



TIPO DE MAPA DE RIESGOS		Institucional				
NOMBRE		Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes				
IDENTIFICACIÓN DEL RIESGO						
Item	ESTADO	FUENTE DE IDENTIFICACIÓN	DESCRIPCIÓN	RIESGO	CAUSA	CONSECUENCIAS
1	Nuevo	Identificación Riesgos de Seguridad Digital	Activo de información Base de Datos de nómina, cartera, contribuyentes, contrato, financiera, almacén, inventario de bienes inmuebles, con criticidad alta	Pérdida de confiabilidad, integridad y/o disponibilidad de la Base de datos de nómina, cartera, contribuyentes, contrato, financiera, almacén, inventario de bienes inmuebles, con criticidad alta	<ul style="list-style-type: none"> * Fallos del equipo * Mal funcionamiento del equipo * Saturación del sistema de información * Mal funcionamiento del software * Incumplimiento en el mantenimiento del sistema de información * Uso no autorizado del equipo * Copia fraudulenta del software * Error en el uso o abuso de derechos * Falsificación de derechos 	<ul style="list-style-type: none"> * Pérdidas económicas * Sanciones * Demandas * Pérdida de información * Interrupción del servicio * Sobrecostos * Mala calidad del servicio * Pérdida de bienes * Pérdida de información
2	Nuevo	Identificación Riesgos de Seguridad Digital	Sistema de Información SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA (SIIIF WEB)	Pérdida, falla parcial o total del sistema de información SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA (SIIIF WEB)	<ul style="list-style-type: none"> * Error en el uso o abuso de derechos * Falsificación de derechos * Mantenimiento insuficiente * Ausencia o insuficiencia de pruebas de software * Ausencia de terminación de sesión * Ausencia de registros de auditoría * Asignación errada de los derechos de acceso * Interfaz de usuario compleja * Ausencia de documentación * Fechas incorrectas * Ausencia de mecanismos de identificación y autenticación de usuarios * Contraseñas sin protección * Software nuevo o inmaduro 	<ul style="list-style-type: none"> * Pérdida de información * Interrupción del servicio * Sobrecostos * Mala calidad del servicio * Pérdida de bienes * Pérdidas económicas

 **COPIA CONTROLADA**
Alcaldía Municipal De Palmira



Alcaldía Municipal
de Palmita
Nit.: 891.380.037-3

SECRETARÍA GENERAL
PROCESO ADMINISTRATIVO DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 1 - Identificación de Riesgos

TIPO DE MAPA DE RIESGOS		Institucional	
NOMBRE		Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes	
IDENTIFICACION DEL RIESGO			
3	Actualizado	Identificación Riesgos de Seguridad Digital	Disponibilidad para lograr mantener actualizada la infraestructura tecnológica de la Alcaldía de Palmita
		Pérdida o fallas graves en los recursos de Telecomunicaciones (Hardware y Software)	<p>de</p> <p>Software nuevo o timorado</p> <p>Tráfico sensible sin protección</p> <p>Ausencia de mecanismos de monitoreo para brechas en la seguridad</p> <p>Ausencia de pruebas de envío o recepción de mensajes</p> <p>Lineas de comunicación sin protección</p> <p>Conexión deficiente de cableado</p> <p>Tráfico sensible sin protección</p> <p>Punto Único de falla</p> <p>Fuego</p> <p>Eventos naturales</p> <p>Fenómenos climáticos</p> <p>Fenómenos sísmicos</p> <p>Pérdidas de los servicios esenciales</p> <p>Fallas en el suministro de aire acondicionado</p> <p>Compromiso de la información</p> <p>Interceptación de servicios de señales de interferencia comprometida</p> <p>Espionaje remoto</p> <p>Fallas técnicas</p> <p>Fallas del equipo</p> <p>Mal funcionamiento del equipo</p> <p>Saturación del sistema de información</p> <p>Mal funcionamiento del software</p> <p>Incumplimiento en el mantenimiento del sistema de información</p> <p>Acciones no autorizadas</p> <p>Uso no autorizado del equipo</p> <p>Copia fraudulenta del software</p> <p>Compromiso de las funciones</p> <p>Error en el uso o abuso de derechos</p> <p>Falsificación de derechos</p>
			<ul style="list-style-type: none"> * Pérdida de información * Interrupción del servicio * Sobrecostos * Mala calidad del servicio * Pérdida de bienes * Pérdidas económicas

COPIA CONTROLADA
Alcaldía Municipal De Palmita

Centro Administrativo Municipal de Palmita
Calle 30 No. 29 - 39' Código Postal 763533
www.palmita.gov.co
Teléfono: 2709505



TIPO DE MAPA DE RIESGOS		Institucional
NOMBRE		Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes
IDENTIFICACIÓN DEL RIESGO		
4	Actualizado	<p>Identificación Riesgos de Seguridad Digital</p> <p>Todo tipo de información relevante y perteneciente a la Alcaldía de Palmira que pueda ser afectada por ataques cibernéticos, virus, fraude o violación de la seguridad-contratos físicos y digitales - infraestructura tecnológica</p> <p>Afectación de la información institucional por causa de virus informático, fraude, ataques informáticos, violación de la seguridad de la información</p> <p> <ul style="list-style-type: none"> Manipulamiento de un software Intercepción de servicios de señales de interferencia comprometida Espionaje remoto Fallas técnicas Fallas del equipo Mal funcionamiento del equipo Acciones no autorizadas Uso no autorizado del equipo Copia fraudulenta del software Compromiso de las funciones Error en el uso o abuso de derechos Falsificación de derechos Plataforma Destrucción de la información Divulgación ilegal de la información Chantaje Destrucción Ventaja competitiva Espionaje electrónico Curiosidad Ganancia monetaria Almacenamiento sin protección Falta de cuidado en la disposición final Copia no controlada Mantenimiento insuficiente Ausencia de esquemas de reemplazo periódico Almacenamiento sin protección Falta de cuidado en la disposición final Copia no controlada Ausencia o insuficiencia de pruebas de software Ausencia de terminación de sesión </p> <p> <ul style="list-style-type: none"> * Fallos generales del sistema y de la red. * Inestabilidad y mal funcionamiento de sistemas. * Pérdida de información. * Interrupción de la prestación del servicio * Pérdidas económicas * Sanciones legales * Alteración de la información * Pérdida de credibilidad y confianza </p>

COPIA CONTROLADA
Alcaldía Municipal De Palmira



Alcaldía Municipal
de Palmira
NIT: 891.380.007-3

TIPO DE MAPA DE RIESGOS		Institucional
NOMBRE		Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes
IDENTIFICACIÓN DEL RIESGO		
5	Actualizado	Identificación Riesgos de Seguridad Digital
		<p>Todo tipo de software que se instale en los equipos de cómputo de la Alcaldía de Palmira</p> <p>Pérdida de la integridad y disponibilidad al contar con software no licenciado</p> <p>Uso no autorizado del equipo</p> <p>Ausencia de mecanismos de autenticación de usuarios</p> <p>Contraseñas sin protección</p> <p>Software nuevo o inmaduro</p> <p>Copia fraudulenta del software</p> <p>Compromiso de las funciones</p> <p>Error en el uso o abuso de derechos</p> <p>Falsificación de derechos</p> <p>Prácticas</p> <p>Sañalientos penales al representante legal</p> <p>* Riesgo de filtración (puede sufrir la intrusión de virus que afectan a toda la red, quedar expuesto al robo de información y al ataque de hackers).</p> <p>* Riesgo de imposibilidad de Acceso (Bloqueo de uno o más programas).</p> <p>* Riesgo de manipulación (Ataques de hackers).</p> <p>* Pérdida de información</p>

mp

COPIA CONTROLADA
Alcaldía Municipal De Palmira



Alcaldía Municipal
de Palmira
Nit: 891.380.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 1 - Identificación de Riesgos

AlfMR-002
Versión: 01
10/09/2019
Página 5 de 6

TIPO DE MAPA DE RIESGOS		Institucional	
NOMBRE Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes			
IDENTIFICACIÓN DEL RIESGO			
6	Actualizado	Identificación Riesgos de Seguridad Digital	<p>Cualquier falla o dificultad que impida la normal continuidad en la prestación del servicio a la ciudadanía en general.</p> <p>Deficiencia en la integridad y disponibilidad en cuanto a la continuidad del servicio</p>
		<p>Interceptación de servicios de señales de interferencia comprometida</p> <p>Espionaje remoto</p> <p>Fallas técnicas</p> <p>Fallas del equipo</p> <p>Mal funcionamiento del equipo</p> <p>Acciones no autorizadas</p> <p>Uso no autorizado del equipo</p> <p>Piratería</p> <p>Divulgación ilegal de la información</p> <p>Espionaje económico</p> <p>Amenazamiento sin protección</p> <p>Mantenimiento insuficiente</p> <p>Ausencia de esquemas de reemplazo periódico</p> <p>Amenazamiento sin protección</p> <p>Interfaz de usuario compleja</p> <p>Ausencia de mecanismos de identificación y autenticación de usuarios</p> <p>Contraseñas sin protección</p> <p>Software nuevo o inmaduro</p> <p>Lineas de comunicación sin protección</p> <p>Conexión deficiente de cableado</p> <p>Tráfico sensible sin protección</p> <p>Punto único de falla</p> <p>Entrenamiento insuficiente</p> <p>Ausencia de proceso para supervisión de derechos de acceso</p> <p>Ausencia de mecanismos de monitoreo para brechas en la seguridad</p> <p>Ausencia de procedimientos y/o de políticas en general</p> <p>(esto aplica para muchas actividades que la entidad no</p>	<p>* Demora en la atención al usuario</p> <p>* Sobrecostos</p> <p>* Pérdidas económicas</p> <p>* Pérdida de información</p> <p>* Pérdida de Credibilidad por parte de los usuarios.</p> <p>* Mala Imagen Institucional</p> <p>* Inestabilidad y mal funcionamiento de sistemas.</p> <p>* Interrupción de la prestación del servicio</p> <p>* Sanciones legales</p> <p>* Alteración de la información</p>



Centro Administrativo Municipal de Palmira
Calle 30 No. 29 -39. Código Postal 763533
www.palmira.gov.co
Teléfono: 2709505



Alcaldía Municipal
de Palmira
Nit.: 891.380.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 1 - Identificación de Riesgos

TIPO DE MAPA DE RIESGOS		Institucional	
NOMBRE		Mapa - Plan de Tratamiento de Riesgos de Seguridad Digital - Incidentes	
IDENTIFICACIÓN DEL RIESGO			
7	Nuevo Identificación Riesgos de Seguridad Digital	Todo tipo de aplicación y/o plataformas institucionales de orden nacional como: SIGEP, FURAG, SISBEN, COLOMBIA, COMPRÁ EFICIENTE, SECOP, SIMAT, SIVIGILA, SUI, etc.	Falta de disponibilidad en los aplicativos y/o plataformas institucionales de orden nacional
8			

- Manipuleo de datos
Intercapción de servicios de señales de interferencia comprometida
Espionaje remoto
Fallas técnicas
Fallas del equipo
Mal funcionamiento del equipo
Acciones no autorizadas
Uso no autorizado del equipo
Piratería
Divulgación ilegal de la información
Espionaje económico
Almacenamiento sin protección
Mantenimiento insuficiente
Ausencia de esquemas de reemplazo periódico
Almacenamiento sin protección
Interfaz de usuario compleja
Ausencia de mecanismos de identificación y autenticación de usuarios
Contraseñas sin protección
Software nuevo o innaduro
Líneas de comunicación sin protección
Conexión deficiente de cableado
Tráfico sensible sin protección
Punto único de falla
Entrenamiento insuficiente
Ausencia de proceso para supervisión de derechos de acceso
Ausencia de mecanismos de monitoreo para brechas en la seguridad
Ausencia de procedimientos y/o de políticas en general
(esto aplica para muchas actividades que la entidad no realiza)
- * Demora en la atención al usuario
 - * Sobrecostos
 - * Pérdidas económicas
 - * Pérdida de información
 - * Pérdida de Credibilidad por parte de los usuarios.
 - * Mala Imagen Institucional
 - * Inestabilidad y mal funcionamiento de sistemas.
 - * Interrupción de la prestación del servicio
 - * Sanciones legales
 - * Alteración de la información

COPIA CONTROLADA
Alcaldía Municipal De Palmira

Centro Administrativo Municipal de Palmira
Calle 30 No. 29 -39: Código Postal 763533
www.palmira.gov.co
Teléfono: 2709505



Alcaldía Municipal
de Palmita
NIT: 891.390.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 2 - Análisis de Riesgos

AIFMR-002
Versión: 01
10/09/2019
Página 1 de 1

Item	RIESGO	CLASE DE RIESGO	CALIFICACION DEL RIESGO INHERENTE										EVALUACION						
			PROBABILIDAD	RIESGO INHERENTE										Valor	Resultado				
Valor	Resultado	Financiero	SST	Nacional	Legal	Imagen	Patrimonio	Comunidad del Municipio	Estadístico	Comercio	Seguridad Digital	Valor	Resultado	Valor	Resultado				
1	Perdida de confidencialidad, integridad y/o disponibilidad de la Base de datos de nómina	Seguridad Digital	1	Raro												4	Moderado		
2	Perdida, falla parcial o total del sistema de información SISTEMA INTEGRADO DE	Seguridad Digital	1	Raro	5											5	Moderado		
3	Perdida o fallas graves en los recursos de Telecomunicaciones (Hardware y Software)	Seguridad Digital	1	Raro	1											4	Moderado		
4	Afectación de la información institucional por causa de virus informático, fraude, ataques	Seguridad Digital	2	Improbable	1											10	Alto		
5	Perdida de la integridad y disponibilidad al contar con software no licenciado	Seguridad Digital	2	Improbable	1											8	Alto		
6	Deficiencia en la integridad y disponibilidad en cuanto a la continuidad del servicio	Seguridad Digital	1	Raro	1			1	2	2	3	3	3	2	5	5	Moderado		
7	Falta de disponibilidad en los aplicativos y/o plataformas institucionales de orden nacional	Seguridad Digital	1	Raro							1	1	1	1	2	2	Menor	2	Bajo
8																			
9																			
10																			
11																			
12																			

COPIA CONTROLADA
Alcaldía Municipal De Palmita



Item	RIESGO	CLASE DE RIESGO	CONTROLES EXISTENTES	VALORACIÓN DE CONTROLES					CALIFICACIÓN DEL RIESGO RESIDUAL				EVALUACIÓN		MEDIDAS DE RESPUESTA (Seleccionar la opción de respuesta)	Actividades	Responsables	Fecha Inicial (Identificada)	Fecha Final (Identificada)	Iniciado		
				Tipo Control	Estado de Implementación	Eficacia del Control	Evidencia del Control	Estimación para reducir riesgo	PUNTAJE FINAL	%	PROBABILIDAD Resultado	IMPACTO Resultado	%	RIESGO RESIDUAL Resultado								
1	Pérdida de confidencialidad, integridad y disponibilidad de la Base de datos de normas, contratos, cotizaciones, inventario de bienes inmuebles, con afectación del	Seguridad Digital	A.12-Regulación de Información A.12-Control de acceso de usuarios	Preventivo	3	3	3	3	3	3,00	1	Bajo	4	Medio	4	Medio	No requiere Plan de Acción					
2	Pérdida total parcial o total del sistema de Información SISTEMA INTEGRADO FINANCIERA (SER WEB)	Seguridad Digital	A.12.1- Gestión de los recursos A.14- Regulación de seguridad de los sistemas de información A.14.2- Seguridad en los procesos de desarrollo y soporte A.16.1- Seguridad de la información en las relaciones con los proveedores.	Preventivo	3	3	3	3	3	3,00	1	Bajo	6	Medio	5	Medio	No requiere Plan de Acción					
3	Pérdida o falta grave en los recursos de Telecomunicaciones (Fiber óptica y Satélite)	Seguridad Digital	A.6.12- Políticas sobre el uso de servicios en red A.11- Aseg. seguros A.11.2- Equipos. A.11.2- Mantenimiento de equipos	Preventivo	3	3	3	2	3	2,00	1	Bajo	4	Medio	4	Medio	No requiere Plan de Acción					
4	Afectación de la información individual por causa de virus informáticos, Weblogs de la seguridad de la información	Seguridad Digital	A.5- Políticas de seguridad de la información A.5.1- Operación estándares por la dirección para la seguridad de la información A.5.1.1- Políticas para la seguridad de la información A.5.1.2- Revision a las políticas para la seguridad de la información	Preventivo/ Correctivo	3	3	3	3	3	3,00	1	Bajo	4	Medio	4	Medio	Rolover		Lider de Proceso de Gestión de Identificación	2019/01/01	2019/12/31	Taller Humano
6	Pérdida de la integridad y disponibilidad de datos con afectación de la información	Seguridad Digital	A.5- Políticas de seguridad de la información A.5.1- Operación estándares por la dirección para la seguridad de la información A.5.1.1- Políticas para la seguridad de la información A.5.1.2- Revision a las políticas para la seguridad de la información A.5.2-Gestión de datos de usuarios	Correctivo	3	3	3	3	3	3,00	2	Medio	3	Medio	4	Medio	No requiere Plan de Acción		Lider de Proceso de Gestión de Identificación	2019/01/01	2019/12/31	Taller Humano

COPIA CONTROLADA
Alcaldía Municipal De Palmita



6	Deficiencia en la seguridad y disponibilidad en cuanto a la continuidad del servicio	Seguridad Digital	A.3 - Políticas de seguridad de la información A.3.1 - Directrices establecidas por la dirección para la seguridad de la información A.3.1.1 - Políticas para la seguridad de la información A.3.1.2 - Revisión de las políticas para la seguridad de la información A.3.2-Cambios de acceso de usuarios	Preventivo	3	3	3	3	3	300	1	Raro	6	Categorías	5	Mediando	No requiere Plan de Acción	En la vigencia 2016 se está realizando la revisión de la página web institucional. Revisión de los textos, contenidos, imágenes y diseño.	Lider de Proceso de Gestión de Información	20/07/2016	31/12/2016	Yanet Humano
7	Falta de disponibilidad en las aplicaciones y/o plataformas tecnológicas de interacción	Seguridad Digital	A.3 - Políticas de seguridad de la información A.3.4 - Control de acceso a sistemas y aplicaciones A.3.1.121 - Equipos A.3.2 - Transferencia de información	Preventivo	3	3	3	3	3	200	1	Raro	2	Mayor	2	Epi	No requiere Plan de Acción					

COPIA CONTROLADA
Alcaldía Municipal De Palmira



Item	RIESGO	CLASE DE RIESGO	Calificación		RIESGO INHERENTE	CONTROLES EXISTENTES	Calificación		RIESGO RESIDUAL	MEDIDAS DE RESPUESTA	PLAN DE ACCIÓN				
			Probabilidad	Impacto			Probabilidad	Impacto			Actividades	Responsable	Fecha Inicial (dd-mm-aaaa)	Fecha Final (dd-mm-aaaa)	Recursos
5	Pérdida de la integridad y disponibilidad al contar con software no licenciado	Seguridad Digital	2	4	Alto	A.5 - Políticas de seguridad de la información A.5.1 - Directrices establecidas por la dirección para la seguridad de la información A.5.1.1 - Políticas para la seguridad de la información A.5.1.2 - Revisión de esas políticas para la seguridad de la información A.9.2-Gestión de acceso de usuarios	2	3	Moderado	No requiere Plan de Acción	Implementación de las políticas de seguridad informática para fomentar la cultura del manejo adecuado en temas como: requisitos para compra de hardware y software, programas informáticos no autorizados, etc. A través de la socialización permanente de circulares normativas.	Lider de Proceso de Gestión de Informática	20/5/2019	31/12/2019	Talento Humano
6	Deficiencia en la integridad y disponibilidad en cuanto a la confiabilidad del servicio	Seguridad Digital	1	5	Moderado	A.5.1.1 - Políticas para la seguridad de la información A.5.1.2 - Revisión de esas políticas para la seguridad de la información A.9.2-Gestión de acceso de usuarios	1	5	Moderado	No requiere Plan de Acción	En la vigencia 2019 se está realizando la actualización de la página web institucional (Registro de dominio, web hosting, Gestión de informática contenidos, mantenimiento y difusión).	Lider de Proceso de Gestión de Informática	20/5/2019	31/12/2019	Talento Humano

COPIA CONTROLADA
Alcaldía Municipal De Palmira



Alcaldía Municipal
de Palmita
N°. 891.380.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No 4- Mapa de Riesgos

Item	RIESGO	CLASE DE RIESGO	Calificación		RIESGO INHERENTE	CONTROLES EXISTENTES	Calificación		RIESGO RESIDUAL	MEDIDAS DE RESPUESTA	PLAN DE ACCIÓN				
			Probabilidad	Impacto			Probabilidad	Impacto			Actividades	Responsable	Fecha Inicial (dd-mm-aaaa)	Fecha Final (dd-mm-aaaa)	Recursos
1	Perdida de confidencialidad, integridad y/o disponibilidad de la Base de datos de nómina, cartera, contribuyentes, contratación, financieros, emisión, inventario de bienes inmuebles, con criticidad alta	Seguridad Digital	1	4	Moderado	A.12.3-Respaldo de información A.9.2-Gestión de acceso de usuarios	1	4	Moderado	No requiere Plan de Acción					
2	Pérdida, falla parcial o total del sistema de información SISTEMA INTEGRADO DE INFORMACION FINANCIERA (SIF WEB)	Seguridad Digital	1	5	Moderado	A.12.6.1- Gestión de las vulnerabilidades A.14.1 - Requisitos de seguridad de los sistemas de información A.14.2 - Seguridad en los procesos de desarrollo y soporte A.15.1 - Seguridad de la información en las relaciones con los proveedores.	1	5	Moderado	No requiere Plan de Acción					
3	Pérdida o fallos graves en los recursos de Telecomunicaciones (Hardware y Software)	Seguridad Digital	1	4	Moderado	A.9.1.2 - política sobre el uso de servicios de red A.11.1 - Areas seguras A.11.2 - Equipos - A.11.2.4 - Mantenimiento de equipos	1	4	Moderado	No requiere Plan de Acción					
4	Afectación de la información institucional por causa de virus informáticos, fraude, ataques informáticos, violación de la seguridad de la información	Seguridad Digital	2	5	Alto	A.5 - Políticas de seguridad de la información A.5.1 - Directrices establecidas por la dirección para la seguridad de la información A.5.1.1 - Políticas para la seguridad de la información A.5.1.2 - Revisión de las políticas para la seguridad de la información	1	4	Moderado	Reducir	Creación de la cultura para el correcto manejo de correos electrónicos a través de la socialización permanente por medio de circulares normativas de las responsabilidades de los funcionarios plasmadas en el Manual de Políticas de seguridad informática. Monitoreo permanente al directorio activo del antivirus McAfee, instalado en todos los equipos de la Alcaldía de Palmita.	Lider de Proceso de Gestión de Informática	20/5/2019	31/12/2019	Talento Humano





SECRETARÍA GENERAL
PROCESO ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 4- Mapa de Riesgos

Item	RIESGO	CLASE DE RIESGO	Calificación		RIESGO INHERENTE	CONTROLES EXISTENTES	Calificación		RIESGO RESIDUAL	MEDIDAS DE RESPUESTA	PLAN DE ACCIÓN				
			Probabilidad	Impacto			Probabilidad	Impacto			Actividades	Responsable	Fecha Inicial (dd-mm-aaaa)	Fecha Final (dd-mm-aaaa)	Recursos
7	Falta de disponibilidad en los aplicativos y/o plataformas institucionales de orden nacional	Seguridad Digital	1	2	Bajo	A.5 - Políticas de seguridad de la información A.9.4 - Control de acceso a sistemas y aplicaciones A.11.121 - Equipos A.13.2 - Transferencia de información	1	2	Bajo	No requiere Plan de Acción					

ELABORADO POR: Nombre: <u>Angela María Valencia Brand</u> Cargo: <u>Profesional Especializado 03</u> Fecha: <u>10/09/2019</u> Firma: <u>Angela M V.B.</u>		REVISADO POR: Nombre: <u>Maria Rosario Tasamé Jiménez</u> Cargo: <u>Directora de Tecnología, Innovación y Ciencia (TIC)</u> Fecha: <u>10/09/2019</u> Firma: <u>[Firma]</u>		APROBADO POR: Nombre: <u>Maria Rosario Tasamé Jiménez</u> Cargo: <u>Directora de Tecnología, Innovación y Ciencia</u> Fecha: <u>10/09/2019</u> Firma: <u>[Firma]</u>	
--	--	---	--	---	--

COPIA CONTROLADA
Alcaldía Municipal De Palmira



SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 5- Materialización de Riesgos

Item	RIESGO MATERIALIZADO	DETALLE DE LA MATERIALIZACIÓN				TRATAMIENTO	
		Descripción	Fecha (dd/mm/aaaa)	Número de Eventos	Tipo de Acción	Descripción	Responsable
1	Afectación de la información institucional por causa de virus informático, fraude, ataques informáticos, violación de la seguridad de la información	Ingreso de programa malicioso que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario, se pudo ir propagando a través de las redes. El malware que nos afectó reiniciaba las máquinas, impidiendo que funcionen adecuadamente en las estaciones de trabajo- El malware inicialmente pudo haber llegado a alguna de las máquinas debido a distintos factores entre los cuales están los siguientes: Un usuario, usuario inexperto, Ciberseguridad, etc. Sin embargo, no se presentó ninguna pérdida de información, solo se generó malestar en los usuarios en el desarrollo de las actividades diarias.	5/02/2019	1	Acción Correctiva	1. ELIMINAR LA AMENAZA COMPLETAMENTE Se realizaron las siguientes actividades: - Actualizaciones completas de sistema operativo - Revisión del antivirus debidamente instalado - Análisis y eliminación de virus 2. MINIMIZAR LA PROBABILIDAD Y EL EFECTO DE LA OCURRENCIA Se deberá realizar una revisión permanente de cada una de las máquinas tanto física como en la consola del antivirus y directorio activo, en conjunto con el contratista del antivirus, la cual garantiza minimizar la probabilidad y el efecto de ocurrencia.	Dirección de TI y C
2	Pérdida de la integridad y disponibilidad al contar con software no licenciado	Los activos hardware y software correspondientes a la Secretaría de Educación, son gestionados de manera independiente y aislada del proceso de Informática y Gobierno en Línea, colocando en riesgo dichos activos y con probabilidad de incumplimiento de la legislación sobre Derechos de Autor del Software utilizado.	21/11/2016	1	Acción Correctiva	El 26/07/2017 Se socializa el Manual de Políticas de Seguridad Informática a los funcionarios de la Dirección de TI y C por parte de la Ing. María Rosario Tasamá Jiménez. Adicionalmente 2 o 3 veces al mes se socializa mediante circulares normativas a toda la Administración los puntos de responsabilidad y cumplimiento específicos, incluidos en el Manual de Políticas de Seguridad Informática.	Dirección de TI y C (Tecnología, Innovación y Ciencia)



COPIA CONTROLADA
Alcaldía Municipal De Palmira



Alcaldía Municipal de Palmita
NIT: 891.380.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 5- Materialización de Riesgos

AFMR-002
Versión:01
10/09/2019
Página 2 de 2

DETALLE DE LA MATERIALIZACIÓN				TRATAMIENTO			
3	Deficiencia en la integridad y disponibilidad en cuanto a la continuidad del servicio	El 24 de febrero de 2017 el Portal Web Institucional www.palmita.gov.co fue atacado por delincuentes informáticos, infiltrando un malware por un código malicioso cambiando el index del portal por una página en blanco en el texto "Hacked by yunkers crew BR" y sin posibilidad de navegación dentro del mismo durante 3 días.	24/02/2017	1	Acción Correctiva	Se adquirió Antivirus Site Lock por medio del Hosting Godaddy.com, con el fin de prevenir ataques futuros. Se implementó el software de Antivirus Site Lock especializado en escanear y mitigar el riesgo de virus en la página web, éste cada 30 min escanea y si encuentra algo malicioso lo deshecha.	Dirección de TI y C (Tecnología, Innovación y Ciencia) - Dirección de Comunicaciones.





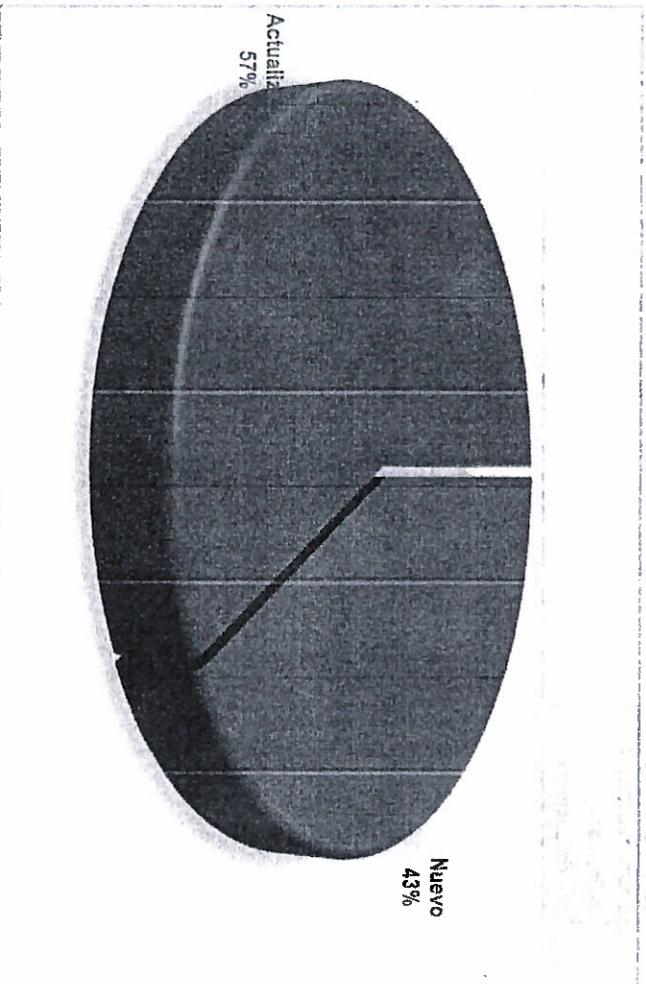
Alcaldía Municipal de Palmira
Nit.: 891.380.007-3

SECRETARÍA GENERAL
PROCESO. ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 6- Resumen

AIFMR-002
Versión.01
10/09/2019
Página 1 de 2

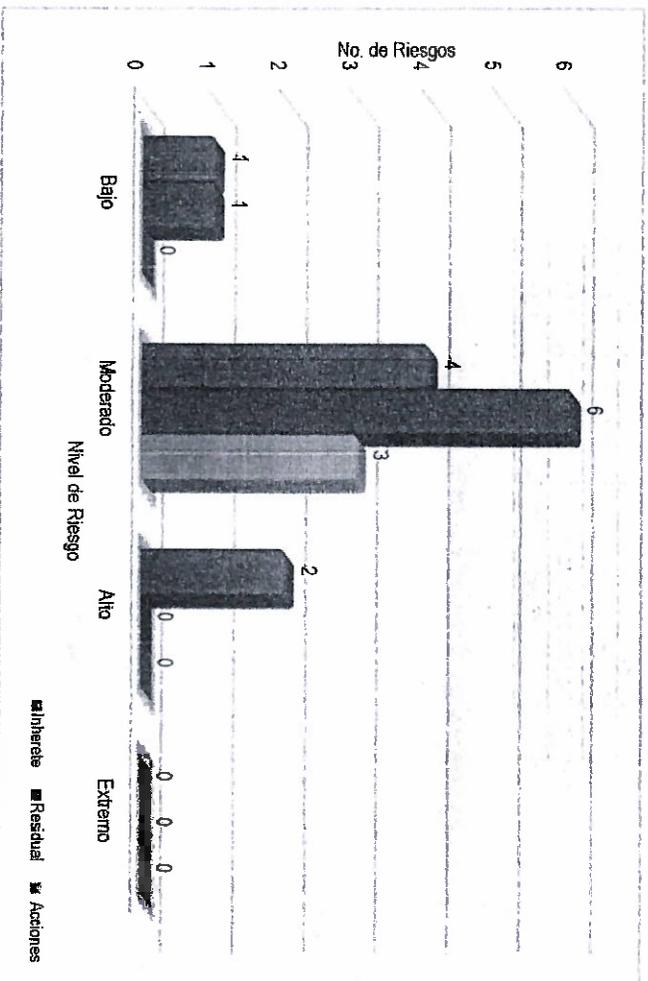
1. Clasificación del Riesgo por el Estado

Item	Estado Riesgo	Cantidad
1	Nuevo	3
2	Actualizado	4
	Total	7



2. Clasificación del Riesgo por Nivel

Item	Nivel	Inherente	Residual	Acciones
1	Bajo	1	1	0
2	Moderado	4	6	3
3	Alto	2	0	0
4	Extremo	0	0	0
	Total	7	7	3



Centro Administrativo Municipal de Palmira
Calle 30 No. 29 -39. Código Postal 763533
www.palmira.gov.co
Teléfono: 2709505

mf



Alcaldía Municipal de Palmira
Nit.: 891.380.007-3

SECRETARÍA GENERAL
PROCESO: ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN
MATRIZ No. 6- Resumen

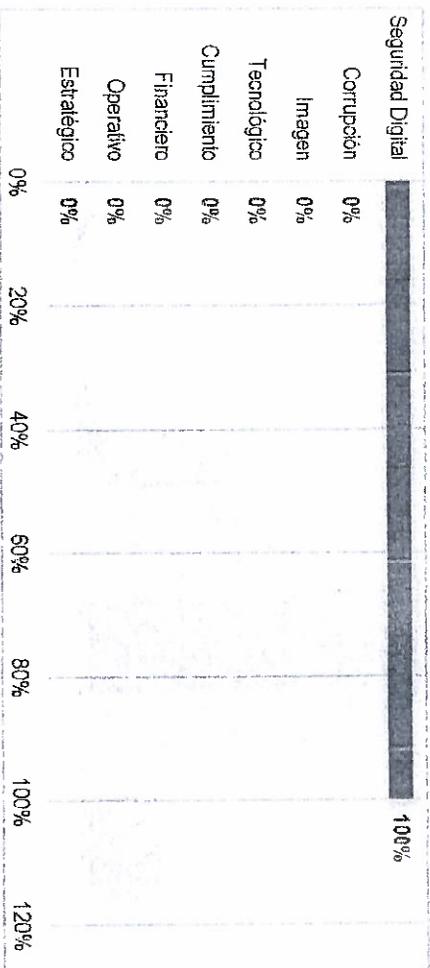
3. Riesgos por Clase

Item	Clase de Riesgo	Cantidad	%
1	Estratégico	0	0%
2	Operativo	0	0%
3	Financiero	0	0%
4	Cumplimiento	0	0%
5	Tecnológico	0	0%
6	Imagen	0	0%
7	Corrupción	0	0%
8	Seguridad Digital	7	100%
Total		7	100%

4. Riesgos Materializados

Item	Vigencia	No. Registros	No. Eventos	No. Riesgos	Eficacia
1	2017	1	1	1	86%
2	2018	0	0	0	
3	2019	1	1	1	86%
4	2020	0	0	0	

Riesgo con mayor registro de materialización:	
---	--



COPIA CONTROLADA
Alcaldía Municipal De Palmira