTUALIZACIÓN DE SOFTWARE

La implementación de políticas de actualización de software y un presupuesto adecuado para ciberseguridad reducen el riesgo de ciberataques al mantener el software actualizado y protegido.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE003	Exposición a ciberataques por falta de actualización de software 	100,000 (Posibles pérdidas de datos y reputación)	9,440 (Política de actualización y refuerzo de ciberseguridad)	Implementar políticas de actualización y asignar recursos para ciberseguridad. Observación: Faltan recursos de actualización. Recuperación: Mitigación de ataques y pérdida de datos valiosos.

RE003 - Implementación de Políticas de Actualización de Software

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Mano de obra (técnico en TI)	Jornada	5	S/ 400.00	S/ 2,000.00
Licencias y actualizaciones de software	Paquete	1	S/ 3,500.00	S/ 3,500.00
Pruebas de ciberseguridad post-actualización	Servicio	1	S/ 1,500.00	S/ 1,500.00
Supervisión y auditoría de cumplimiento	Jornada	2	S/ 500.00	S/ 1,000.00
Subtotal				S/ 8,000.00
IGV (18%)				S/ 1,440.00
Total Mitigación RE003				S/ 9,440.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.4 RE004 - POLÍTICAS DE BACKUP Y MEJORA DE INFRAESTRUCTURA

Para asegurar la integridad de los datos críticos, se establecen políticas de respaldo con backups automáticos en infraestructuras seguras, minimizando el riesgo de pérdida de datos y garantizando la continuidad de la información.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE004	<p>Pérdida de datos críticos por falta de respaldo</p> 	200,000 (Pérdida de datos irreversibles)	17,936 (Infraestructura de backup y políticas de respaldo)	Implementar políticas de respaldo automáticas. Observación: Sin backup anterior. Recuperación: Garantía de recuperación y continuidad en operaciones.

RE004 - Implementación de Políticas de Backup y Mejora de Infraestructura

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Servidores de backup	Unidad	1	S/ 10,000.00	S/ 10,000.00
Mano de obra (técnico en sistemas)	Jornada	3	S/ 500.00	S/ 1,500.00
Software de gestión de backups	Licencia	1	S/ 2,500.00	S/ 2,500.00
Pruebas de recuperación de datos	Servicio	1	S/ 1,200.00	S/ 1,200.00
Subtotal				S/ 15,200.00
IGV (18%)				S/ 2,736.00
Total Mitigación RE004				S/ 17,936.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.5 RE005 - GESTIÓN DE CONTRASEÑAS Y SEGURIDAD DE ACCESO

Se capacita al personal en la gestión segura de contraseñas y se establecen políticas de autenticación robustas, asegurando el acceso controlado a los sistemas y previniendo accesos no autorizados.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE005	<p>Acceso no autorizado a sistemas por mal manejo de contraseñas</p> 	30,000 (Restauración de sistemas comprometidos)	5,000 (Capacitación y gestión de contraseñas)	<p>Fortalecer seguridad de contraseñas y autenticación.</p> <p>Observación: Falta de capacitación. Recuperación: Protección preventiva y reducción de incidentes.</p>

RE005 - Gestión de Contraseñas y Seguridad en el Acceso

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Capacitación en gestión de contraseñas	Jornada	2	S/ 400.00	S/ 800.00
Software de gestión de contraseñas	Licencia	1	S/ 4,000.00	S/ 4,000.00
Supervisión de accesos y monitoreo	Jornada	2	S/ 400.00	S/ 800.00
Subtotal				S/ 5,600.00
IGV (18%)				S/ 1,008.00
Total Mitigación RE005				S/ 6,608.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.6 RE006 - CONFIGURACIÓN SEGURA DE RED

Con la configuración segura de red y un monitoreo continuo, se evitan accesos no autorizados que podrían poner en riesgo la infraestructura de TI.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE006	Vulnerabilidad de red por conexiones inseguras 	40,000 (Costos de incidentes de acceso no autorizado)	12,000 (Mejoras en configuración y monitoreo de red)	Configurar y monitorear accesos a la red. Observación: Falta de controles de acceso. Recuperación: Protección de la infraestructura y seguridad de red.

RE006 - Fortalecimiento de la Configuración de Red

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Configuración y actualización de red	Servicio	1	S/ 5,000.00	S/ 5,000.00
Monitoreo y auditoría de accesos	Jornada	4	S/ 500.00	S/ 2,000.00
Equipo de seguridad de red	Paquete	1	S/ 5,000.00	S/ 5,000.00
Subtotal				S/ 12,000.00
IGV (18%)				S/ 2,160.00
Total Mitigación RE006				S/ 14,160.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.7 RE007 - DESARROLLO DE PLANES DE CONTINGENCIA EN TI

La creación de planes de recuperación de TI con pruebas periódicas garantiza que, ante fallas, la recuperación de sistemas sea rápida y efectiva, minimizando los tiempos de inactividad.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE007	Incapacidad de recuperación ante fallas de TI por falta de planes de contingencia 	150,000 (Interrupción y pérdida de productividad)	30,000 (Desarrollo y pruebas de planes de recuperación)	Crear planes de recuperación y contingencia. Observación: No existen planes actuales. Recuperación: Garantiza disponibilidad ante fallas graves.

RE007 - Planes de Contingencia para Recuperación en TI

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Desarrollo de planes de recuperación	Servicio	1	S/ 15,000.00	S/ 15,000.00
Pruebas de recuperación y simulaciones	Jornada	4	S/ 2,000.00	S/ 8,000.00
Capacitación en planes de contingencia	Jornada	3	S/ 1,000.00	S/ 3,000.00
Subtotal				S/ 26,000.00
IGV (18%)				S/ 4,680.00
Total Mitigación RE007				S/ 30,680.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.8 RE008 - POLÍTICA BYOD Y CONTROL DE ENDPOINTS

Estableciendo políticas de uso seguro para dispositivos personales, Bring Your Own Device (BYOD) y control de puntos de acceso, se mitiga el riesgo de fuga de información corporativa, especialmente en entornos donde se permite el uso de dispositivos externos.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE008	Fugas de información por uso de dispositivos personales inseguros 	60,000 (Pérdidas de datos y riesgo reputacional)	18,000 (Políticas BYOD y control de dispositivos)	Establecer políticas BYOD y asegurar dispositivos. Observación: Sin control de BYOD previo. Recuperación: Evita fugas y asegura integridad de datos.

RE008 - Política de BYOD y Control de Endpoints

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Implementación de políticas BYOD	Servicio	1	S/ 8,000.00	S/ 8,000.00
Herramientas de control de endpoints	Paquete	1	S/ 8,000.00	S/ 8,000.00
Capacitación en seguridad de dispositivos	Jornada	2	S/ 1,200.00	S/ 2,400.00
Subtotal				S/ 18,400.00
IGV (18%)				S/ 3,312.00
Total Mitigación RE008				S/ 21,712.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.9 RE009 - CAPACITACIÓN CONTINUA EN TI

Se implementa un programa de capacitación continua para el personal de TI, disminuyendo los errores humanos y aumentando la competencia operativa, lo cual es esencial para reducir incidentes derivados de desconocimiento.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE009	Errores humanos en TI debido a falta de capacitación 	20,000 (Incidentes y errores de operación)	10,000 (Programa de capacitación continua)	Implementar programa de entrenamiento en TI. Observación: Alta rotación de personal. Recuperación: Previene errores y mejora eficiencia.

RE009 - Capacitación Continua en TI

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Programa de entrenamiento anual	Jornada	5	S/ 1,500.00	S/ 7,500.00
Materiales de capacitación	Paquete	1	S/ 2,000.00	S/ 2,000.00
Supervisión y evaluación	Jornada	1	S/ 500.00	S/ 500.00
Subtotal				S/ 10,000.00
IGV (18%)				S/ 1,800.00
Total Mitigación RE009				S/ 11,800.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.10 RE010 - MONITOREO Y OPTIMIZACIÓN DE SERVIDORES CRÍTICOS

La actualización de hardware en servidores críticos y el monitoreo constante de recursos aseguran la continuidad del servicio, evitando interrupciones por sobrecarga.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE010	Interrupción del servicio por sobrecarga de servidores 	100,000 (Caídas y pérdidas en sistemas críticos)	22,000 (Monitoreo y actualización de recursos)	Optimizar recursos de servidores y monitorear. Observación: Sin monitoreo actual. Recuperación: Evita caídas costosas y garantiza continuidad.

RE010 - Monitoreo y Optimización de Servidores Críticos

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Actualización de hardware en servidores	Unidad	2	S/ 8,000.00	S/ 16,000.00
Monitoreo de recursos	Servicio	1	S/ 5,000.00	S/ 5,000.00
Supervisión	Jornada	1	S/ 1,000.00	S/ 1,000.00
Subtotal				S/ 22,000.00
IGV (18%)				S/ 3,960.00
Total Mitigación RE010				S/ 25,960.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.11 RE011 - ACTUALIZACIÓN DE EQUIPOS DE RED

Para mejorar la conectividad y evitar problemas de lentitud, se decide actualizar los equipos de red obsoletos y establecer un plan de renovación de tecnología, con lo que se optimiza el rendimiento de la infraestructura.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE011	Lentitud y pérdida de conexión por equipos de red antiguos 	35,000 (Pérdida de productividad y conexión)	15,000 (Actualización de equipos de red)	Renovar y actualizar equipos de red. Observación: Equipos obsoletos sin presupuesto. Recuperación: Mejora la velocidad y confiabilidad de la red.

RE011 - Actualización de Equipos de Red

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Equipos de red nuevos	Unidad	3	S/ 4,000.00	S/ 12,000.00
Instalación y configuración	Jornada	2	S/ 1,000.00	S/ 2,000.00
Supervisión	Jornada	1	S/ 1,000.00	S/ 1,000.00
Subtotal				S/ 15,000.00
IGV (18%)				S/ 2,700.00
Total Mitigación RE011				S/ 17,700.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.12 RE012 - DEFINICIÓN DE SLAS Y EVALUACIÓN DE PROVEEDORES

Definir acuerdos de nivel de servicio (SLAs) y realizar evaluaciones periódicas de proveedores permite asegurar un soporte técnico confiable, reduciendo el riesgo de interrupciones de servicio.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE012	Fallos en soporte técnico por proveedores poco confiables 	70,000 (Respuesta deficiente ante incidentes)	10,000 (Definición de SLAs y evaluación de proveedores)	Establecer SLAs y evaluar proveedores. Observación: No se evaluó confiabilidad de proveedores. Recuperación: Mejora el soporte técnico y garantiza respuesta adecuada.

RE012 - Definición de SLAs y Evaluación de Proveedores

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Consultoría para definición de SLAs	Servicio	1	S/ 7,000.00	S/ 7,000.00
Evaluación y auditoría de proveedores	Jornada	2	S/ 1,500.00	S/ 3,000.00
Subtotal				S/ 10,000.00
IGV (18%)				S/ 1,800.00
Total Mitigación RE012				S/ 11,800.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.13 RE013 - IMPLEMENTACIÓN DE HERRAMIENTAS DE MONITOREO DE RED

La implementación de herramientas de monitoreo de red y asignación de personal de soporte permite identificar y resolver problemas de red antes de que causen caídas inesperadas, asegurando la estabilidad de la red.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE013	Caídas inesperadas de la red por falta de monitoreo 	120,000 (Interrupciones no detectadas y costosas)	15,000 (Herramientas de monitoreo y soporte)	Implementar herramientas y monitoreo continuo. Observación: Falta de monitoreo constante. Recuperación: Minimiza interrupciones y garantiza operatividad.

RE013 - Implementación de Herramientas de Monitoreo

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Herramientas de monitoreo de red	Paquete	1	S/ 12,000.00	S/ 12,000.00
Capacitación en uso de herramientas	Jornada	2	S/ 1,500.00	S/ 3,000.00
Subtotal				S/ 15,000.00
IGV (18%)				S/ 2,700.00
Total Mitigación RE013				S/ 17,700.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.14 RE014 - PLAN DE ACTUALIZACIÓN DE SOFTWARE

Un plan de actualización y gestión de versiones de software previene problemas de compatibilidad y asegura que los sistemas operen de manera óptima con nuevas tecnologías.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE014	Incompatibilidad con nuevos sistemas por software obsoleto 	90,000 (Problemas de integración y retrasos)	20,000 (Plan de actualizaciones de software)	Crear plan de actualización de software. Observación: Sin actualizaciones desde versiones previas. Recuperación: Facilita la integración y reduce problemas de compatibilidad.

RE014 - Plan de Actualización de Software

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Actualización de software	Licencia	1	S/ 15,000.00	S/ 15,000.00
Configuración y pruebas de compatibilidad	Jornada	2	S/ 2,500.00	S/ 5,000.00
Subtotal				S/ 20,000.00
IGV (18%)				S/ 3,600.00
Total Mitigación RE014				S/ 23,600.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.15 RE015 - IMPLEMENTACIÓN DE CIFRADO EN TRANSMISIÓN DE DATOS

La implementación de cifrado en la transmisión de datos y políticas de seguridad protegen la información sensible contra interceptaciones y aseguran la confidencialidad durante la transmisión de datos.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE015	Robo de información durante transmisión por falta de cifrado 	80,000 (Exposición de datos sensibles)	12,000 (Políticas de cifrado y seguridad)	Implementar cifrado de datos y transmisión segura. Observación: No se cifraban datos sensibles. Recuperación: Evita interceptación de información sensible y mejora seguridad.

RE015 - Implementación de Cifrado en Transmisión de Datos

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Herramientas de cifrado	Licencia	1	S/ 10,000.00	S/ 10,000.00
Configuración y prueba de cifrado	Jornada	1	S/ 2,000.00	S/ 2,000.00
Subtotal				S/ 12,000.00
IGV (18%)				S/ 2,160.00
Total Mitigación RE015				S/ 14,160.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.16 RE016 - FORTALECIMIENTO DE SEGURIDAD FÍSICA Y CONTROL DE ACCESOS

Fortalecer los controles de acceso físico en áreas restringidas reduce el riesgo de accesos no autorizados y asegura que las áreas críticas estén protegidas.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE016	<p>Acceso no autorizado a áreas restringidas por fallos en control de acceso</p> 	50,000 (Compromiso de seguridad física)	10,000 (Actualización del sistema de control)	Fortalecer control de acceso a áreas seguras. Observación: Sistema obsoleto. Recuperación: Mejora la seguridad y evita accesos no autorizados.

RE016 - Fortalecimiento de Seguridad Física y Control de Accesos

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Sistema de control de acceso actualizado	Unidad	1	S/ 8,000.00	S/ 8,000.00
Instalación y configuración	Jornada	1	S/ 2,000.00	S/ 2,000.00
Subtotal				S/ 10,000.00
IGV (18%)				S/ 1,800.00
Total Mitigación RE016				S/ 11,800.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.17 RE017 - ASESORÍA LEGAL PARA CUMPLIMIENTO NORMATIVO

Para prevenir sanciones legales, se contrata asesoría legal y se realizan auditorías periódicas, asegurando que se cumplan todas las normativas aplicables y evitando penalizaciones.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE017	<p>Sanciones legales por incumplimiento de normativas</p> 	30,000 (Multas y penalidades legales)	7,000 (Asesoría legal y auditorías de cumplimiento)	<p>Contar con asesoría legal y realizar auditorías. Observación: Sin evaluación previa de cumplimiento. Recuperación: Asegura el cumplimiento y evita sanciones futuras.</p>

RE017 - Asesoría Legal para Cumplimiento Normativo

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Asesoría legal en cumplimiento normativo	Servicio	1	S/ 5,000.00	S/ 5,000.00
Auditoría de normativas	Jornada	1	S/ 2,000.00	S/ 2,000.00
Subtotal				S/ 7,000.00
IGV (18%)				S/ 1,260.00
Total Mitigación RE017				S/ 8,260.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.18 RE018 - PRUEBAS DE RECUPERACIÓN EN CASO DE DESASTRES

Realizar pruebas periódicas de recuperación y actualizar los planes de recuperación asegura que los servicios críticos puedan ser restaurados de forma efectiva tras un desastre, mitigando el impacto de interrupciones.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE018	Fallos en recuperación de desastres por falta de pruebas 	200,000 (Impacto en restauración de servicios)	25,000 (Pruebas de recuperación y mejora en planes)	Realizar pruebas y mejorar planes de recuperación. Observación: Sin pruebas actuales. Recuperación: Asegura restauración rápida y evita pérdidas prolongadas.

RE018 - Pruebas de Recuperación en Caso de Desastres

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Pruebas de recuperación de desastres	Servicio	1	S/ 20,000.00	S/ 20,000.00
Capacitación en recuperación ante desastres	Jornada	2	S/ 2,500.00	S/ 5,000.00
Subtotal				S/ 25,000.00
IGV (18%)				S/ 4,500.00
Total Mitigación RE018				S/ 29,500.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.19 RE019 - IMPLEMENTACIÓN DE SEGMENTACIÓN DE RED

La configuración de segmentación en la red limita la propagación de ataques, protegiendo los sistemas y garantizando una mayor seguridad en la infraestructura de red.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE019	Propagación de ataques en red por falta de segmentación 	100,000 (Compromiso general de sistemas)	15,000 (Segmentación de red y refuerzo de seguridad)	Implementar segmentación de red y seguridad. Observación: Sin políticas de segmentación. Recuperación: Reduce el alcance de ataques y protege integridad de la red.

RE019 - Implementación de Segmentación de Red

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Configuración de segmentación de red	Servicio	1	S/ 12,000.00	S/ 12,000.00
Pruebas de segmentación	Jornada	1	S/ 3,000.00	S/ 3,000.00
Subtotal				S/ 15,000.00
IGV (18%)				S/ 2,700.00
Total Mitigación RE019				S/ 17,700.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.20 RE020 - DIVERSIFICACIÓN DE PROVEEDORES CRÍTICOS

Diversificar proveedores reduce la dependencia de un solo proveedor, asegurando que la cadena de suministro no se vea afectada ante un fallo o interrupción de servicio por parte de uno de ellos.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE020	<p>Fallo del proveedor crítico por dependencia de un solo proveedor</p> 	150,000 (Riesgo de interrupción de servicios críticos)	18,000 (Diversificación y contingencias con proveedores)	<p>Diversificar proveedores y establecer contingencias.</p> <p>Observación: Dependencia excesiva. Recuperación: Minimiza impacto de fallos y asegura continuidad de servicio.</p>

RE020 - Diversificación de Proveedores

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Búsqueda y evaluación de proveedores	Servicio	1	S/ 15,000.00	S/ 15,000.00
Documentación y acuerdos de contingencia	Jornada	1	S/ 3,000.00	S/ 3,000.00
Subtotal				S/ 18,000.00
IGV (18%)				S/ 3,240.00
Total Mitigación RE020				S/ 21,240.00




**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

10.21 RE021 - PLAN DE MANTENIMIENTO PREVENTIVO DE EQUIPOS DE OBRA

Establecer un plan de mantenimiento preventivo para equipos de obra y capacitar al personal minimiza el riesgo de fallos en el equipo, asegurando la continuidad operativa en campo.

PROPUESTA DE MITIGACION

Código de Riesgo	Descripción del Evento	Pérdida Financiera (S/.)	Costo de Mitigación (S/.)	Conclusión
RE021	Fallo de equipos en campo por falta de mantenimiento 	60,000 (Impacto operativo en sitios de trabajo)	12,000 (Programas de mantenimiento y capacitación)	Implementar plan de mantenimiento preventivo. Observación: Sin mantenimiento previo. Recuperación: Reduce interrupciones y prolonga vida útil de equipos.

RE021 - Plan de Mantenimiento Preventivo de Equipos de Obra

Descripción	Unidad	Cantidad	Precio Unitario (S/.)	Costo Total (S/.)
Mantenimiento de equipos	Servicio	1	S/ 10,000.00	S/ 10,000.00
Capacitación del personal	Jornada	1	S/ 2,000.00	S/ 2,000.00
Subtotal				S/ 12,000.00
IGV (18%)				S/ 2,160.00
Total Mitigación RE021				S/ 14,160.00



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11 ELABORACIÓN PLANES DE RESPUESTAS A INCIDENTES CON MEDIDAS DE CONTENCIÓN Y MITIGACIÓN RECOMENDADAS.

11.1 PLAN DE RESPUESTA AL INCIDENTE RE001 - CÓDIGO: PDA001 - "FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA"

11.1.1 INCIDENCIA:

Pérdida de funcionamiento de servidores, internet y equipos por fallas en el sistema eléctrico y cableado obsoleto.

11.1.2 ENCARGADO:

Juan López Marín, Jefe de TI

11.1.3 MATERIALES O RECURSOS:

- Herramientas de diagnóstico eléctrico
- Multímetros y analizadores de red
- Material de cableado eléctrico
- UPS de respaldo
- Equipos de protección personal
- 5 técnicos electricistas
- Documentación técnica

11.1.4 COMENTARIO:

Se requiere actualización urgente del sistema eléctrico debido a la obsolescencia del cableado actual y el incremento de equipos. La situación presenta un riesgo crítico para la operación continua de los sistemas.

11.1.5 TIEMPO:

5.5 horas totales (2 horas contención inicial + 3.5 horas resolución)

11.1.6 ACTIVIDADES PASO A PASO – FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA:

Evaluación inicial rápida del sistema eléctrico y activación de UPS/sistemas de respaldo (30 min)

Desconexión de sistemas no críticos para reducir la carga eléctrica (30 min)

Diagnóstico detallado del sistema eléctrico y puntos de fallo (1 hora)

Reparación y actualización del cableado eléctrico deteriorado (2 horas)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

Redistribución de cargas eléctricas según capacidad de los circuitos (1 hora)

Pruebas de funcionamiento y verificación de sistemas (1 hora)

Documentación de cambios realizados y actualización de planos eléctricos (30 min)

Tabla 12: CÓDIGO: PDA001 - FALLO ELÉCTRICO EN INFRAESTRUCTURA CRÍTICA

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Pérdida de funcionamiento de servidores, internet y equipos por fallas en el sistema eléctrico y cableado obsoleto.	Juan López Marín, Jefe de TI	<ul style="list-style-type: none">• Herramientas de diagnóstico eléctrico• Multímetros y analizadores de red• Material de cableado eléctrico• UPS de respaldo• Equipos de protección personal• 5 técnicos electricistas• Documentación técnica
COMENTARIO:		TIEMPO
Se requiere actualización urgente del sistema eléctrico debido a la obsolescencia del cableado actual y el incremento de equipos. La situación presenta un riesgo crítico para la operación continua de los sistemas.		5.5 horas totales (2 horas contención inicial + 3.5 horas resolución)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.2 PLAN DE RESPUESTA AL INCIDENTE RE002 - CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"

11.2.1 INCIDENCIA:

Sanciones legales y administrativas por uso de software sin licencias y falta de control de inventario.

11.2.2 ENCARGADO:

Claudia Torres Velarde, Legal

11.2.3 MATERIALES O RECURSOS:

- Licencias de software
- Software de gestión de inventario
- Personal de TI para instalación
- Documentación legal de licencias
- Sistema de control de activos
- Personal para capacitación
- Presupuesto asignado

11.2.4 COMENTARIO:

Urgente regularización de licencias de software y establecimiento de un sistema de control de inventario para evitar futuras sanciones. El incumplimiento actual representa un riesgo legal y financiero significativo.

11.2.5 TIEMPO:

5.75 horas totales (1.5 horas evaluación inicial + 4.25 horas implementación)

11.2.6 ACTIVIDADES PASO A PASO – REGULARIZACIÓN DE LICENCIAS DE SOFTWARE:

Inventario y auditoría inicial de software instalado (1 hora)
Evaluación de requerimientos legales y licencias faltantes (30 min)
Gestión de adquisición de licencias necesarias (2 horas)
Implementación de sistema de control de inventario (1.5 horas)
Instalación y registro de licencias adquiridas (30 min)
Configuración de políticas de control de software (15 min)
Capacitación básica al personal y documentación (15 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.3 PLAN DE RESPUESTA AL INCIDENTE RE002 - CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"

Tabla 13: CÓDIGO: PDA002 - "REGULARIZACIÓN DE LICENCIAS DE SOFTWARE"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Sanciones legales y administrativas por uso de software sin licencias y falta de control de inventario.	Claudia Torres Velarde, Legal	<ul style="list-style-type: none"> • Licencias de software • Software de gestión de inventario • Personal de TI para instalación • Documentación legal de licencias • Sistema de control de activos • Personal para capacitación • Presupuesto asignado
COMENTARIO:		TIEMPO
Urgente regularización de licencias de software y establecimiento de un sistema de control de inventario para evitar futuras sanciones. El incumplimiento actual representa un riesgo legal y financiero significativo.		5.75 horas totales (1.5 horas evaluación inicial + 4.25 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.4 PLAN DE RESPUESTA AL INCIDENTE RE003 - CÓDIGO: PDA003 - "VULNERABILIDAD EN SEGURIDAD DE SOFTWARE"

11.4.1 INCIDENCIA:

Exposición a amenazas de seguridad por falta de actualización de software, ausencia de políticas de actualización y recursos insuficientes.

11.4.2 ENCARGADO:

Pedro Cáceres Lujan, Seguridad

11.4.3 MATERIALES O RECURSOS:

- Software de actualización automática
- Herramientas de diagnóstico de seguridad
- Antivirus empresarial actualizado
- Personal técnico especializado
- Documentación de políticas
- Equipos de prueba
- Recursos de capacitación

11.4.4 COMENTARIO:

Se requiere implementación inmediata de políticas de actualización y asignación de recursos para ciberseguridad. La situación actual expone a la organización a vulnerabilidades críticas que podrían comprometer la seguridad de los sistemas.

11.4.5 TIEMPO:

3.5 horas totales (1 hora evaluación + 2.5 horas implementación)

11.4.6 ACTIVIDADES PASO A PASO – VULNERABILIDAD EN SEGURIDAD DE SOFTWARE:

- Evaluación inmediata de vulnerabilidades críticas en sistemas (30 min)
- Identificación y priorización de actualizaciones pendientes (30 min)
- Implementación de parches de seguridad críticos (1 hora)
- Configuración de políticas de actualización automática (45 min)
- Instalación y configuración de herramientas de monitoreo (30 min)
- Realización de pruebas de seguridad post-actualización (15 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Documentación y establecimiento de protocolos de seguridad (15 min)

Tabla 14: CÓDIGO: PDA003 - "VULNERABILIDAD EN SEGURIDAD DE SOFTWARE"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Exposición a amenazas de seguridad por falta de actualización de software, ausencia de políticas de actualización y recursos insuficientes.	Pedro Cáceres Lujan, Seguridad	<ul style="list-style-type: none"> • Software de actualización automática • Herramientas de diagnóstico de seguridad • Antivirus empresarial actualizado • Personal técnico especializado • Documentación de políticas • Equipos de prueba • Recursos de capacitación
COMENTARIO:		TIEMPO
Se requiere implementación inmediata de políticas de actualización y asignación de recursos para ciberseguridad. La situación actual expone a la organización a vulnerabilidades críticas que podrían comprometer la seguridad de los sistemas.		3.5 horas totales (1 hora evaluación + 2.5 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.5 PLAN DE RESPUESTA AL INCIDENTE RE004 - CÓDIGO: PDA004 - "PÉRDIDA DE DATOS CRÍTICOS"

11.5.1 INCIDENCIA:

Pérdida de información crucial de proyectos por falta de respaldo de datos, ausencia de políticas de backup e infraestructura inadecuada.

11.5.2 ENCARGADO:

María Valverde Rojas, TI

11.5.3 MATERIALES O RECURSOS:

- Servidores de backup
- Software de gestión de backups
- Personal técnico en sistemas
- Herramientas de recuperación de datos
- Documentación de procedimientos
- Infraestructura de almacenamiento
- Sistemas de monitoreo

11.5.4 COMENTARIO:

Se requiere implementación urgente de políticas de respaldo automáticas para asegurar la continuidad de la información. La falta de sistemas de backup representa un riesgo crítico para la preservación de datos importantes.

11.5.5 TIEMPO:

4.5 horas totales (1.5 horas evaluación + 3 horas implementación)

11.5.6 ACTIVIDADES PASO A PASO – PÉRDIDA DE DATOS CRÍTICOS:

-
- Evaluación inicial del alcance de pérdida de datos (30 min)
- Identificación de fuentes de recuperación disponibles (30 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Implementación de sistema de backup temporal (1 hora)
- Configuración de políticas de respaldo automático (1 hora)
- Recuperación de datos desde fuentes alternativas (1 hora)
- Verificación de integridad de datos recuperados (30 min)
- Documentación de procedimientos y políticas de backup (15 min)

Tabla 15: CÓDIGO: PDA004 - "PÉRDIDA DE DATOS CRÍTICOS"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Pérdida de información crucial de proyectos por falta de respaldo de datos, ausencia de políticas de backup e infraestructura inadecuada.	María Valverde Rojas, TI	<ul style="list-style-type: none">• Servidores de backup• Software de gestión de backups• Personal técnico en sistemas• Herramientas de recuperación• Documentación de procedimientos• Infraestructura de almacenamiento• Sistemas de monitoreo
COMENTARIO:		TIEMPO
Se requiere implementación urgente de políticas de respaldo automáticas para asegurar la continuidad de la información. La falta de sistemas de backup representa un riesgo crítico para la preservación de datos importantes.		4.5 horas totales (1.5 horas evaluación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.6 PLAN DE RESPUESTA AL INCIDENTE RE005 - CÓDIGO: PDA005 - "COMPROMISO DE ACCESO NO AUTORIZADO"

11.6.1 INCIDENCIA:

Compromiso de sistemas críticos por mal manejo de contraseñas, ausencia de políticas de seguridad y falta de capacitación.

11.6.2 ENCARGADO:

Francisco Ruiz Luna, Seguridad

11.6.3 MATERIALES O RECURSOS:

- Software de gestión de contraseñas
- Herramientas de auditoría de accesos
- Sistema de autenticación de dos factores
- Material de capacitación
- Documentación de políticas
- Personal de soporte técnico
- Herramientas de monitoreo

11.6.4 COMENTARIO:

Necesidad urgente de implementar políticas de gestión de contraseñas y fortalecer los controles de acceso. La situación actual compromete la seguridad de los sistemas críticos.

11.6.5 TIEMPO:

3 horas totales (1 hora evaluación + 2 horas implementación)

11.6.6 ACTIVIDADES PASO A PASO – COMPROMISO DE ACCESO NO AUTORIZADO:

- Revisión inmediata de registros de acceso y detección de anomalías (30 min)
- Cambio forzado de contraseñas en sistemas comprometidos (30 min)
- Implementación de política de contraseñas seguras (45 min)
- Configuración de autenticación de dos factores (30 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Revisión y actualización de permisos de usuario (20 min)
- Capacitación rápida al personal en seguridad básica (15 min)
- Documentación de nuevas políticas y procedimientos (10 min)

Tabla 16: CÓDIGO: PDA005 - "COMPROMISO DE ACCESO NO AUTORIZADO"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Compromiso de sistemas críticos por mal manejo de contraseñas, ausencia de políticas de seguridad y falta de capacitación.	Francisco Ruiz Luna, Seguridad	<ul style="list-style-type: none"> • Software de gestión de contraseñas • Herramientas de auditoría de accesos • Sistema de autenticación de dos factores • Material de capacitación • Documentación de políticas • Personal de soporte técnico • Herramientas de monitoreo
COMENTARIO:		TIEMPO
Necesidad urgente de implementar políticas de gestión de contraseñas y fortalecer los controles de acceso. La situación actual compromete la seguridad de los sistemas críticos.		3 horas totales (1 hora evaluación + 2 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.7 PLAN DE RESPUESTA AL INCIDENTE RE006-CÓDIGO: PDA006 - "ACCESO NO AUTORIZADO A LA RED"

11.7.1 INCIDENCIA:

Vulnerabilidad en infraestructura por conexiones inseguras, configuración inadecuada y falta de monitoreo.

11.7.2 ENCARGADO:

Elena Moreno Guerra, Redes

11.7.3 MATERIALES O RECURSOS:

- Herramientas de análisis de red
- Firewalls y sistemas de seguridad
- Software de monitoreo de red
- Equipos de networking
- Personal técnico especializado
- Documentación de configuración
- Herramientas de diagnóstico

11.7.4 COMENTARIO:

Se requiere revisión y reconfiguración urgente de las conexiones de red para garantizar la seguridad de la infraestructura. La configuración actual presenta vulnerabilidades significativas.

11.7.5 TIEMPO:

4 horas totales (1.5 horas diagnóstico + 2.5 horas implementación)

11.7.6 ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A LA RED:

- Análisis inicial de vulnerabilidades en la red (30 min)
- Identificación de conexiones no autorizadas (30 min)
- Implementación de controles de acceso inmediatos (1 hora)
- Reconfiguración de dispositivos de red (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Actualización de políticas de firewall (30 min)
- Pruebas de seguridad de red (20 min)
- Documentación de cambios y nuevas configuraciones (10 min)

Tabla 17: CÓDIGO: PDA006 - "ACCESO NO AUTORIZADO A LA RED"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Vulnerabilidad en infraestructura por conexiones inseguras, configuración inadecuada y falta de monitoreo.	Elena Moreno Guerra, Redes	<ul style="list-style-type: none">• Herramientas de análisis de red• Firewalls y sistemas de seguridad• Software de monitoreo de red• Equipos de networking• Personal técnico especializado• Documentación de configuración• Herramientas de diagnóstico
COMENTARIO:		TIEMPO:
Se requiere revisión y reconfiguración urgente de las conexiones de red para garantizar la seguridad de la infraestructura. La configuración actual presenta vulnerabilidades significativas.		4 horas totales (1.5 horas diagnóstico + 2.5 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.8 PLAN DE RESPUESTA AL INCIDENTE RE007-CÓDIGO: PDA007 - "TIEMPO DE INACTIVIDAD POR FALLAS EN TI"

11.8.1 INCIDENCIA:

Incapacidad de recuperación crítica por ausencia de planes de contingencia, procedimientos DR/BC y pruebas de recuperación.

11.8.2 ENCARGADO:

Marco Torres Mayta, Infraestructura

11.8.3 MATERIALES O RECURSOS:

- Documentación de procedimientos DR/BC
- Herramientas de recuperación
- Sistemas de respaldo
- Personal técnico especializado
- Equipos de contingencia
- Software de monitoreo
- Recursos para pruebas

11.8.4 COMENTARIO:

Urgente necesidad de implementar planes de contingencia y procedimientos de recuperación ante desastres. La ausencia de estos planes pone en riesgo la continuidad operativa.

11.8.5 TIEMPO:

4.5 horas totales (1.5 horas planificación + 3 horas implementación)

11.8.6 ACTIVIDADES PASO A PASO – TIEMPO DE INACTIVIDAD POR FALLAS EN TI:

- Evaluación inicial de sistemas críticos afectados (30 min)
- Desarrollo rápido de plan de contingencia básico (30 min)
- Implementación de medidas de recuperación inmediatas (1 hora)
- Configuración de sistemas de respaldo (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Realización de pruebas de recuperación iniciales (45 min)
- Documentación de procedimientos de contingencia (30 min)
- Capacitación rápida del personal en procedimientos (15 min)

Tabla 18: CÓDIGO: PDA007 - "TIEMPO DE INACTIVIDAD POR FALLAS EN TI"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Incapacidad de recuperación crítica por ausencia de planes de contingencia, procedimientos DR/BC y pruebas de recuperación.	Marco Torres Mayta, Infraestructura	<ul style="list-style-type: none"> • Documentación de procedimientos DR/BC • Herramientas de recuperación • Sistemas de respaldo • Personal técnico especializado • Equipos de contingencia • Software de monitoreo • Recursos para pruebas
COMENTARIO:		TIEMPO:
Urgente necesidad de implementar planes de contingencia y procedimientos de recuperación ante desastres. La ausencia de estos planes pone en riesgo la continuidad operativa.		4.5 horas totales (1.5 horas planificación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.9 PLAN DE RESPUESTA AL INCIDENTE RE008-CÓDIGO: PDA008 - "FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES"

11.9.1 INCIDENCIA:

Compromiso de datos corporativos por dispositivos personales inseguros, ausencia de políticas BYOD y falta de control de endpoints.

11.9.2 ENCARGADO:

Sofía Vega Cañón, Ciberseguridad

11.9.3 MATERIALES O RECURSOS:

- Software de gestión de dispositivos móviles (MDM)
- Herramientas de control de endpoints
- Políticas BYOD documentadas
- Sistema de monitoreo de accesos
- Software de seguridad para dispositivos
- Personal técnico especializado
- Materiales de capacitación

11.9.4 COMENTARIO:

Es necesaria la implementación inmediata de políticas BYOD y controles de seguridad para dispositivos personales. La situación actual expone información sensible a riesgos significativos.

11.9.5 TIEMPO:

4 horas totales (1 hora evaluación + 3 horas implementación)

11.9.6 ACTIVIDADES PASO A PASO – FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES:

- Evaluación inicial de dispositivos y accesos actuales (30 min)
- Desarrollo de política BYOD básica (30 min)
- Implementación de sistema MDM (1 hora)
- Configuración de controles de seguridad en endpoints (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Registro y control de dispositivos autorizados (30 min)
- Pruebas de seguridad y acceso (20 min)
- Capacitación de usuarios en nuevas políticas (10 min)

Tabla 19: CÓDIGO: PDA008 - "FUGA DE INFORMACIÓN POR DISPOSITIVOS PERSONALES"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Compromiso de datos corporativos por dispositivos personales inseguros, ausencia de políticas BYOD y falta de control de endpoints.	Sofía Vega Cañón, Ciberseguridad	<ul style="list-style-type: none">• Software de gestión MDM• Herramientas de control de endpoints• Políticas BYOD documentadas• Sistema de monitoreo de accesos• Software de seguridad para dispositivos• Personal técnico especializado• Materiales de capacitación
COMENTARIO:		TIEMPO:
Es necesaria la implementación inmediata de políticas BYOD y controles de seguridad para dispositivos personales. La situación actual expone información sensible a riesgos significativos.		4 horas totales (1 hora evaluación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.10 PLAN DE RESPUESTA AL INCIDENTE RE009-CÓDIGO: PDA009 - "ERRORES HUMANOS EN TI"

11.10.1 INCIDENCIA:

Incidentes por desconocimiento debido a falta de capacitación del personal, ausencia de programas de entrenamiento y alta rotación.

11.10.2 ENCARGADO:

Adrián Torres Luna, Capacitación

11.10.3 MATERIALES O RECURSOS:

- Material de capacitación actualizado
- Plataforma de e-learning
- Sala de entrenamiento
- Equipos de práctica
- Documentación técnica
- Personal instructor calificado
- Herramientas de evaluación

11.10.4 COMENTARIO:

Se requiere implementación urgente de un programa de capacitación intensivo para reducir errores operativos. La falta de entrenamiento está generando incidentes frecuentes.

11.10.5 TIEMPO:

4 horas totales (1 hora preparación + 3 horas ejecución)

11.10.6 ACTIVIDADES PASO A PASO – ERRORES HUMANOS EN TI:

- Evaluación rápida de necesidades de capacitación (30 min)
- Preparación de material de entrenamiento básico (30 min)
- Sesión de capacitación intensiva inicial (1 hora)
- Implementación de guías y procedimientos (45 min)
- Evaluación práctica de conocimientos adquiridos (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Retroalimentación y ajustes al programa (20 min)
- Documentación del proceso y seguimiento (10 min)

Tabla 20: CÓDIGO: PDA009 - "ERRORES HUMANOS EN TI"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Incidentes por desconocimiento debido a falta de capacitación del personal, ausencia de programas de entrenamiento y alta rotación.	Adrián Torres Luna, Capacitación	<ul style="list-style-type: none"> • Material de capacitación actualizado • Plataforma de e-learning • Sala de entrenamiento • Equipos de práctica • Documentación técnica • Personal instructor calificado • Herramientas de evaluación
COMENTARIO:		TIEMPO:
Se requiere implementación urgente de un programa de capacitación intensivo para reducir errores operativos. La falta de entrenamiento está generando incidentes frecuentes.		4 horas totales (1 hora preparación + 3 horas ejecución)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.11 PLAN DE RESPUESTA AL INCIDENTE RE010-CÓDIGO: PDA010 - "INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA"

11.11.1 INCIDENCIA:

Caída de sistemas críticos por sobrecarga de servidores, capacidad inadecuada y falta de monitoreo de recursos.

11.11.2 ENCARGADO:

Diego Rosales Arnao, Operaciones

11.11.3 MATERIALES O RECURSOS:

- Herramientas de monitoreo de servidores
- Software de análisis de rendimiento
- Hardware de respaldo
- Herramientas de balanceo de carga
- Personal técnico especializado
- Documentación de sistemas
- Recursos de optimización

11.11.4 COMENTARIO:

Necesidad urgente de optimizar recursos y establecer monitoreo continuo de servidores para evitar interrupciones del servicio. La sobrecarga actual está afectando la disponibilidad de sistemas críticos.

11.11.5 TIEMPO:

4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)

11.11.6 ACTIVIDADES PASO A PASO – INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA:

- Diagnóstico inmediato de servidores afectados (30 min)
- Identificación de procesos críticos y consumo de recursos (30 min)
- Implementación de balanceo de carga inmediato (1 hora)
- Optimización de recursos del servidor (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Configuración de herramientas de monitoreo (45 min)
- Pruebas de carga y rendimiento (30 min)
- Documentación de configuraciones y umbrales (15 min)

Tabla 21: CÓDIGO: PDA010 - "INTERRUPCIÓN DEL SERVICIO POR SOBRECARGA"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Caída de sistemas críticos por sobrecarga de servidores, capacidad inadecuada y falta de monitoreo de recursos.	Diego Rosales Arnao, Operaciones	<ul style="list-style-type: none">• Herramientas de monitoreo de servidores• Software de análisis de rendimiento• Hardware de respaldo• Herramientas de balanceo de carga• Personal técnico especializado• Documentación de sistemas• Recursos de optimización
COMENTARIO:		TIEMPO:
Necesidad urgente de optimizar recursos y establecer monitoreo continuo de servidores para evitar interrupciones del servicio. La sobrecarga actual está afectando la disponibilidad de sistemas críticos.		4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.12 PLAN DE RESPUESTA AL INCIDENTE RE011- CÓDIGO: PDA011 - "DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS"

11.12.1 INCIDENCIA:

Degradación del servicio de red por equipos antiguos, falta de presupuesto para renovación y ausencia de plan de actualización.

11.12.2 ENCARGADO:

Natalia Reyes Marín, Redes

11.12.3 MATERIALES O RECURSOS:

- Equipos de red nuevos
- Herramientas de diagnóstico de red
- Software de monitoreo
- Personal técnico calificado
- Documentación de red
- Herramientas de instalación
- Material de cableado

11.12.4 COMENTARIO:

Se requiere renovación urgente de equipos de red y establecimiento de un plan de actualización tecnológica. El rendimiento actual de la red está severamente comprometido por equipos obsoletos.

11.12.5 TIEMPO:

3.5 horas totales (1 hora evaluación + 2.5 horas implementación)

11.12.6 ACTIVIDADES PASO A PASO – DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS:

- Diagnóstico de puntos críticos de la red (30 min)
- Identificación de equipos prioritarios para reemplazo (30 min)
- Instalación de nuevos equipos de red (1 hora)
- Configuración y optimización de equipos (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Pruebas de rendimiento de red (30 min)
- Actualización de documentación de red (10 min)
- Verificación final de conectividad (5 min)

Tabla 22: CÓDIGO: PDA011 - "DEGRADACIÓN DE RED POR EQUIPOS OBSOLETOS"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Degradación del servicio de red por equipos antiguos, falta de presupuesto para renovación y ausencia de plan de actualización.	Natalia Reyes Marín, Redes	<ul style="list-style-type: none"> • Equipos de red nuevos • Herramientas de diagnóstico de red • Software de monitoreo • Personal técnico calificado • Documentación de red • Herramientas de instalación • Material de cableado
COMENTARIO:		TIEMPO:
Se requiere renovación urgente de equipos de red y establecimiento de un plan de actualización tecnológica. El rendimiento actual de la red está severamente comprometido por equipos obsoletos.		3.5 horas totales (1 hora evaluación + 2.5 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.13 PLAN DE RESPUESTA AL INCIDENTE RE012-CÓDIGO: PDA012 - "FALLOS DE SOPORTE TÉCNICO"

11.13.1 INCIDENCIA:

Respuesta inadecuada ante incidentes por proveedores poco confiables, ausencia de SLAs definidos y falta de evaluación de proveedores.

11.13.2 ENCARGADO:

Fernanda López García, Proveedores

11.13.3 MATERIALES O RECURSOS:

- Documentación de SLAs
- Herramientas de seguimiento
- Sistema de tickets
- Material de evaluación
- Plantillas de contratos
- Personal de evaluación
- Métricas de servicio

11.13.4 COMENTARIO:

Urgente necesidad de establecer SLAs claros y procedimientos de evaluación de proveedores. La falta de acuerdos formales está impactando la calidad del soporte técnico.

11.13.5 TIEMPO:

4 horas totales (1.5 horas análisis + 2.5 horas implementación)

11.13.6 ACTIVIDADES PASO A PASO – FALLOS DE SOPORTE TÉCNICO:

- Revisión de incidentes y fallos de soporte actuales (30 min)
- Análisis de necesidades de servicio (30 min)
- Desarrollo de SLAs básicos (1 hora)
- Implementación de sistema de seguimiento (45 min)
- Evaluación inicial de proveedores actuales (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Establecimiento de métricas de servicio (20 min)
- Documentación de procesos y acuerdos (10 min)

Tabla 23: CÓDIGO: PDA012 - "FALLOS DE SOPORTE TÉCNICO"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Respuesta inadecuada ante incidentes por proveedores poco confiables, ausencia de SLAs definidos y falta de evaluación de proveedores.	Fernanda López García, Proveedores	<ul style="list-style-type: none">• Documentación de SLAs• Herramientas de seguimiento• Sistema de tickets• Material de evaluación• Plantillas de contratos• Personal de evaluación• Métricas de servicio
COMENTARIO:		TIEMPO:
Urgente necesidad de establecer SLAs claros y procedimientos de evaluación de proveedores. La falta de acuerdos formales está impactando la calidad del soporte técnico.		4 horas totales (1.5 horas análisis + 2.5 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.14 PLAN DE RESPUESTA AL INCIDENTE RE013-CÓDIGO: PDA013 - "CAÍDAS INESPERADAS DE LA RED"

11.14.1 INCIDENCIA:

Interrupciones no detectadas por falta de monitoreo de red, ausencia de herramientas de monitoreo y personal insuficiente.

11.14.2 ENCARGADO:

Jorge Navarro Ramirez, Redes

11.14.3 MATERIALES O RECURSOS:

- Software de monitoreo de red
- Herramientas de diagnóstico
- Sistema de alertas
- Personal técnico especializado
- Equipos de medición
- Documentación de red
- Consola de administración

11.14.4 COMENTARIO:

Se requiere implementación inmediata de herramientas de monitoreo y asignación de personal para supervisión de red. La falta de monitoreo está causando interrupciones imprevistas.

11.14.5 TIEMPO:

4 horas totales (1 hora configuración + 3 horas implementación)

11.14.6 ACTIVIDADES PASO A PASO – CAÍDAS INESPERADAS DE LA RED:

- Instalación de software de monitoreo básico (30 min)
- Configuración de puntos de monitoreo críticos (30 min)
- Implementación de sistema de alertas (1 hora)
- Establecimiento de umbrales y métricas (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Configuración de reportes automáticos (45 min)
- Pruebas de detección de fallos (20 min)
- Capacitación básica del personal (10 min)

Tabla 24: CÓDIGO: PDA013 - "CAÍDAS INESPERADAS DE LA RED"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Interrupciones no detectadas por falta de monitoreo de red, ausencia de herramientas de monitoreo y personal insuficiente.	Jorge Navarro Ramirez, Redes	<ul style="list-style-type: none">• Software de monitoreo de red• Herramientas de diagnóstico• Sistema de alertas• Personal técnico especializado• Equipos de medición• Documentación de red• Consola de administración
COMENTARIO:		TIEMPO:
Se requiere implementación inmediata de herramientas de monitoreo y asignación de personal para supervisión de red. La falta de monitoreo está causando interrupciones imprevistas.		4 horas totales (1 hora configuración + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.15 PLAN DE RESPUESTA AL INCIDENTE RE014-CÓDIGO: PDA014 - "INCOMPATIBILIDAD CON NUEVOS SISTEMAS"

11.15.1 INCIDENCIA:

Problemas de integración por software obsoleto, resistencia al cambio y ausencia de plan de actualizaciones.

11.15.2 ENCARGADO:

Valeria Ortiz Cocco, TI

11.15.3 MATERIALES O RECURSOS:

- Software actualizado
- Herramientas de migración
- Personal técnico capacitado
- Documentación técnica
- Ambiente de pruebas
- Material de capacitación
- Equipos de respaldo

11.15.4 COMENTARIO:

Urgente necesidad de actualizar sistemas y establecer plan de actualizaciones periódicas. La resistencia al cambio y software obsoleto están generando problemas críticos de integración.

11.15.5 TIEMPO:

5 horas totales (2 horas análisis + 3 horas implementación)

11.15.6 ACTIVIDADES PASO A PASO – INCOMPATIBILIDAD CON NUEVOS SISTEMAS:

- Análisis de sistemas actuales y compatibilidad (45 min)
- Identificación de actualizaciones críticas necesarias (45 min)
- Implementación de actualizaciones prioritarias (1 hora)
- Migración de datos esenciales (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Pruebas de integración con nuevos sistemas (45 min)
- Capacitación básica a usuarios clave (30 min)
- Documentación de cambios y procedimientos (15 min)

Tabla 25: CÓDIGO: PDA014 - "INCOMPATIBILIDAD CON NUEVOS SISTEMAS"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Problemas de integración por software obsoleto, resistencia al cambio y ausencia de plan de actualizaciones.	Valeria Ortiz Cocco, TI	<ul style="list-style-type: none">• Software actualizado• Herramientas de migración• Personal técnico capacitado• Documentación técnica• Ambiente de pruebas• Material de capacitación• Equipos de respaldo
COMENTARIO:		TIEMPO:
Urgente necesidad de actualizar sistemas y establecer plan de actualizaciones periódicas. La resistencia al cambio y software obsoleto están generando problemas críticos de integración.		5 horas totales (2 horas análisis + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.16 PLAN DE RESPUESTA AL INCIDENTE RE015-CÓDIGO: PDA015 - "ROBO DE INFORMACIÓN EN TRANSMISIÓN"

11.16.1 INCIDENCIA:

Intercepción de datos sensibles por falta de cifrado, configuraciones inseguras y ausencia de políticas de seguridad.

11.16.2 ENCARGADO:

Rafael Pérez Vila, Seguridad

11.16.3 MATERIALES O RECURSOS:

- Software de cifrado
- Herramientas de seguridad
- Certificados SSL/TLS
- Personal especializado
- Documentación de políticas
- Equipos de monitoreo
- Sistemas de detección

11.16.4 COMENTARIO:

Implementación urgente de cifrado y políticas de seguridad para transmisión de datos. La falta de protección actual expone información sensible a interceptaciones.

11.16.5 TIEMPO:

4 horas totales (1 hora evaluación + 3 horas implementación)

11.16.6 ACTIVIDADES PASO A PASO – ROBO DE INFORMACIÓN EN TRANSMISIÓN:

- Evaluación de vulnerabilidades en transmisión de datos (30 min)
- Identificación de canales de comunicación críticos (30 min)
- Implementación de cifrado en puntos críticos (1 hora)
- Configuración de certificados de seguridad (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Establecimiento de políticas de transmisión segura (45 min)
- Pruebas de seguridad en comunicaciones (20 min)
- Documentación de configuraciones de seguridad (10 min)

Tabla 26: CÓDIGO: PDA015 - "ROBO DE INFORMACIÓN EN TRANSMISIÓN"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Interceptación de datos sensibles por falta de cifrado, configuraciones inseguras y ausencia de políticas de seguridad.	Rafael Pérez Vila, Seguridad	<ul style="list-style-type: none"> • Software de cifrado • Herramientas de seguridad • Certificados SSL/TLS • Personal especializado • Documentación de políticas • Equipos de monitoreo • Sistemas de detección
COMENTARIO:		TIEMPO:
Implementación urgente de cifrado y políticas de seguridad para transmisión de datos. La falta de protección actual expone información sensible a interceptaciones.		4 horas totales (1 hora evaluación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.17 PLAN DE RESPUESTA AL INCIDENTE RE016-CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"

11.17.1 INCIDENCIA:

Compromiso de seguridad física por fallos en control de acceso, sistema obsoleto y configuración incorrecta.

11.17.2 ENCARGADO:

Alejandro Castillo Vega, Seguridad

11.17.3 MATERIALES O RECURSOS:

- Sistema de control de acceso
- Lectoras biométricas
- Tarjetas de identificación
- Cámaras de seguridad
- Software de gestión de accesos
- Personal de seguridad
- Logs de registro

11.17.4 COMENTARIO:

Necesidad inmediata de actualizar los sistemas de control de acceso y establecer políticas de seguridad física. Los fallos actuales comprometen la seguridad de áreas restringidas.

11.17.5 TIEMPO:

4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)

11.17.6 ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS:

- Evaluación de puntos de acceso vulnerables (30 min)
- Revisión de registros de acceso actuales (30 min)
- Implementación de controles temporales inmediatos (1 hora)
- Actualización de sistema de control de acceso (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Configuración de nuevas políticas de acceso (45 min)
- Pruebas de seguridad y verificación (30 min)
- Capacitación del personal de seguridad (15 min)

Tabla 27: CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Compromiso de seguridad física por fallos en control de acceso, sistema obsoleto y configuración incorrecta.	Alejandro Castillo Vega, Seguridad	<ul style="list-style-type: none">• Sistema de control de acceso• Lectoras biométricas• Tarjetas de identificación• Cámaras de seguridad• Software de gestión de accesos• Personal de seguridad• Logs de registro
COMENTARIO:		TIEMPO:
Necesidad inmediata de actualizar los sistemas de control de acceso y establecer políticas de seguridad física. Los fallos actuales comprometen la seguridad de áreas restringidas.		4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.18 PLAN DE RESPUESTA AL INCIDENTE RE016 - CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"

11.18.1 INCIDENCIA:

Compromiso de seguridad física por fallos en control de acceso, sistema obsoleto y configuración incorrecta.

11.18.2 ENCARGADO:

Alejandro Castillo Vega, Seguridad

11.18.3 MATERIALES O RECURSOS:

- Sistema de control de acceso
- Lectoras biométricas
- Tarjetas de identificación
- Cámaras de seguridad
- Software de gestión de accesos
- Personal de seguridad
- Logs de registro

11.18.4 COMENTARIO:

Necesidad inmediata de actualizar los sistemas de control de acceso y establecer políticas de seguridad física. Los fallos actuales comprometen la seguridad de áreas restringidas.

11.18.5 TIEMPO:

4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)

11.18.6 ACTIVIDADES PASO A PASO – ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS:

- Evaluación de puntos de acceso vulnerables (30 min)
- Revisión de registros de acceso actuales (30 min)
- Implementación de controles temporales inmediatos (1 hora)
- Actualización de sistema de control de acceso (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Configuración de nuevas políticas de acceso (45 min)
- Pruebas de seguridad y verificación (30 min)
- Capacitación del personal de seguridad (15 min)

Tabla 28: CÓDIGO: PDA016 - "ACCESO NO AUTORIZADO A ÁREAS RESTRINGIDAS"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Compromiso de seguridad física por fallos en control de acceso, sistema obsoleto y configuración incorrecta.	Alejandro Castillo Vega, Seguridad	<ul style="list-style-type: none">• Sistema de control de acceso• Lectoras biométricas• Tarjetas de identificación• Cámaras de seguridad• Software de gestión de accesos• Personal de seguridad• Logs de registro
COMENTARIO:		TIEMPO:
Necesidad inmediata de actualizar los sistemas de control de acceso y establecer políticas de seguridad física. Los fallos actuales comprometen la seguridad de áreas restringidas.		4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.19 PLAN DE RESPUESTA AL INCIDENTE RE017 - CÓDIGO: PDA017 - "SANCIONES POR INCUMPLIMIENTO NORMATIVO"

11.19.1 INCIDENCIA:

Penalizaciones normativas por incumplimiento de regulaciones, desconocimiento legal y falta de asesoría.

11.19.2 ENCARGADO:

Andrea Méndez Huayta, Legal

11.19.3 MATERIALES O RECURSOS:

- Documentación legal actualizada
- Software de compliance
- Servicios de asesoría legal
- Personal especializado
- Material de capacitación
- Registros normativos
- Herramientas de auditoría

11.19.4 COMENTARIO:

Necesidad urgente de implementar programa de cumplimiento normativo y obtener asesoría legal especializada. Las deficiencias actuales están generando riesgos legales significativos.

11.19.5 TIEMPO:

4 horas totales (1.5 horas revisión + 2.5 horas implementación)

11.19.6 ACTIVIDADES PASO A PASO – SANCIONES POR INCUMPLIMIENTO NORMATIVO:

- Evaluación de requisitos normativos actuales (30 min)
- Identificación de incumplimientos críticos (30 min)
- Implementación de medidas correctivas inmediatas (1 hora)
- Desarrollo de programa de cumplimiento básico (45 min)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Establecimiento de controles de monitoreo (45 min)
- Capacitación inicial en normativas clave (20 min)
- Documentación de procedimientos de cumplimiento (10 min)

Tabla 29: - CÓDIGO: PDA017 - "SANCIONES POR INCUMPLIMIENTO NORMATIVO"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Penalizaciones normativas por incumplimiento de regulaciones, desconocimiento legal y falta de asesoría.	Andrea Méndez Huayta, Legal	<ul style="list-style-type: none"> • Documentación legal actualizada • Software de compliance • Servicios de asesoría legal • Personal especializado • Material de capacitación • Registros normativos • Herramientas de auditoría
COMENTARIO:		TIEMPO:
Necesidad urgente de implementar programa de cumplimiento normativo y obtener asesoría legal especializada. Las deficiencias actuales están generando riesgos legales significativos.		4 horas totales (1.5 horas revisión + 2.5 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.20 PLAN DE RESPUESTA AL INCIDENTE RE018 - CÓDIGO: PDA018 - "FALLOS EN RECUPERACIÓN DE DESASTRES"

11.20.1 INCIDENCIA:

Incapacidad de restaurar servicios por falta de pruebas de recuperación, ausencia de procedimientos y ambiente de pruebas.

11.20.2 ENCARGADO:

Antonio Díaz Pena, TI

11.20.3 MATERIALES O RECURSOS:

- Plan de recuperación DR/BC
- Ambiente de pruebas
- Software de backup
- Herramientas de recuperación
- Personal especializado
- Documentación de procesos
- Infraestructura de respaldo

11.20.4 COMENTARIO:

Implementación urgente de procedimientos de recuperación ante desastres y realización de pruebas periódicas. La falta de preparación actual compromete la continuidad del servicio.

11.20.5 TIEMPO:

5 horas totales (2 horas planificación + 3 horas implementación)

11.20.6 ACTIVIDADES PASO A PASO – FALLOS EN RECUPERACIÓN DE DESASTRES:

- Evaluación de procedimientos actuales de recuperación (30 min)
- Identificación de sistemas críticos y prioridades (30 min)
- Desarrollo de procedimientos básicos de DR (1 hora)
- Configuración de ambiente de pruebas (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Implementación de pruebas iniciales (1 hora)
- Ajustes basados en resultados de pruebas (45 min)
- Documentación de procedimientos actualizados (15 min)

Tabla 30: CÓDIGO: PDA018 - "FALLOS EN RECUPERACIÓN DE DESASTRES"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Incapacidad de restaurar servicios por falta de pruebas de recuperación, ausencia de procedimientos y ambiente de pruebas.	Antonio Díaz Pena, TI	<ul style="list-style-type: none">• Plan de recuperación DR/BC• Ambiente de pruebas• Software de backup• Herramientas de recuperación• Personal especializado• Documentación de procesos• Infraestructura de respaldo
COMENTARIO:		TIEMPO:
Implementación urgente de procedimientos de recuperación ante desastres y realización de pruebas periódicas. La falta de preparación actual compromete la continuidad del servicio.		5 horas totales (2 horas planificación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.21 PLAN DE RESPUESTA AL INCIDENTE RE019 - CÓDIGO: PDA019 - "PROPAGACIÓN DE ATAQUES EN RED"

11.21.1 INCIDENCIA:

Compromiso general de sistemas por red no segmentada, diseño inadecuado y ausencia de políticas de segmentación.

11.21.2 ENCARGADO:

Manuel Serrano Tulio, Infraestructura

11.22 MATERIALES O RECURSOS:

- Equipos de networking
- Software de segmentación
- Herramientas de monitoreo
- Firewalls internos
- Personal especializado
- Documentación de red
- Políticas de segmentación

11.22.1 COMENTARIO:

Necesidad crítica de implementar segmentación de red y fortalecer las políticas de seguridad para prevenir la propagación de ataques entre segmentos.

11.22.2 TIEMPO:

4.5 horas totales (1.5 horas análisis + 3 horas implementación)

11.22.3 ACTIVIDADES PASO A PASO – PROPAGACIÓN DE ATAQUES EN RED:

- Análisis de la topología de red actual (30 min)
- Identificación de segmentos críticos (30 min)
- Diseño de nueva arquitectura de segmentación (1 hora)
- Implementación de VLANs y subredes (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Configuración de políticas de enrutamiento (45 min)
- Pruebas de conectividad y seguridad (30 min)
- Documentación de nueva estructura (15 min)

Tabla 31: CÓDIGO: PDA019 - "PROPAGACIÓN DE ATAQUES EN RED"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Compromiso general de sistemas por red no segmentada, diseño inadecuado y ausencia de políticas de segmentación.	Manuel Serrano Tulio, Infraestructura	<ul style="list-style-type: none"> • Equipos de networking • Software de segmentación • Herramientas de monitoreo • Firewalls internos • Personal especializado • Documentación de red • Políticas de segmentación
COMENTARIO:		TIEMPO:
Necesidad crítica de implementar segmentación de red y fortalecer las políticas de seguridad para prevenir la propagación de ataques entre segmentos.		4.5 horas totales (1.5 horas análisis + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.23 PLAN DE RESPUESTA AL INCIDENTE RE020 - CÓDIGO: PDA020 - "FALLO DE PROVEEDOR CRÍTICO"

11.23.1 INCIDENCIA:

Interrupción de servicios críticos por dependencia de proveedor único, falta de alternativas y contratos restrictivos.

11.23.2 ENCARGADO:

Felipe Ruiz Vega, Proveedores

11.23.3 MATERIALES O RECURSOS:

- Base de datos de proveedores
- Documentación de servicios
- Plantillas de contratos
- Herramientas de evaluación
- Personal de evaluación
- Criterios de selección
- Material de análisis

11.23.4 COMENTARIO:

Urgente necesidad de diversificar proveedores y establecer planes de contingencia para servicios críticos. La dependencia actual de un único proveedor representa un riesgo operativo significativo.

11.23.5 TIEMPO:

5 horas totales (2 horas evaluación + 3 horas implementación)

11.23.6 ACTIVIDADES PASO A PASO – FALLO DE PROVEEDOR CRÍTICO:

- Evaluación de servicios críticos afectados (45 min)
- Identificación de proveedores alternativos (45 min)
- Análisis de requisitos de servicio (1 hora)
- Evaluación inicial de nuevos proveedores (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Desarrollo de plan de contingencia (45 min)
- Establecimiento de acuerdos preliminares (30 min)
- Documentación de nuevos procedimientos (15 min)

Tabla 32: CÓDIGO: PDA020 - "FALLO DE PROVEEDOR CRÍTICO"

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Interrupción de servicios críticos por dependencia de proveedor único, falta de alternativas y contratos restrictivos.	Felipe Ruiz Vega, Proveedores	<ul style="list-style-type: none"> • Base de datos de proveedores • Documentación de servicios • Plantillas de contratos • Herramientas de evaluación • Personal de evaluación • Criterios de selección • Material de análisis
COMENTARIO:		TIEMPO:
Urgente necesidad de diversificar proveedores y establecer planes de contingencia para servicios críticos. La dependencia actual de un único proveedor representa un riesgo operativo significativo.		5 horas totales (2 horas evaluación + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

11.24 PLAN DE RESPUESTA AL INCIDENTE RE021 - CÓDIGO: PDA021 - "FALLO DE EQUIPOS DE OBRA"

11.24.1 INCIDENCIA:

Interrupciones operativas en sitios de trabajo por falta de mantenimiento de equipos, condiciones adversas y personal no capacitado.

11.24.2 ENCARGADO:

Laura Medina Rojas, Operaciones

11.24.3 MATERIALES O RECURSOS:

- Herramientas de mantenimiento
- Equipos de diagnóstico
- Repuestos críticos
- Personal técnico
- Manuales de equipo
- Material de capacitación
- EPPs necesarios

11.24.4 COMENTARIO:

Se requiere implementación inmediata de programa de mantenimiento preventivo y capacitación del personal técnico. Las fallas actuales están causando interrupciones significativas en las operaciones de obra.

11.24.5 TIEMPO:

4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)

11.24.6 ACTIVIDADES PASO A PASO – FALLO DE EQUIPOS DE OBRA:

- Evaluación inicial del estado de equipos críticos (30 min)
- Diagnóstico detallado de fallas recurrentes (30 min)
- Implementación de reparaciones urgentes (1 hora)
- Establecimiento de rutinas de mantenimiento (1 hora)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

- Capacitación básica a operadores (45 min)
- Verificación de funcionamiento de equipos (30 min)
- Documentación de procedimientos de mantenimiento (15 min)

INCIDENCIA	ENCARGADO	MATERIALES O RECURSOS
Interrupciones operativas en sitios de trabajo por falta de mantenimiento de equipos, condiciones adversas y personal no capacitado.	Laura Medina Rojas, Operaciones	<ul style="list-style-type: none">• Herramientas de mantenimiento• Equipos de diagnóstico• Repuestos críticos• Personal técnico• Manuales de equipo• Material de capacitación• EPPs necesarios
COMENTARIO:		TIEMPO:
Se requiere implementación inmediata de programa de mantenimiento preventivo y capacitación del personal técnico. Las fallas actuales están causando interrupciones significativas en las operaciones de obra.		4.5 horas totales (1.5 horas diagnóstico + 3 horas implementación)



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.



**“INSTITUTO SUPERIOR TECNOLÓGICO PÚBLICO
“MISIONEROS MONFORTIANOS”**

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”.

12 GALERÍA DE FOTOGRAFÍAS – CEFOISA



Ilustración 9: Capacitación DE CIBERSEGURIDAD CEFOISA -OBRA



Ilustración 10: Incidente - Tomacorriente no es de tipo circular, mala adaptación para conectar router