Alcaldía de Itagüí

PLAN DE TRATAMIENTO DE RIESGOS

DIRECCION ADMINISTRATIVA DE TIC

MUNICIPIO DE ITAGÜÍ

PLAN DE TRATAMIENTO DE RIESGOS
Junio 2018

Código del Documento	[*Definir código del Sistema de Gestión Documental*]
Versión	1.0
Fecha de Versión	2018-06-13
Creado por	Gustavo David Velásquez Monsalve
Aprobado por	[*Director Administrativo de las TIC*]
Nivel de Confidencialidad	Bajo

NIT. 890.980.093-8 • PBX: 373 76 76 • Cra. 51 No. 51 - 55
Centro Administrativo Municipal de Itagüí (CAMI)
Código postal: 055412 • Itagüí - Colombia

www.itagui.gov.co

CRONOLOGIA

Control de gobierno documento

Nombre	Plan de tratamiento de riesgo	
Creado por:	Gustavo David Velásquez Monsalve	Fecha: 02/05/2018
Revisado por:	Jorge León Guarín Comité Técnico TIC Comité Gobierno en Línea	Fecha:
Aprobado por:	Comité Tecnico	Fecha: 19 dic 2019

Control de versiones

Fecha	Ver	Responsable	Descripción Cambio
02/05/2018	0.1	Gustavo David Velásquez M.	Elaboración
20/05/2018	0.3	Gustavo David Velásquez M.	Cambios en tablas
13/06/2018	1.0	Gustavo David Velásquez M.	Para Revisión Director DATIC
Dic/2019	1.1	Comité Tecnico DATIC	Revisión en comité técnico DATIC del 19 de diciembre

NIT. 890.980.093-8 • PBX: 373 76 76 • Cra. 51 No. 51 - 55
Centro Administrativo Municipal de Itagüí (CAMI)
Código postal: 055412 • Itagüí - Colombia
www.itagui.gov.co

Tabla de contenido

NIT. 890.980.093-8 • PBX: 373 76 76 • Cra. 51 No. 51 - 55
Centro Administrativo Municipal de Itagüí (CAMI)
Código postal: 055412 • Itagüí - Colombia
www.itagui.gov.co

1. PROPÓSITO, ALCANCE Y USUARIOS

- El propósito de este documento es definir cuáles controles de seguridad o salvaguardas de MAGERIT son los apropiados para enfrentar las amenazas de cada uno de los activos y mitigar los riesgos en la Dirección Administrativa de las TIC del Municipio de Itagüí, así como definir el tratamiento de cada uno de ellos.

- Este documento también determina cuáles controles de seguridad del Anexo A del estándar ISO/IEC 27001:2013 son aplicables al alcance del Sistema de Gestión de la Seguridad de la Información propuesto para la DATIC en fase de planeación.

2. DOCUMENTOS DE REFERENCIA

- Estándar ISO/IEC 27001:2013, cláusulas 8.2. y 8.3.
- Anexo A del estándar ISO/IEC 27001:2013.
- Estándar ISO/IEC 27002:2013.
- Documento de las Políticas de la Seguridad de la Información (en revisión por la DATIC).
- Metodología de Análisis y Evaluación de Riesgos MAGERIT (Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información).

NIT. 890.980.093-8 • PBX: 373 76 76 • Cra. 51 No. 51 - 55
Centro Administrativo Municipal de Itagüí (CAMI)
Código postal: 055412 • Itagüí - Colombia
www.itagui.gov.co

3. TRATAMIENTO DE RIESGOS

El tipo de tratamiento que se le dará a cada riesgo: ***Asumirlos (AS)***, ***Definir Controles (DC)*** o ***Transferirlos a Terceros (TT)***.

4. APLICABILIDAD DE CONTROLES DE SEGURIDAD

Con el objetivo de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad basados en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013.

NIT. 890.980.093-8 • PBX: 373 76 76 • Cra. 51 No. 51 - 55
Centro Administrativo Municipal de Itagüí (CAMI)
Código postal: 055412 • Itagüí - Colombia
www.itagui.gov.co

[D] DATOS/INFORMACIÓN

CÓDIGO	ACTIVO	NAZA	GO_ID	RIES	IESGO	TRATAM	IENTO	SALVAGUARDAS	ANEXO A ISO/IEC
D _BCK	Copias de Seguridad de los Sistemas de Información	E*, A*	_BCK	R_D	A	D C		Protección de la Información Copias de seguridad de los datos (backup) Cifrado de la información	A.8.2.* A.12.3.1 A.10.1.*
D _CNT	Contratos	E*, A*	_CNT	R_D	M A	D C		Cifrado de la información Uso de firmas electrónicas Aseguramiento de la integridad	A.10.1.*
D _PUB	Publicaciones	E*, A*	_PUB	R_D	M B	D C		Copias de seguridad de los datos (backup)	A.12.3.1
D _LOG	Registros de Actividad	E*, A*	_LOG	R_D	A	D C		Protección de la Información Cifrado de la información	A.8.2.* A.10.1.*
D _SRC	Códigos Fuentes	E*, A*	_SRC	R_D	M A	D C		Protección de la Información Cifrado de la información	A.8.2.* A.10.1.*

[S] SERVICIOS

CÓDIGO	ACTIVO	AMENAZA	CRITERIO	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
S_MAI	Correo Electrónico	E*, A*	R_S_MAI	A	D C	Protección del correo electrónico Protección de servicios y aplicaciones web	A.13.2.3 A.12.5.1
S_GID	Gestión de Identidades	E*, A*	R_S_GID	M A	D C	Aseguramiento de la disponibilidad Protección del directorio Se aplican perfiles de seguridad	A.17.1.* A.8.2.* A.9.4.3
S_INT	Servicios Internos	E*, A*	R_S_INT	M A	D C	Aseguramiento de la disponibilidad Protección del servidor de nombres de dominio (DNS)	A.17.1.* A.9.4.*
S_WWW	Páginas web de acceso público	E*, A*	R_S_WWW	A	D C	Aseguramiento de la disponibilidad Protección de servicios y aplicaciones web	A.17.1.* A.12.5.1

[SW] SOFTWARE

CÓDIGO ACTIVO	AMENAZA	CRITERIO	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
SW_SWP Software de Desarrollo Propio	I*, E*, A*	R_SW_SWP	M A	D C	Protección de las Aplicaciones Informáticas Copias de seguridad (backup) Se aplican perfiles de seguridad Puesta en producción	A.14.2.* A.12.3.1
SW_STD Software Estándar	I*, E*, A*	R_SW_STD	M A	D C	Protección de las Aplicaciones Informáticas Copias de seguridad (backup) Se aplican perfiles de seguridad	A.14.2.* A.12.3.1
SW_MAI Software para Correo Electrónico	I*, E*, A*	R_SW_MAI	M A	D C	Protección de las Aplicaciones Informáticas Se aplican perfiles de seguridad	A.14.2.*

CÓDIGO ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
SW_DBS	Gestores de Bases de Datos	I*, E*, A*	R_SW_DBS	MA	DC	Protección de las Aplicaciones Informáticas Copias de seguridad (backup) Cambios (actualizaciones y mantenimiento) Se aplican perfiles de seguridad	A.14.2.* A.12.3.1
SW_OFM	Ofimática	I*, E*, A*	R_SW_OFM	B	DC	Protección de las Aplicaciones Informáticas Copias de seguridad (backup) Se aplican perfiles de seguridad	A.14.2.* A.12.3.1
SW_AVS	Software de Antivirus	I*, E*, A*	R_SW_AVS	M	DC	Protección de las Aplicaciones Informáticas Se aplican perfiles de seguridad	A.12.2.1
SW_OPS	Sistemas Operativos	I*, E*, A*	R_SW_OPS	M	DC	Protección de las Aplicaciones Informáticas Copias de seguridad (backup) Se aplican perfiles de seguridad	A.14.2.* A.12.3.1 A.12.2.1 A.12.5.1 A.12.6.*

[HW] HARDWARE

CÓDIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
HW_BCK	Dispositivos de Respaldo	I*, E*, A*	R_HW_BCK	MA	DC	Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1 A.12.3.1
HW_FRW	Firewall	I*, E*, A*	R_HW_FRW	MA	DC	Protección de los Equipos Informáticos Aseguramiento de la disponibilidad Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_ANT	Antenas	I*, E*, A*	R_HW_ANT	M	DC	Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_HOS	Servidores	I*, E*, A*	R_HW_HOS	MA	DC	Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
						• Aseguramiento de la disponibilidad • Se aplican perfiles de seguridad	A.11.2.1
HW_PCM	Computadores Portátiles de Uso Institucional	I*, E*, A*	R_HW_PCM	B	DC	• Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PCP	Computadores de Escritorio de Uso Institucional	I*, E*, A*	R_HW_PCP	B	DC	• Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PRT	Impresoras	I*, E*, A*	R_HW_PRT	MB	AS	• Protección de los Equipos Informáticos • Reproducción de documentos	A.11.1.1 A.11.1.2 A.11.2.1
HW_ROU	Router	I*, E*, A*	R_HW_ROU	A	DC	• Protección de los Equipos Informáticos • Aseguramiento de la disponibilidad • Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_SCN	Escáner	I*, E*, A*	R_HW_SCN	MB	AS	• Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_SWH	Switch	I*, E*, A*	R_HW_SWH	A	DC	• Protección de los Equipos Informáticos • Aseguramiento de la disponibilidad • Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_WAP	Puntos de Acceso Inalámbricos	I*, E*, A*	R_HW_WAP	B	DC	• Protección de los Equipos Informáticos • HW.A Aseguramiento de la disponibilidad	A.11.1.1 A.11.1.2 A.11.2.1

[COM] COMUNICACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
COM_INT	Internet	E*, A*	R_COM_INT	M A	D C	Protección de las Comunicaciones Aseguramiento de la disponibilidad Protección criptográfica de la confidencialidad de los datos intercambiados	A.9.1.2 A.10.1.1 A.11.2.3 A.13.1.* A.13.2.1 A.13.2.2
COM_LAN	Red de Área Local	E*, A*	R_COM_LAN	M A	D C	Protección de las Comunicaciones Aseguramiento de la disponibilidad Protección criptográfica de la confidencialidad de los datos intercambiados	A.9.1.2 A.10.1.1 A.11.2.3 A.13.1.* A.13.2.1 A.13.2.2
COM_WIF	Conectividad Inalámbrica	E*, A*	R_COM_WIF	M	D C	Protección de las Comunicaciones Aseguramiento de la disponibilidad Protección criptográfica de la confidencialidad de los datos intercambiados Seguridad Wireless(WiFi)	A.9.1.2 A.10.1.1 A.13.1.* A.13.2.1 A.13.2.2

[AUX] EQUIPO AUXILIAR

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
AUX_FBO	Fibra Óptica	I*, E*, A*	R_AUX_FBO	M A	D C	Aseguramiento de la disponibilidad Climatización Suministro eléctrico	A.11.2.2 A.11.2.3 A.11.2.6 A.13.2.1
AUX_RCK	Rack	I*, E*, A*	R_AUX_RCK	A	D C	Aseguramiento de la disponibilidad Climatización Suministro eléctrico	A.11.2.2 A.11.2.3 A.13.2.1
AUX_PWR	Fuente de Alimentación	I*, E*, A*	R_AUX_PWR	M A	D C	Aseguramiento de la disponibilidad Climatización Suministro eléctrico	A.11.2.2 A.11.2.3 A.13.2.1

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
AUX_UPS	Sistema de Alimentación Ininterrumpida	I*, E*, A*	R_AUX_UPS	A	DC	Aseguramiento de la disponibilidad Climatización Suministro eléctrico	A.11.2.2 A.11.2.3 A.13.2.1
AUX_WIR	Cableado Eléctrico	I*, E*, A*	R_AUX_WIR	MA	DC	Aseguramiento de la disponibilidad Suministro eléctrico Protección del cableado	A.11.2.2 A.11.2.3 A.11.2.6 A.13.2.1

[L] INSTALACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
L_SIT	Oficina DATIC	N*, I*, E*, A*	R_L_SIT	A	AS	Protección de las Instalaciones Aseguramiento de la disponibilidad Control de los accesos físicos	A.11.1.* A.17.*

[P] PERSONAL

CÓDIGO	ACTIVO	AMENAZAS	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC
P_ADM	Administrador de Sistema	E*, A*	R_P_ADM	A	T	Gestión del Personal Aseguramiento de la disponibilidad Formación y concienciación	A.7.*
P_COM	Administrador de Comunicaciones	E*, A*	R_P_COM	MA	T	Gestión del Personal Aseguramiento de la disponibilidad Formación y concienciación	A.7.*
P_DBA	Administrador de Bases de Datos	E*, A*	R_P_DBA	MA	T	Gestión del Personal Aseguramiento de la disponibilidad Formación y concienciación	A.7.*
P_DES	Desarrolladores de Software	E*, A*	R_P_DES	M	T	Gestión del Personal Aseguramiento de la disponibilidad Formación y concienciación	A.7.*

Anexo

AMENAZAS

N: amenaza de tipo natural referirse al libro 2 de metodología MAGERIT
I: amenaza de tipo Industrial referirse al libro 2 de metodología MAGERIT
E: amenaza por errores o fallas no intencionales referirse al libro 2 de metodología MAGERIT
A: amenaza por ataques referirse al libro 2 de metodología MAGERIT

VALORACION DEL RIESGO (la sustentación de esta valoración hace parte del documento general de la propuesta del SGSI para la Dirección Administrativa TIC)

MA: Muy Alta
A: Alta
M: Media
B: Baja
MB: Muy Baja