SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION EMPRESA GEOSURVEY S.A LIMA

INDICE

INDICE 2
CAPITULO 1 5
ETAPA 1: GESTION DE ACTIVOS 5
1.1 IDENTIFICACION DE LOS ACTIVOS 5
1.2 ANALISIS DE ACTIVOS Y AMENAZAS 8
1.3 CALCULOS DE RIESGO DE LOS ACTIVOS 104
1.4 TABLAS DE ACTIVOS, VUNERABILIDADES Y CONTROLES 227
CAPITULO 2 279
ETAPA 2: PLAN HACER 279
2.1.1 DOMINIO: 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS 279
2.1.1.1 OBJETIVO DEL DOMINIO 279
2.1.1.2 R7.1: ANTES DE LA CONTRATACIÓN 280
2.1.1.3 R7.2 DURANTE LA CONTRATACIÓN 280
2.1.1.4 NORMATIVA DE SEGURIDAD DE CONTRATACIÓN DEL PERSONAL DE LA EMPRESA GEOSURVEY: 281
2.1.2 DOMINIO: 8. GESTION DE ACTIVOS 282
2.1.2.1 OBJETIVO DEL DOMINIO 282
2.1.2.2 R8.2 CLASIFICACIÓN DE LA INFORMACIÓN 282
2.1.2.3 R8.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO 282
2.1.2.4 NORMATIVA DE SEGURIDAD ACERCA DE GESTIÓN DE ACTIVOS DE LA EMPRESA GEOSURVEY: 283
2.1.3 DOMINIO: 9. CONTROL DE ACCESO 283
2.1.3.1 OBJETIVO DEL DOMINIO 283
2.1.3.2 R9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS 284
2.1.3.3 R9.2 GESTIÓN DE ACCESO DE USUARIO 284
2.1.3.4 NORMATIVA DEL CONTROL DE ACCESO DE LA EMPRESA GEOSURVEY: 285
2.1.4 DOMINIO: 10. CIFRADO 285
2.1.4.1 OBJETIVO DEL DOMINIO 285
2.1.4.2 R10.1 CONTROLES CRIPTOGRÁFICOS 286
2.1.4.3 NORMATIVA DEL CIFRADO DE SEGURIDAD DE LA EMPRESA GEOSURVEY: 286
2.1.5 DOMINIO: 11. SEGURIDAD FISICA Y AMBIENTAL 286

2.1.5.1 OBJETIVO DEL DOMINIO 286
5.1.5.2 R11.1 ÁREAS SEGURAS 287
5.1.5.2 R11.2 SEGURIDAD DE LOS EQUIPOS 288
5.1.5.3 NORMATIVA DE SEGURIDAD EXTERNA Y AMBIENTAL DE LA EMPRESA GEOSURVEY: 288
2.1.6 DOMINIO: 12. SEGURIDAD OPERATIVA 289
2.1.6.1 OBJETIVO DEL DOMINIO: 289
5.1.6.2 R12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN 290
5.1.6.3 R12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO 290
5.1.6.4 R12.3 COPIAS DE SEGURIDAD 290
5.1.6.5 R12.4 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN 290
5.1.6.6 R12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN 291
5.1.6.7 R12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 291
5.1.6.8 NORMATIVA DE LA SEGURIDAD OPERATIVA DE LA EMPRESA GEOSURVEY: 291
2.1.7 DOMINIO: 13. SEGURIDAD DE TELECOMUNICACIONES 291
2.1.7.1 OBJETIVO DEL DOMINIO 291
5.1.7.2 R13.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES 292
5.1.7.3 R13.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS 292
5.1.7.4 NORMATIVA DE SEGURIDAD DE LA TELECOMUNICACIÓN DE LA EMPRESA GEOSURVEY: 293
2.1.8 DOMINIO: 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 294
2.1.8.1 OBJETIVO DEL DOMINIO 294
2.1.8.2 R14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE 294
2.1.8.3 R14.3 DATOS DE PRUEBA 295
2.1.8.4 NORMATIVAS DE SEGURIDAD DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN DE LA EMPRESA GEOSURVEY: 295
2.1.9 DOMINIO: 18. CUMPLIMIENTO 295
2.1.9.1 OBJETIVO DEL DOMINIO 295
2.1.9.2 R18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN 296
2.1.9.3 NORMATIVA DE CUMPLIMIENTO DE SEGURIDAD DE LA EMPRESA GEOSURVEY: 296
CAPITULO 3 297

ETAPA 3: GESTION DE INCIDENTES 297
3.1 CONTROL DE INCIDENCIAS 297
3.2 REPORTES ESTADISTICOS 310
CAPITULO 4 315
ETAPA 4: PLAN DE MEJORA CONTINUA 315
4.1 PLANIFICACION DE LAS ETAPAS DE CAPACITACIONES EN SEGURIDAD DE LA INFORMACION 315
4.2 ETAPAS PREVENTIVAS Y CORRECTIVAS SEGÚN EL DOMINIO DE LA SEGURIDAD 316
4.2.1 DOMINIO 7: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS 316
4.2.2 DOMINIO 8: GESTION DE ACTIVOS 316
4.2.3 DOMINIO 9: CONTROL DE ACCESO 317
4.2.4 DOMINIO 10: CIFRADO DE INFORMACION 318
4.2.5 DOMINIO 11: SEGURIDAD FISICA Y AMBIENTAL 318
4.2.6 DOMINIO 12: SEGURIDAD OPERATIVA 319
4.2.7 DOMINIO 13: SEGURIDAD DE TELECOMUNICACIONES 319
4.2.8 DOMINIO 14: ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION 320
4.2.9 DOMINIO 18: CUMPLIMIENTO 320

SISTEMA DE GESTION DE SISTEMAS DE SEGURIDAD DE LA INFORMACION

CAPITULO 1

ETAPA 1: GESTION DE ACTIVOS

1.1 IDENTIFICACION DE LOS ACTIVOS

TABLA 1: DATOS E INFORMACION

I= ISIGNIFICANTE

B=BAJO

M=MEDIANO

A=ALTO

Elementos de Información	Clasificación			Magnitud de Daño			
Datos e Información	**Confidencial, Privado, Sensitivo**	**Obligación por ley / Contrato / Convenio**	**Costo de recuperación (tiempo, económico, material, imagen, emocional)**	**I**	**B**	**M**	**A**
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	X						X
Finanzas		X				X	
RR.HH	X					X	

Directorio de Contactos	X					X	
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)		X			X		
Correo electrónico			X			X	
Bases de datos internos			X				X
Bases de datos externos			X				X
Bases de datos colaborativos			X				X
Página Web interna (Intranet)			X			X	
Página Web externa			X			X	
Respaldos			X				X
Infraestructura (Planos, Documentación, etc.)	X					X	
Informática (Planos, Documentación, etc.)	X					X	
Navegación en Internet			X		X		
Chat interno			X		X		
Llamadas telefónicas internas			X		X		
Llamadas telefónicas externas			X		X		

TABLA 2: SISTEMAS E INFRAESTRUCTURA

Elementos de Información	Clasificación	Magnitud de Daño

Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	I	B	M	A
Equipos de la red cableada (router, switch, etc.)			X				X
Equipos de la red inalámbrica (router, punto de acceso, etc.)			X			X	
Cortafuego			X			X	
Antivirus			X		X		
Servidores	X						X
Computadoras		X				X	
Portátiles		X			X		
Programas de administración (contabilidad, manejo de personal, etc.)			X				X
Impresoras		X			X		
Memorias portátiles			X		X		
Celulares	X				X		
Edificio (Oficinas, Recepción, Sala de espera, etc.)			X		X		
Vehículos		X			X		

TABLA 3: SISTEMAS E INFRAESTRUCTURA

Elementos de Información	Clasificación			Magnitud de Daño			
Personal	**Imagen pública de alto perfil, indispensable para funcionamiento institucional**	**Perfil medio, experto en su área**	**Perfil bajo, no indispensable para funcionamiento institucional**	**I**	**B**	**M**	**A**

Junta Directiva	X						X
Dirección / Coordinación	X						X
Administración		X				X	
Personal técnico			X		X		
Recepción			X		X		
Informática / Soporte técnico interno		X					X
Soporte técnico externo		X				X	
Servicio de limpieza de planta			X	X			

1.2 ANALISIS DE ACTIVOS Y AMENAZAS

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico

Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Documentos institucionales	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono

(Proyectos, Planes, Evaluaciones, Informes, etc.)	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo

Finanzas	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
RR.HH	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
	Incendio
	Inundación / deslave

RR.HH	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
RR.HH	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono

	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo

Directorio de Contactos	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Directorio de Contactos	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'

Directorio de Contactos	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica

	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)

	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Correo electrónico	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración

	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Correo electrónico	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos

Correo electrónico	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política

Bases de datos internos	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Bases de datos internos	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos

Bases de datos internos	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado

	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Bases de datos externos	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Bases de datos externos	Incendio
	Inundación / deslave
	Sismo

	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Bases de datos externos	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal

	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Bases de datos colaborativos	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)

	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Bases de datos colaborativos	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo

Bases de datos colaborativos	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Página Web interna (Intranet)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Página Web interna (Intranet)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS

Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Página Web interna (Intranet)	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos

	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Página Web externa	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
	Incendio

Página Web externa	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Página Web externa	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono

	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo

Respaldos	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Respaldos	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'

Respaldos	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Infraestructura (Planes, Documentación, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Infraestructura (Planes, Documentación, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo

	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Infraestructura (Planes, Documentación, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)

	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Informática (Planes, Documentación, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna

	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Informática (Planes, Documentación, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado

Informática (Planes, Documentación, etc.)	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS

Datos e Información	Actos originados por la criminalidad común y motivación política
Navegación en Internet	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Navegación en Internet	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Navegación en Internet	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado

	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Chat interno	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Chat interno	Incendio
	Inundación / deslave
	Sismo

	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Chat interno	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal

	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Llamadas telefónicas internas	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)

	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Llamadas telefónicas internas	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo

Llamadas telefónicas internas	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Datos e Información	Actos originados por la criminalidad común y motivación política
Llamadas telefónicas externas	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Datos e Información	Sucesos de origen físico
Llamadas telefónicas externas	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS

Datos e Información	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Llamadas telefónicas externas	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos

	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Equipos de la red cableada (router, switch, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
	Incendio

Equipos de la red cableada (router, switch, etc.)	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono

Equipos de la red cableada (router, switch, etc.)	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo

Equipos de la red inalámbrica (router, punto de acceso, etc.)	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos

Equipos de la red inalámbrica (router, punto de acceso, etc.)	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Cortafuego	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Cortafuego	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica

	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Cortafuego	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)

	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Antivirus	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración

	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Antivirus	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos

Antivirus	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política

Servidores	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Servidores	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos

Servidores	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado

	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Computadoras	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Computadoras	Incendio
	Inundación / deslave
	Sismo
	Polvo

	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Computadoras	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal

	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Portátiles	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)

	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Portátiles	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo

Portátiles	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Programas de administración (contabilidad, manejo de personal, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Programas de administración (contabilidad, manejo de personal, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Programas de administración (contabilidad, manejo de personal, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos

	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Impresoras	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS

Sistemas e Infraestructura	Sucesos de origen físico
Impresoras	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados

Impresoras	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)

Memorias portátiles	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Memorias portátiles	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'

Memorias portátiles	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Celulares	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Celulares	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)

	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Celulares	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)

	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)

Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)

Vehículos	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos de origen físico
Vehículos	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas

Vehículos	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo

	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Junta Directiva	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Junta Directiva	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación

	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Junta Directiva	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)

	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Dirección / Coordinación	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna

	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Dirección / Coordinación	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado

Dirección / Coordinación	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Administración	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Administración	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS

Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Administración	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos

	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Personal técnico	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Personal técnico	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)

Personal técnico	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)

Recepción	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Recepción	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas

Recepción	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo

	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Piloto / conductor	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Piloto / conductor	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación

	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Piloto / conductor	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)

	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Informática / Soporte técnico interno	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna

	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Informática / Soporte técnico interno	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado

Informática / Soporte técnico interno	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Soporte técnico externo	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Soporte técnico externo	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS

Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Soporte técnico externo	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos

	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
Servicio de limpieza de planta	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo
	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
	Incendio

Servicio de limpieza de planta	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
Servicio de limpieza de planta	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos
	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono

	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

ACTIVO	AMENAZAS
Personal	Actos originados por la criminalidad común y motivación política
	Allanamiento (ilegal, legal)
	Persecución (civil, fiscal, penal)
	Sabotaje (ataque físico y electrónico)
	Daños por vandalismo

Servicio de limpieza externo	Extorsión
	Fraude / Estafa
	Robo / Hurto (físico)
	Robo / Hurto de información electrónica
	Intrusión a Red interna
	Infiltración
	Virus / Ejecución no autorizado de programas

ACTIVO	AMENAZAS
Personal	Sucesos de origen físico
Servicio de limpieza externo	Incendio
	Inundación / deslave
	Sismo
	Polvo
	Falta de ventilación
	Electromagnetismo
	Sobrecarga eléctrica
	Falla de corriente (apagones)
	Falla de sistema / Daño disco duro

ACTIVO	AMENAZAS
Personal	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales
	Falta de inducción, capacitación y sensibilización sobre riesgos
	Mal manejo de sistemas y herramientas
	Utilización de programas no autorizados / software 'pirateado'
	Falta de pruebas de software nuevo con datos productivos

Servicio de limpieza externo	Perdida de datos
	Infección de sistemas a través de unidades portables sin escaneo
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)
	Unidades portables con información sin cifrado
	Transmisión no cifrada de datos críticos
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	Compartir contraseñas o permisos a terceros no autorizados
	Transmisión de contraseñas por teléfono
	Exposición o extravío de equipo, unidades de almacenamiento, etc.
	Falta de definición de perfil, privilegios y restricciones del personal
	Falta de mantenimiento físico (proceso, repuestos e insumos)
	Falta de actualización de software (proceso y recursos)
	Fallas en permisos de usuarios (acceso a archivos)
	Acceso electrónico no autorizado a sistemas externos
	Acceso electrónico no autorizado a sistemas internos
	Red cableada expuesta para el acceso no autorizado
	Red inalámbrica expuesta al acceso no autorizado
	Dependencia a servicio técnico externo
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
	Ausencia de documentación

1.3 CALCULOS DE RIESGO DE LOS ACTIVOS

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
	Incendio	4	1	4
	Inundación / deslave	4	1	4

Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8

Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8
	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Finanzas	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Finanzas	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Finanzas	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
RR.HH	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
RR.HH	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
RR.HH	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Directorio de Contactos	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Directorio de Contactos	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Directorio de Contactos	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Correo electrónico	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Correo electrónico	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Correo electrónico	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Bases de datos internos	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Bases de datos internos	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Bases de datos internos	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Bases de datos externos	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Bases de datos externos	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Bases de datos externos	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Bases de datos colaborativos	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Bases de datos colaborativos	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Bases de datos colaborativos	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Página Web interna (Intranet)	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Página Web interna (Intranet)	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Página Web interna (Intranet)	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Página Web externa	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Página Web externa	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Página Web externa	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Respaldos	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Respaldos	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Respaldos	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Infraestructura (Planes, Documentación, etc.)	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Infraestructura (Planes, Documentación, etc.)	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Infraestructura (Planes, Documentación, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Informática (Planes, Documentación, etc.)	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Informática (Planes, Documentación, etc.)	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Informática (Planes, Documentación, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Navegación en Internet	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Navegación en Internet	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Navegación en Internet	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Chat interno	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Chat interno	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Chat interno	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Llamadas telefónicas internas	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Llamadas telefónicas internas	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Llamadas telefónicas internas	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Llamadas telefónicas externas	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Llamadas telefónicas externas	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Llamadas telefónicas externas	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**			
Equipos de la red cableada (router, switch, etc.)	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Sistemas e Infraestructura	**Sucesos de origen físico**			
Equipos de la red cableada (router, switch, etc.)	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Equipos de la red cableada (router, switch, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Actos originados por la criminalidad común y motivación política**			
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Sistemas e Infraestructura	**Sucesos de origen físico**			
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Actos originados por la criminalidad común y motivación política**			
Cortafuego	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Sistemas e Infraestructura	**Sucesos de origen físico**			
Cortafuego	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Cortafuego	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Antivirus	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Antivirus	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Antivirus	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo Sistema e Infraestructura	Amenazas Actos originados por la criminalidad común y motivación política	Magnitud de Daño	Prob. De Amenaza	Total
Servidores	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo Sistemas e Infraestructura	Amenazas Sucesos de origen físico	Magnitud de Daño	Prob. De Amenaza	Total
Servidores	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Servidores	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo Sistemas e Infraestructura	Amenazas Actos originados por la criminalidad común y motivación política	Magnitud de Daño	Prob. De Amenaza	Total
Computadoras	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9

Activo Sistemas e Infraestructura	Amenazas Sucesos de origen físico	Magnitud de Daño	Prob. De Amenaza	Total
Computadoras	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Computadoras	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6

	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6
	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Portátiles	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Portátiles	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Portátiles	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**			
Programas de administración (contabilidad, manejo de personal, etc.)	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Sistemas e Infraestructura	**Sucesos de origen físico**			
Programas de administración (contabilidad, manejo de personal, etc.)	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Programas de administración (contabilidad, manejo de personal, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8

	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8
	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Impresoras	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Impresoras	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Impresoras	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Memorias portátiles	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Memorias portátiles	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Memorias portátiles	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Celulares	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Celulares	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Celulares	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4

	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4
	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Vehículos	Allanamiento (ilegal, legal)	1	1	1
	Persecución (civil, fiscal, penal)	1	1	1
	Sabotaje (ataque físico y electrónico)	1	1	1
	Daños por vandalismo	1	1	1
	Extorsión	1	2	2
	Fraude / Estafa	1	2	2
	Robo / Hurto (físico)	1	2	2
	Robo / Hurto de información electrónica	1	2	2
	Intrusión a Red interna	1	2	2
	Infiltración	1	2	2
	Virus / Ejecución no autorizado de programas	1	3	3
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Vehículos	Incendio	1	1	1
	Inundación / deslave	1	1	1
	Sismo	1	2	2
	Polvo	1	2	2
	Falta de ventilación	1	1	1
	Electromagnetismo	1	2	2
	Sobrecarga eléctrica	1	2	2
	Falla de corriente (apagones)	1	3	3
	Falla de sistema / Daño disco duro	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Vehículos	Falta de inducción, capacitación y sensibilización sobre riesgos	1	3	3
	Mal manejo de sistemas y herramientas	1	2	2
	Utilización de programas no autorizados / software 'pirateado'	1	2	2
	Falta de pruebas de software nuevo con datos productivos	1	1	1
	Perdida de datos	1	2	2
	Infección de sistemas a través de unidades portables sin escaneo	1	3	3
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	1	3	3
	Unidades portables con información sin cifrado	1	3	3
	Transmisión no cifrada de datos críticos	1	2	2
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	1	2	2
	Compartir contraseñas o permisos a terceros no autorizados	1	2	2
	Transmisión de contraseñas por teléfono	1	2	2
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	1	3	3
	Falta de definición de perfil, privilegios y restricciones del personal	1	2	2

	Falta de mantenimiento físico (proceso, repuestos e insumos)	1	2	2
	Falta de actualización de software (proceso y recursos)	1	2	2
	Fallas en permisos de usuarios (acceso a archivos)	1	2	2
	Acceso electrónico no autorizado a sistemas externos	1	1	1
	Acceso electrónico no autorizado a sistemas internos	1	1	1
	Red cableada expuesta para el acceso no autorizado	1	2	2
	Red inalámbrica expuesta al acceso no autorizado	1	2	2
	Dependencia a servicio técnico externo	1	2	2
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	1	3	3
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	1	3	3
	Ausencia de documentación	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Junta Directiva	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Junta Directiva	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Junta Directiva	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8
	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8

	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Dirección / Coordinación	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Dirección / Coordinación	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Dirección / Coordinación	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8
	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8

	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Administración	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Administración	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Administración	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6
	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6

	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Personal técnico	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Personal técnico	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Personal técnico	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4
	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4

	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Recepción	Allanamiento (ilegal, legal)	2	1	2
	Persecución (civil, fiscal, penal)	2	1	2
	Sabotaje (ataque físico y electrónico)	2	1	2
	Daños por vandalismo	2	1	2
	Extorsión	2	2	4
	Fraude / Estafa	2	2	4
	Robo / Hurto (físico)	2	2	4
	Robo / Hurto de información electrónica	2	2	4
	Intrusión a Red interna	2	2	4
	Infiltración	2	2	4
	Virus / Ejecución no autorizado de programas	2	3	6
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Recepción	Incendio	2	1	2
	Inundación / deslave	2	1	2
	Sismo	2	2	4
	Polvo	2	2	4
	Falta de ventilación	2	1	2
	Electromagnetismo	2	2	4
	Sobrecarga eléctrica	2	2	4
	Falla de corriente (apagones)	2	3	6
	Falla de sistema / Daño disco duro	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Recepción	Falta de inducción, capacitación y sensibilización sobre riesgos	2	3	6
	Mal manejo de sistemas y herramientas	2	2	4
	Utilización de programas no autorizados / software 'pirateado'	2	2	4
	Falta de pruebas de software nuevo con datos productivos	2	1	2
	Perdida de datos	2	2	4
	Infección de sistemas a través de unidades portables sin escaneo	2	3	6
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	2	3	6
	Unidades portables con información sin cifrado	2	3	6
	Transmisión no cifrada de datos críticos	2	2	4
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	2	2	4
	Compartir contraseñas o permisos a terceros no autorizados	2	2	4
	Transmisión de contraseñas por teléfono	2	2	4
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	2	3	6
	Falta de definición de perfil, privilegios y restricciones del personal	2	2	4
	Falta de mantenimiento físico (proceso, repuestos e insumos)	2	2	4

	Falta de actualización de software (proceso y recursos)	2	2	4
	Fallas en permisos de usuarios (acceso a archivos)	2	2	4
	Acceso electrónico no autorizado a sistemas externos	2	1	2
	Acceso electrónico no autorizado a sistemas internos	2	1	2
	Red cableada expuesta para el acceso no autorizado	2	2	4
	Red inalámbrica expuesta al acceso no autorizado	2	2	4
	Dependencia a servicio técnico externo	2	2	4
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	2	3	6
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	2	3	6
	Ausencia de documentación	2	2	4

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Piloto / conductor	Allanamiento (ilegal, legal)	1	1	1
	Persecución (civil, fiscal, penal)	1	1	1
	Sabotaje (ataque físico y electrónico)	1	1	1
	Daños por vandalismo	1	1	1
	Extorsión	1	2	2
	Fraude / Estafa	1	2	2
	Robo / Hurto (físico)	1	2	2
	Robo / Hurto de información electrónica	1	2	2
	Intrusión a Red interna	1	2	2
	Infiltración	1	2	2
	Virus / Ejecución no autorizado de programas	1	3	3
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Piloto / conductor	Incendio	1	1	1
	Inundación / deslave	1	1	1
	Sismo	1	2	2
	Polvo	1	2	2
	Falta de ventilación	1	1	1
	Electromagnetismo	1	2	2
	Sobrecarga eléctrica	1	2	2
	Falla de corriente (apagones)	1	3	3
	Falla de sistema / Daño disco duro	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Piloto / conductor	Falta de inducción, capacitación y sensibilización sobre riesgos	1	3	3
	Mal manejo de sistemas y herramientas	1	2	2
	Utilización de programas no autorizados / software 'pirateado'	1	2	2
	Falta de pruebas de software nuevo con datos productivos	1	1	1
	Perdida de datos	1	2	2
	Infección de sistemas a través de unidades portables sin escaneo	1	3	3
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	1	3	3
	Unidades portables con información sin cifrado	1	3	3
	Transmisión no cifrada de datos críticos	1	2	2
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	1	2	2
	Compartir contraseñas o permisos a terceros no autorizados	1	2	2
	Transmisión de contraseñas por teléfono	1	2	2
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	1	3	3
	Falta de definición de perfil, privilegios y restricciones del personal	1	2	2

	Falta de mantenimiento físico (proceso, repuestos e insumos)	1	2	2
	Falta de actualización de software (proceso y recursos)	1	2	2
	Fallas en permisos de usuarios (acceso a archivos)	1	2	2
	Acceso electrónico no autorizado a sistemas externos	1	1	1
	Acceso electrónico no autorizado a sistemas internos	1	1	1
	Red cableada expuesta para el acceso no autorizado	1	2	2
	Red inalámbrica expuesta al acceso no autorizado	1	2	2
	Dependencia a servicio técnico externo	1	2	2
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	1	3	3
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	1	3	3
	Ausencia de documentación	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Informática / Soporte técnico interno	Allanamiento (ilegal, legal)	4	1	4
	Persecución (civil, fiscal, penal)	4	1	4
	Sabotaje (ataque físico y electrónico)	4	1	4
	Daños por vandalismo	4	1	4
	Extorsión	4	2	8
	Fraude / Estafa	4	2	8
	Robo / Hurto (físico)	4	2	8
	Robo / Hurto de información electrónica	4	2	8
	Intrusión a Red interna	4	2	8
	Infiltración	4	2	8
	Virus / Ejecución no autorizado de programas	4	3	12
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Informática / Soporte técnico interno	Incendio	4	1	4
	Inundación / deslave	4	1	4
	Sismo	4	2	8
	Polvo	4	2	8
	Falta de ventilación	4	1	4
	Electromagnetismo	4	2	8
	Sobrecarga eléctrica	4	2	8
	Falla de corriente (apagones)	4	3	12
	Falla de sistema / Daño disco duro	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Informática / Soporte técnico interno	Falta de inducción, capacitación y sensibilización sobre riesgos	4	3	12
	Mal manejo de sistemas y herramientas	4	2	8
	Utilización de programas no autorizados / software 'pirateado'	4	2	8
	Falta de pruebas de software nuevo con datos productivos	4	1	4
	Perdida de datos	4	2	8
	Infección de sistemas a través de unidades portables sin escaneo	4	3	12
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	4	3	12
	Unidades portables con información sin cifrado	4	3	12
	Transmisión no cifrada de datos críticos	4	2	8
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	4	2	8
	Compartir contraseñas o permisos a terceros no autorizados	4	2	8
	Transmisión de contraseñas por teléfono	4	2	8
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	4	3	12
	Falta de definición de perfil, privilegios y restricciones del personal	4	2	8
	Falta de mantenimiento físico (proceso, repuestos e insumos)	4	2	8

	Falta de actualización de software (proceso y recursos)	4	2	8
	Fallas en permisos de usuarios (acceso a archivos)	4	2	8
	Acceso electrónico no autorizado a sistemas externos	4	1	4
	Acceso electrónico no autorizado a sistemas internos	4	1	4
	Red cableada expuesta para el acceso no autorizado	4	2	8
	Red inalámbrica expuesta al acceso no autorizado	4	2	8
	Dependencia a servicio técnico externo	4	2	8
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	4	3	12
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	4	3	12
	Ausencia de documentación	4	2	8

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Actos originados por la criminalidad común y motivación política**			
Soporte técnico externo	Allanamiento (ilegal, legal)	3	1	3
	Persecución (civil, fiscal, penal)	3	1	3
	Sabotaje (ataque físico y electrónico)	3	1	3
	Daños por vandalismo	3	1	3
	Extorsión	3	2	6
	Fraude / Estafa	3	2	6
	Robo / Hurto (físico)	3	2	6
	Robo / Hurto de información electrónica	3	2	6
	Intrusión a Red interna	3	2	6
	Infiltración	3	2	6
	Virus / Ejecución no autorizado de programas	3	3	9
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Personal	**Sucesos de origen físico**			
Soporte técnico externo	Incendio	3	1	3
	Inundación / deslave	3	1	3
	Sismo	3	2	6
	Polvo	3	2	6
	Falta de ventilación	3	1	3
	Electromagnetismo	3	2	6
	Sobrecarga eléctrica	3	2	6
	Falla de corriente (apagones)	3	3	9
	Falla de sistema / Daño disco duro	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Personal	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Soporte técnico externo	Falta de inducción, capacitación y sensibilización sobre riesgos	3	3	9
	Mal manejo de sistemas y herramientas	3	2	6
	Utilización de programas no autorizados / software 'pirateado'	3	2	6
	Falta de pruebas de software nuevo con datos productivos	3	1	3
	Perdida de datos	3	2	6
	Infección de sistemas a través de unidades portables sin escaneo	3	3	9
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	3	3	9
	Unidades portables con información sin cifrado	3	3	9
	Transmisión no cifrada de datos críticos	3	2	6
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	3	2	6
	Compartir contraseñas o permisos a terceros no autorizados	3	2	6
	Transmisión de contraseñas por teléfono	3	2	6
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	3	3	9
	Falta de definición de perfil, privilegios y restricciones del personal	3	2	6
	Falta de mantenimiento físico (proceso, repuestos e insumos)	3	2	6

	Falta de actualización de software (proceso y recursos)	3	2	6
	Fallas en permisos de usuarios (acceso a archivos)	3	2	6
	Acceso electrónico no autorizado a sistemas externos	3	1	3
	Acceso electrónico no autorizado a sistemas internos	3	1	3
	Red cableada expuesta para el acceso no autorizado	3	2	6
	Red inalámbrica expuesta al acceso no autorizado	3	2	6
	Dependencia a servicio técnico externo	3	2	6
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	3	3	9
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	3	3	9
	Ausencia de documentación	3	2	6

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Servicio de limpieza de planta	Allanamiento (ilegal, legal)	1	1	1
	Persecución (civil, fiscal, penal)	1	1	1
	Sabotaje (ataque físico y electrónico)	1	1	1
	Daños por vandalismo	1	1	1
	Extorsión	1	2	2
	Fraude / Estafa	1	2	2
	Robo / Hurto (físico)	1	2	2
	Robo / Hurto de información electrónica	1	2	2
	Intrusión a Red interna	1	2	2
	Infiltración	1	2	2
	Virus / Ejecución no autorizado de programas	1	3	3
Activo	**Amenazas**	**Magnitud de Daño**	**Prob. De Amenaza**	**Total**
Datos e Información	**Sucesos de origen físico**			
Servicio de limpieza de planta	Incendio	1	1	1
	Inundación / deslave	1	1	1
	Sismo	1	2	2
	Polvo	1	2	2
	Falta de ventilación	1	1	1
	Electromagnetismo	1	2	2
	Sobrecarga eléctrica	1	2	2
	Falla de corriente (apagones)	1	3	3
	Falla de sistema / Daño disco duro	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Servicio de limpieza de planta	Falta de inducción, capacitación y sensibilización sobre riesgos	1	3	3
	Mal manejo de sistemas y herramientas	1	2	2
	Utilización de programas no autorizados / software 'pirateado'	1	2	2
	Falta de pruebas de software nuevo con datos productivos	1	1	1
	Perdida de datos	1	2	2
	Infección de sistemas a través de unidades portables sin escaneo	1	3	3
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	1	3	3
	Unidades portables con información sin cifrado	1	3	3
	Transmisión no cifrada de datos críticos	1	2	2
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	1	2	2
	Compartir contraseñas o permisos a terceros no autorizados	1	2	2
	Transmisión de contraseñas por teléfono	1	2	2
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	1	3	3
	Falta de definición de perfil, privilegios y restricciones del personal	1	2	2

	Falta de mantenimiento físico (proceso, repuestos e insumos)	1	2	2
	Falta de actualización de software (proceso y recursos)	1	2	2
	Fallas en permisos de usuarios (acceso a archivos)	1	2	2
	Acceso electrónico no autorizado a sistemas externos	1	1	1
	Acceso electrónico no autorizado a sistemas internos	1	1	1
	Red cableada expuesta para el acceso no autorizado	1	2	2
	Red inalámbrica expuesta al acceso no autorizado	1	2	2
	Dependencia a servicio técnico externo	1	2	2
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	1	3	3
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	1	3	3
	Ausencia de documentación	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Actos originados por la criminalidad común y motivación política**			
Servicio de limpieza externo	Allanamiento (ilegal, legal)	1	1	1
	Persecución (civil, fiscal, penal)	1	1	1
	Sabotaje (ataque físico y electrónico)	1	1	1
	Daños por vandalismo	1	1	1
	Extorsión	1	2	2
	Fraude / Estafa	1	2	2
	Robo / Hurto (físico)	1	2	2
	Robo / Hurto de información electrónica	1	2	2
	Intrusión a Red interna	1	2	2
	Infiltración	1	2	2
	Virus / Ejecución no autorizado de programas	1	3	3

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos de origen físico**			
Servicio de limpieza externo	Incendio	1	1	1
	Inundación / deslave	1	1	1
	Sismo	1	2	2
	Polvo	1	2	2
	Falta de ventilación	1	1	1
	Electromagnetismo	1	2	2
	Sobrecarga eléctrica	1	2	2
	Falla de corriente (apagones)	1	3	3
	Falla de sistema / Daño disco duro	1	2	2

Activo	Amenazas	Magnitud de Daño	Prob. De Amenaza	Total
Datos e Información	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**			
Servicio de limpieza externo	Falta de inducción, capacitación y sensibilización sobre riesgos	1	3	3
	Mal manejo de sistemas y herramientas	1	2	2
	Utilización de programas no autorizados / software 'pirateado'	1	2	2
	Falta de pruebas de software nuevo con datos productivos	1	1	1
	Perdida de datos	1	2	2
	Infección de sistemas a través de unidades portables sin escaneo	1	3	3
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	1	3	3
	Unidades portables con información sin cifrado	1	3	3
	Transmisión no cifrada de datos críticos	1	2	2
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	1	2	2
	Compartir contraseñas o permisos a terceros no autorizados	1	2	2
	Transmisión de contraseñas por teléfono	1	2	2
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	1	3	3
	Falta de definición de perfil, privilegios y restricciones del personal	1	2	2

	Falta de mantenimiento físico (proceso, repuestos e insumos)	1	2	2
	Falta de actualización de software (proceso y recursos)	1	2	2
	Fallas en permisos de usuarios (acceso a archivos)	1	2	2
	Acceso electrónico no autorizado a sistemas externos	1	1	1
	Acceso electrónico no autorizado a sistemas internos	1	1	1
	Red cableada expuesta para el acceso no autorizado	1	2	2
	Red inalámbrica expuesta al acceso no autorizado	1	2	2
	Dependencia a servicio técnico externo	1	2	2
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	1	3	3
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	1	3	3
	Ausencia de documentación	1	2	2

1.4 TABLAS DE ACTIVOS, VUNERABILIDADES Y CONTROLES

Activo	Amenazas	Vulnerabilidad	Controles de Seguridad
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Equipos de la red cableada (router, switch, etc.)	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	13.1.2 Mecanismos de seguridad asociados a servicios en red
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada.

			11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
Equipos de la red cableada (router, switch, etc.)	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras

	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**		
	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo.

Equipos de la red cableada (router, switch, etc.)			14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4

			Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.

	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	13.1.1 Controles de red.
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo	13.1.2 Mecanismos de seguridad asociados a servicios en red.

		interés para estas normas de uso	

Activo	Amenazas	Vulnerabilidad	Controles de Seguridad
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	13.1.2 Mecanismos de seguridad asociados a servicios en red
	Fraude / Estafa		

	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
Equipos de la red inalámbrica (router, punto de acceso, etc.)	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos

	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**		
	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no	✓Instalación de software libre que	12.2.1 Controles contra el código

Equipos de la red inalámbrica (router, punto de acceso, etc.)	autorizados / software 'pirateado'	pueden dañar el funcionamiento	malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.

	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.

	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	13.1.1 Controles de red.

	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	13.1.2 Mecanismos de seguridad asociados a servicios en red.

Activo	Amenazas	Vulnerabilidad	Controles de Seguridad
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Cortafuego	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta	11.1.1 Perímetro de seguridad física.

		zonas no autorizadas	
	Extorsión	✓ Ingreso a las redes por varias personas	13.1.2 Mecanismos de seguridad asociados a servicios en red
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		

Cortafuego	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**		
	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los	7.2.2 Concienciación, educación y capacitación en segur. de la información

Cortafuego		usuarios de estas conexiones	
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.

	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico	✓Conexiones antiguas sin	11.2.4 Mantenimiento de los equipos.

	(proceso, repuestos e insumos)	mantenimiento actual	
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		

	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	13.1.1 Controles de red.
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	13.1.2 Mecanismos de seguridad asociados a servicios en red.

Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Antivirus	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.3 Seguridad del cableado.

			11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	13.1.2 Mecanismos de seguridad asociados a servicios en red
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con	12.2.1 Controles contra el código malicioso

		conexiones de wifi no autorizados	
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
Antivirus	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y**		

	decisiones institucionales		
Antivirus	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.

	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios.

			9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de	11.2.3 Seguridad del cableado.

		acceso libre o sin autorización	
	Dependencia a servicio técnico externo		
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	13.1.1 Controles de red.
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	13.1.2 Mecanismos de seguridad asociados a servicios en red.

Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Servidores	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.

	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	13.1.2 Mecanismos de seguridad asociados a servicios en red
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2

			Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
Servidores	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	

Sistemas e Infraestructura	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		Controles de Seguridad
Servidores	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..

	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales.

			9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.

	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		15.2.1 Supervisión y revisión de los servicios prestados por terceros
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	13.1.1 Controles de red.
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	13.1.2 Mecanismos de seguridad asociados a servicios en red.
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	13.1.2 Mecanismos de seguridad asociados a servicios en red.

Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Computadoras	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.

	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	9.1.1 Política de control de accesos:
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red

	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
Computadoras	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.

	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**		
Computadoras	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.

	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de

			autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con	13.2.3 Mensajería electrónica.

		la confidencialidad	13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		15.2.1 Supervisión y revisión de los servicios prestados por terceros
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés	

		para estas normas de uso	

Activo	Amenazas	Vulnerabilidad	Controles de Seguridad
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
Portátiles	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas no autorizadas	11.1.1 Perímetro de seguridad física.
	Extorsión	✓ Ingreso a las redes por varias personas	9.1.1 Política de control de accesos:
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada.

		de los equipos de red	11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso
Activo **Sistemas e Infraestructura**	**Amenazas** **Sucesos de origen físico**	**Vulnerabilidad**	**Controles de Seguridad**
Portátiles	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos

	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**		
	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.

Portátiles	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del servicio de redes	10.1.1 Política de uso de los controles criptográficos..
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.

	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.

	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		15.2.1 Supervisión y revisión de los servicios prestados por terceros
	Falta de normas y reglas claras (no	✓Normas no usadas por el	

	institucionalizar el estudio de los riesgos)	personal o bajo interés a estas.	
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	

Activo Sistema e Infraestructura	Amenazas Actos originados por la criminalidad común y motivación política	Vulnerabilidad	Controles de Seguridad
Impresoras	Allanamiento (ilegal, legal)	✓ Acceso no permitido a personas no capacitadas	11.1.1 Perímetro de seguridad física. 11.2.1 Emplazamiento y protección de equipos.
	Persecución (civil, fiscal, penal)	✓ Acceso red no autorizada	11.2.1 Emplazamiento y protección de equipos.
	Sabotaje (ataque físico y electrónico)	✓ No existe una vigilancia permanente, aparte del personal encargado	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.4 Mantenimiento de los equipos
	Daños por vandalismo	✓ El ingreso de público en horario de atención, hasta zonas	11.1.1 Perímetro de seguridad física.

		no autorizadas	
	Extorsión	✓ Ingreso a las redes por varias personas	9.1.1 Política de control de accesos:
	Fraude / Estafa		
	Robo / Hurto (físico)	✓ Fácil ubicación y desprotección de los equipos de red	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.6 Áreas de acceso público, carga y descarga.
	Robo / Hurto de información electrónica	✓ La configuración para el ingreso a estos recursos es de fácil ingreso y configuración de las claves y usuarios	13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.
	Intrusión a Red interna	Alojamiento a computadoras o aparatos móviles no permitidos para la conexión a estos recursos	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Infiltración		13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Virus / Ejecución no autorizado de programas	La conexión de aparatos con conexiones de wifi no autorizados	12.2.1 Controles contra el código malicioso

Activo Sistemas e Infraestructura	Amenazas Sucesos de origen físico	Vulnerabilidad	Controles de Seguridad
Impresoras	Incendio	✓ Recurso inflamables	11.1.3 Seguridad de oficinas, despachos y recursos
	Inundación / deslave		11.1.3 Seguridad de oficinas, despachos y recursos
	Sismo	✓ Recurso frágiles	11.1.5 El trabajo en áreas seguras
	Polvo	✓ Recurso no contienen un gabinete especial	11.2.4 Mantenimiento de los equipos.
	Falta de ventilación		11.2.4 Mantenimiento de los equipos.
	Electromagnetismo	✓ Recurso podrían estar mal conectados	11.2.4 Mantenimiento de los equipos.
	Sobrecarga eléctrica	✓ Sobrecargas eléctricas	11.2.3 Seguridad del cableado.
	Falla de corriente (apagones)		11.2.3 Seguridad del cableado.
	Falla de sistema / Daño disco duro	✓ Conexiones antiguas en malas condiciones	11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.
Activo **Sistemas e Infraestructura**	**Amenazas** **Sucesos derivados de la impericia, negligencia de usuarios/as y**	**Vulnerabilidad**	**Controles de Seguridad**

	decisiones institucionales		
Impresoras	Falta de inducción, capacitación y sensibilización sobre riesgos	✓Poco conocimiento de redes o cableados por parte de los usuarios de estas conexiones	7.2.2 Concienciación, educación y capacitación en segur. de la información
	Mal manejo de sistemas y herramientas	✓Poco conocimiento de algunas herramientas de red	9.4.4 Uso de herramientas de administración de sistemas.
	Utilización de programas no autorizados / software 'pirateado'	✓Instalación de software libre que pueden dañar el funcionamiento	12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad.
	Falta de pruebas de software nuevo con datos productivos	✓Fallo de algunas conexiones y configuraciones	14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.
	Perdida de datos	✓Conexiones obsoletas o antiguas	12.3.1 Copias de seguridad de la información.
	Infección de sistemas a través de unidades portables sin escaneo	✓Unidades extraíbles con dudoso contenido e procedencia	8.3.1 Gestión de soportes extraíbles.
	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	✓Errores cometidos por el personal al manejo de datos del	10.1.1 Política de uso de los controles criptográficos..

		servicio de redes	
	Unidades portables con información sin cifrado	✓Conexiones antiguas en malas condiciones	8.3.1 Gestión de soportes extraíbles.
	Transmisión no cifrada de datos críticos	✓Unidades extraíbles con dudoso contenido e procedencia	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.
	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	✓Mal uso de contraseñas y aún más manipuladas al azar por el personal	9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Compartir contraseñas o permisos a terceros no autorizados	✓Contraseñas compartidas sin alguna autorización del personal a cargo	9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Transmisión de contraseñas por teléfono	✓Intercambio de datos no autorizados por celulares	9.2.4 Gestión de información confidencial de autenticación de usuarios.
	Exposición o extravío de equipo, unidades de almacenamiento, etc.	✓El bajo interés e importancia del personal que usa estos activos	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

	Falta de definición de perfil, privilegios y restricciones del personal	✓Los usuarios no están establecidos por niveles	9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	Falta de mantenimiento físico (proceso, repuestos e insumos)	✓Conexiones antiguas sin mantenimiento actual	11.2.4 Mantenimiento de los equipos.
	Falta de actualización de software (proceso y recursos)	✓Software descontinuado o sin actualización permitida	12.5.1 Instalación del software en sistemas en producción.
	Fallas en permisos de usuarios (acceso a archivos)	✓El control de usuarios no adecuado y muchas veces demasiada compartida	9.2.6 Retirada o adaptación de los derechos de acceso 9.2.1 Gestión de altas/bajas en el registro de usuarios.
	Acceso electrónico no autorizado a sistemas externos	✓Usuarios no consientes con la confidencialidad	13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.
	Acceso electrónico no autorizado a sistemas internos	✓Usuarios no consientes con la confidencialidad internamente	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica.

			13.2.4 Acuerdos de confidencialidad y secreto.
	Red cableada expuesta para el acceso no autorizado	✓Cableado a la vista de las personas	11.2.3 Seguridad del cableado.
	Red inalámbrica expuesta al acceso no autorizado	✓Algunas conexiones de acceso libre o sin autorización	11.2.3 Seguridad del cableado.
	Dependencia a servicio técnico externo		
	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	✓Normas no usadas por el personal o bajo interés a estas.	
	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	✓Mecanismos de verificación poco eficaces	
	Ausencia de documentación	✓Reglamento de uso o condiciones de uso no practicadas o bajo interés para estas normas de uso	

Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistema e Infraestructura	**Actos originados por la criminalidad común y motivación política**		
	Allanamiento (ilegal, legal)	✓ Ingreso de personas no autorizadas	11.1.1 Perimetro de seguridad física

Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Persecución (civil, fiscal, penal)	✓	11.1.4 Protección contra las amenazas externas y ambientales
	Sabotaje (ataque físico y electrónico)	✓	11.1.5 Trabajo en áreas seguras
	Daños por vandalismo	✓	11.1.3 Seguridad de oficinas, despachos y recursos
	Extorsión	✓	11.1.5 Trabajo en áreas seguras
	Fraude / Estafa		11.1.5 Trabajo en áreas seguras
	Robo / Hurto (físico)	✓	11.1.5 Trabajo en áreas seguras
	Robo / Hurto de información electrónica	✓	
	Intrusión a Red interna		
	Infiltración		11.1.6 Áreas de acceso público, carga y descarga
	Virus / Ejecución no autorizado de programas		
Activo	**Amenazas**	**Vulnerabilidad**	**Controles de Seguridad**
Sistemas e Infraestructura	**Sucesos de origen físico**		
	Incendio	✓	11.1.5 Trabajo en áreas seguras
	Inundación / deslave		11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales

Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	Sismo	✓	11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales
	Polvo	✓	
	Falta de ventilación		11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales
	Electromagnetismo	✓	11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales
	Sobrecarga eléctrica	✓	11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales
	Falla de corriente (apagones)		11.1.5 Trabajo en áreas seguras 11.1..4 Protección contra las amenazas externas y ambientales
	Falla de sistema / Daño disco duro	✓	11.1.5 Trabajo en áreas seguras

CAPITULO 2

ETAPA 2: PLAN HACER
POLITICAS DE SEGURIDAD

5.1 FASES DE CONTROLES PARA LA POLITICAS DE SEGURIDAD DE INFORMACIÓN

2.1.1 DOMINIO: 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

2.1.1.1 OBJETIVO DEL DOMINIO

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

Suele ser responsabilidad del Área de Recursos Humanos incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa de sus obligaciones respecto

del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios respecto a las necesidades actuales en seguridad.

El Responsable del Área Jurídica participa en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención.

2.1.1.2 R7.1: ANTES DE LA CONTRATACIÓN

- ✓ 7.1.1 Investigación de antecedentes: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

- ✓ 7.1.2 Términos y condiciones de contratación: Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

2.1.1.3 R7.2 DURANTE LA CONTRATACIÓN

- ✓ 7.2.2 Concienciación, educación y capacitación en SI: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

2.1.1.4 NORMATIVA DE SEGURIDAD DE CONTRATACIÓN DEL PERSONAL DE LA EMPRESA GEOSURVEY:

Art 1: La EMPRESA GEOSURVEY al realizar los concursos deberá fijarse en los antecedentes policiales, legales de las personas clasificadas para laborar en la entidad municipal.

Art 2: El personal a contratar deberá presentar una hoja de vida legalizada, foliada y conjunto con sus antecedentes.

Art 3: La EMPRESA GEOSURVEY, deberé proveer al empleado a contratar los términos y condiciones de contratación, así mismo explicar si en caso tenga alguna duda el empleado

Art 4: la EMPRESA GEOSURVEY, debe presentar el manual de reglamento interno de dicha entidad, donde debe estar formalizado los deberes y derechos del empleado en la entidad.

Art 5: la EMPRESA deberá realizar la capacitación previa o inicial al empleado en la labor que desarrollará para explicarle sus funciones; también la EMPRESA provincial deberá dar charlas de seguridad de información y de activos a cargo de los ingenieros de sistemas e informática para evitar algún fallo de protección de activos de la entidad,

Art 6: La EMPRESA debe velar por que su empleado esté capacitado en cada uno de las formalidades que debe cumplir, así como la protección de la entidad misma y sus activos.

2.1.2 DOMINIO: 8. GESTION DE ACTIVOS

2.1.2.1 OBJETIVO DEL DOMINIO

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada por la propia organización. Se debería considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

2.1.2.2 R8.2 CLASIFICACIÓN DE LA INFORMACIÓN

- ✓ 8.2.2 Etiquetado y manipulado de la información: Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

2.1.2.3 R8.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO

- ✓ 8.3.1 Gestión de soportes extraíbles: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.

2.1.2.4 NORMATIVA DE SEGURIDAD ACERCA DE GESTIÓN DE ACTIVOS DE LA EMPRESA GEOSURVEY:

Art 7: la EMPRESA en conjunto de sus ingenieros de sistemas y otros representantes deberá definir responsabilidades de los encargados de cada oficina así como los activos en dichas oficinas.

Art 8: Cada encargado debe realizar su etiquetado lo cual permitirá a la EMPRESA realizar una guía de manipulación de cada tipo de activo, lo cual en este se velará la seguridad, confidencialidad, integridad de los activos previamente etiquetados.

Art 9: la EMPRESA podría usar software como OCS Inventory NG, que siendo su función especial es la creación de inventarios detallados y funcionales, muy aparte que es de distribución gratuita; este tipo de software para inventarios realizara un proceso más efectivo, confiable al momento de etiquetar cada activo.

2.1.3 DOMINIO: 9. CONTROL DE ACCESO

2.1.3.1 OBJETIVO DEL DOMINIO

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos

de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

2.1.3.2 R9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

- ✓ 9.1.2 Control de acceso a las redes y servicios asociados: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

2.1.3.3 R9.2 GESTIÓN DE ACCESO DE USUARIO

9.2.1 Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

- ✓ 9.2.2 Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
- ✓ 9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

- ✓ 9.2.4 Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

- ✓ 9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

- ✓ 9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

2.1.3.4 NORMATIVA DEL CONTROL DE ACCESO DE LA EMPRESA GEOSURVEY:

Art 10: La EMPRESA deberá integrar a sus sistemas los niveles de usuario correspondiente para así evitar que información confidencial sea vista por usuarios no autorizados

Art.11: La EMPRESA deberá establecer restricciones de acceso por medio de la red y privilegias de acuerdo al cargo de los usuarios.

Art.12: Tiene que haber una persona de confianza y que se quede a cargo para controlar los accesos de los usuarios y ver que todo siga bien.

2.1.4 DOMINIO: 10. CIFRADO

2.1.4.1 OBJETIVO DEL DOMINIO

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La aplicación de medidas de cifrado se debería desarrollar en base a una política

sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

2.1.4.2 R10.1 CONTROLES CRIPTOGRÁFICOS

- ✓ 10.1.1 Política de uso de los controles criptográficos: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.
- ✓ 10.1.2 Gestión de claves: Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

2.1.4.3 NORMATIVA DEL CIFRADO DE SEGURIDAD DE LA EMPRESA GEOSURVEY:

Art.13: La EMPRESA debe utilizar software de cifrado o encriptación.

Art.14: La EMPRESA debe deberá cifrar o encriptar los archivos o datos críticos para volverlos ilegibles. De esta manera, el archivo se vuelve prácticamente inservible para un usuario no autorizado a leerlo ya que incluso si lo ha interceptado o lo ha copiado, si no cuenta con el password correspondiente, no podrá leerlo o visualizarlo.

2.1.5 DOMINIO: 11. SEGURIDAD FISICA Y AMBIENTAL

2.1.5.1 OBJETIVO DEL DOMINIO

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento

de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

5.1.5.2 R11.1 ÁREAS SEGURAS

- ✓ 11.1.1 Perímetro de seguridad física: Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.
- ✓ 11.1.2 Controles físicos de entrada: Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.
- ✓ 11.1.3 Seguridad de oficinas, despachos y recursos: Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
- ✓ 11.1.4 Protección contra las amenazas externas y ambientales: Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

- ✓ 11.1.5 El trabajo en áreas seguras: Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.
- ✓ 11.1.6 Áreas de acceso público, carga y descarga: Se deberían controlar puntos de acceso a la organización como las áreas de entrega y

carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

5.1.5.2 R11.2 SEGURIDAD DE LOS EQUIPOS

- ✓ 11.2.1 Emplazamiento y protección de equipos: Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
- ✓ 11.2.3 Seguridad del cableado: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.
- ✓ 11.2.4 Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

- ✓ 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

5.1.5.3 NORMATIVA DE SEGURIDAD EXTERNA Y AMBIENTAL DE LA EMPRESA GEOSURVEY:

Art.15: La EMPRESA debe establecer zonas seguras en caso de desastres naturales.

Art. 16: La EMPRESA debe contar con sistemas que ayuden a prevenir algunos accidentes o atentados físicos.

Art.17: Se debe contar con un sistema de inventario de equipos y de servicio técnico.

Art.18: Se debe llevar un cronograma de mantenimiento de equipos por áreas.

Art.19: Se debe contar con mapa de las instalaciones de red como de las instalaciones eléctricas.

2.1.6 DOMINIO: 12. SEGURIDAD OPERATIVA

2.1.6.1 OBJETIVO DEL DOMINIO:

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permiten garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización.

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

Finalmente, se deberían verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

5.1.6.2 R12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

- ✓ 12.1.1 Documentación de procedimientos de operación: Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

5.1.6.3 R12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

- ✓ 12.2.1 Controles contra el código malicioso: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

5.1.6.4 R12.3 COPIAS DE SEGURIDAD

- ✓ 12.3.1 Copias de seguridad de la información: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

5.1.6.5 R12.4 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

- ✓ 12.4.2 Protección de los registros de información: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.

5.1.6.6 R12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN

- ✓ 12.5.1 Instalación del software en sistemas en producción: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

5.1.6.7 R12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- ✓ 12.6.2 Restricciones en la instalación de software: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

5.1.6.8 NORMATIVA DE LA SEGURIDAD OPERATIVA DE LA EMPRESA GEOSURVEY:

Art.20: La EMPRESA deberá hacer uso de antivirus con sus licencias actualizadas para evitar cualquier contagio de virus.

Art.21: Se deberá hacer restricciones de páginas para evitar que el usuario entre a páginas que infecten de virus al equipo.

Art. 22: Se debe llevar un control de copias de seguridad y un encargado el cual siempre saque copias de seguridad de los datos.

2.1.7 DOMINIO: 13. SEGURIDAD DE TELECOMUNICACIONES

2.1.7.1 OBJETIVO DEL DOMINIO

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.

Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

5.1.7.2 R13.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES

- ✓ 13.1.1 Controles de red: Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones
  .
- ✓ 13.1.2 Mecanismos de seguridad asociados a servicios en red: Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

5.1.7.3 R13.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS

- ✓ 13.2.1 Políticas y procedimientos de intercambio de información: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

- ✓ 13.2.2 Acuerdos de intercambio: Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

- ✓ 13.2.3 Mensajería electrónica: Se debería proteger adecuadamente la información referida en la mensajería electrónica.

- ✓ 13.2.4 Acuerdos de confidencialidad y secreto: se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

5.1.7.4 NORMATIVA DE SEGURIDAD DE LA TELECOMUNICACIÓN DE LA EMPRESA GEOSURVEY:

Art.23: Se deberá hacer uso de una red segura para la transferencia de archivos con información confidencial.

Art.24: Se debe controlar los accesos a la red (NAC) cuyos objetivos son:

- Mitigar ataques de día cero

  El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.

- Refuerzo de políticas

  Las soluciones NAC permiten a los operadores de red definir políticas, tales como tipos de ordenadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers.

- Administración de acceso e identidad

  Donde las redes IPs convencionales refuerzan las políticas de acceso con base en direcciones IP, los dispositivos NAC lo realizan basándose en

identidades de usuarios autenticados, al menos para usuarios finales de equipos portátiles y sobremesa.

2.1.8 DOMINIO: 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

2.1.8.1 OBJETIVO DEL DOMINIO

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

2.1.8.2 R14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

- ✓ 14.2.4 Restricciones a los cambios en los paquetes de software: Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

- ✓ 14.2.6 Seguridad en entornos de desarrollo: Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

- ✓ 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas: Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.

- ✓ 14.2.9 Pruebas de aceptación: Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

2.1.8.3 R14.3 DATOS DE PRUEBA

- ✓ 14.3.1 Protección de los datos utilizados en prueba: Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

2.1.8.4 NORMATIVAS DE SEGURIDAD DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN DE LA EMPRESA GEOSURVEY:

Art.25: La EMPRESA debe hacer uso de software o programas para comprobar la integridad de los archivos.

Art.26: La EMPRESA debe realizar distintas pruebas a los programas y sistemas antes de que estos sean implementados.

2.1.9 DOMINIO: 18. CUMPLIMIENTO

2.1.9.1 OBJETIVO DEL DOMINIO

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información

2.1.9.2 R18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

- ✓ 18.2.2 Cumplimiento de las políticas y normas de seguridad: Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
- ✓ 18.2.3 Comprobación del cumplimiento: Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

2.1.9.3 NORMATIVA DE CUMPLIMIENTO DE SEGURIDAD DE LA EMPRESA GEOSURVEY:

Art.27: Fomentar a los trabajadores a cumplir con las normas y reglas que se establecen en temas de seguridad de la información.

Art.28: Realizar chequeos periódicamente de que se están respetando dichas normas y reglas.

CAPITULO 3

ETAPA 3: GESTION DE INCIDENTES

3.1 CONTROL DE INCIDENCIAS

Ticket #	Estado	Prioridad	Incidencia	Área	Descripción	Abierto el día	Informado por:	Asignado a:	Fecha de Resolución
1	Resuelto	Media	Sin acceso al sistema	Gerencia Administrativa	Servidor de Datos	17/01/2017	Joel Cajas	Victor Ramirez	18/01/2017
2	Abierto	Media	Necesita Formateo	Contabilidad	pc11	25/02/2017	Arturo Santos	Victor Ramirez	
3	Resuelto	Urgente	No reconoce la conexión	Ventas	Servidor Web	21/01/2017	Joel Cajas	Victor Ramirez	21/01/2017
4	Resuelto	Baja	Ayuda en modificacion de un archivo	Marketing y Publicidad	pc16	21/10/2017	Hugo Ramirez	Victor Ramirez	21/10/2017
5	Abierto	Media	Fuente Quemada	Ventas	pc15	15/02/2017	Joel Cajas	Victor Ramirez	
6	Abierto	Media	Falta Mantenimiento	Ventas	Servidor Web	27/02/2017	Patricia Ramirez	Victor Ramirez	
7	Abierto	Baja	Acceso a Internet	Operativa	pc03	18/02/2017	Aldo Torres	Victor Ramirez	
8	Resuelto	Alta	Equipo mojado por lluvia	Marketing y Publicidad	PC1-alcaldia	06/01/2017	Dionisio Malpartida	Hugo Ramirez	11/01/2017
9	Resuelto	Media	Falta subir archivos	Marketing y Publicidad	pc03	10/01/2017	Pedro Rivera	Hugo Ramirez	12/01/2017
10	Resuelto	Baja	Sin acceso al sistema	Marketing y Publicidad	Servidor de Correos	04/02/2017	Andre Santiago	Hugo Ramirez	04/02/2017

11	Abierto	Baja	Fallo con la tarjeta de video	Marketing y Publicidad	Proyector Negro	17/07/2017	Ivan Trujillo	Hugo Ramirez	
12	Resuelto	Media	Creacion de usuarios en el sistema	Topografia	Sistema Tramite	03/01/2017	Ivan Trujillo	Hugo Ramirez	04/01/2017
13	Resuelto	Alta	Modificacion del sistema	Contabilidad	Sistema Pagos	07/01/2017	Cesar Augusto Pinedo	Aldo Torres	07/01/2017
14	Resuelto	Media	Se desconecto	Marketing y Publicidad	Servidor de Datos	25/02/2017	Nestor Quispe	Aldo Torres	25/02/2017
15	Abierto	Alta	Agregar modulos al sistema	Operativa	Sistema de intranet	11/01/2017	Yolanda del Poma	Aldo Torres	
16	Resuelto	Urgente	Falta subir archivos	Operativa	Pagina Web	01/01/2017	Jose Victor Carranza	Patricia Ramirez	02/01/2017
17	Resuelto	Baja	Ayuda en modificacion de un archivo	Contabilidad	pc08	19/01/2017	Juan Carlos Mendieta	Aldo Torres	
18	Resuelto	Media	Correcion de un registro por medio del sistema	Medio Ambiente y Seguridad	Sistema Tramite	12/01/2017	Jose Estrada	Aldo Torres	12/01/2017
19	Resuelto	Alta	Recepcion de Documentos Derivados al area	Contabilidad	pc10	18/02/2017	Flor Santamaria	Patricia Ramirez	18/02/2017
20	Resuelto	Urgente	Modificacion en la base de datos	Ventas	Sistema Pagos	13/01/2017	Alfredo Cajas	Aldo Torres	13/01/2017
21	Abierto	Alta	Modificacion de modulos del sistema	Ventas	Sistema Tramite	27/02/2017	Ana Torres	Aldo Torres	
22	Resuelto	Baja	Correcion de un registro por medio del sistema	Topografia	Sistema Tramite	26/01/2017	Antonio Jara	Aldo Torres	26/01/2017
23	Abierto	Media	No enciende	Medio Ambiente y Seguridad	Impresora01	28/02/2017	Luis Dias	Aldo Torres	28/02/2017
24	Resuelto	Baja	Correcion de un registro por medio del sistema	Gerencia General	Sistema Tramite	26/01/2017	Cesar Augusto Pinedo	Victor Ramirez	26/01/2017
25	Resuelto	Baja	Conversion de Archivos	Gerencia Administrativa	pc14	06/01/2017	Ana Torrejon	Victor Ramirez	06/01/2017

26	Resuelto	Alta	Sin acceso al sistema	Contabilidad	pc17	25/01/2017	Andres Santos	Victor Ramirez	25/01/2017
27	Resuelto	Baja	Formateo	Marketing y Publicidad	USB	04/02/2017	Luis Loarte	Victor Ramirez	04/02/2017
28	Abierto	Media	Modificacion de modulos del sistema	Ventas	Sistema de intranet	25/02/2017	Ivan Trujillo	Victor Ramirez	
29	Resuelto	Media	No imprime	Operativa	Impresora02	13/01/2017	Andres Malpartida	Victor Ramirez	25/01/2017
30	Abierto	Media	Fallo con la tarjeta de video	Medio Ambiente y Seguridad	pc10	27/01/2017	Leidy Suarez	Karla Santos	15/02/2017
31	Resuelto	Baja	La pantalla esta parpadeando	Topografia	pc11	19/01/2017	Andres Malpartida	Victor Ramirez	22/01/2017
32	Abierto	Baja	Falta Conectar	Medio Ambiente y Seguridad	Impresora02	16/01/2017	Estefanny Echaverria	Victor Ramirez	16/01/2017
33	Resuelto	Alta	Prestamo de Equipo Multimedia	Gerencia Administrativa	Proyector Blanco	06/01/2017	Dionisio Malpartida	Victor Ramirez	06/01/2017
34	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	19/01/2017	Patricia Ramirez	Hugo Ramirez	19/01/2017
35	Resuelto	Media	No tiene internet	Ventas	pc07	02/02/2017	Aldo Torres	Hugo Ramirez	02/02/2017
36	Resuelto	Media	Cambio de clave de usuario	Marketing y Publicidad	Sistema Pagos	10/01/2017	Dionisio Malpartida	Hugo Ramirez	10/01/2017
37	Resuelto	Baja	Malogrado	Ventas	pc05	13/02/2017	Pedro Rivera	Hugo Ramirez	17/02/2017
38	Abierto	Media	No enciende	Ventas	pc03	16/02/2017	Andre Santiago	Hugo Ramirez	
39	Resuelto	Baja	Formateo	Operativa	pc03	03/02/2017	Ivan Trujillo	Aldo Torres	08/02/2017
40	Resuelto	Baja	Limpieza de virus	Marketing y Publicidad	USB	09/02/2017	Ivan Trujillo	Aldo Torres	09/02/2017

41	Resuelto	Media	Equipo mojado por lluvia	Marketing y Publicidad	pc02	24/01/2017	Cesar Augusto Pinedo	Aldo Torres	24/01/2017
42	Abierto	Baja	Reemplazo de esponja	Marketing y Publicidad	Impresora01	13/02/2017	Nestor Quispe	Patricia Ramirez	
43	Resuelto	Alta	Fatla Instalar Drivers	Marketing y Publicidad	pc04	21/01/2017	Yolanda del Poma	Aldo Torres	10/02/2017
44	Resuelto	Baja	Correcion de un registro por medio del sistema	Topografia	Sistema Tramite	12/02/2017	Jose Victor Carranza	Aldo Torres	12/02/2017
45	Resuelto	Baja	Conversion de Archivos	Contabilidad	pc03	18/01/2017	Patricia Ramirez	Patricia Ramirez	18/01/2017
46	Resuelto	Urgente	Falta Conectar	Marketing y Publicidad	Servidor Web	22/02/2017	Aldo Torres	Aldo Torres	22/02/2017
47	Resuelto	Media	Cambio de clave de usuario	Operativa	Sistema Tramite	16/02/2017	Dionisio Malpartida	Victor Ramirez	16/02/2017
48	Resuelto	Media	Agregar modulos al sistema	Operativa	Sistema de intranet	07/01/2017	Pedro Rivera	Victor Ramirez	21/02/2017
49	Resuelto	Media	Fatla Instalar Drivers	Contabilidad	pc03	09/02/2017	Andre Santiago	Hugo Ramirez	09/02/2017
50	Abierto	Baja	Placa malograda	Gerencia Administrativa	pc03	26/01/2017	Ivan Trujillo	Hugo Ramirez	
51	Resuelto	Baja	Limpieza de virus	Contabilidad	USB	19/02/2017	Ana Torrejon	Hugo Ramirez	19/02/2017
52	Resuelto	Media	Sin acceso al sistema	Ventas	pc01	08/01/2017	Cesar Augusto Pinedo	Hugo Ramirez	08/01/2017
53	Resuelto	Baja	Prestamo de Equipo Multimedia	Marketing y Publicidad	Proyector Negro	07/02/2017	Nestor Quispe	Hugo Ramirez	07/02/2017
54	Abierto	Media	Creacion de un sistema	Ventas	Sistema Tramite	01/02/2017	Yolanda del Poma	Aldo Torres	
55	Resuelto	Baja	Correcion de un registro por medio del sistema	Ventas	Sistema de intranet	07/02/2017	Jose Victor Carranza	Aldo Torres	07/02/2017

56	Resuelto	Baja	Correcion de un registro por medio del sistema	Operativa	Sistema de intranet	07/02/2017	Juan Carlos Mendieta	Aldo Torres	07/02/2017
57	Resuelto	Media	Fallo con la tarjeta de video	Marketing y Publicidad	pc04	16/01/2017	Jose Estrada	Patricia Ramirez	16/01/2017
58	Resuelto	Baja	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	25/01/2017	Flor Santamaria	Aldo Torres	25/01/2017
59	Resuelto	Baja	Limpieza de virus	Marketing y Publicidad	USB	24/01/2017	Alfredo Cajas	Aldo Torres	24/01/2017
60	Resuelto	Baja	actualizacion del antivirus	Marketing y Publicidad	pc02	10/02/2017	Andres Malpartida	Patricia Ramirez	10/02/2017
61	Resuelto	Urgente	Se desconecto la base de datos	Topografia	Servidor de Datos	14/02/2017	Leidy Suarez	Aldo Torres	14/02/2017
62	Resuelto	Baja	Formateo	Contabilidad	USB	04/02/2017	Andres Malpartida	Victor Ramirez	04/02/2017
63	Abierto	Media	Modificacion de modulos del sistema	Marketing y Publicidad	Sistema de intranet	25/02/2017	Estefanny Echaverria	Victor Ramirez	
64	Resuelto	Baja	Correcion de un registro por medio del sistema	Operativa	Sistema de intranet	17/02/2017	Dionisio Malpartida	Hugo Ramirez	17/02/2017
65	Resuelto	Media	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	08/01/2017	Patricia Ramirez	Hugo Ramirez	08/01/2017
66	Resuelto	Alta	Creacion de correo institucional	Contabilidad	Servidor de Correos	23/02/2017	Aldo Torres	Hugo Ramirez	23/02/2017
67	Resuelto	Media	Cambio de clave de usuario	Medio Ambiente y Seguridad	Sistema Tramite	08/02/2017	Dionisio Malpartida	Hugo Ramirez	08/02/2017
68	Resuelto	Urgente	Falta subir archivos	Contabilidad	Pagina Web	01/01/2017	Pedro Rivera	Hugo Ramirez	02/01/2017
69	Resuelto	Baja	Limpieza de virus	Ventas	USB	14/01/2017	Andre Santiago	Aldo Torres	14/01/2017
70	Resuelto	Baja	Prestamo de Equipo Multimedia	Ventas	Proyector Negro	17/02/2017	Ivan Trujillo	Aldo Torres	17/02/2017
71	Resuelto	Media	Creacion de usuarios en el sistema	Topografia	Sistema Pagos	21/01/2017	Ivan Trujillo	Aldo Torres	21/01/2017

72	Resuelto	Baja	Correcion de un registro por medio del sistema	Medio Ambiente y Seguridad	Sistema Tramite	22/01/2017	Cesar Augusto Pinedo	Patricia Ramirez	22/01/2017
73	Abierto	Media	Formateo	Gerencia General	pc05	14/01/2017	Nestor Quispe	Aldo Torres	14/01/2017
74	Resuelto	Media	Creacion de usuarios en el sistema	Gerencia Administrativa	Sistema Pagos	21/01/2017	Yolanda del Poma	Aldo Torres	21/01/2017
75	Resuelto	Baja	Fatla Instalar Drivers	Contabilidad	pc01	05/01/2017	Jose Victor Carranza	Patricia Ramirez	05/01/2017
76	Resuelto	Baja	Limpieza de virus	Marketing y Publicidad	USB	19/02/2017	Patricia Ramirez	Aldo Torres	19/02/2017
77	Resuelto	Media	Sin acceso al sistema	Ventas	pc01	08/01/2017	Aldo Torres	Patricia Ramirez	08/01/2017
78	Resuelto	Baja	Limpieza de virus	Operativa	USB	24/02/2017	Dionisio Malpartida	Pedro Rivera	24/02/2017
79	Abierto	Media	Modificacion de modulos del sistema	Medio Ambiente y Seguridad	Sistema de intranet	25/02/2017	Pedro Rivera	Pedro Rivera	
80	Resuelto	Baja	Correcion de un registro por medio del sistema	Topografia	Sistema de intranet	17/02/2017	Andre Santiago	Dionisio Malpartida	17/02/2017
81	Resuelto	Media	Correcion de un registro por medio del sistema	Medio Ambiente y Seguridad	Sistema Tramite	12/01/2017	Ivan Trujillo	Patricia Ramirez	12/01/2017
82	Abierto	Media	Formateo	Contabilidad	pc03	13/01/2017	Ana Torrejon	Victor Ramirez	13/01/2017
83	Resuelto	Media	Fatla Instalar Drivers	Marketing y Publicidad	pc02	19/01/2017	Cesar Augusto Pinedo	Arturo Santos	19/01/2017
84	Resuelto	Media	Cambio de clave de usuario	Operativa	Sistema Tramite	08/02/2017	Nestor Quispe	Patricia Ramirez	08/02/2017
85	Resuelto	Urgente	Falta subir archivos	Operativa	Pagina Web	01/01/2017	Yolanda del Poma	Aldo Torres	02/01/2017
86	Abierto	Baja	Falta Conectar	Contabilidad	Impresora02	26/01/2017	Jose Victor Carranza	Aldo Torres	26/01/2017

87	Abierto	Baja	Acceso a Internet	Gerencia Administrativa	pc03	21/02/2017	Juan Carlos Mendieta	Patricia Ramirez	
88	Resuelto	Alta	Equipo mojado por lluvia	Contabilidad	pc01	23/02/2017	Jose Estrada	Aldo Torres	23/02/2017
89	Resuelto	Baja	Cambio de clave de usuario	Ventas	Sistema Pagos	15/01/2017	Flor Santamaria	Patricia Ramirez	15/01/2017
90	Resuelto	Media	Fatla Instalar Drivers	Marketing y Publicidad	pc02	19/01/2017	Alfredo Cajas	Pedro Rivera	19/01/2017
91	Resuelto	Baja	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	09/01/2017	Andres Malpartida	Pedro Rivera	09/01/2017
92	Resuelto	Alta	Recepcion de Documentos Derivados al area	Ventas	pc01	28/02/2017	Leidy Suarez	Dionisio Malpartida	28/02/2017
93	Resuelto	Baja	Falta Conectar	Operativa	Impresora03	18/01/2017	Andres Malpartida	Patricia Ramirez	18/01/2017
94	Abierto	Media	Modificacion de modulos del sistema	Marketing y Publicidad	Sistema de intranet	25/02/2017	Estefanny Echaverria	Victor Ramirez	
95	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	03/01/2017	Dionisio Malpartida	Arturo Santos	03/01/2017
96	Resuelto	Alta	Creacion de correo institucional	Marketing y Publicidad	Servidor de Correos	23/02/2017	Patricia Ramirez	Patricia Ramirez	23/02/2017
97	Resuelto	Baja	Prestamo de Equipo Multimedia	Operativa	Proyector Negro	17/02/2017	Aldo Torres	Aldo Torres	17/02/2017
98	Resuelto	Baja	Prestamo de Equipo Multimedia	Operativa	Proyector Negro	17/02/2017	Dionisio Malpartida	Aldo Torres	17/02/2017
99	Resuelto	Alta	Prestamo de Equipo Multimedia	Contabilidad	Proyector Blanco	06/01/2017	Pedro Rivera	Patricia Ramirez	06/01/2017
100	Resuelto	Media	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema Tramite	19/01/2017	Andre Santiago	Aldo Torres	19/01/2017
101	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	17/02/2017	Ivan Trujillo	Patricia Ramirez	17/02/2017
102	Resuelto	Baja	Fatla Instalar Drivers	Ventas	pc01	21/02/2017	Ivan Trujillo	Pedro Rivera	21/02/2017

103	Resuelto	Baja	Fatla Instalar Drivers	Marketing y Publicidad	pc02	21/02/2017	Cesar Augusto Pinedo	Pedro Rivera	21/02/2017
104	Resuelto	Baja	Fatla Instalar Drivers	Ventas	pc03	21/02/2017	Nestor Quispe	Dionisio Malpartida	21/02/2017
105	Resuelto	Baja	Fatla Instalar Drivers	Contabilidad	pc04	21/02/2017	Yolanda del Poma	Patricia Ramirez	21/02/2017
106	Resuelto	Alta	Creacion de correo institucional	Marketing y Publicidad	Servidor de Correos	23/02/2017	Jose Victor Carranza	Victor Ramirez	23/02/2017
107	Resuelto	Baja	Falta Conectar	Operativa	Impresora03	18/01/2017	Patricia Ramirez	Arturo Santos	18/01/2017
108	Abierto	Media	Modificacion de modulos del sistema	Operativa	Sistema de intranet	25/02/2017	Aldo Torres	Patricia Ramirez	
109	Resuelto	Baja	Correcion de un registro por medio del sistema	Contabilidad	Sistema de intranet	17/02/2017	Dionisio Malpartida	Aldo Torres	17/02/2017
110	Resuelto	Baja	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema de intranet	23/02/2017	Pedro Rivera	Aldo Torres	23/02/2017
111	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	12/01/2017	Andre Santiago	Patricia Ramirez	12/01/2017
112	Resuelto	Alta	Recepcion de Documentos Derivados al area	Ventas	pc01	18/02/2017	Ivan Trujillo	Aldo Torres	18/02/2017
113	Resuelto	Urgente	Modificacion en la base de datos	Marketing y Publicidad	Sistema Pagos	13/01/2017	Ana Torrejon	Patricia Ramirez	13/01/2017
114	Resuelto	Baja	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	12/02/2017	Cesar Augusto Pinedo	Pedro Rivera	12/02/2017
115	Resuelto	Baja	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	12/02/2017	Nestor Quispe	Pedro Rivera	12/02/2017
116	Resuelto	Media	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	16/01/2017	Yolanda del Poma	Dionisio Malpartida	16/01/2017
117	Resuelto	Baja	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	25/01/2017	Jose Victor Carranza	Patricia Ramirez	25/01/2017

118	Resuelto	Baja	Limpieza de virus	Marketing y Publicidad	USB	04/02/2017	Juan Carlos Mendieta	Victor Ramirez	04/02/2017
119	Abierto	Baja	Acceso a Internet	Marketing y Publicidad	pc03	21/02/2017	Jose Estrada	Arturo Santos	
120	Resuelto	Alta	Equipo mojado por lluvia	Marketing y Publicidad	pc01	23/02/2017	Flor Santamaria	Patricia Ramirez	23/02/2017
121	Resuelto	Media	Falta subir archivos	Topografia	Pagina Web	18/01/2017	Alfredo Cajas	Aldo Torres	18/01/2017
122	Resuelto	Baja	Cambio de clave de usuario	Contabilidad	Sistema de intranet	25/01/2017	Andres Malpartida	Aldo Torres	25/01/2017
123	Resuelto	Urgente	Falta subir archivos	Marketing y Publicidad	Pagina Web	15/01/2017	Leidy Suarez	Patricia Ramirez	15/01/2017
124	Resuelto	Alta	Creacion de correo institucional	Contabilidad	Servidor de Correos	25/01/2017	Andres Malpartida	Aldo Torres	25/01/2017
125	Resuelto	Media	Creacion de usuarios en el sistema	Marketing y Publicidad	Sistema Pagos	21/01/2017	Estefanny Echaverria	Patricia Ramirez	21/01/2017
126	Resuelto	Media	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	16/01/2017	Dionisio Malpartida	Pedro Rivera	16/01/2017
127	Resuelto	Baja	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	25/01/2017	Patricia Ramirez	Pedro Rivera	25/01/2017
128	Resuelto	Baja	Limpieza de virus	Operativa	USB	24/01/2017	Aldo Torres	Aldo Torres	24/01/2017
129	Resuelto	Baja	actualizacion del antivirus	Operativa	pc02	10/02/2017	Dionisio Malpartida	Patricia Ramirez	10/02/2017
130	Resuelto	Urgente	Se desconecto la base de datos	Contabilidad	Servidor de Datos	14/02/2017	Pedro Rivera	Aldo Torres	14/02/2017
131	Resuelto	Media	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema Tramite	12/01/2017	Andre Santiago	Patricia Ramirez	12/01/2017
132	Resuelto	Urgente	Falta subir archivos	Contabilidad	Pagina Web	01/01/2017	Ivan Trujillo	Pedro Rivera	02/01/2017
133	Resuelto	Alta	Creacion de correo institucional	Ventas	Servidor de Correos	04/02/2017	Ivan Trujillo	Pedro Rivera	04/02/2017

134	Resuelto	Media	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	16/01/2017	Cesar Augusto Pinedo	Dionisio Malpartida	16/01/2017
135	Resuelto	Baja	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	25/01/2017	Nestor Quispe	Patricia Ramirez	25/01/2017
136	Resuelto	Baja	Limpieza de virus	Ventas	USB	17/02/2017	Yolanda del Poma	Victor Ramirez	17/02/2017
137	Abierto	Media	Necesita Formateo	Operativa	pc06	25/02/2017	Jose Victor Carranza	Arturo Santos	
138	Resuelto	Urgente	No reconoce la conexión	Marketing y Publicidad	Camaras Digitales	21/01/2017	Patricia Ramirez	Patricia Ramirez	21/01/2017
139	Resuelto	Baja	Ayuda en modificacion de un archivo	Contabilidad	pc01	21/10/2017	Aldo Torres	Aldo Torres	21/10/2017
140	Abierto	Media	Fuente Quemada	Marketing y Publicidad	pc02	15/02/2017	Dionisio Malpartida	Aldo Torres	
141	Resuelto	Baja	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	12/01/2017	Pedro Rivera	Patricia Ramirez	12/01/2017
142	Resuelto	Alta	Creacion de correo institucional	Operativa	Servidor de Correos	25/01/2017	Andre Santiago	Aldo Torres	25/01/2017
143	Resuelto	Media	Creacion de usuarios en el sistema	Contabilidad	Sistema Pagos	21/01/2017	Ivan Trujillo	Patricia Ramirez	21/01/2017
144	Resuelto	Media	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema Tramite	16/01/2017	Ana Torrejon	Aldo Torres	16/01/2017
145	Resuelto	Baja	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	25/01/2017	Cesar Augusto Pinedo	Patricia Ramirez	25/01/2017
146	Resuelto	Media	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	22/01/2017	Nestor Quispe	Aldo Torres	22/01/2017
147	Resuelto	Alta	Equipo mojado por lluvia	Marketing y Publicidad	pc01	23/02/2017	Yolanda del Poma	Patricia Ramirez	23/02/2017
148	Resuelto	Media	Falta subir archivos	Ventas	Pagina Web	18/01/2017	Jose Victor Carranza	Pedro Rivera	18/01/2017

149	Resuelto	Baja	Cambio de clave de usuario	Contabilidad	Sistema de intranet	25/01/2017	Juan Carlos Mendieta	Pedro Rivera	25/01/2017
150	Resuelto	Urgente	Falta subir archivos	Marketing y Publicidad	Pagina Web	15/01/2017	Jose Estrada	Dionisio Malpartida	15/01/2017
151	Resuelto	Baja	Limpieza de virus	Operativa	USB	11/01/2017	Flor Santamaria	Patricia Ramirez	11/01/2017
152	Resuelto	Media	Correcion de un registro por medio del sistema	Operativa	Sistema Tramite	12/01/2017	Alfredo Cajas	Victor Ramirez	12/01/2017
153	Resuelto	Urgente	Falta subir archivos	Contabilidad	Pagina Web	01/01/2017	Andres Malpartida	Arturo Santos	02/01/2017
154	Resuelto	Alta	Creacion de correo institucional	Gerencia Administrativa	Servidor de Correos	04/02/2017	Leidy Suarez	Patricia Ramirez	04/02/2017
155	Resuelto	Media	Creacion de usuarios en el sistema	Contabilidad	Sistema Pagos	21/01/2017	Andres Malpartida	Aldo Torres	21/01/2017
156	Resuelto	Media	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	12/01/2017	Estefanny Echaverria	Aldo Torres	12/01/2017
157	Resuelto	Media	Cambio de clave de usuario	Marketing y Publicidad	Sistema Tramite	17/02/2017	Dionisio Malpartida	Patricia Ramirez	17/02/2017
158	Abierto	Baja	Falta Mantenimiento	Ventas	pc02	16/01/2017	Patricia Ramirez	Aldo Torres	16/01/2017
159	Resuelto	Alta	Recepcion de Documentos Derivados al area	Ventas	pc01	16/02/2017	Aldo Torres	Patricia Ramirez	16/02/2017
160	Resuelto	Baja	Cambio de clave de usuario	Operativa	Sistema de intranet	25/01/2017	Dionisio Malpartida	Aldo Torres	25/01/2017
161	Resuelto	Baja	Prestamo de Equipo Multimedia	Marketing y Publicidad	Proyector Negro	05/02/2017	Pedro Rivera	Patricia Ramirez	05/02/2017
162	Resuelto	Baja	Prestamo de Equipo Multimedia	Marketing y Publicidad	Proyector Negro	05/02/2017	Andre Santiago	Aldo Torres	05/02/2017
163	Resuelto	Baja	Prestamo de Equipo Multimedia	Marketing y Publicidad	Proyector Negro	05/02/2017	Ivan Trujillo	Patricia Ramirez	05/02/2017
164	Resuelto	Media	Creacion de usuarios en el sistema	Marketing y Publicidad	Sistema Pagos	20/01/2017	Ivan Trujillo	Pedro Rivera	20/01/2017

165	Resuelto	Baja	Limpieza de virus	Topografia	USB	09/01/2017	Cesar Augusto Pinedo	Pedro Rivera	09/01/2017
166	Abierto	Baja	Falta Mantenimiento	Contabilidad	pc02	16/01/2017	Nestor Quispe	Dionisio Malpartida	16/01/2017
167	Resuelto	Alta	Recepcion de Documentos Derivados al area	Marketing y Publicidad	pc01	16/02/2017	Yolanda del Poma	Patricia Ramirez	16/02/2017
168	Abierto	Media	Formateo	Contabilidad	pc04	14/01/2017	Jose Victor Carranza	Victor Ramirez	14/01/2017
169	Resuelto	Baja	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	12/02/2017	Patricia Ramirez	Arturo Santos	12/02/2017
170	Resuelto	Media	Cambio de clave de usuario	Operativa	Sistema Tramite	17/02/2017	Aldo Torres	Patricia Ramirez	17/02/2017
171	Abierto	Baja	Falta Mantenimiento	Operativa	pc02	16/01/2017	Dionisio Malpartida	Aldo Torres	16/01/2017
172	Resuelto	Baja	Falta Conectar	Operativa	impresora01	06/01/2017	Pedro Rivera	Aldo Torres	06/01/2017
173	Resuelto	Baja	Correcion de un registro por medio del sistema	Operativa	Sistema de intranet	28/02/2017	Andre Santiago	Patricia Ramirez	28/02/2017
174	Resuelto	Baja	Correcion de un registro por medio del sistema	Contabilidad	Sistema de intranet	28/02/2017	Ivan Trujillo	Aldo Torres	28/02/2017
175	Resuelto	Baja	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema de intranet	28/02/2017	Ana Torrejon	Patricia Ramirez	28/02/2017
176	Resuelto	Baja	Limpieza de virus	Contabilidad	USB	16/02/2017	Cesar Augusto Pinedo	Patricia Ramirez	16/02/2017
177	Resuelto	Media	Cambio de clave de usuario	Ventas	Sistema Tramite	17/02/2017	Nestor Quispe	Aldo Torres	17/02/2017
178	Abierto	Baja	Falta Mantenimiento	Marketing y Publicidad	pc02	16/01/2017	Yolanda del Poma	Patricia Ramirez	16/01/2017
179	Resuelto	Alta	Recepcion de Documentos Derivados al area	Ventas	pc01	16/02/2017	Jose Victor Carranza	Pedro Rivera	16/02/2017

180	Resuelto	Media	Correcion de un registro por medio del sistema	Ventas	Sistema Tramite	25/02/2017	Juan Carlos Mendieta	Pedro Rivera	25/02/2017
181	Resuelto	Alta	Creacion de correo institucional	Operativa	Servidor de Correos	04/02/2017	Jose Estrada	Dionisio Malpartida	04/02/2017
182	Resuelto	Media	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	16/01/2017	Flor Santamaria	Patricia Ramirez	16/01/2017
183	Resuelto	Baja	Cambio de clave de usuario	Contabilidad	Sistema de intranet	05/01/2017	Alfredo Cajas	Victor Ramirez	05/01/2017
184	Resuelto	Media	Creacion de usuarios en el sistema	Marketing y Publicidad	Sistema Pagos	28/02/2017	Andres Malpartida	Arturo Santos	28/02/2017
185	Resuelto	Media	Cambio de clave de usuario	Operativa	Sistema Tramite	28/02/2017	Leidy Suarez	Patricia Ramirez	28/02/2017
186	Abierto	Baja	Falta Mantenimiento	Operativa	pc02	16/01/2017	Andres Malpartida	Aldo Torres	16/01/2017
187	Resuelto	Alta	Recepcion de Documentos Derivados al area	Contabilidad	pc01	16/02/2017	Estefanny Echaverria	Aldo Torres	16/02/2017
188	Resuelto	Media	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema Tramite	23/01/2017	Dionisio Malpartida	Patricia Ramirez	23/01/2017
189	Resuelto	Alta	Recepcion de Documentos Derivados al area	Contabilidad	pc01	25/02/2017	Patricia Ramirez	Aldo Torres	25/02/2017
190	Abierto	Media	Formateo	Ventas	PC5-Mesa de Partes	14/01/2017	Aldo Torres	Patricia Ramirez	14/01/2017
191	Resuelto	Baja	Cambio de clave de usuario	Marketing y Publicidad	Sistema de intranet	25/01/2017	Dionisio Malpartida	Pedro Rivera	25/01/2017
192	Resuelto	Media	Cambio de clave de usuario	Ventas	Sistema Tramite	28/02/2017	Pedro Rivera	Pedro Rivera	28/02/2017
193	Abierto	Baja	Falta Mantenimiento	Contabilidad	pc02	16/01/2017	Andre Santiago	Aldo Torres	16/01/2017
194	Resuelto	Baja	Correcion de un registro por medio del sistema	Marketing y Publicidad	Sistema Tramite	15/02/2017	Ivan Trujillo	Patricia Ramirez	15/02/2017
195	Resuelto	Alta	Recepcion de Documentos Derivados al area	Operativa	pc01	01/02/2017	Ivan Trujillo	Aldo Torres	01/02/2017

196	Resuelto	Alta	Creacion de correo institucional	Operativa	Servidor de Correos	04/02/2017	Cesar Augusto Pinedo	Patricia Ramirez	04/02/2017
197	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	16/01/2017	Nestor Quispe	Pedro Rivera	16/01/2017
198	Resuelto	Baja	Correcion de un registro por medio del sistema	Gerencia Administrativa	Sistema Tramite	18/01/2017	Yolanda del Poma	Pedro Rivera	18/01/2017
199	Resuelto	Media	Correcion de un registro por medio del sistema	Contabilidad	Sistema Tramite	29/01/2017	Jose Victor Carranza	Dionisio Malpartida	29/01/2017
200	Abierto	Baja	Falta Mantenimiento	Ventas	pc02	16/01/2017	Patricia Ramirez	Patricia Ramirez	16/01/2017
201	Resuelto	Alta	Recepcion de Documentos Derivados al area	Marketing y Publicidad	pc01	16/02/2017	Aldo Torres	Victor Ramirez	16/02/2017
202	Resuelto	Media	Cambio de clave de usuario	Ventas	Sistema Tramite	30/01/2017	Dionisio Malpartida	Arturo Santos	30/01/2017
203	Resuelto	Baja	Falta Conectar	Ventas	impresora01	21/02/2017	Pedro Rivera	Patricia Ramirez	21/02/2017
204	Abierto	Media	No carga	Operativa	Servidor de Datos	20/11/2017	Andre Santiago	Aldo Torres	21/11/2017

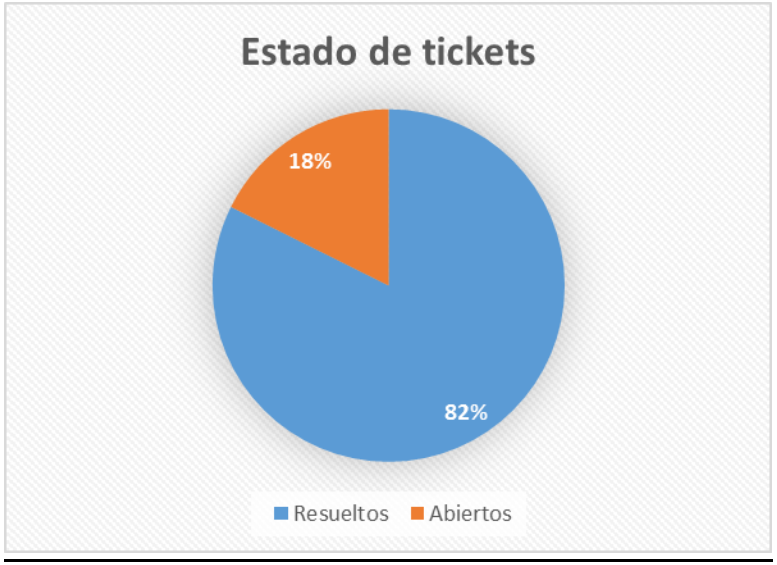
3.2 REPORTES ESTADISTICOS

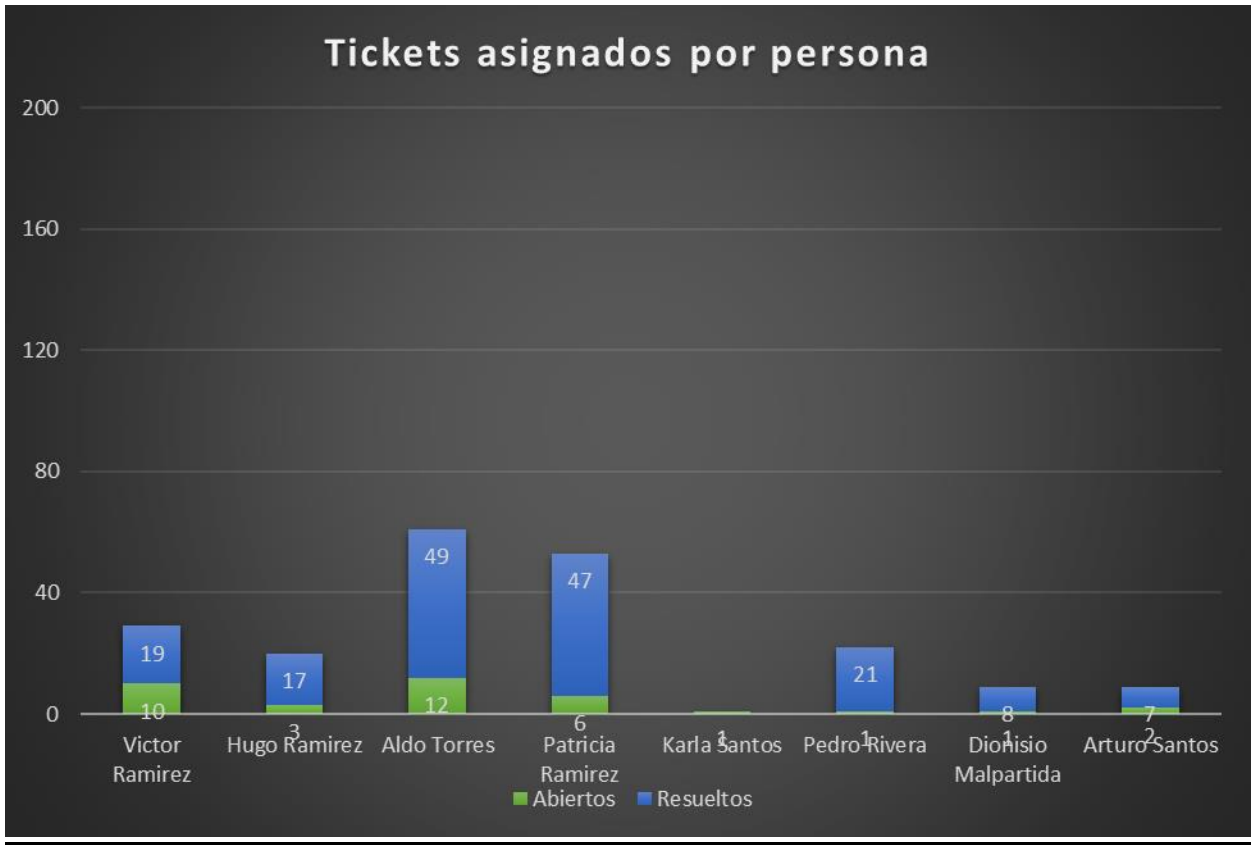
Link Registro	Ticket #	Prioridad	Descripción	Antigüedad (días)
Ubicar en registro	15	Alta	Agregar módulos al sistema	303
Ubicar en registro	21	Alta	Modificación de módulos del sistema	256
Ubicar en registro	82	Media	Formateo	301
Ubicar en registro	73	Media	Formateo	300
Ubicar en registro	168	Media	Formateo	300
Ubicar en registro	190	Media	Formateo	300
Ubicar en registro	30	Media	Fallo con la tarjeta de video	287
Ubicar en registro	54	Media	Creación de un sistema	282
Ubicar en registro	5	Media	Fuente Quemada	268
Ubicar en registro	140	Media	Fuente Quemada	268
Ubicar en registro	38	Media	No enciende	267
Ubicar en registro	2	Media	Necesita Formateo	258
Ubicar en registro	28	Media	Modificación de módulos del sistema	258
Ubicar en registro	63	Media	Modificación de módulos del sistema	258
Ubicar en registro	79	Media	Modificación de módulos del sistema	258
Ubicar en registro	94	Media	Modificación de módulos del sistema	258
Ubicar en registro	108	Media	Modificación de módulos del sistema	258
Ubicar en registro	137	Media	Necesita Formateo	258
Ubicar en registro	6	Media	Falta Mantenimiento	256
Ubicar en registro	23	Media	No enciende	255
Ubicar en registro	32	Baja	Falta Conectar	298
Ubicar en registro	158	Baja	Falta Mantenimiento	298
Ubicar en registro	166	Baja	Falta Mantenimiento	298
Ubicar en registro	171	Baja	Falta Mantenimiento	298
Ubicar en registro	178	Baja	Falta Mantenimiento	298
Ubicar en registro	186	Baja	Falta Mantenimiento	298
Ubicar en registro	193	Baja	Falta Mantenimiento	298
Ubicar en registro	200	Baja	Falta Mantenimiento	298
Ubicar en registro	50	Baja	Placa malograda	288
Ubicar en registro	86	Baja	Falta Conectar	288

Ubicar en registro	42	Baja	Reemplazo de esponja	270
Ubicar en registro	7	Baja	Acceso a Internet	265
Ubicar en registro	87	Baja	Acceso a Internet	262
Ubicar en registro	119	Baja	Acceso a Internet	262
Ubicar en registro	11	Baja	Fallo con la tarjeta de video	116

Tabla Resumen

Tickets	Urgente	Alta	Media	Baja
Abiertos	0	2	18	15
Resueltos	14	28	54	72
% Resueltos	100%	93%	75%	83%




Tickets asignados por persona
200
160
120
80
40
0
19
10
17
3
49
12
47
6
1
1
21
1
8
1
7
2
Victor Ramirez
Hugo Ramirez
Aldo Torres
Patricia Ramirez
Karla Santos
Pedro Rivera
Dionisio Malpartida
Arturo Santos
Abiertos
Resueltos


Tiempo promedio de resolución por severidad (días)
Baja
0,166666667
Media
1,5
Alta
0,892857143
Urgente
0,357142857
0
0,2
0,4
0,6
0,8
1
1,2
1,4
1,6

CAPITULO 4

ETAPA 4: PLAN DE MEJORA CONTINUA

4.1 PLANIFICACION DE LAS ETAPAS DE CAPACITACIONES EN SEGURIDAD DE LA INFORMACION

La EMPRESA GEOSURVEY como ente público capacitara a sus empleados trabajadores de manera preventiva para evitar algún daño físico y digital a sus activos como la información, edificación, entre otros.

Para lo cual se dará de la siguiente manera mensualmente:

- ✓ Capacitación del Personal laboral Sobre la Seguridad de manera física de los activos:
    - Se tomará los 2 días primeros laborales de cada 3 meses para la capacitación de los empleados a cargo del personal encargado.
    - Se les entregara un folleto rescatando puntos importantes de la seguridad física de los activos
    - Al final del segundo día se les encuestara a los empleados capacitados sobre la seguridad física de la información.
    - Luego el personal encargado de la capacitación pasara a revisar cada incidente que pudo haber durante los tres meses antes de la nueva capacitación.

- ✓ Capacitación del Personal Laboral sobre la Seguridad digital de los activos:
    - La capacitación de este punto se realizará a los 2 primeros días de la tercera semana de cada 2 meses a cargo de los empleados encargados de Sistemas de la EMPRESA.
    - Se brindará un folleto con la información de la seguridad de manera preventiva y correctiva a todos los empleados en capacitación.
    - Al final de cada capacitación se evaluará la comprensión a los capacitados de los temas tocados en dicho evento.

- Al final de la capacitación el personal encargado de esta responderá preguntas respecto a alguna duda.

4.2 ETAPAS PREVENTIVAS Y CORRECTIVAS SEGÚN EL DOMINIO DE LA SEGURIDAD

4.2.1 DOMINIO 7: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

En este punto recalcaremos las maneras seguras de la contratación del personal que laborara en la EMPRESA GEOSURVEY.

Preventivas:

- ✓ Al realizar un concurso público se debe establecer normas de ingreso de documentación, presentación de los documentos del público concursante de manera física como digital para evitar algún tipo de falsificación de datos de la persona entrante al concurso.
- ✓ La unidad de recursos humanos debe realizar una inspección de cada dato de los concursantes o ya empleados para evitar algún personal que sea contratado sin algún tipo de conocimiento de su labor o todo caso que no tenga antecedentes ni judiciales ni policiales.

Correctivas:

- ✓ El personal de recursos humanos debe evaluar el desempeño y los papeles que realiza el empleado, también velara por capacitar a los empleados municipales.
- ✓ En caso que algún empleado haya ocultado información vital de su persona la oficina de recursos humanos deberá suspender al personal infractor para que subsane esos inconvenientes; en caso de no dar esta subsanación se dará como retiro de la EMPRESA.

4.2.2 DOMINIO 8: GESTION DE ACTIVOS

En este punto se tendrá en cuenta la forma de etiquetación de los activos como su respectiva clasificación y su manejo de almacenamiento para cada uno de los tipos de activos que se tienen.

Preventiva:

- ✓ Se debe clasificar como etiquetar cada activo perteneciente a la EMPRESA como el fin de poder uno saber cada tipo de activo que se tiene para prevenir cualquier perdida o perjudicarían de estos activos.

- ✓ Realizar un listado de activos físicos como digitales para evitar alguna perdida, lo cual con este listado permitirá su seguimiento y su cuidado de este mismo activo.
    - La realización de inspecciones de activos de cada fin de mes para el control mismo de estos.

Correctiva:

- ✓ En caso de algún activo no fuese categorizado o etiquetado, este debe darse un informe y luego ser etiquetado para su cuidado.
- ✓ En caso que un activo este dañado o tenga alguna perdida este debe ser automáticamente presentado mediante un informe y registrado en el cuaderno de control de incidencias para su pronta observacion y su solución para evitar alguna perdida perjudicial a la entidad.

4.2.3 DOMINIO 9: CONTROL DE ACCESO

En este punto del dominio nos basaremos al control de acceso a los sistemas de información de la misma entidad, para evitar algún tipo de incidencia.

Preventiva:

- ✓ Uno cada persona que tendría acceso a los sistemas como a los activos debe registrarse con sus datos completos en los sistemas para evitar algún tipo de infiltración de persona ajena o no autorizada.
- ✓ Cada personal se le brindara un listado de códigos de acceso únicos para su propio acceso y no transferibles.
- ✓ Se educará al personal para el uso de sus accesos y su normativa que están tienen como:
    - Los códigos entregados son personales e intransferibles.
    - Cada tipo de código tiene su propio nivel de acceso y sus limitaciones.

Correctivas:

- ✓ En caso que algún personal municipal permita el uso de sus códigos a personas ajenas o no autorizadas este se le impondrá una sanción por dicho acto y esto es continuo entonces se le evaluara su acceso al sistema o se le restringirá el acceso que tiene.
- ✓ En caso de perder el personal se le brindara unos nuevos códigos, pero esto si esto negligencia de pérdida o accidental.

4.2.4 DOMINIO 10: CIFRADO DE INFORMACION

En este dominio se prioriza el ingreso de cifrado o contraseñas para los documentos importantes, lo cual solo personas autorizadas podrán leerlo, editarlo o eliminarlo.

Para lo cual este dominio tiene relación con el dominio 9 que es con respecto al control de acceso a los activos, por lo que presentamos la mejora preventiva y correctiva.

Preventivo:

- ✓ Cada activo digital al ser ingresado al sistema informático debe contener una contraseña para evitar alguna forma de daño o perjudicial al activo.
- ✓ Cada documento tendrá un nivel de acceso permitido por lo cual, esto evitará que personas sin el permiso de nivel pueda leerlo. Editarlo, o eliminarlo.
- ✓ Cada cifrado debe ser concerniente al documento para poder el ingreso más fácil a su personal autorizado.

Correctiva:

- ✓ En caso de ser editado o eliminado el sistema informático informara al personal encargado de sistemas para la verificación de la eliminación, brindando el usuario y contraseña del ultimo usuario que toco dicho archivo.
- ✓ En caso que el archivo tenga alguna vulnerabilidad de acceso este será informado al personal de sistemas para su verificación y su encriptación inmediata de acuerdo a su nivel de autorización del documento o activo digital.

4.2.5 DOMINIO 11: SEGURIDAD FISICA Y AMBIENTAL

En todo este dominio nos centraremos en la seguridad de oficinas, inmueble y así como cada componente tecnológico.

Preventivas:

- ✓ La instalación de cámaras de seguridad en todo el perímetro de la EMPRESA GEOSURVEY, dando así al área de vigilancia estaría al pendiente al perímetro y a las personas que ingresan a la entidad.
- ✓ Se pondrá anuncios de seguridad donde solo puedan ingresar el personal autorizado.
- ✓ Se realizará las instalaciones correctamente de los equipos tecnológicos como equipos de escritorio para que el lugar de trabajo sea una área segura y protegida.
- ✓ Cada componente tecnológico debe ser instalado por un personal capacitado y con medios de seguridad.

- ✓ Se debe poner señalización de las áreas de seguras en caso de cualquier incidente de desastre natural y/o provocado, para lo cual al personal se le debe capacitar en defensa civil para así evitar alguna perdida humana.

Correctiva:

- ✓ En caso de tener ya realizadas las conexiones tecnológicas se recomienda inspeccionarlas y ver el estado, funcionamiento, y prever algún daño a este tipo de tecnologías.
- ✓ El revisa miento de las cámaras de seguridad se ya estén instaladas deben ser monitoreadas con la finalidad de ver su funcionamiento, en caso que este esté dañado o no esté funcionando bien se debe realizar un reporte a las áreas de sistemas, para su evaluación y solución al problema.
- ✓ Cada instalación antigua debe modificarse a una actual o dar mantenimiento a estas instalaciones para verla la seguridad y dar mejor funcionamiento a estas conexiones ya realizadas.

4.2.6 DOMINIO 12: SEGURIDAD OPERATIVA

Buscamos mejorar la seguridad de procesos, haciendo que estos cumplan cada paso y lleguen a su finalidad con seguridad que este no haya sido dañado, ni perjudicado en su contenido, para lo cual mostraremos una manera preventiva y correctiva a este tipo de seguridad de activo.

Preventiva:

- ✓ ayuda

Correctiva:

- ✓ ayuda

4.2.7 DOMINIO 13: SEGURIDAD DE TELECOMUNICACIONES

En este dominio daremos pautas de cómo prevenir y corregir algún daño en las redes de telecomunicaciones.

Preventivas:

- ✓ Realizar las conexiones de manera segura y poniéndoles una capa de seguridad física como por ejemplo canaletas, gabinetes para los servidores o switch, entre otrosl
- ✓ Cada conexión de switch debe estar correctamente etiquetado para facilitar en caso de algún problema, la detección de esta.

- ✓ El área de servidores debe estar adecuadamente a una temperatura permitida para el buen funcionamiento de estos mismos.
- ✓ La persona a cargo de los servidores y conexiones deben estar capacitados a menudamente sobre el mantenimiento e instalación de cableado de telecomunicación.

Correctiva:

- ✓ Cada instalación antigua debe ser retirada y realizarse una nueva instalación para que el sistema siga manteniendo un buen funcionamiento.
- ✓ Cada conexión se debe revisar periódicamente para evitar algún fallo en la telecomunicación.

4.2.8 DOMINIO 14: ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION

Preventiva:

- ✓ Verificar la compatibilidad de los software o programas con los Sistemas Operativos antes de cambiarlos.
- ✓ Incluir mejoras de seguridad en los software desarrollados.
- ✓ Fijar un único lenguaje o sistema gestor de base de datos para que no haya problemas para unir la información.
- ✓ Crear back up constantes de los archivos.

Correctiva:

- ✓ Pasar todos los sistemas a un solo lenguaje de código.
- ✓ Buscar la forma de unificar los sistemas.

4.2.9 DOMINIO 18: CUMPLIMIENTO

Preventiva:

- ✓ Realizar capacitaciones a los empleados sobre seguridad de la información.
- ✓ Fomentar su uso adecuado entre todos los empleados.
- ✓ Hacer conocer las normas y reglas de seguridad y que estas sean respetadas.

Correctiva:

- ✓ Sancionar a algún empleado que cometa actos que atenten contra la seguridad de la información.