	FORMATO MATRIZ DE RIESGOS	Código: DE-F-01 Versión: 01 Página: 1 de 1

	Gestión de Tecnologías e Información
	Dirigir, gestionar y controlar las soluciones y los servicios tecnológicos, mediante la implementación de sistemas de información, herramientas e instrumentos organizacionales y administrativos, para asegurar la disponibilidad, capacidad

IDENTIFICACIÓN DEL RIESGO				ANÁLISIS DEL RIESGO				VALORACIÓN DEL RIESGO		
RIESGO	TIPO DE RIESGO	CAUSAS	CONSECUENCIAS	CALIFICACIÓN		EVALUACIÓN DEL RIESGO	MEDIDAS DE RESPUESTA	CONTROLES	TIPO DE CONTROL	
				PROBABILIDAD	IMPACTO				Preventivo	Correctivo
Vulnerabilidad en la seguridad de los equipos	Tecnológico	Desactualización de los sistemas operativos de las estaciones de trabajo.	1. Acceso a información confidencial por personas no autorizadas. 2. Pérdida de información importante almacenada en los equipos de los contratistas. 3. Pérdida de confianza e imagen de la Entidad ante la comunidad. 4. Incumplimiento de las obligaciones de la Entidad.	1	4	Alto	Reducir el riesgo, compartir, evitar o trasferir	Plan de trabajo para revisar, monitorear y actualizar todos los equipos con los últimos parches de Seguridad de Microsoft.	x	
Infección de virus informático	Tecnológico	Desactualización del sistema antivirus en las estaciones de trabajo	1. Pérdida de información importante almacenada en los equipos de los contratistas. 2. Acceso a información confidencial por personas no autorizadas. 3. Pérdida de confianza e imágen de la Entidad ante la comunidad. 4. Incumplimiento de las obligaciones de la Entidad.	1	4	Alto	Reducir el riesgo, compartir, evitar o trasferir	Plan de trabajo para revisar, monitorear y actualizar todos los equipos con los últimos archivos de Mcafee. 2.Proceso de compra de lincencias de Antivirus Mcafee para máquinas propias en producción.	x	
Desconexión de enlace de Internet que impida la conexión a los servicios de información principales	Tecnológico	Fallas del Operador de Internet	1. Demora en la atención a la comunidad para la realización de sus trámites. 2. Pérdida de confianza e imagen de la Entidad ante la comunidad. 3. Suspensión del servicio	4	2	Alto	Reducir el riesgo, compartir, evitar o trasferir	Implementar enlaces de respaldo	x	
								Disponer de equipos que nos brinden la posibilidad de conexión.	x	
								Realizar migración de infraestructura de SAFIX a la nube de Oracle	x	
Suplantación de identidad en los sistemas de información.	Tecnológico	1. No tener un sistema centralizado de Seguridad de Windows. 2. Tener contraseñas identicas y no poder gestionar su cambio. 3. Imposibilidad para aplicar politicas de Seguridad de usuario.	1. Acciones judiciales en contra de la Entidad. 2. Acceso a información confidencial por personas no autorizadas. 3. Manipulación de los datos y la información	1	4	Alto	Reducir el riesgo, compartir, evitar o trasferir	Implementar un Dominio de Seguridad y establecer relaciones de confianza con el Dominio del municipio.	x	

Alcaldía de Medellín Control Interno FONVALMED	**FORMATO** MATRIZ DE RIESGOS	Código: DE-F-01 Versión: 01 Página: 1 de 1

	Gestión de Tecnologías e Información									
	Dirigir, gestionar y controlar las soluciones y los servicios tecnológicos, mediante la implementación de sistemas de información, herramientas e instrumentos organizacionales y administrativos, para asegurar la disponibilidad, capacidad									
Modificar la información del Sistema SAFIX intencionalmente para beneficio particular.	Tecnológico	1. Falla en la seguridad del sistema SAFIX 2. Amenazas provenientes de fuentes externas (pnal de Xenco) e internas (contratistas de la entidad)	1. Pérdidas económicas por fraude. 2. Pérdida de confinaza e imagen.	4	4	Extremo	Reducir el riesgo, compartir, evitar o trasferir	Plan de Seguridad SAFIX	x	
Acceso indebido para manipular o adulterar datos almacenados en los servidores de la Entidad, en beneficio propio o de un tercero.	Tecnológico	1.Falta de revisión de los módulos y permisos que tienen los usuarios. 2.Traslado o cambio de rol de los funcionarios sin informar a Tecnología para realizar los ajustes	1.Pérdida de la integridad de la información. 2.Procesos poco transparentes. 3.Pérdida de imagen institucional. 4.Responsabilidades Disciplinarias y/o fiscales.	1	4	Alto	Reducir el riesgo, compartir, evitar o trasferir	Control de acceso al sistema.	x	
Errores en Hardware y Software	Tecnológico	1.Daños en los servidores ó en la Red. 2.Fallas en los programas o en las bases de datos 3.Suspensión del servicio eléctrico al centro de cómputo.	1.Suspensión del servicio. 2.Pérdida de imagen. 3.Pérdida de información.	1	3	Bajo	Asumir el riesgo	Revisar el diseño de la plataforma y hacer las pruebas de contingencia. Validar el backup de datos y hacer las pruebas de restauración.	x	
Pérdida de información en las estaciones	Tecnológico	1. Daño en los equipos y sus discos duros. 2. Infección de Virus en las máquinas. 3. Daño por malas condiciones eléctricas.	Demora en la respuesta a los contribuyentes.	3	3	Bajo	Asumir el riesgo	Disponibilidad del repositorio en la nube para almacenar la información	x	

	l y continuidad de la plataforma, de los servicios y el cubrimiento a los procesos que operan en toda la Entidad

PLAN DE MANEJO DEL RIESGO

RIESGO	ACCIONES	RESPONSABLE	CRONOGRAMA		INDICADORES	FUENTES DE VERIFICACIÓN - REGISTRO
			FECHA INICIO	FECHA FINAL		
Vulnerabilidad en la seguridad de los equipos	1. Definir Plan de trabajo (Se identificó las necesidades de las actividades a realizar y para el 2018 se hará el plan de trabajo)	Coordinador proceso de tecnología	02/01/2018	05/03/2018	Nro total de equipos actualizados/Total de Equipos*100	Plan de trabajo
	2.Revisar los equipos periódicamente para garantizar que su sistema operativo cuenta con todas las actualizaciones de seguridad.		02/01/2018	31/12/2018		
	3. Implementar un controlador de dominio		01/08/2018	31/12/2018	Porcentaje de implementación	
Infección de virus informático	1. Definir Plan de trabajo 2.Revisar los equipos periodicamente para garantizar que su sistema Antivirus este actualizado y funcionando. Nota: En el 2017 se solucionaron incidentes en algunas máquinas que se presentaron problemas de actualización.	Coordinador proceso de tecnología	02/01/2018	31/12/2018	Nro total de equipos actualizados/Total de Equipos*100	Plan de trabajo Hoja de cálculo con registro de incidentes de Tecnologia.
	3. Solicitar proceso de compra de licencias Mcafee.					
Desconexión de enlace de Internet que impida la conexión a los servicios de información principales	1. Diseñar e implementar infraestructura de telecomunicaciones y servidores para el acceso a los servicios	Coordinador proceso de tecnología	01/03/2018	01/06/2018	Infraestructura de telecomunicaciones aprobada	Informe de propuesta, presentaciones
			01/03/2018	01/06/2018		
			23/07/2018	31/12/2018	Infraestructura migrada	Plan de trabajo
Suplantación de identidad en los sistemas de información.	1.Implementar un plan de acción de seguridad con el fin de que cada funcionario sea el único que conozca la contraseña de los usuarios de los diferentes aplicativos y servicios. 2.Establecer un dominio de seguridad que concentre las estaciones y los usuarios de FONVALMED. 3.Garantizar que cada usuario pueda cambiar sus contraseñas e implementar controles de solicitud de cambio automaticamente.	Coordinador proceso de tecnología	01/03/2018	31/12/2018	NA	Plan de acción de seguridad

	d y continuidad de la plataforma, de los servicios y el cubrimiento a los procesos que operan en toda la Entidad

Modificar la información del Sistema SAFIX intencionalmente para beneficio particular.	1.Desarrollar e implementar un plan de seguridad para SAFIX con el fin de garantizar que los usuarios tengan los permisos necesarios para el desempeño de sus funciones. 2.Activar las opciones de auditoría en las que quede registro de las operaciones realizadas en la plataforma. 3.Activación del Log de la base de datos	Coordinador proceso de tecnología	02/01/2018	30/04/2018	Plan de trabajo con xenco aprobado	Plan de seguridad SAFIX
Acceso indebido para manipular o adulterar datos almacenados en los servidores de la Entidad, en beneficio propio o de un tercero.	1.Administrar eficientemente el control de acceso de los usuarios al sistema. 2.Monitorear y validar las opciones que tienen los usuarios. Nota: Se atendieron solicitudes e incidentes referentes a los permisos de los usuarios frente a los cambios del ROL.	Coordinador proceso de tecnología	02/01/2018	31/12/2018	N/A	Hoja de cálculo con registro de incidentes de Tecnologia.
Errores en Hardware y Software	Revisar diseño de plataforma. Revisar esquemas de backup Pruebas de restauración Pruebas de contingencia	Coordinador proceso de tecnología	02/01/2018	31/12/2018	N/A	Informe de pruebas
Pérdida de información en las estaciones	Rvisar que los usuarios estén usando el repositorio. Capacitar a los usuarios para el uso del repositorio.	Coordinador proceso de tecnología	02/01/2018	31/12/2018	N/A	Documentos con firmas de los contratistas

		EVALUACION CONTROL INTERNO	
RIESGO	**FECHA SEGUIMIENTO**	**EVIDENCIA ACCIÓN O CONTROL**	**EVALUACIÓN EFECTIVIDAD**
Vulnerabilidad en la seguridad de los equipos	16/12/2018	Se genera un informe de las actualizaciones.	80%
Infección de virus informático	16/12/2018	Informe enero / febrero se ejecuto en marzo. Queda pendiente suministrarlo	98%
Desconexión de enlace de Internet que impida la conexión a los servicios de información principales	16/12/2018	Se comenzó con la migración del ERP - SAFIX a la Nube de Oracle como plataforma IAAS	70%
Suplantación de identidad en los sistemas de información.	16/12/2018	Montar un dominio de seguridad de windows	10%

Modificar la información del Sistema SAFIX intencionalmente para beneficio particular.	16/12/2018	Documento que evidencia la activacion de auditoria. Correo de municipio con resultado del log.	73%
Acceso indebido para manipular o adulterar datos almacenados en los servidores de la Entidad, en beneficio propio o de un tercero.	16/12/2018	Control de permisos de usuario en la hoja de calculo correspondiente.	100%
Errores en Hardware y Software	16/12/2018	se tiene esquema, todavia no ha avanzado sus respectivas pruebas por el cambio de infraestructura	15%
Pérdida de información en las estaciones	16/12/2018	Se ha realizado con dos procesos de la entidad	40%

RIESGO	OBSERVACIÓN / RECOMENDACIÓN
Vulnerabilidad en la seguridad de los equipos	tener en cuenta las maquinas que posiblemnete se actulicen automaticamente.
Infección de virus informático	da dos meses se hace la revision de zequipos. Se esta en proceso de activar consola centraliza
Desconexión de enlace de Internet que impida la conexión a los servicios de información principales	Adicional, para el 2019 se realizará mejora del equipo de seguridad perimetral de la entidad
Suplantación de identidad en los sistemas de información.	Se realizó una configuración de prueba y se espera instalar en el 2019

Modificar la información del Sistema SAFIX intencionalmente para beneficio particular.	Se pasaran los documentos para su analisis.
Acceso indebido para manipular o adulterar datos almacenados en los servidores de la Entidad, en beneficio propio o de un tercero.	Informe de permisos actuales de SAFIX
Errores en Hardware y Software	Realizar restauracion de BD de SAFIX de manera local.
Pérdida de información en las estaciones	se debe implementar este control debido que mucha informacion no esta respaldada.