Superservicios
Superintendencia de Servicios Públicos Domiciliarios

MAPA DE RIESGOS 26/04/2022

SIGME

Proceso/Subproceso: TODOS LOS PROCESOS

Objetivo Proceso/Subproceso: N/A

IDENTIFICACIÓN DEL RIESGO / RIESGO INHERENTE

Proceso / Subproceso	Objetivo Estratégico	Objetivo del Proceso / Objetivo Estratégico	Estado Riesgo	Fecha cambio de estado	Tipo de Activo	Nombre de Riesgo	Tipo de Riesgo	Codigo de Riesgo	Descripción de Riesgo	Vulnerabilidades	Amenaza	Consecuencias: Consecuencia	Consecuencias: Grado de impacto	Consecuencias: Valor de impacto	¿Se ha Materializado el Riesgo?	Descripción de Materialización	Frecuencia de la Materialización	Riesgo Inherente: Probabilidad Descripcion	Riesgo Inherente: Impacto Descripcion	Zona
COMUNICACIONES	Objetivo Estratégico	Divulgar a través de los medios de comunicación disponibles, en forma oportuna y confiable, las políticas, planes, programas, proyectos y resultados de la gestión de la Superintendencia de Servicios Públicos Domiciliarios a sus diferentes públicos de interés, para contribuir al posicionamiento de la entidad y al logro de los objetivos institucionales.	APROBADO	15/02/2022 11:11:37 a.m.	INFORMACION / DATO	Información / Dato	PERDIDA DE CONFIDENCIALIDAD	RSI-004-CO	Posibilidad de 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 moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.	3	No		La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	MODERADO	Moderada
										EQUIPAMIENTO MÓVIL PROCLIVE A SER ROBADO		Afectación de disponibilidad	Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros	3						
										INADECUADOS DERECHOS DE USUARIO		Afectación de Integridad	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros	3						
										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 DISCIPLINARIO INTERNO	Objetivo Estratégico	Conocer y fallar los procesos disciplinarios que se adelanten contra servidores y ex-servidores públicos de la Superintendencia de Servicios Públicos Domiciliarios, aplicando los procedimientos y términos establecidos en la Ley 734 de 2002, a fin de preservar el correcto desarrollo de la función pública.	APROBADO	25/02/2022 2:54:03 p.m.	INFORMACION / DATO	INFORMACIÓN DATO	PERDIDA DE CONFIDENCIALIDAD	RSI-003-CD	Posibilidad de alteración, eliminación o intento de modificación no autorizada de la información que posee la OCDI con las siguientes vulnerabilidades: (i); INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS (ii); INADECUADOS DERECHOS DE USUARIO, (iii) ACCESO NO RESTRINGIDO A INSTALACIONES (iv) FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO POR RETIRO, que pueden ser afectadas por la fuga o revelación de información, lo que generaría afectación en su confidencialidad, integridad y disponibilidad	ACCESO NO RESTRINGIDO A INSTALACIONES	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Sin afectación.	1	No		La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	LEVE	Moderada
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS		Afectación de disponibilidad	Sin afectación.	1						
										INADECUADOS DERECHOS DE USUARIO		Afectación de Integridad	Sin afectación.	1						
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO										
DIRECCIONAMIENTO ESTRATÉGICO	Objetivo Estratégico	Formular los instrumentos de planeación de corto, mediano y largo plazo, articulados con las prioridades del Gobierno Nacional y sectoriales y las necesidades, expectativas y requisitos de las partes interesadas pertinentes, para la atenciónoportuna, eficaz y eficiente de los servicios y de las funciones asignadas a la Superservicios.	APROBADO	10/03/2022 5:12:19 p.m.	SOFTWARE	SISTEMAS DE INFORMACIÓN INTERNOS Y EXTERNOS DE OAPII	PERDIDA DE CONFIDENCIALIDAD	RSI-003-DE	Posibilidad de acceso no autorizado a los sistemas de información debido a una inadecuada gestión de contraseñas inseguras, cuentas de usuario generadas por sistema cuyas contraseñas permanecen sin modificación, falta de desactivación de cuentas de usuario luego de finalizado el empleo o información disponible para personas no autorizadas, lo que podría generar una afectación a la confidencialidad, integridad y disponibilidad de la información.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Sin afectación.	1	No		La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	LEVE	Moderada
										CUENTAS DE USUARIO GENERADAS POR SISTEMA CUYAS CONTRASEÑAS PERMANECEN SIN MODIFICACIÓN		Afectación de disponibilidad	Sin afectación.	1						
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO		Afectación de Integridad	Sin afectación.	1						
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS										
GESTIÓN ADMINISTRATIVA Y LOGÍSTICA	Objetivo Estratégico	Gestionar los servicios administrativos y los bienes muebles e inmuebles necesarios para la operación de la Superservicios.	APROBADO	22/02/2022 7:09:34 a.m.	HARDWARE	Planta eléctrica de la sede principal ubicada en la ciudad de Bogotá D.C	PERDIDA DE DISPONIBILIDAD	RSI-003-GA	Posibilidad de falla en el funcionamiento de la planta eléctrica que podría generar intermitencia o cortes en el suministro eléctrico en el suministro eléctrico y perdida de la disponibilidad de la información	MANTENIMIENTO INADECUADO	ERRORES DE MANTENIMIENTO	1. AFECTACIÓN ECONÓMICA	Menor o igual al 0.5% del presupuesto general asignado a la entidad	1	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	MENOR	Moderada
										USO DE EQUIPAMIENTO OBSOLETO		2. REPUTACIONAL	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	2						
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	N/A	Desarrollar la estrategia de tecnologías de la información (TI) a través de la implementación del portafolio de proyectos y servicios de TI, para la generación de valor público, el cumplimiento del direccionamiento estratégico y de las funciones legales de la Superintendencia de Servicios Públicos Domiciliarios.	APROBADO	22/02/2022 7:11:07 a.m.	SOFTWARE	SISTEMAS DE INFORMACION ASOCIADOS AL PLAN DE BACK	PERDIDA DE DISPONIBILIDAD	RSI-008-03	Posible afectación a la disponibilidad de los sistemas de información por inadecuadas estrategias de respaldo y restauración.	COPIADO SIN CONTROL	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de disponibilidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	MENOR	Moderada
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Objetivo Estratégico	Desarrollar la estrategia de tecnologías de la información (TI) a través de la implementación del portafolio de proyectos y servicios de TI, para la generación de valor público, el cumplimiento del direccionamiento estratégico y de las funciones legales de la Superintendencia de Servicios Públicos Domiciliarios.	APROBADO	22/02/2022 7:12:28 a.m.	REDES	REDES E INFRAESTRUCTURA TECNOLÓGICA DE LA ENTIDAD	PERDIDA DE CONFIDENCIALIDAD	RSI-009-03	Posibilidad de acceso no autorizado a la red, debido a las siguientes vulnerabilidades i)REGLAS PARA TRABAJO AFUERA DE LAS INSTALACIONES NO DEFINIDAS CON CLARIDAD ii)DESCARGAS DE INTERNET SIN CONTROL iii) CONEXIONES DE RED PÚBLICA SIN PROTECCIÓN iv)INADECUADA GESTIÓN DE REDES, lo que generaría perdida de confidencialidad, disponibilidad e integridad de la información.	REGLAS PARA TRABAJO AFUERA DE LAS INSTALACIONES NO DEFINIDAS CON CLARIDAD	ACCESO NO AUTORIZADO A LA RED	Afectación de confidencialidad	Sin afectación.	1	No		La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	MEDIA	MENOR	Moderada
										DESCARGAS DE INTERNET SIN CONTROL		Afectación de disponibilidad	Leve.	2						

VALORACIÓN CONTROLES / RIESGO RESIDUAL / TRATAMIENTO DEL RIESGO / INDICADORES / SEGUIMIENTOS

Codigo de Riesgo	Dominio	Objetivo	Nombre del Control	Descripción del Control	¿El control se encuentra documentado?	¿Cual es la frecuencia en que se aplica el control?	¿El control permite evidencia de su ejecución?	Nombre 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 Proposito del Control?	¿Cómo se Realiza la Actividad de Control?	¿Qué Pasa con las Observaciones o Desviaciones?	¿Existen Evidencia de la Ejecución del Control?	¿De que manera se implementa el control?	Riesgo Residual: Probabilidad Descripcion	Riesgo Residual: Impacto Descripcion	Zona	Opciones de Manejo del Riesgo Residual	Proceso	Código	Justificación de Manejo	Indicador	Seguimientos Lider	Seguimientos OAPII
RSI-004-CO	A.16. GESTIÓN DE INCIDENTES.	A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A.16.1.2 REPORTE DE 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 GIC-I-004 - Instructivo para la gestión de incidentes de seguridad y privacidad de la información; a través de la herramienta de Gestión de Servicios Tecnológicos (Mesa de ayuda - Aranda) para su análisis y tratamiento. El responsable del canal atenderá las orientaciones de la Mesa de Ayuda. 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 Tecnologías de la Información y las Comunicaciones y/o la Oficina Asesora de Planeación e Innovación Institucional; y generar las actuaciones administrativas que tenga previstas la entidad, según cada caso en particular. Evidencia: Casos Aranda - Categoría manejo de incidentes.	Documentado	Continua	Con registro	GIC-I-004 - Instructivo para la gestión de incidentes de seguridad y privacidad de la información	Asignado	Adecuado	Oportuna	Correctivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	BAJA	MODERADO	Moderada	REDUCIR	COMUNICACIONES	AP-CO-006	Fortalecimiento de controles	Incidentes que afectan la seguridad y privacidad de la información	1. 18/04/2022 Creada por: [DIEGO FELIPE CASTIBLANCO CARVAJAL] - NO se ha materializado el riesgo - En el primer trimestre no se materializó el riesgo. Se aplicaron los controles definidos en el mapa de riesgos. Se solicitó apertura de aplicativos por el ingreso de nuevos funcionarios y contratistas. Se dio trámite a los correos sospechosos recibidos en diferentes cuentas. Se estableció mecanismo para seguimiento de cambio trimestral de contraseñas de correos y aplicativos de divulgación a cargo de la oficina. Evidencias de casos Arandas, reporte de correos electrónicos sospechosos y cambio trimestral de contraseñas en https://drive.google.com/drive/folders/1mf7HpLp5eReQmolMdE4KGI85rStdaade?usp=sharing.	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se realizó el seguimiento trimestral a los controles A.16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN, A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS y A.9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS, que se encuentran identificados en el riesgo de seguridad digital para el proceso de Comunicaciones RSI-004-CO y se constató lo siguiente: - El líder del proceso realizó el seguimiento al riesgo y la publicación de evidencias de los controles de manera oportuna. - Durante el periodo se reportaron eventos de seguridad de la información relacionados con phishing. - Se revisaron los casos ARANDA relacionados en el reporte y se evidencia el correcto diligenciamiento del formato TI-F-034.
	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	Cada vez que ingresa o se retira un funcionario o contratista de la Oficina Asesora de Comunicaciones, el líder del proceso solicita a la Oficina de Tecnologías de la Información y las Comunicaciones 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). 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 Dirección de Talento Humano o el Grupo de Contratos y Adquisiciones no expedirá el respectivo paz y salvo para formalizar dicho retiro. Evidencia: Casos Aranda.	Documentado	Continua	Con registro	Manual de Servicios Tecnológicos TI-M-002, el Instructivo TI-I-013 Gestión de Usuarios. Formato TI-F-034 Administración de usuarios y Formato TI-F-035 Solicitud y autorización de acceso a la red LAN para colaboradores.	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual										
	A.9. CONTROL DE ACCESO.	A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A.9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	Trimestralmente, los funcionarios encargados de la administración de canales de divulgación a cargo de la Oficina Asesora de Comunicaciones, que requieran usuario y contraseña de acceso, deberán aplicar los criterios definidos en el Manual de Divulgación Institucional CO-M-003, numeral 6.1.3 Protocolos básicos de seguridad de la información en los canales de divulgación, literal a) Gestión de acceso, privacidad y contraseñas, en lo relacionado con cambio y seguridad de contraseñas.	Documentado	Continua	Con registro	Manual de Divulgación Institucional CO-M-003	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	No existe	Manual										
RSI-003-CD	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	La Jefe de la Oficina de Control Disciplinario Interno cada vez que ingresa un colaborador a la Oficina 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, SIGME y Sisgestión), 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 para lo anterior se crean casos en la plataforma Aranda directamente desde el usuario autorizado (Jefe de Oficina). Evidencia: Casos Aranda.	Documentado	Continua	Con registro	TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS y TI-F-034 "Administración de usuarios"	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	BAJA	LEVE	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 8/04/2022 Creada por: [MAGDA YANETH CASTAÑEDA GUTIERREZ] - NO se ha materializado el riesgo - En el período no ingresaron nuevos colaboradores a la dependencia, por lo que no fue necesaria el diligenciamiento del formato.	1. 18/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se realizó el seguimiento trimestral al control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS que se encuentra identificado en el riesgo de seguridad digital para el proceso de Control Disciplinario Interno y se constató lo siguiente: - El líder del proceso realizó el seguimiento al riesgo de manera oportuna. - Durante el periodo no se reportaron solicitudes a la mesa de servicios de acuerdo a lo verificado directamente en la herramienta Aranda.
RSI-003-DE	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	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.	Documentado	Continua	Con registro	Instructivo para la Formulación y Seguimiento a la Planeación Institucional - Código DE-I-001 Versión 13 Julio 2021, numeral 3.3 SOLICITUD DE ACCESO A LOS APLICATIVOS EXTERNOS E INTERNOS	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	BAJA	LEVE	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 20/04/2022 Creada por: [LIDA CONSTANZA CUBILLOS HERNANDEZ] - NO se ha materializado el riesgo - No se ha materializado el riesgo. Durante el primer trimestre de la vigencia, se atendieron once (11) solicitudes de creación de usuarios y asignación de roles en el Sistema para la Formulación y Seguimiento a la Planeación Institucional - SisGestión, los cuales corresponden a perfil de jefe de oficina, usuario para registro del plan, y usuarios de consulta para la Oficina de Control Interno Evidencia https://drive.google.com/drive/u/0/folders/1mxUW0-QRNmx9q9wOttvByq0vgaYB2zlx Durante este primer semestre no se crearon o eliminaron usuarios del SPI y SUIFP.	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS para este primer trimestre de 2022, asociado al sistema de información SISGESTIÓN, y se constató el cumplimiento del control con las evidencias presentadas.
	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	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 e Innovación Institucional 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.	Documentado	Continua	Con registro	DE-M-003 MANUAL DEL USUARIO DEL SISTEMA PARA LA FORMULACIÓN Y SEGUIMIENTO A LA PLANEACIÓN INSTITUCIONAL SISGESTION - Numeral 5.1 Ingreso al aplicativo.	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual										
RSI-003-GA	A.11. SEGURIDAD FÍSICA Y DEL ENTORNO.	A.11.1 ÁREAS SEGURAS	A.11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	Anualmente el coordinador de servicios administrativos para la sede ubicada en la ciudad de Bogotá, Calle 84 de acuerdo a lo estipulado en el manual de servicios administrativos e instalaciones GA-M-001, dentro de su planeación establecen los contratos de mantenimiento requeridos para el buen funcionamiento de las plantas eléctricas y tableros de eléctricos que se encuentran instaladas en la sede de la ciudad de Bogotá, Calle 84 con el propósito de garantizar el buen estado y funcionamiento de dichos equipos especializados. En dado caso de que no se pueda efectuar el proceso de contratación la entidad analizara alternativas para suplir la prestación del servicio de mantenimiento preventivo a las plantas de la entidad. Las evidencias estarán registradas en los expedientes de los respectivos contratos	Documentado	Continua	Con registro	GA-M-001 MANUAL SERVICIOS ADMINISTRATIVOS E INSTALACIONES	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 19/04/2022 Creada por: [DIANA MARCELA NIÑO TAPIA] - NO se ha materializado el riesgo - El día 18 de marzo del 2022 se adjudico el contrato para le mantenimiento de plantas eléctricas de la sede principal Calle 84, cuyo objeto es: ""Prestar el servicio de mantenimiento preventivo y correctivo de equipos de presión, equipos de bombeo de agua potable, equipo eyector, planta eléctrica de emergencia y puerta eléctrica de parqueadero, así como el lavado de los tanques de almacenamiento de agua potable y tanque pozo eyector, planta eléctrica de emergencia y puerta eléctrica de parqueadero, así como el lavado de los tanques de almacenamiento de agua potable y tanque pozo eyector de la sede principal de la Superservicios en la ciudad de Bogotá D.C". De acuerdo a lo definido en las obligaciones del contrato se encuentra pendiente por parte del proveedor GPS ELECTRONICS LTDA remitir el cronograma de mantenimientos de equipo. Finalmente se encuentra pendiente la adjudicación del contrato para el mantenimiento de tableros eléctricos el cual esta programado para el mes de abril. Ver Documento	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES para este primer trimestre de 2022, asociado a la adjudicación del contrato para el mantenimiento de plantas eléctricas de la sede principal de la calle 84, y se constató el cumplimiento del control con las evidencias presentadas.
	A.11. SEGURIDAD FÍSICA Y DEL ENTORNO.	A.11.1 ÁREAS SEGURAS	A.11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	El profesional encargado del apoyo a la supervisión del contrato de mantenimiento de planta eléctrica, realizará seguimiento trimestral al desarrollo de las actividades para el mantenimiento preventivo y correctivo definidas por el contratista en el cronograma de trabajo, el cual se consignará en formato de control de asistencia junto con los soportes que evidencien el desarrollo de las actividades. En el momento de identificarse desviaciones en el desarrollo del control se enviara comunicado oficial al contratista por posible incumplimiento.	Documentado	Continua	Con registro	GA-M-001 MANUAL SERVICIOS ADMINISTRATIVOS E INSTALACIONES	Asignado	Adecuado	Oportuna	Detectivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual										
RSI-008-03	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.3 COPIAS DE RESPALDO	A.12.3.1 RESPALDO DE LA INFORMACIÓN	Con el fin de mantener la disponibilidad de la información actualizada en los sistemas de información, el profesional de OTIC, encargado de realizar las copias de respaldo de la información, programa a demanda las políticas en la herramienta de backup de acuerdo a la periodicidad establecida en el plan de backup, Desviación: En caso que se identifique en la herramienta de backup que un respaldo en un servidor no fue ejecutado se toman las acciones pertinentes. evidencia: Informe de Backup	Documentado	Continua	Con registro	TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico	BAJA	MENOR	Moderada	REDUCIR	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	AP-TI-013	Se crea ACPM para fortalecer los controles definidos para el riesgo	Incidentes que afectan la seguridad y privacidad de la información	1. 12/04/2022 Creada por: [DANIEL JOAQUIN RODRIGUEZ MORALES] - NO se ha materializado el riesgo - Durante los meses de enero, febrero y marzo se han afinado las políticas correspondientes, para mayor información https://drive.google.com/drive/folders/1qjbPTHVd_3sv5jruBxhSqJiVLnBQNRc1?usp=sharing.	1. 18/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS y se constató su cumplimiento con las evidencias presentadas para el primer trimestre de 2021, no obstante, se recomienda incluir en los siguientes reportes, las acciones tomadas cuando se presentó la novedad "Number of Failed Jobs", de acuerdo a como está descrito el control.
RSI-009-03	A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A.13.1.1 CONTROLES DE REDES	Control 1. Cada vez que se requiera un acceso a red LAN se recibe a traves de la mesa de servicio el caso con el formato (TI-F-035 para funcionarios y contratistas ó en el TI-F-043 para contratos externos) debidamente diligenciado por el Jefe o Supervisor, esta solicitud es revisada por la Oficina Informática para su aprobación, pasa a la mesa de servicio para la gestión y creación de la vpn, La mesa de servicio identifica en los formatos (TI-F-035 /TI-F-043) la fecha de vencimiento para configurar hasta cuando estará activa conexiones externas por VPN, asi mismo el Especialista networking realiza las configuraciones a los accesos requeridos por el usuario y mensualmente verifica el estado de las VPN configuradas. Se le informa a los usuarios teletrabajadores al final de año que en la nueva vigencia deberan formalizar la continuidad de la VPN en TI-F-035. Sin embargo, los usuarios teletrabajadores /funcionarios/contratistas para las VPNs están controlados por directorio activo, por lo que si se llegase a presentar un retiro de la entidad este sería deshabilitado y no podría conectarse a los recursos de la entidad. Evidencia: Casos de Aranda. Informe de gestion mensual. El control se califica como no confiable porque no cubre la totalidad de los colaboradores que trabajan de forma remota.	Documentado	Continua	Con registro	TI-M-002 Manual de Servicios Tecnológicos	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 21/04/2022 Creada por: [DANIEL JOAQUIN RODRIGUEZ MORALES] - NO se ha materializado el riesgo - Se ha realizado la gestión pertinente para dar acceso a 145 colaboradores a traves de VPB, para mayor detalle se adjunta el archivo. Ver Documento 2. 25/04/2022 Creada por: [DANIEL JOAQUIN RODRIGUEZ MORALES] - NO se ha materializado el riesgo - A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS, se reporta el reporte del ENR para el primer trimestre. Ver Documento 3. 25/04/2022 Creada por: [DANIEL JOAQUIN RODRIGUEZ MORALES] - NO se ha materializado el riesgo - A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS, se crea caso con STS para corregir la revisión de codigo malisioso en los archivos adjuntos en formatos pdf excel y word del correo institucional. Se actualiza firmware de fortimail y se realizan pruebas para verificar que funciona correctamente. Ver Documento 4. 25/04/2022 Creada por: [DANIEL JOAQUIN RODRIGUEZ MORALES] - NO se ha materializado el riesgo - A.12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS, se adjunta el informe en el cual se relaciona los filtros de seguridad aplicados para revisión de todo el trafico que pasa por cada una de las aplicaciones, verificado por el WAF. Ver Documento	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.13.1.1 CONTROLES DE REDES para este primer trimestre de 2022, asociado a la gestión de VPN y de acuerdo con la evidencia publicada se constató que se gestionaron 109 solicitudes con fecha de corte 31 de marzo de 2022.
	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	Control 2. Cada vez que se configura un equipo propio de SSPD, la mesa de ayuda instala el antivirus y el EDR (Endpoint Detection and Response). El antivirus brinda protección para detectar y eliminar el 'malware', mediante un escaneo completo una vez a la semana y siempre que se conecte a una unidad externa. Y si no logra eliminar el virus lo coloca en cuarentena. El EDR Proporciona protección contra malware y otro tipo de ataques más sofisticados que el antivirus no puede detectar: como rootkits, ataques de día cero y spyware que se transforma. Protege a cada equipo donde está instalado toda la cadena de ataque usando las siguientes etapas: intromisión, infección, invasión y extracción, y reparación e inoculación, basándose en inteligencia artificial. Desviación: si el antivirus no detecta un malware, es muy probable que la capa adicional EDR si lo haga. Si ninguno de los dos	Documentado	Continua	Con registro	DE-M-004 MANUAL DE POLÍTICAS COMPLEMENTARIAS DEL SIGESPI , POLITICA .5.14	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico										

																								lo hace, existen dos controles en la capa de red: SIEM e IDS que pueden detectar comportamientos anómalos. Evidencia: Informe de consola del antivirus y consola del EDR donde se observa que estén instalados en todos los equipos de la SSPD y funcionando, y también se evidencia el malware detectado y su tratamiento.																						
										CONEXIONES DE RED PUBLICA SIN PROTECCIÓN		Afectación de Integridad	Leve.	2							A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	Control 3. Cada vez que ingresa o sale un correo de la red de la SSPD el Fortimail realiza la inspección de salida o entrada para detectar spam, malware o correos maliciosos, analizando cada correo frente a listas negras (palabras o direcciones de correo). El administrador de la plataforma de correo es responsable de configurar el del Fortimail. Cuando los correos contienen archivos adjuntos el Fortimail determina de forma automática, dependiendo de la configuración de la herramienta cuales son sospechosos y los envía a la herramienta Fortisandbox en nube. Si el archivo ya ha sido reconocido como malicioso no deja pasar el correo, si es un archivo sospechoso nuevo, observa cómo se comporta en un ambiente controlado, y si determina que es malicioso no deja pasar el correo.La evidencia de Fortimail y Fortisanbox se puede consultar directamente en el SaaS por internet en la opción de pistas de auditoría. En caso de desviación, es decir si el Fortimail deja pasar un correo sospechoso, los usuarios lo reportan y el rol de analista de seguridad informática gestiona el incidente. Evidencia: Informes de configuración de Fortimail y casos de aranda por reporte de incidentes en caso de presentarse	Documentado	Continua	Con registro	DE-M-004 MANUAL DE POLÍTICAS COMPLEMENTARIAS DEL SIGESPI , POLITICA .5.12	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico										
										INADECUADA GESTIÓN DE REDES											A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	A.12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	El profesional de la OTIC solicita a demanda la integración de los portales web públicos o internos de la Entidad sobre la solución de aplicaciones web (WAF IMPERVA) la finalidad de esta funcionalidad evitar denegaciones de servicios, fuga de información o alteración de los portales web. Desviación: una vez se reportan las alertas y los informes, se analizan y si es el caso se realizan los cambios en la configuración de los servicios web. Evidencia: Cambios HGSTI	Documentado	Continua	Con registro	DE-M-004 MANUAL DE POLÍTICAS COMPLEMENTARIAS DEL SIGESPI , POLITICA DESARROLLO SEGURO - INFRAESTRUCTURA	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico										
GESTIÓN DEL TALENTO HUMANO	Objetivo Estratégico	Liderar y ejecutar las actividades propias de las administración y gestión del talento humano, aplicando la normatividad vigente y los procedimientos establecidos en la entidad para contribuir a la consecución de los objetivos institucionales.	APROBADO	25/02/2022 7:56:45 a.m.	SOFTWARE	Software de la Dirección de Talento Humano (hojas de cálculo y sistema de información de nómina)	PERDIDA DE CONFIDENCIALIDAD	RSI-004-01	Posibilidad de interrupción de los servicios de software de la Dirección de Talento Humano por instalación de mejoras o actualizaciones que pueden generar afectación en la disponibilidad de la información.	INADECUADA CAPACIDAD DE GESTIÓN	MODIFICACIÓN ACCIDENTAL DE DATOS DEL SISTEMA DE INFORMACIÓN	1. AFECTACIÓN ECONÓMICA	Menor o igual al 0.5% del presupuesto general asignado a la entidad	1	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	LEVE	Baja	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A.12.1.2 GESTIÓN DE CAMBIOS	La Coordinadora del grupo de Nómina y Seguridad Social cada vez que se requiera realizan la actualización o modificación de las bases de datos y software de nómina ,de acuerdo con las novedades presentadas, con el propósito de mantener la información actualizada, para lo cual se realiza la solicitud a través de la plataforma de ayuda del aplicativo de nómina y las diferentes fuentes de información para la alimentación adecuada de las hojas de cálculo, en caso de identificar inconsistencias se realiza el ajuste pertinente. Las evidencias se encuentran en la plataforma de ayuda del aplicativo de nómina y correo electrónico	Sin documentar	Continua	Con registro	N.A	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	BAJA	LEVE	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 4/04/2022 Creada por: [GERALDINE GIRALDO MORENO] - NO se ha materializado el riesgo - El riesgo no se ha materializó, durante el primer trimestre de 2022, se implementó el control para lo cual se gestionaron 31 solicitudes, con el fin de mantener actualizada la información del aplicativo de nómina, de acuerdo a las necesidades del Grupo de Nómina y Seguridad Social. La evidencia del control se anexa en el siguiente archivo:. Ver Documento	1. 18/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.12.1.2 GESTIÓN DE CAMBIOS, para este primer trimestre de 2022, y se constató el cumplimiento de dicho control con la evidencia presentada.
										INADECUADO CONTROL DE CAMBIOS		2. REPUTACIONAL	El riesgo afecta la imagen de algún área de la organización.	1																																
GESTIÓN DOCUMENTAL	N/A	Orientar la realización de las actividades necesarias para la administración y conservación de los documentos producidos y recibidos por la entidad, aplicando la normatividad archivística, el sistema de gestión documental automatizado, garantizando la integridad y conservación de la información.	APROBADO	25/02/2022 9:56:05 a.m.	INFORMACION / DATO	Información que reposa en los archivos de gestión y en el archivo central físico y electrónico de Grupo Centro de gestión documental y Correspondendía.	PERDIDA DE CONFIDENCIALIDAD	RSI-003-GD	Acceso no restringido a instalaciones de almacenamiento de los archivos de gestión y central donde reposa el acervo documental de la Entidad, y la falta de desactivación de cuentas de usuario luego de finalizado el empleo; podría ocasionar pérdida de la confidencialidad,disponibilidad,e integridad de la información.	ACCESO NO RESTRINGIDO A INSTALACIONES	MODIFICACIÓN NO AUTORIZADA DE REGISTROS	Afectación de confidencialidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	MENOR	Moderada	A.11. SEGURIDAD FÍSICA Y DEL ENTORNO.	A.11.1 ÁREAS SEGURAS	A.11.1.2 CONTROLES DE ACCESO FÍSICOS	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 FORMATO DE INSPECCIÓN DE ALMACENAMIENTO E INSTALACIONES FÍSICAS DEL PLAN DE CONSERVACIÓN DOCUMENTAL.: 1. estructura, 2. condiciones ambientales, 3. distribución,4. seguridad. 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.	Documentado	Continua	Con registro	PLAN DE CONSERVACIÓN DOCUMENTAL DEL SISTEMA INTEGRADO DE CONSERVACIÓN. GD-F-002 Sistema integrado de Conservación visita técnica a bodegas externas	Asignado	Adecuado	Oportuna	Detectivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 11/04/2022 Creada por: [MAURICIO DE JESUS ARAQUE TEJADA] - NO se ha materializado el riesgo - A.11.1.2 CONTROLES DE ACCESO FÍSICOS: Durante el primer trimestre de la vigencia 2022 se realizo el diligenciamiento del formato GDF-002 donde se encuentra el cumplimiento de lo establecido en el Sistema Integrado de Conservación teniendo en cuenta el Acuerdo 06 del 2014. Donde se realizó inspección y seguimiento a los de acuerdo a lo definido en el Plan de Conservación Documental en: 1. estructura. 2. condiciones ambientales. 3. distribución.4. seguridad. El cual no se evidencio ninguna anomalía, cumpliendo con los criterios de conservación documental. Ver Documento 2. 11/04/2022 Creada por: [MAURICIO DE JESUS ARAQUE TEJADA] - NO se ha materializado el riesgo - A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS: Durante el primer trimestre de la vigencia 2022 se recepcionaron 298 solicitudes sobre Activación o Inactivación de usuarios de Orfeo II mediante el correo Orfeo@superservicios.gov.co, el cual 246 fueron solicitudes de activación o creación de usuarios y 52 Inactivaciones de Usuarios. Ver Documento 3. 25/04/2022 Creada por: [MAURICIO DE JESUS ARAQUE TEJADA] - NO se ha materializado el riesgo - Teniendo en cuenta el reporte anterior se publica el documento el cual complementa la inspección de las bodegas faltantes A.11.1.2 CONTROLES DE ACCESO FÍSICOS: Durante el primer trimestre de la vigencia 2022 se realizó el diligenciamiento del formato GDF-002 donde se encuentra el cumplimiento de lo establecido en el Sistema Integrado de Conservación teniendo en cuenta el Acuerdo 06 del 2014. Donde se realizó inspección y seguimiento a los de acuerdo a lo definido en el Plan de Conservación Documental en: 1. estructura. 2. condiciones ambientales. 3. distribución.4. seguridad. El cual no se evidencio ninguna anomalía, cumpliendo con los criterios de conservación documental. Ver Documento 4. 26/04/2022 Creada por: [MAURICIO DE JESUS ARAQUE TEJADA] - NO se ha materializado el riesgo - Teniendo en cuenta el reporte anterior se publica el documento el cual complementa la inspección de las bodegas de almacenamiento del acervo documental de la entidad. Ver Documento	
										INADECUADA CAPACIDAD DE GESTIÓN		Afectación de disponibilidad	Leve.	2							A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	El técnico administrativo del Grupo de Gestión Documental cada que se realice una solicitud por el correo electrónico orfeo@superservicios.gov.co de creación o inactivación de usuarios en el sistema de gestión documental deberá realizar la acción solicitada por el correo electrónico y notificará al solicitante el cumplimiento de la solicitud realizada.	Sin documentar	Continua	Con registro	Correo Electrónico	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual										
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS		Afectación de Integridad	Leve.	2																																
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO																																				
GESTIÓN FINANCIERA	Objetivo Estratégico	Dirigir la ejecución de la planeación, ejecución y control financiero de la Superservicios.	APROBADO	28/02/2022 3:07:39 p.m.	INFORMACION / DATO	INFORMACIÓN/DATO Y SOFTWARE	PERDIDA DE CONFIDENCIALIDAD	RSI-005-0	CONTRASEÑAS INSEGURAS, FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO, INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS PUEDE(N) SER AFECTADA(S) POR LA ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN, PUEDE OCURRIR PERDIDA DE CONFIDENCIALIDAD, PERDIDA DE DISPONIBILIDAD, PERDIDA DE INTEGRIDAD, LO QUE GENERARÍA LA AFECTACIÓN DE DISPONIBILIDAD, AFECTACIÓN DE CONFIDENCIALIDAD, AFECTACIÓN DE INTEGRIDAD	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	MENOR	Moderada	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	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. De igual manera el sistema de Información SIIF Nación tiene configurado inactivar todos los usuarios que se hayan autenticado en un tiempo mínimo de 15 días, Como evidencia se tienen los formatos diligenciados y los correos electrónicos relacionados con dichas solicitudes.	Documentado	Continua	Con registro	Decreto 1068 de 2015 del Ministerio de Hacienda	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Automatico	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 12/04/2022 Creada por: [PATRICIA EUGENIA GONZALEZ ROBLES] - NO se ha materializado el riesgo - NO SE MATERIALIZO el riesgo en el primer trimestre de la vigencia 2022,se lleva control con el líder de proceso mediante solicitud de los privilegios o cambios requeridos con el fin de asegurar el acceso y la gestión de información de la entidad., 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. https://drive.google.com/drive/u/3/folders/1QQm1IXHV2Vies3AuEgHJ6EkKvz97qSXV. Ver Documento	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se realizó el seguimiento del primer trimestre de 2022 al control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS, que se encuentra identificado en el riesgo de seguridad digital para el proceso de Gestión Financiera RSI-005-0 y se constató la gestión de los usuarios dentro de la plataforma SIIF, con todos los exigentes requerimientos por parte del Ministerio de Hacienda.
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO																																				
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS																																				
MEDIDAS PARA EL CONTROL	Objetivo Estratégico	Aplicar las medidas necesarias para controlar, normalizar y restablecer la prestación de los servicios públicos domiciliarios o conminar a las personas que los prestan a la mejora de las condiciones de la prestación.	APROBADO	25/02/2022 3:19:32 p.m.	INFORMACION / DATO	Repositorio y sistemas de información	PERDIDA DE CONFIDENCIALIDAD	RSI-002-CT	Posibilidad de fuga o revelación de información debido a la alteración, eliminación o intento de modificación no autorizada de la información que poseen las Superintendencias Delegadas con las siguientes vulnerabilidades: (i) INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS (ii); INADECUADOS DERECHOS DE USUARIO; (iii) FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO POR RETIRO, lo que generaría afectación en su confidencialidad, integridad y disponibilidad.	INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	MENOR	Moderada	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	Los responsables designados cada vez que ingresa o se retira un colaborador de la Superintendencias Delegadas, realizan la solicitud de creación, activación o inactivación de usuarios mediante el formato TI-F-034 "Administración de usuarios", para asegurar la correcta gestión de los usuarios a los diferentes sistemas de información o repositorios, en caso de no solicitar esos accesos los colaboradores no podrán acceder ni estarán autorizados a dichas herramientas, para lo anterior se crean casos en la plataforma Aranda directamente desde el usuario autorizado	Documentado	Continua	Con registro	TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS y TI-F-034 "Administración de usuarios"	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 10/04/2022 Creada por: [DIEGO ALEJANDRO OSSA URREA] - NO se ha materializado el riesgo - NO se ha materializado el riesgo - Se revisaron los 07 expedientes que se han creado durante el primer trimestre del 2022, por parte de la Dirección de Investigaciones de la Superintendencia Delegada para Energía y Gas Combustible, encontrando que todos los expedientes se encuentran en estado privatizado. Ver Documento 2. 26/04/2022 Creada por: [MILTON EDUARDO BAYONA BONILLA] - NO se ha materializado el riesgo - Se revisaron los 62 expedientes que se han crearon durante los meses de enero, febrero y marzo de 2022, por parte de la Dirección de Investigaciones de la Superintendencia Delegada de Acueducto, Alcantarillado y Aseo, encontrando que los 62 expedientes se encuentran en estado privatizado. Así mismo, se reporta la base de datos con las mesas de ayuda que se colocaron por parte de los responsables para la activación/desactivación de usuarios cada vez que un colaborador que ingresa o se retira de la Entidad. Ver Documento	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO, para este primer trimestre de 2022, y se constató que los 7 expedientes creados por la Dirección de Investigaciones de la Superintendencia Delegada para Energía y Gas Combustible, se encuentran privatizados.
										INADECUADOS DERECHOS DE USUARIO		Afectación de disponibilidad	Leve.	2							A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	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 necesiten. 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.	Documentado	Continua	Con registro	Guía de ayuda No. 17 Instructivo de seguridad para Expedientes y Radicados	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual										
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO		Afectación de Integridad	Leve.	2																																
MEDIDAS PARA EL CONTROL	Objetivo Estratégico	Aplicar las medidas necesarias para controlar, normalizar y restablecer la prestación de los servicios públicos domiciliarios o conminar a las personas que los prestan a la mejora de las condiciones de la prestación.	APROBADO	25/02/2022 3:05:03 p.m.	INFORMACION / DATO	Sistemas de información y repositorios que utiliza la DEIL	PERDIDA DE CONFIDENCIALIDAD	RSI-001-CT	Posibilidad de fuga o revelación de información debido a la alteración, eliminación o intento de modificación no autorizada de la información que posee la DEIL con las siguientes vulnerabilidades: (i) INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS (ii); INADECUADOS DERECHOS DE USUARIO; (iii) ACCESO NO RESTRINGIDO A INSTALACIONES y (iv) FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO POR RETIRO, lo que generaría afectación en su confidencialidad, integridad y disponibilidad.	ACCESO NO RESTRINGIDO A INSTALACIONES	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	MUY BAJA	MENOR	Baja	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	La Directora de Entidades Intervenidas y en Liquidación cada vez que ingresa o se retira un colaborador de la Dirección, realiza la solicitud de creación, activación o inactivación de usuarios mediante el formato TI-F-034 "Administración de usuarios", para asegurar la correcta gestión de los usuarios a los diferentes sistemas de información o repositorios, en caso de no solicitar esos accesos los colaboradores no podrán acceder ni estarán autorizados a dichas herramientas, para lo anterior se crean casos en la plataforma Aranda directamente desde el usuario autorizado (Directora).	Documentado	Continua	Con registro	TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS y TI-F-034 "Administración de usuarios"	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 5/04/2022 Creada por: [LUCIA HERNANDEZ RESTREPO] - NO se ha materializado el riesgo - Durante el primer trimestre se gestionaron 11 activación de usuarios de la Dirección, utilizando el formato TI-F-034 "Administración De usuarios", correspondiente a: ADM rups del usuario Naosorio, usuario pc a Vilma Nieto, correo electrónico a empresas intervenidas P&K E.S.P. y ESSMAR E.S.P, activación de usuarios de Damara Gualtero, Juan Carlos Guasca, Claudia Cerón, Luis Gamboa, Samuel Alfonso, Yecyd Pardo y Andrea Mora solicitud de acceso a O3 y reportes SUI. Ver Documento	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se realizó el seguimiento del primer trimestre de 2022 al control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS, que se encuentra identificado en el riesgo de seguridad digital para el proceso de Medidas para el Control RSI-001-CT y se constató la gestión de los usuarios dentro de la plataforma ARANDA.
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS		Afectación de disponibilidad	Leve.	2																																
										INADECUADOS DERECHOS DE USUARIO		Afectación de Integridad	Leve.	2																																
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO																																				
MEJORA E INNOVACIÓN	Objetivo Estratégico	Promover el mejoramiento continuo y el desarrollo de mecanismos de innovación para fortalecer el desempeño institucional.	APROBADO	15/03/2022 3:36:49 p.m.	INFORMACION / DATO	NORMATIVIDAD RELACIONADA CON SIGESPI	PERDIDA DE DISPONIBILIDAD	RSI-003-MI	POSIBILIDAD DE INCUMPLIMIENTO DE REQUISITOS LEGALES DEL SIGESPI DEBIDO A UN INADECUADO CONTROL DE CAMBIOS O INADECUADO NIVEL DE CONOCIMIENTO POR PARTE DEL OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, LO QUE PODRÍA GENERAR LA PÉRDIDA DE DISPONIBILIDAD DE LA INFORMACIÓN.	INADECUADO CONTROL DE CAMBIOS	INCUMPLIMIENTO DE LEYES	Afectación de disponibilidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	MUY BAJA	MENOR	Baja	A.18. CUMPLIMIENTO.	A.18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A.18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES	El profesional encargado del Sistema de Gestión de Seguridad y Privacidad de la Información revisa semestralmente si existen modificaciones a los requisitos legales y otros requisitos relacionados con seguridad de la información y tratamiento de datos personales, con el propósito de mantener actualizado el normograma de acuerdo con la normatividad vigente, en caso de que se identifique que la norma se encuentre obsoleta o haya sido actualizada, se procederá a actualizar el normograma. Como evidencia se realiza la solicitud de actualización del registro, plan de trabajo y la publicación del documento actualizado en la plataforma SIGME.	Documentado	Continua	Con registro	DE-M-005 Manual del Sistema Integrado de gestión y Mejora.	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 20/04/2022 Creada por: [LIDA CONSTANZA CUBILLOS HERNANDEZ] - NO se ha materializado el riesgo - No se ha materializado el riesgo - Para dar cumplimiento al control A.18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES, se referencia el vínculo del registro MI-R-001 NORMOGRAMA PROCESO DE MEJORA E INNOVACIÓN. Evidencia: http://sigmecalidad.superservicios.gov.co/SSPD/Isodoc/consultas.nsf/442a1ae7d450e3b44052577690063105/b4d07e387d05c7ec052586fc007ade27?OpenDocument.	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES, para este primer trimestre de 2022, y se constató el cumplimiento de dicho control con la evidencia presentada.
										INADECUADO NIVEL DE CONOCIMIENTO Y/O CONCIENCIACIÓN DE EMPLEADOS																																				
MEJORA E INNOVACIÓN	Objetivo Estratégico	Promover el mejoramiento continuo y el desarrollo de mecanismos de innovación para fortalecer el desempeño institucional.	APROBADO	15/03/2022 3:38:38 p.m.	SOFTWARE	APLICATIVO SIGME	PERDIDA DE CONFIDENCIALIDAD	RSI-004-MI	POSIBILIDAD DE ACCESO A LA PLATAFORMA SIGME DEBIDO A UNA INADECUDA GESTIÓN DE CONTRASEÑAS INSEGURAS, CUENTAS DE USUARIO GENERADAS POR SISTEMA CUYAS CONTRASEÑAS PERMANECEN SIN MODIFICACIÓN, FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO O INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS, LO QUE PODRÍA GENERAR UNA AFECTACIÓN A LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN.	CONTRASEÑAS INSEGURAS	ACCESO NO AUTORIZADO AL SISTEMA DE INFORMACIÓN	Afectación de confidencialidad	Sin afectación.	1	No		La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	BAJA	LEVE	Baja	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	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	Documentado	Continua	Con registro	DE-M-005 MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN Y MEJORA Numeral 5.20 SOLICITUD ACCESO PLATAFORMA SIGME	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	BAJA	LEVE	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información	1. 20/04/2022 Creada por: [LIDA CONSTANZA CUBILLOS HERNANDEZ] - NO se ha materializado el riesgo - No se ha materializado el riesgo - Durante el primer trimestre del año, se realizó el seguimiento al control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS, que se encuentra identificado en el riesgo de seguridad digital para el proceso de Mejora Integral de la Gestión Institucional RSI-002-MI y se constató lo siguiente: - El líder del proceso realizó el seguimiento al riesgo de manera oportuna. - Durante el periodo no hubo reportes de incidentes de seguridad de la información. - Creación de 13 cadenas de conexión en 13 solicitudes a la mesa de ayuda, para la creación de usuarios en la aplicación SIGME. - No se presentaron solicitudes de eliminación de usuarios para la aplicación SIGME. Evidencia: Correo con reporte de solicitudes de creación cadena de conexión SIGME: https://drive.google.com/drive/u/1/folders/1b2Dlxnps2TwKddBVOn2XJtJrpa5Fc6f5.	1. 25/04/2022 Creada por: [JHON RAFAEL REDONDO CAMPOS] - NO se ha materializado el riesgo - Se revisó el control A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS, para este primer trimestre de 2022, y se constató el cumplimiento de dicho control con la evidencia presentada.
										CUENTAS DE USUARIO GENERADAS POR SISTEMA CUYAS CONTRASEÑAS PERMANECEN SIN MODIFICACIÓN		Afectación de disponibilidad	Sin afectación.	1																																
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO		Afectación de Integridad	Sin afectación.	1																																
										INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS																																				
PROTECCIÓN AL USUARIO	Objetivo Estratégico	Establecer las actividades necesarias para la interacción entre la entidad y las partes interesadas, a través de canales efectivos de comunicación que brinden una atención oportuna con el fin de resolver sus requerimientos conforme a lo establecido según la ley y la garantía de sus derechos.	APROBADO	28/02/2022 7:22:07 a.m.	SOFTWARE	Sistemas de información que utiliza el proceso Protección al Usuario y Fortalecimiento del Control Social	PERDIDA DE CONFIDENCIALIDAD	RSI-001-PU	Posibilidad de alteración, eliminación o intento de modificación no autorizada de la información que posee la SDPUGT con las siguientes vulnerabilidades: (i); INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS (ii); INADECUADOS DERECHOS DE USUARIO y (iii) FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO POR RETIRO, que pueden ser afectadas por la fuga o revelación de información, lo que generaría afectación en su confidencialidad, integridad y disponibilidad.	INFORMACIÓN DISPONIBLE PARA PERSONAS NO AUTORIZADAS	FUGA O REVELACIÓN DE INFORMACIÓN	Afectación de confidencialidad	Leve.	2	No		La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	MUY BAJA	MENOR	Baja	A.9. CONTROL DE ACCESO.	A.9.2 GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	El líder del proceso, Director Territorial o Coordinador cada vez que ingresa un colaborador a la dependencia, 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 sistemas de información (Orfeo, SIGME, Sancionados, Sistema de Vigilancia y Control, Sisgestión, O3, Mesa de Ayuda y SUI), 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 de mesa de ayuda directamente desde el usuario autorizado. Evidencia: Casos Aranda.	Documentado	Continua	Con registro	TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS y TI-F-034 "Administración de usuarios"	Asignado	Adecuado	Oportuna	Preventivo	Confiable	Se investigan y resuelven oportunamente	Completa	Manual	MUY BAJA	MENOR	Baja	ACEPTAR				Incidentes que afectan la seguridad y privacidad de la información		
										INADECUADOS DERECHOS DE USUARIO		Afectación de disponibilidad	Leve.	2																																
										FALTA DE DESACTIVACIÓN DE CUENTAS DE USUARIO LUEGO DE FINALIZADO EL EMPLEO		Afectación de Integridad	Leve.	2																																