Superservicios
Superintendencia de Servicios Públicos Domiciliarios

MAPA DE RIESGOS

SIGME

Proceso/Subproceso:	TODOS LOS PROCESOS	Objetivo Proceso/Subproceso:	N/A

IDENTIFICACIÓN DEL RIESGO													RIESGO INHERENTE			VALORACIÓN CONTROLES													RIESGO RESIDUAL						TRATAMIENTO DEL RIESGO			INDICADORES
							Consecuencias						Probabilidad	Impacto										Diseño		Ejecución						Probabilidad	Impacto					
Proceso / Subproceso	Tipo de Activo	Nombre de Riesgo	Tipo de Riesgo	Codigo de Riesgo	Descripción de Riesgo	Vulnerabilidades	Amenaza	Consecuencia	Grado de impacto	Valor de impacto	¿Se ha Materializado el Riesgo?	Descripción de Materialización	Frecuencia de la Materialización	Descriptor	Descriptor	Zona	Descripción del control	Nombre del documento donde se relaciona el control	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control?	¿Existe una adecuada segregación y autoridad del responsable?	¿La frecuencia de ejecución del control ha demostrado ser oportuna?	¿Cual es el propósito del control?	¿Cómo se realiza la actividad de control?	¿Qué pasa con las observaciones o desviaciones?	¿Existen evidencia de la ejecución del control?	Ruta evidencia	Calificación Cuantitativa	Calificación Cualitativa	Calificación Cuantitativa	Calificación Cualitativa	Calificación de la Solidez del Conjunto de Controles	¿Los Controles Ayudan a Disminuir la Probabilidad?	¿Los Controles Ayudan a Disminuir el Impacto?	Descriptor	Descriptor	Zona	Opciones de Manejo del Riesgo Residual	Proceso	Código	Justificación de Manejo	Indicador
COMUNICACIONES	INFORMACION / DATO	Información / Dato	PERDIDA DE CONFIDENCIALIDAD	RSI-003-CO	Publicación, eliminación o modificación no autorizada de información en los canales electrónicos de divulgación a cargo del Grupo de Comunicaciones (portal web, redes sociales, intranet y correos electrónicos corporativos), por inadecuada gestión en el otorgamiento o retiro de derechos de acceso a usuarios a las plataformas de administración de los mismos, que pueden afectar la confidencialidad, integridad y disponibilidad de sus contenidos ante accesos no controlados.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4	No			RARA VEZ	MAYOR	Alta	Informar a través de los canales de gestión apropiados tan pronto como sea posible, los eventos de seguridad de la información. Cada vez que se detecte una alerta o posible incidente de seguridad en el portal web, intranet, redes sociales y correos electrónicos corporativos, el responsable del canal atenderá lo dispuesto en el documento TI-I-008 - Instructivo para la gestión de incidentes de seguridad y privacidad de la información; con el fin de reportar la situación para su análisis y tratamiento a la Oficina de Informática, a través de la herramienta de Gestión de Servicios Tecnológicos (Mesa de ayuda - Aranda). El responsable del canal atenderá las orientaciones de la Oficina de Informática. En caso de no reportar el incidente, podría materializarse la afectación de la disponibilidad, confidencialidad e integridad de la información. Si esto sucede, corresponde realizar una investigación para determinar causas y responsabilidades; aplicar los correctivos técnicos necesarios con el apoyo de la Oficina de Informática; y generar las actuaciones administrativas que tenga previsto la entidad, según cada caso en particular Evidencia: Casos Aranda - Categoría manejo de incidentes.	TI-I-008 - Instructivo para la gestión de incidentes de seguridad y privacidad de la información	No Asignado	Inadecuado	Oportuna	Detectar	Confiable	Se investigan y resuelven oportunamente	Completa	Carpeta Drive adminweb@superservicios: https://drive.google.com/drive/folders/151BBTx8cOVYjlrWxDo2L8_S1_eQVl6uD?usp=sharing	65	DÉBIL	10		MODERADO	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MODERADO	Moderada	REDUCIR	COMUNICACIONES	AP-CO-005	Se requiere documentar tratamientos formales para la asignación de contraseñas, responsables de accesos a los canales de divulgación, reserva de contraseñas, entre otros aspectos para mejorar los controles del riesgo.	Eficacia de las acciones relacionadas con gestión de brechas de seguridad de la información.
						EQUIPAMIENTO MÓVIL PROCLIVE A SER ROBADO		Afectación de disponibilidad	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.	4							Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Cada vez que ingrese o se retire un funcionario o contratista del Grupo de Comunicaciones, el líder del proceso solicita a la Oficina de Informática la activación o desactivación de usuarios en los sistemas de información y repositorios de la entidad, según sea el caso, diligenciando el formato TI-F-034 Administración de usuarios, el cual se tramitará a través de la herramienta de Gestión de Servicios Tecnológicos (Mesa de ayuda - Aranda), dispuesta por la Oficina de Informática. Este trámite incluye la solicitud de habilitación del perfil de administrador de contenidos del portal web y la intranet para el personal que sea asignado a esta labor. En caso de requerirse conexión remota para acceso fuera de la entidad, el líder del proceso formaliza la solicitud, mediante el formato TI-F-035 Solicitud y autorización de acceso a la red LAN para colaboradores, a través de la herramienta Aranda. En caso de que el líder del proceso no solicite la activación de usuarios, el personal no podrá acceder a ningún repositorio o sistema de información de la entidad. En caso de no solicitar la desactivación de algún colaborador por su retiro de la entidad, la Oficina de Talento Humano o la Oficina de Contratos no expedirá el respectivo paz y salvo para formalizar dicho retiro. Evidencia: Casos Aranda - Categoría manejo de cuentas.	Formato TI-F-034 Administración de usuarios y el instructivo TI-I-013 Gestión de Usuarios.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	Aranda	100	FUERTE	10											
						INADECUADOS DERECHOS DE USUARIO		Afectación de Integridad	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.	4																													
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS																																	
						NIVEL DE CONFIDENCIALIDAD																															

						NO DEFINIDO CON CLARIDAD																																		
						REGLAS PARA TRABAJO AFUERA DE LAS INSTALACIONES NO DEFINIDAS CON CLARIDAD																																
CONTROL	INFORMACION / DATO	INFORMACIÓN / DATO	PERDIDA DE CONFIDENCIALIDAD	RSI-003-CT	FUGA O REVELACIÓN DE INFORMACIÓN EN LOS EXPEDIENTES DEL ÁREA DE INVESTIGACIÓN QUE SE ENCUENTRAN PUBLICADOS EN EL SISTEMA DE GESTIÓN DOCUMENTAL ORFEO, DEBIDO A QUE LA INFORMACIÓN SE ENCUENTRA DISPONIBLE PARA PERSONAL NO AUTORIZADO, LO QUE PODRÍA GENERAR UNA AFECTACIÓN GRAVE A LA CONFIDENCIALIDAD DE LA INFORMACIÓN	INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4	No			RARA VEZ	MAYOR	Alta	Cada vez que se requiera asignar o modificar un permiso a los expedientes del sistema de información documental ORFEO, el propietario del expediente utiliza la opción "Confidencial/Nivel de Seguridad", de acuerdo con la guía de ayuda No. 17 Instructivo de seguridad para Expedientes y Radicados, con el fin de asegurar la confidencialidad de los documentos que lo necesitan. El dueño del expediente cuando se de cuenta o sea notificado podrá asignar estos permisos. Como evidencia se tiene la trazabilidad de las actividades en la pestaña histórico del ORFEO.	Guía de ayuda No. 17 Instructivo de seguridad para Expedientes y Radicados	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	ORFEO/HISTORICOS	100	FUERTE	10		FUERTE	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MENOR	Baja	ACEPTAR				Eficacia de las acion ejecutadas con gestión de riesgos de seguridad de la información.
DIRECCIONAMIENTO ESTRATÉGICO	INFORMACION / DATO	INFORMACIÓN / DATO	PERDIDA DE CONFIDENCIALIDAD	RSI-002-OE	INADECUADA GESTIÓN DE USUARIOS PARA ACCESO A PLATAFORMAS INTERNAS Y EXTERNAS QUE PUEDEN IMPACTAR EN EL CUMPLIMIENTO DE LOS TIEMPOS ESTABLECIDOS DE LA EJECUCIÓN DE ACTIVIDADES DEL PROCESO LO QUE GENERARÍA LA PÉRDIDA DE LA INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	Si	Se presentan usuarios que pueden acceder a los sistemas de información sin los privilegios adecuados o permitidos.	Al menos una vez en el último año	PROBABLE	MODERADO	Alta	Cada vez que se requiera crear, modificar o eliminar un usuario en los sistemas de información externos, el líder de proceso solicita a la entidad responsable del sistema de información los privilegios o cambios requeridos con el fin de asegurar el acceso y la gestión de información de la entidad. De acuerdo a las instrucciones recibidas por la entidad responsable del sistema de información, a través de correo electrónico y en caso de requerir correcciones a la solicitud, se reenvía el correo y se comunica con el soporte de la entidad responsable.Como evidencia se tienen los correos electrónicos de radicación de la solicitud.	No existe documentación interna asociada.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Incompleta	Ruta DRIVE	95	MODERADO	5		MODERADO	DIRECTAMENTE	INDIRECTAMENTE	POSIBLE	MODERADO	Alta	REDUCIR		DIRECCIONAMIENTO ESTRATÉGICO	AP-DE-008	Fortalecer el control del riesgo	Eficacia de las acion ejecutadas con gestión de riesgos de seguridad de la información.
						CUENTAS DE USUARIO GENERADAS POR SISTEMA CUYAS CONTRASEÑAS PERMANECEN SIN MODIFICACIÓN		Afectación de Integridad	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros	3							Cada vez que se requiera crear, modificar o eliminar un usuario en los sistemas de información internos, el jefe de dependencia solicita a la Oficina Asesora de Planeación los privilegios o cambios requeridos con el fin de asegurar el acceso y la gestión de información de la dependencia, a través de correo electrónico se realiza la solicitud y en caso de requerir correcciones se reenvía el correo y se comunica con el administrador de los sistemas de información internos.Como evidencia se tienen los correos electrónicos de radicación de la solicitud.	No existe documentación interna asociada.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	Ruta Drive	100	FUERTE	10											
						FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO																																
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS																																
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	INFORMACION / DATO	Repositorios de información oficiales	PERDIDA DE CONFIDENCIALIDAD	RSI-005-03	Alteración o intento de modificación no autorizada de los datos almacenados en los repositorios oficiales de la entidad con las siguientes vulnerabilidades: (i) Conexiones de red pública sin protección; (ii) Contraseñas inseguras; (iii) Falta de desactivación de cuentas de usuario luego de finalizado el empleo y (iv) Información disponible para personas no autorizadas, que pueden ser afectadas por el acceso no autorizado al sistema de información, puede ocurrir pérdida de confidencialidad y pérdida de integridad, lo que generaría la pérdida de información crítica para la entidad.	CONEXIONES DE RED PÚBLICA SIN PROTECCIÓN	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Perdida de información crítica para la entidad	Que puede ser recuperada de forma parcial	4	No			RARA VEZ	MAYOR	Alta	Cada vez que ingrese un funcionario o un contratista a la Entidad y con el fin de asegurar la gestión de registro y cancelación de usuarios para los repositorios oficiales de la entidad, el Profesional de la Oficina de Informática recibe del supervisor o Jefe Inmediato la solicitud para la activación o inactivación de usuarios para acceso o restricción a los repositorios oficiales, mediante el formato TI-F-024 administración de usuarios, el cual se adjunta en una solicitud de la mesa de servicios, en caso de no solicitar estos accesos los colaboradores no podrán acceder a repositorios de la Entidad. Evidencia: casos aranda categoría manejo de cuentas.	Formato TI-F-034 Administración de usuarios y el instructivo TI-I-013 Gestión de Usuarios.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	\\172.16.0.235\colsoft\Operación\	100	FUERTE	10		MODERADO	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MODERADO	Moderada	REDUCIR		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	AP-TI-010	Se adoptan medidas para reducir la probabilidad del riesgo, dado a la implementación de controles.	No de incidentes reportados que afectaron la confidencialidad de los repositorios oficiales de la entidad
						CONTRASEÑAS INSEGURAS												El profesional de la oficina de informática valida semestralmente que la información de usuarios en el directorio activo se encuentre vigente. Con el fin con el fin de asegurar la gestión de contraseñas en los repositorios oficiales de la entidad y para ello compara la información del personal activo suministrada por Gestión del Talento Humano y Gestión de Adquisición de Bienes y Servicios, en caso de encontrar usuarios activos que ya no tienen vinculación a la Entidad se desactivan del directorio activo. Como evidencia se genera el archivo Depuración de Usuarios.	MC-M-001 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN Y MEJORA, Numeral 6 Anexo, Políticas complementarias, 8. POLÍTICA DE CONTROL DE ACCESO Y USO DE CONTRASEÑAS8.POLÍTICA DE RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	https://docs.google.com/spreadsheets/d/1WR4OTB660Qz8Ay5TMxVPv_dKYIOD8Fvy-rdyMaP8PM/ucd8jg/sd=965975889	100	FUERTE	10											
						FALTA DE												Cada vez que	MC-M-001 MANUAL DEL	Asignado	Adecuado	Oportuna	Prevenir	No	Se investigan y	Completa	Casos mesa de servicios (Aranda)	85	DÉBIL	10											

						DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO										Ingresa un funcionario o un contratista a la Entidad y con el fin de restringir el acceso a la información, el profesional de la Oficina de informática recibe del supervisor o Jefe Inmediato la solicitud para la asignación de un usuario y contraseña de acceso a los repositorios oficiales, mediante el formato TI-F-034 administración de usuarios, el cual se adjuntia en un caso de la mesa de servicios, en caso de no solicitar estos accesos los colaboradores no podrán acceder a repositorios de la Entidad. Evidencia: casos aranda categoría manejo de cuentas.	SISTEMA INTEGRADO DE GESTIÓN Y MEJORA, Numeral 8 Anexo, Politicas complementarias, 8. POLÍTICA DE CONTROL DE ACCESO Y USO DE CONTRASEÑA$4 POLÍTICA DE RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN				Confiable	Resuelven oportunamente																		
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS										Con el fin de asegurar los servicios de red, cada vez que se generan alarmas de accesos no autorizados a la red, o anomalías del tráfico malicioso sospechoso, las herramientas de seguridad informática validan o bloquean de acuerdo con las políticas configuradas por el profesional de la oficina informática. En los casos donde no se logre bloquear se generan reportes y el Profesional Oficina Informática realiza las remediaciones correspondientes. Evidencia: Reportes de las herramientas de seguridad informática.	MC-M-001 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN Y MEJORA, Numeral 8 Anexo, Politicas complementarias, 5. POLÍTICA DE USO DE LA INFRAESTRUCTURA TECNOLÓGICA	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	\\172.16.0.235\colsoft\Operación\	100	FUERTE	10													
GESTIÓN DOCUMENTAL	INFORMACION DATO	Información dato que reposa en los archivos de gestión y en el archivo central de Grupo Centro de gestión documental y Correspondencia.	PERDIDA DE CONFIDENCIALIDAD	RSI-002-GD-	Acceso no restringido a los archivos de gestión y la inadecuada capacidad de gestión pueden ser afectadas por el acceso físico no autorizado, lo que generaría perdida de la confidencialidad, disponibilidad e integridad de la información.	ACCESO NO RESTRINGIDO A INSTALACIONES	ACCESO FÍSICO NO AUTORIZADO	Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4	No			RARA VEZ	MAYOR	Alta	El Técnico de Gestión Documental realiza una verificación mensual a las bodegas del Grupo Centro de Gestión Documental y correspondencia, con el objetivo de realizar control y seguimiento al cumplimiento de los estándares definidos por la normatividad archivística, mediante el diligenciamiento del formato GD-F-002 Sistema Integrado de Conservación visita técnica a bodegas externas a los siguientes aspectos: 1. estructura, 2. condiciones ambientales, 3.distribución,4. seguridad, 5.actividades de mantenimiento. En caso de que se presente alguna inconsistencia el técnico de Gestión Documental, deberá entregar un informe donde se encuentren las evidencias de incumplimiento al supervisor del contrato, para que así mismo se realice el debido requerimiento al contratista para que implemente las oportunidades de mejora. Las evidencias se encuentran en el respectivo expediente creado en Orfeo del contratista.	PLAN DE CONSERVACIÓN DOCUMENTAL DEL SISTEMA INTEGRADO DE CONSERVACIÓN. GD-F-002 Sistema integrado de Conservación visita técnica a bodegas externas	Asignado	Adecuado	Oportuna	Detectar	No confiable	Se investigan y resuelven oportunamente	Incompleta	Expediente en Orfeo 2020529221700003E	75	DÉBIL	5	MODERADO	NO DISMINUYE	NO DISMINUYE	RARA VEZ	MAYOR	Alta	REDUCIR	GESTIÓN DOCUMENTAL	AP-GD-008	se realizara seguimiento para prevenir que se materialice el riesgo para la seguridad de la información.	Eficacia de las acciones relacionadas con gestión de riesgos de seguridad de la información.
						INADECUADA CAPACIDAD DE GESTIÓN		Afectación de disponibilidad	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.	4																															
GESTIÓN FINANCIERA	INFORMACION DATO	INFORMACIÓNDATO Y SOFTWARE	PERDIDA DE CONFIDENCIALIDAD	RSI-004-0	ACCESO NO AUTORIZADO AL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA (SIIF NACIÓN), QUE PUEDE IMPACTAR EN EL USO INADECUADO DE LA INFORMACIÓN Y EL CUMPLIMIENTO DE LOS OBJETIVOS DEL PROCESO, LO QUE GENERARÍA LA PÉRDIDA DE LA INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de disponibilidad	Leve.	2	No			RARA VEZ	MAYOR	Alta	Cada vez que se requiera crear, modificar o eliminar un usuario en el sistema de información SIIF Nación, el líder de proceso solicita al coordinador o delegado responsable del sistema de información los privilegios o cambios requeridos con el fin de asegurar el acceso y la gestión de información de la entidad. De acuerdo con los lineamientos establecidos en el decreto 1068 de 2015 del Ministerio de Hacienda, cuando se trata de creación de usuarios se realiza la solicitud por la página web, se imprime el formulario y se hace firmar por el usuario, el jefe inmediato y el coordinador de SIIF Nación y se envía por la sede electrónica, cuando se trate de modificación, actualización, corrección o eliminación, el coordinador o el delegado lo hará directamente en la plataforma a través del correo electrónico. Como evidencia se tienen los formatos diligenciados y los correos electrónicos relacionados con dichas solicitudes.	Decreto 1068 de 2015 del Ministerio de Hacienda	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Incompleta	Correo electrónico - Físico	95	MODERADO	5	MODERADO	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MODERADO	Moderada	REDUCIR	GESTIÓN FINANCIERA	AP-GF-009	Fortalecer el control del riesgo.	Eficacia de las acciones relacionadas con gestión de riesgos de seguridad de la información.
						FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO		Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4																																	
						INFORMACIÓN DISPONIBLE PARA		Afectación de Integridad	Afectación grave de la	4																															

						PERSONAS NO AUTORIZADAS			Integridad de la información debido al interés particular de los empleados y terceros																																
INTERVENCIÓN	INFORMACION / DATO	Información/Dato	PERDIDA DE CONFIDENCIALIDAD	RSI-004-IT	Alteración, eliminación o intento de modificación no autorizada de la información que posee de sus entidades Intervenidas con las siguientes vulnerabilidades: (ii) INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS (ii); INADECUADOS DERECHOS DE USUARIO, que pueden ser afectadas por la fuga o revelación de información, lo que generaría afectación en su confidencialidad, integridad y disponibilidad.	INADECUADOS DERECHOS DE USUARIO	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4	No			RARA VEZ	MAYOR	Alta	La Directora de Entidades Intervenidas y en Liquidación cada vez que ingresa un colaborador a la Dirección realiza la solicitud de creación o activación de usuarios mediante el formato TI-F-034 "Administración de usuarios" para asegurar la correcta gestión de los usuarios a los diferentes repositorios de información (Orfeo, FileServer y Siagestión), en caso de no solicitar esos accesos los colaboradores no podrán acceder ni estarán autorizados a dichos repositorios ni a los sistemas de información, para lo anterior se crean casos en la plataforma Aranda directamente desde el usuario autorizado (Directora).	TI-F-034 - Administración de usuarios.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	Herramienta Mesa de Ayuda: http://mesadeayuda.superservicios.gov.co	100	FUERTE	10		FUERTE	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MENOR	Baja	ACEPTAR				Eficacia de las acpm relacionadas con gestión de riesgos de seguridad de la información.
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS		Afectación de disponibilidad	Leve.	2																															
MEJORA INTEGRAL DE LA GESTIÓN INSTITUCIONAL	INFORMACION / DATO	INFORMACIÓN / DATO	PERDIDA DE CONFIDENCIALIDAD	RSI-001-MC	INADECUADA GESTIÓN DE USUARIOS PARA EL ACCESO A LA PLATAFORMA SIGME, QUE PUEDE IMPACTAR EN EL ACCESO INDEBIDO DE PERSONAS NO AUTORIZADAS, LO QUE GENERARÍA LA PÉRDIDA DE LA INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	No			RARA VEZ	MAYOR	Alta	Cada vez que se requiera crear, modificar o eliminar un usuario en la plataforma SIGME, el líder de proceso solicita al administrador vía correo electrónico los privilegios o cambios requeridos con el fin de asegurar el acceso. En caso de requerir correcciones a la solicitud, el líder del proceso reenvía el correo y se comunica con el administrador de la plataforma SIGME. Como evidencia se tienen los correos electrónicos de radicación de la solicitud.	No existe documentación interna asociada.	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Se investigan y resuelven oportunamente	Completa	Correos Administrador Sigme - sigmeadmin@superservicios.gov.co	100	FUERTE	10		FUERTE	DIRECTAMENTE	INDIRECTAMENTE	RARA VEZ	MODERADO	Moderada	REDUCIR	MEJORA INTEGRAL DE LA GESTIÓN INSTITUCIONAL	AP-MC-011	Fortalecer el control del riesgo.	Eficacia de las acpm relacionadas con gestión de riesgos de seguridad de la información.
						CUENTAS DE USUARIO, GENERADAS POR SISTEMA CUYAS CONTRASEÑAS PERMANECEN SIN MODIFICACIÓN		Afectación de Integridad	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros	4																															
						FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO																																			
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS																																			
PARTICIPACIÓN Y SERVICIO AL CIUDADANO	INFORMACION / DATO	Información / Dato	PERDIDA DE CONFIDENCIALIDAD	RSI-003-PS	FUGA O REVELACIÓN DE INFORMACIÓN DE DATOS PERSONALES DE AQUELLOS USUARIOS QUE ASISTEN A LAS DIFERENTES ACTIVIDADES DE PARTICIPACIÓN CIUDADANA, DEBIDO A QUE LA INFORMACIÓN SE ENCUENTRA DISPONIBLE PARA PERSONAL NO AUTORIZADO, LO QUE PODRÍA GENERAR UNA AFECTACIÓN GRAVE A LA CONFIDENCIALIDAD DE LA INFORMACIÓN.	INADECUADOS DERECHOS DE USUARIO	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4	No			RARA VEZ	MAYOR	Alta	Cada vez que se requiera crear un expediente en ORFEO por la realización de una actividad de participación ciudadana, el encargado de documentar la actividad activará la opción de privado de acuerdo con la guía de ayuda No. 17 Instructivo de seguridad para Expedientes y Radicados, con el fin de proteger los datos personales de los ciudadanos. En caso que no se active la opción, el personal encargado de participación ciudadana de la DGT, revisa que ésta sea activada. La evidencia se encuentra en las bases de datos de PS-F-008 y PS-F-007 y en los seguimientos de la DGT.	Guía de ayuda No. 17 Instructivo de seguridad para expedientes y radicados	Asignado	Adecuado	Oportuna	Prevenir	No confiable	Se investigan y resuelven oportunamente	Completa	https://docs.google.com/spreadsheets/d/10jdsx4Xj9wJLVJokExGAlIAKB5VR1rN7/edit?rtpof=true&sd=835706583	85	DÉBIL	10		MODERADO	DIRECTAMENTE	DIRECTAMENTE	RARA VEZ	MODERADO	Moderada	REDUCIR	PARTICIPACIÓN Y SERVICIO AL CIUDADANO	AP-PS-008	Fortalecimiento del control	Eficacia de las acpm relacionadas con gestión de riesgos de seguridad de la información.
						INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS		Afectación de disponibilidad	Leve.	2																													
						NIVEL DE CONFIDENCIALIDAD NO DEFINIDO CON CLARIDAD		Afectación de Integridad	Leve.	2																															
						REGLAS PARA CONTROL DE ACCESO NO DEFINIDOS CON CLARIDAD																																			

/