PROCESO GESTIÓN INTEGRAL DEL RIESGO: SUBPROCESO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
GERENCIA DE TECNOLOGÍA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL - UNIDAD ADMINISTRATIVA ESPECIAL DE CATASTRO DISTRITAL 2022

Elaboró: Luis Albeiro Cortés C, Oficial de Seguridad de la Información / Lourdes María Acuña Acuña - Contratista - Gerencia de Tecnología

Revisó: Héctor Henry Pedraza Piñeros - Gerente de Tecnología / Comité Institucional de Gestión y Desempeño UAECD

Aprobó: Comité Institucional de Gestión y Desempeño UAECD

Fecha actualización: 2021-12-30

3. CAPTURA DE INFORMACIÓN - GCAU

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-03-7	CAPTURA DE INFORMACIÓN (GCAU)	Actualizar y conservar el 100% de la ciudad y normatividad vigentes	Informes electronicos	Perdida de confidencialidad de los informes electrónicos	Seguridad Digital	1. Ausencia de control de información a publicar. 2. Entrenamiento insuficiente en seguridad de información	El funcionario responsable de solicitar a comunicaciones la publicación de los informes, verifica previamente que esta conforme al formato establecido y que la información incluida no contiene datos sensibles o personales, esto lo realiza conforme a la periodad de los informes mensula, trimestral o semestral y queda documentado en la mesa de servicio de comunicaciones . EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	EXTREMO	MODERADO	ALTO	REDUCIR	Realizar instructivo de informes que presenta la GCAU en el que se incluya condiciones de operación y control que deben realizar los funcionarios que intervienen en la elaboracion del informe y en la publicacion del mismo	Meta= 1 Indicador instructivo elaborado / 1 instructivo programado	Documentacion-funcionarios que partiipan en la actividad	Funcionario delegado de documentar SGI Responsable del proceso Gerente GCAU	30/06/2023

3. CAPTURA DE INFORMACIÓN - GIC - SIFJ - SIE

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-03-11	CAPTURA DE INFORMACIÓN	Actualizar y conservar el 100% de los predios de la ciudad de acuerdo con la programación y la normatividad vigente.	Recurso Humano de la GIC	Pérdida de Confidencialidad del Recurso Humano	Seguridad Digital	1. Entrenamiento insuficiente en seguridad 2. Uso incorrecto de software y hardware 3. Falta de conciencia acerca de la seguridad	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario designado de RRHH y/o OAI cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado los deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no esté firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (RRH o OAI)	MODERADO	FUERTE	MODERADO	REDUCIR	Solicitar sensibilizaciones para el recurso humano de la GIC con el fin que se conozcan los deberes que tienen como funcionarios y/o contratistas respecto a la seguridad de la información	Meta: 1 Número de Sensibilizaciones a los funcionarios y/o contratistas de la GIC / Número de sensibilizaciones programadas	Recursos Humanos. Recursos Tecnológicos	1. GIC	30/06/2022

4. INTEGRACIÓN DE INFORMACION

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-04-5	INTEGRACIÓN DE INFORMACIÓN	Integrar y disponer información geográfica en la Infraestructura de Datos Espaciales para el Distrito Capital mediante la concertación y articulación interinstitucional, el desarrollo y fortalecimiento de capacidades de la comunidad, y la gestión de las acciones requeridas para facilitar el acceso, uso e intercambio de información geográfica, asegurando el cumplimiento del 100% de las metas definidas para la infraestructura durante la vigencia.	1. Bases de Datos con Información Personal entregada por Entidades públicas y privadas (Bases de Datos)	Pérdida de Confidencialidad e Integridad Bases de Datos en Excel	Seguridad Digital	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia cada vez que se requiera, con el propósito que se otorguen los permisos correspondientes al funcionario y poder evitar el acceso no autorizado a la información. El jefe de dependencia registra la solicitud en la mesa de servicios de TI. En caso que se realice la asignación por parte de personal diferente al jefe de dependencia, esta solicitud es cerrada y no resuelta por la mesa de servicios de TI. La evidencia de la solicitud queda registrada en la mesa de servicios de TI. El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO El controlador de dominio cada vez que un usuario se identifica en un equipo de cómputo con sus credenciales verifica que es un usuario autorizado en la red. Si el usuario accede con credenciales autenticas le da ingreso al equipo, de lo contrario no permite el acceso. La evidencia del control queda registrada en el sistema. El controlador de dominio cada vez que verifica que un usuario (equipo de computo) esta inactivo más del tiempo estipulado, desactiva el usuario con el fin que este se vuelva a identificar con sus credenciales en el equipo. La evidencia del control queda registrada al inicio de sesión en el equipo de computo.	MODERADO	FUERTE	MODERADO	REDUCIR	1. Continuar realizando la revisión del reporte de cuentas de usuario (control) 2. Solicitar sensibilizaciones para los funcionarios/ contratistas (indicando número de funcionarios/contratistas) en temas de seguridad de la información relacionados con el control de acceso a la información digital que puedan mitigar riesgos de perdida de confidencialidad e integridad de la información.	Meta1 = 1 Indicador1 Revisiones realizadas / revisiones programadas*100 Meta2= 100% funcionarios/contratistas de la dependencia sensibilizados Indicador # personas sensibilizadas / # personas convocadas*100	Recursos Humanos, Tecnológicos	Gerente de Ideca / Subgerente de Operaciones	30/06/2022

6. GESTIÓN DEL TALENTO HUMANO

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-06-1	GESTIÓN DEL TALENTO HUMANO	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	1. Historias Laborales 2. Nómina - Novedades de Nómina 3. Expedientes de Provisión de personal - (Información Análoga)	Pérdida de Confidencialidad y Integridad Historias Laborales/ Novedades Nomina/Expedientes de Provisión de personal (Información Análoga)	Seguridad Digital	1. Ausencia de control de acceso 2. Desconocimiento o no aplicación de las politicas de seguridad y privacidad de la información	El jefe de dependencia una vez se retira el servidor de la entidad, solita a la Subgerencia Administrativa y Financiera la eliminación de los accesos al archivo físico de la Subgerencia de Talento Humano, con el propósito de garantizar que el ex - servidor no pueda acceder al archivo donde se encuentran los documentos. Se debe remitir un correo electronico ala SAF indicando la novedad. En caso de no remitir el correo electronico se puede materializar el riesgo La evidencia de la ejecución del control es el correo electronico. Cada vez que un servidor o contratista ingresa identificandose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	ALTO	FUERTE	ALTO	REDUCIR	Solicitar sensibilizaciones en seguridad de la información para los funcionarios de a SRH en gestión de accesos a la información física Asignar rol para control de los documentos físicos	Meta= 100% de funcionarios de la SRH sensibilizados Indicador # de personas que sensibilizadas / # personas convocadas * 100 Meta2= 1 Indicador 1 persona asignada en la dependencia	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-2	GESTIÓN DEL TALENTO HUMANO	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	1. Historias Laborales 2. Nómina - Novedades de Nómina 3. Expedientes de Provisión de personal - (Información Análoga	Pérdida de Disponibilidad Historias Laborales/ Novedades Nomina/Expedientes de Provisión de personal (Información Análoga)	Seguridad Digital	1. Entrenamiento insuficiente en seguridad 2. Falta de conciencia acerca de la seguridad 3. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos 3. No tener las historias laborales escaneadas en su totalidad	El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO Cada vez que un servidor o contratista ingresa identificandose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO	ALTO	FUERTE	ALTO	REDUCIR	Solicitar sensibilizaciones en seguridad de la información para los funcionarios de a SRH en gestión de accesos a la información física	Meta= 100% de funcionarios de la SRH sensibilizados Indicador # de personas que sensibilizadas / # personas convocadas * 100	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-3	GESTIÓN DEL TALENTO HUMANO	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	1 . Historias Laborales 2. Nómina - Novedades de Nómina 3. Novedades de Nómina 4. Expedientes de Provisión de personal - (Información Digital / Electrónica)	Pérdida de Confidencialidad e Integridad Historias Laborales/ Novedades Nomina/Expedientes de Provisión de personal (Información Digital / Electrónica)	Seguridad Digital	1. Entrenamiento insuficiente en seguridad 2. Falta de conciencia acerca de la seguridad 3. Acceso intencionado por parte de personal no autorizado 4. Deficiencia en la asignación de permisos	El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asisteron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO Cada vez que un servidor o contratista ingresa identificandose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. – DETECTIVO El propietario del activo cada vez que se presente un incidente de seguridad debera reportar la vulberabilidad en la Mesa de Servicios de TI con el fin que se verifique el mismo. La evidencia del control queda registrada en la Mesa de Servicios de TI	ALTO	MODERADO	MODERADO	REDUCIR	1. Reforzar los controles existentes Control : Revisión de reporte de cuentas de usuario 2. Solicitar Solicitar sensibilizaciones en temas de seguridad de la información relacionados con el control de acceso a la información digital para los funcionarios de la dependencia.	Meta1 = 3 Revisiones realizadas / revisiones programadas*100 Meta2= 100% de funcionarios de la dependencia capacitados. # Personas sensibilizadas / # Personas convocadas*100	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022

RS-06-5	**GESTIÓN DEL TALENTO HUMANO**	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	Bases de Datos con información sensible de los servidores públicos de la UAECD	Pérdida de Confidencialidad e Integridad Bases de Datos con información sensible de los servidores públicos de la UAECD	Seguridad Digital	1. Gestión deficiente de las contraseñas 2. No existencia de una copia de seguridad 3. Ubicación no adecuada de la información (equipos de los funcionarios)	El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO Cada vez que un servidor o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. – DETECTIVO El propietario del activo cada vez que se presente un incidente de seguridad debera reportar la vulberabilidad en la Mesa de Servicios de TI con el fin que se verifique el mismo. La evidencia del control queda registrada en la Mesa de Servicios de TI	ALTO	MODERADO	MODERADO	REDUCIR	1. Reforzar los controles existentes Control : Revisión de reporte de cuentas de usuario 2. Solicitar Solicitar sensibilizaciones en temas de seguridad de la información relacionados con el control de acceso a la información digital para los funcionarios de la dependencia.	Meta1 = 3 Revisiones realizadas / revisiones programadas * 100 Meta2= 100% de funcionarios de la dependencia capacitados. # Personas sensibilizadas / # Personas convocadas* 100	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-7	**GESTIÓN DEL TALENTO HUMANO**	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	Archivo de Gestión de la SRH (Instalaciones)	Pérdida de Confidencialidad e Integridad Archivo de Gestión de la SRH	Seguridad Digital	1. Ausencia de control de accesos 2. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos 3. Desconocimiento de políticas de seguridad	Cada vez que un servidor o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	ALTO	FUERTE	ALTO	REDUCIR	1. Reforzar los controles existentes 2. Solicitar sensibilizaciones en seguridad de la información para los funcionarios de a SRH en gestión de accesos a areas seguras	Meta= 100% de funcionarios de la SRH sensibilizados Indicador # de personas que sensibilizadas / # personas convocadas * 100	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-8	**GESTIÓN DEL TALENTO HUMANO**	Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	Archivo de Gestión de la SRH (Instalaciones)	Perdida de Disponibilidad Archivo de Gestión de la SRH	Seguridad Digital	1. Ausencia de control de acceso 2. Desconocimiento o no aplicación de las politicas de seguridad y privacidad de la información	Cada vez que un servidor o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el servidor no esté autorizado para ingresar al área, el Sistema biométrico NO concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO El oficial de seguridad de la información cada mes, revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programe nuevamente a la siguiente jornada de sensibilización. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	ALTO	FUERTE	ALTO	REDUCIR	Solicitar sensibilizaciones en seguridad de la información para los funcionarios de a SRH en gestión de accesos a areas seguras	Meta= 100% de funcionarios de la SRH sensibilizados Indicador # de personas que sensibilizadas / # personas convocadas * 100	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-11		Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	Correos Electrónicos de SRH	Pérdida de confidencialidad e integridad de correos electrónicos de la Subgerencia de Talento Humano	Seguridad Digital	1. Desconocimiento de las politicas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia del correo electronico de la dependencia. La evidencia de la asignación queda registrada en la herramienta de teams, correo electrónico o mesa de servicios de ser el caso. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	1. Solicitar capacitaciones en seguridad de la información 2. Recordatorios a través de piezas comunicacionales a los servidores sobre los controles de seguridad que se deben implementar	# de servidores sensibilizados/Total de servidores convocados x 100 Piezas comunicativas publicadas en la Intranet	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022
RS-06-12		Gestionar el talento humano de la Unidad en el ciclo de vida del servidor público (ingreso, desarrollo y retiro), con el propósito de aportar a su desarrollo integral; así como, propiciar un clima y cultura organizacional que apoyen el cumplimiento de la misión de la Entidad.	Correos Electrónicos de SRH	Pérdida de disponibilidad de correos electrónicos de la Subgerencia de Talento Humano	Seguridad Digital	1. Desconocimiento de las politicas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	La Mesa de Servicios de TI cada vez que se presenta una falla en el equipo de grabación se contacta con el proveedor del servicio con el fin que se atienda la falla correspondiente. En caso que el inconveniente no sea resuelto por el proveedor, el profesional encargado de la Mesa de Servicios de TI informa al proveedor para que se reprograme y atienda el requerimiento. La evidencia del control queda registrada en el reporte realizado por el profesional de la Mesa de Servicios de TI EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – PREVENTIVO El administrador de la plataforma diariamente valida las plataformas que administran con el fin de verificar que se encuentren disponibles y en correcto funcionamiento. En caso de que se presente alguna falla, verifican la plataforma administrada, diagnosticando la posible falla o evento y validan la disponibilidad de los servicios en las diferentes herramientas de administración. De ser necesario remiten falla al proveedor para su respectiva atención. La evidencia del control queda en la herramienta de teams del equipo de infraestructura y check list diario que maneja cada uno de los administradores de plataforma La herramienta SIEM monitorea los servicios de la infraestructura tecnológica (incluido urls) y una vez se evidencia indisponibilidad del servicio, alertas de seguridad notifica mediante correo electrónico a los administradores de plataforma o a los ingenieros que realizan monitoreo de la herramienta en la Subgerencia de Infraestructura Tecnológica, con el fin que se verifique y atienda la indisponibilidad del servicio o incidente presentado. La evidencia del control queda registrada en la herramienta SIEM y /o monitoreo realizado por el personal de infraestructura.	MODERADO	FUERTE	MODERADO	REDUCIR	1. Solicitar capacitaciones en seguridad de la información 2. Recordatorios a través de piezas comunicacionales a los servidores sobre los controles de seguridad que se deben implementar	# de servidores sensibilizados/Total de servidores convocados x 100 Piezas comunicativas publicadas en la Intranet	Recursos Humanos, Tecnológicos	Subgerente de Talento Humano	30/06/2022

8. GESTIÓN DOCUMENTAL

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital).	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-08-2	**GESTIÓN DOCUMENTAL**	Administrar mensualmente el 100% del archivo central de la Unidad; a través de la conservación, custodia y salvaguarda de la misma; dando respuesta a los requerimientos recibidos por el área de manera oportuna, veraz y eficiente.	1. COMUNICACIONES OFICIALES ENVIADAS 2. INVENTARIOS DOCUMENTALES (Información Análoga)	Pérdida de Disponibilidad Comunicaciones Oficiales - Inventarios Documentales - Análoga	Seguridad Digital	Controles de acceso físico inadecuados Desconocimiento de Políticas de Seguridad	Gestión documental debe tener actualizado el listado de personal con permiso de acceso a los diferentes espacios de archivo de gestión y central. El sistema biométrico cada vez que un funcionario o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el funcionario no esté autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO Desde gestión documental se suministra al oficial de seguridad de la información el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal del equipo de gestión documental asista al proceso programado. Se verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron el oficial de seguridad de la información remite correo al enlace del grupo de gestión documental para que se programen a los funcionarios y contratistas nuevamente. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	Realizar sensibilizaciones al personal de Gestión Documental con el fin que se conozcan los controles relacionados con el manejo de información análoga con el fin de evitar la perdida de disponibilidad de esta información	Meta. 100% funcionarios/contratistas de Gestión documental sensibilizados Indicador Funcionarios/contratistas sensibilizados/funcionarios y contratista de GD	Recursos Humanos y Tecnológicos	Lider de proceso Gestión Documental	30/06/2022
RS-08-5	**GESTIÓN DOCUMENTAL**	Administrar mensualmente el 100% del archivo central de la Unidad; a través de la conservación, custodia y salvaguarda de la misma; dando respuesta a los requerimientos recibidos por el área de manera oportuna, veraz y eficiente.	1. Archivo Central 2. Centro Documental (Archivo Intermedio)	Pérdida de Confidencialidad e Integridad Archivo Central Centro Documental	Seguridad Digital	1. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos 2. Desconocimiento de Políticas de Seguridad	Gestión documental debe tener actualizado el listado de personal con permiso de acceso a los diferentes espacios de archivo de gestión y central. El sistema biométrico cada vez que un funcionario o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el funcionario no esté autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO Desde gestión documental se suministra al oficial de seguridad de la información el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal del equipo de gestión documental asista al proceso programado. Se verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron el oficial de seguridad de la información remite correo al enlace del grupo de gestión documental para que se programen a los funcionarios y contratistas nuevamente. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	Realizar sensibilizaciones al personal de Gestión Documental con el fin que se conozcan los controles relacionados con el manejo de información análoga con el fin de evitar la perdida de confidencialidad e integridad enlas instalaciones (archivo central y centro de documental)	Meta. 100% funcionarios/contratistas de Gestión documental sensibilizados Indicador Funcionarios/contratistas sensibilizados/funcionarios y contratista de GD	Recursos Humanos y Tecnológicos	Lider de proceso Gestión Documental	30/06/2022
RS-08-6	**GESTIÓN DOCUMENTAL**	Administrar mensualmente el 100% del archivo central de la Unidad; a través de la conservación, custodia y salvaguarda de la misma; dando respuesta a los requerimientos recibidos por el área de manera oportuna, veraz y eficiente.	1. Archivo Central 2. Centro Documental (Archivo Intermedio)	Pérdida de Disponibilidad Archivo Central-Centro Documental - (incluidos los documentos electrónicos con tiempos de retención superiores a 10 años y disposición final de conservación total y selección).	Seguridad Digital	Ubicación en un área susceptible de inundación Ausencia de protección física de la edificación, puertas y ventanas Ausencia de Controles de Acceso asociado al instrumento archivistico Tablas de Control de Acceso -TCA- No aplicación de las Tablas de Retención Documental -TRD-	Gestión documental debe tener actualizado el listado de personal con permiso de acceso a los diferentes espacios de archivo de gestión y central. El sistema biométrico cada vez que un funcionario o contratista ingresa identificándose con su tarjeta de proximidad o huella a un área segura (archivo de gestión), verifica si está autorizado para ingresar al área con el fin de conceder el acceso correspondiente. En caso de que el funcionario no esté autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. PREVENTIVO Desde gestión documental se suministra al oficial de seguridad de la información el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal del equipo de gestión documental asista al proceso programado. Se verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron el oficial de seguridad de la información remite correo al enlace del grupo de gestión documental para que se programen a los funcionarios y contratistas nuevamente. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	Realizar sensibilizaciones al personal de Gestión Documental con el fin que se conozcan los controles relacionados con el manejo de información análoga con el fin de evitar la perdida de disponibilidad de (archivo central y centro documental)	Meta. 100% funcionarios/contratistas de Gestión documental sensibilizados Indicador Funcionarios/contratistas sensibilizados/funcionarios y contratista de GD	Recursos Humanos y Tecnológicos	Lider de proceso Gestión Documental	30/06/2022

9. GESTIÓN FINANCIERA

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN

RS-09-1	GESTIÓN FINANCIERA	Gestionar y hacer seguimiento al 100% de los recursos financieros necesarios para cumplir con los objetivos y metas de la entidad durante cada vigencia.	Carpeta Digital Expediente de Contratos (Información Digital)	Pérdida de Confidencialidad e Integridad Carpeta Digital Expediente de Contratos (Información Digital)	Seguridad Digital	1. Ausencia en el control de acceso al fileserver. 2. Asignación erronea de permisos de acceso. 3. Desconocimiento de políticas de seguridad de la información.	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia cada vez que se requiera, con el propósito de que se otorguen los permisos correspondientes al funcionario y poder evitar el acceso no autorizado a la información. El jefe de dependencia registra la solicitud en la mesa de servicios de TI. En caso que se realice la asignación por parte de personal diferente al jefe de dependencia, esta solicitud es cerrada y no resuelta por la mesa de servicios de TI. La evidencia de la solicitud queda registrada en la mesa de servicios de TI. El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	MODERADO	MODERADO	REDUCIR	1. Continuar reforzando los controles existentes y dejar evidencia de la ejecución estos (Revisa reporte cuenta de usuario) y ejecutarlo de acuerdo como esta establecido en el procedimiento de gestión de accesos. 2. Solicitar sensibilizaciones en seguridad de la información para los funcionarios de Financiera respecto a la gestión de accesos y controles para el manejo de la información digital ubicada en los medios de almacenamiento.	Meta1 = 1 # reportes entregados /# reportes programados*100 Meta2 = 100% de las personas de la dependencia sensibilizadas #personas sensibilizadas / # personas convocadas * 100	Recursos Humanos, Técnicos y Tecnológicos	Subgerente Administrativo y Financiero	30/06/2022
RS-09-9	GESTIÓN FINANCIERA	Gestionar y hacer seguimiento al 100% de los recursos financieros necesarios para cumplir con los objetivos y metas de la entidad durante cada vigencia.	Funcionarios de Financiera	Pérdida de Confidencialidad Funcionarios	Seguridad Digital	1. Ausencia de copias de respaldo. 2. Desconocimiento de políticas de seguridad de la información. 3. Ausencia de planes de continuidad.	El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO Cada vez que se va a vincular un funcionario o contratista de la dependencia desde la Subgerencia de recursos Humanos / Oficina Asesora Jurídica revisan que se encuentre firmado el acuerdo de confidencialidad para el manejo de la información de la Unidad. La evidencia es el documento firmado por cada funcionario / contratista , al cual queda anexo al expediente laboral/contractual correspondiente. En caso que se detecte que el compromiso de confidencialidadno se encuentre firmado, se solicita al funcionario/contratista la firma del mismo.	MODERADO	FUERTE	MODERADO	REDUCIR	Solicitar sensibilizaciones para los funcionarios de Financiera en temas de seguridad de la información respecto a las responsabilidades como usuarios del SGSI.	Meta1 = 100% de las personas de la dependencia sensibilizadas #personas sensibilizadas / # personas convocadas * 100	Recursos Humanos, Técnicos y Tecnológicos	Subgerente Administrativo y Financiero	30/06/2022

10. GESTIÓN JURÍDICA

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-10-1	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Expedientes de Acciones Constitucionales (Información Análoga)	Pérdida de Confidencialidad e Integridad Expedientes Acciones Constitucionales (Información Análoga)	Seguridad Digital	1. Ausencia de control de acceso a los expedientes	El sistema biométrico cada vez que un funcionario o contratista ingresa identificandose con su tarjeta de proximidad a un área segura (archivo de gestión), verifica si esta autorizada para ingresar al área con el fin de conceder el acceso correspondiente. En caso que el funcionario no este autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. Cada Vez que llega un documento físico relacionado con una acción constitucional se genera una copia digital la cual es cargada en el Aplicativo SIPROJ. En caso quela información no sea digitalizada, no se puede actualizar el aplicativo SIPROJ ni socializar la información, la evidencia del control queda registrada en el Sistema de PRocesos Judiciales. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con las sensibilizaciones en temas de seguridad de la información (acceso a la información Física) para los abogados	Meta=50% de abogados sensibilizados # Personas sensibilizadas / # Personas convocadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022
RS-10-2	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Expedientes de Acciones Constitucionales (Información Análoga)	Pérdida de Disponibilidad Expedientes Acciones Constitucionales (Información Análoga)	Seguridad Digital	1. Ausencia de control de acceso a los expedientes 2. Desconocimiento de Políticas de seguridad de la información 3. Ausencia de planes de continuidad	El sistema biométrico cada vez que un funcionario o contratista ingresa identificandose con su tarjeta de proximidad a un área segura (archivo de gestión), verifica si esta autorizada para ingresar al área con el fin de conceder el acceso correspondiente. En caso que el funcionario no este autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. Cada Vez que llega un documento físico relacionado con una acción constitucional se genera una copia digital la cual es cargada en el Aplicativo SIPROJ. En caso quela información no sea digitalizada, no se puede actualizar el aplicativo SIPROJ ni socializar la información, la evidencia del control queda registrada en el Sistema de PRocesos Judiciales. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con las sensibilizaciones en temas de seguridad de la información (acceso a la información Física) para los abogados	Meta=50% de abogados sensibilizados # Personas sensibilizadas / # Personas convocadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022
RS-10-4	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Expedientes de Acciones Constitucionales (Información Digital/Electrónica)	Pérdida de Disponibilidad Expedientes Acciones Constitucionales (Información Digital/Electrónica)	Seguridad Digital	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de Políticas de Seguridad de la información 3. Ausencia de Planes de continuidad	El jefe de dependencia revisa cada año la matriz de copias de respaldo y recuperación, remitida por el gestor de accesos, con el fin de verificar que se realice el respaldo correspondiente a la información vital del proceso. El jefe de dependencia revisa la matriz y en caso de ser necesario solicita realizar las modificaciones pertinentes. La evidencia queda registrada en una mesa de servicios de TI. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con el fortalecimiento del control. Control : Revisión anual de la matriz de copias de respaldo	Meta = 1 Revisiones realizadas / revisiones programadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022
RS-10-5	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Archivo de Gestión OAJ (Instalaciones)	Pérdida de Confidencialidad e Integridad Archivo de Gestión OAJ	Seguridad Digital	1. Ausencia de control de acceso a los expedientes	El sistema biométrico cada vez que un funcionario o contratista ingresa identificandose con su tarjeta de proximidad a un área segura (archivo de gestión), verifica si esta autorizada para ingresar al área con el fin de conceder el acceso correspondiente. En caso que el funcionario no este autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con las sensibilizaciones en temas de seguridad de la información (acceso a la información Física) para los abogados	Meta=50% de abogados sensibilizados # Personas sensibilizadas / # Personas convocadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022
RS-10-6	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Archivo de Gestión OAJ (Instalaciones)	Pérdida de Disponibilidad Archivo de Gestión OAJ	Seguridad Digital	1. Ausencia de control de acceso a los expedientes 2. Desconocimiento de Políticas de seguridad de la información 3. Ausencia de planes de continuidad	El sistema biométrico cada vez que un funcionario o contratista ingresa identificandose con su tarjeta de proximidad a un área segura (archivo de gestión), verifica si esta autorizada para ingresar al área con el fin de conceder el acceso correspondiente. En caso que el funcionario no este autorizado para ingresar al área, el sistema no concede el acceso correspondiente. La evidencia del control queda registrada en la base de datos del sistema biométrico. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con las sensibilizaciones en temas de seguridad de la información (acceso a la información Física) para los abogados	Meta=50% de abogados sensibilizados # Personas sensibilizadas / # Personas convocadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022
RS-10-8	GESTIÓN JURÍDICA	Atender oportunamente el 100% de las actuaciones administrativas radicadas en la OAJ, así como del ejercicio de la defensa judicial y la asesoría en asuntos normativos con el fin de proveer los instrumentos legales necesarios y prevenir el daño antijurídico, en los términos y condiciones legales aplicables.	1. Fileserver /OAJ (Servicio)	Pérdida de Disponibilidad Fileserver /OAJ	Seguridad Digital	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de Políticas de Seguridad de la información 3. Ausencia de Planes de continuidad	El jefe de dependencia revisa cada año la matriz de copias de respaldo y recuperación, remitida por el gestor de accesos, con el fin de verificar que se realice el respaldo correspondiente a la información vital del proceso. El jefe de dependencia revisa la matriz y en caso de ser necesario solicita realizar las modificaciones pertinentes. La evidencia queda registrada en una mesa de servicios de TI. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Continuar con el fortalecimiento del control. Control : Revisión anual de la matriz de copias de respaldo	Meta = 1 Revisiones realizadas / revisiones programadas*100	Recursos Humanos, Tecnológicos	Gerente Jurídico	30/06/2022

12. GESTIÓN DE COMUNICACIONES

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-12-1	GESTIÓN DE COMUNICACIONES	Diseñar y ejecutar el 100% de las estrategias y atender el 85% de los requerimientos internos y externos de comunicación que requiera la Unidad durante la vigencia para lograr el posicionamiento de la entidad ante el público de interés.	Portal Web (Servicio)	Pérdida de Confidencialidad e integridad del Portal web	Seguridad Digital	1. Ausencia de parametros de seguridad 1a. Ausencia de copias de respaldo 2. Ausencia de control de acceso al administrador de contenidos 2a. Asignación errada de los derechos de acceso a nivel de administración de la base de datos.	El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. El jefe de dependencia revisa cada año la matriz de copias de respaldo y recuperación, remitida por el funcionario encargado de los accesos, con el fin de verificar que se realice el respaldo correspondiente a la información vital del proceso. El jefe de dependencia revisa la matriz y en caso de ser necesario solicita realizar las modificaciones pertinentes. La evidencia queda registrada en una mesa de servicios de TI. El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos indicando los ajustes requeridos. El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	ALTO	MODERADO	MODERADO	REDUCIR	1.Continuar con el fortalecimiento del control revisión reporte de cuentas de usuario. 2. Continuar con el fortalecimiento control revisión matriz de copias de respaldo.	Meta 1 = 1 Revisiones realizadas / revisiones programadas*100 Meta 2 = 1 Revisiones realizadas / revisiones programadas*100	Recursos Humanos, Tecnológicos	Asesor de Comunicaciones	30/06/2022

RS-12-2	**GESTIÓN DE COMUNICACIONES**	Diseñar y ejecutar el 100% de las estrategias y atender el 85% de los requerimientos internos y externos de comunicación que requiere la Unidad durante la vigencia para lograr el posicionamiento de la entidad ante el público de interés.	Portal Web (Servicio)	Pérdida de Disponibilidad del Portal web	Seguridad Digital	1. Ausencia de parametros de seguridad 1a. Ausencia de copias de respaldo 2. Ausencia de control técnico sobre el software	El jefe de dependencia revisa cada año la matriz de copias de respaldo y recuperación, remitida por el funcionario encargado de los accesos, con el fin de verificar que se realice el respaldo correspondiente a la información vital del proceso. El jefe de dependencia revisa la matriz y en caso de ser necesario solicita realizar las modificaciones pertinentes. La evidencia queda registrada en una mesa de servicios de TI. La herramienta SIEM monitorea los servicios de la infraestructura tecnológica (incluido urls) y una vez se evidencia indisponibilidad del servicio, alertas de seguridad notifica mediante correo electrónico a los administradores de plataforma o a los ingenieros de que realizan monitoreo de la herramienta en la Subgerencia de Infraestructura Tecnológica, con el fin que se verifique y atienda la indisponibilidad del servicio o incidente presentado. La evidencia del control queda registrada en la herramienta SIEM y /o monitoreo realizado por el personal de infraestructura.	ALTO	MODERADO	MODERADO	REDUCIR	1. Continuar con el fortalecimiento del control revisión matriz de copias de respaldo	Meta = 1 Revisiones realizadas / revisiones programadas*100	Recursos Humanos, Tecnológicos	Asesor de Comunicaciones	30/06/2022
RS-12-7	**GESTIÓN DE COMUNICACIONES**	Diseñar y ejecutar el 100% de las estrategias y atender el 85% de los requerimientos internos y externos de comunicación que requiere la Unidad durante la vigencia para lograr el posicionamiento de la entidad ante el público de interés.	Comunicadores sociales (recurso humano)	Pérdida de Confidencialidad en el personal (comunicadores sociales)	Seguridad Digital	Entrenamiento insuficiente en seguridad Falta de conciencia acerca de la seguridad	El oficial de seguridad de la información cada mes verifica el listado de las personas que no han asistido a las charlas de sensibilización en seguridad, con el fin de convocarlas para la siguiente charla. En caso que las personas no asistan , remite correo al personal , elnace de seguridad y jefe de dependencia para que se promueva la asistencia del mismo. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario designado de RRHH y/o OAI cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado llos deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no esté firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (SRH o OAJ)	MODERADO	FUERTE	MODERADO	REDUCIR	Capacitar al equipo de comunicaciones en temas de seguridad de la información relacionado con la pérdida de confidencialidad en el recurso humano.	Meta: 100% de colaboradores capacitados Indicador colaboradores capacitados / colaboradores del equipo de comunicaciones * 100	Recursos Humanos, Tecnológicos	Asesor de Comunicaciones	30/06/2022
RS-12-8	**GESTIÓN DE COMUNICACIONES**	Diseñar y ejecutar el 100% de las estrategias y atender el 85% de los requerimientos internos y externos de comunicación que requiere la Unidad durante la vigencia para lograr el posicionamiento de la entidad ante el público de interés.	Comunicadores sociales (recurso humano)	Pérdida de Disponibilidad en el personal (comunicadores sociales)	Seguridad Digital	Ausencia del personal Afectaciones en la salud del personal (COVID19)	El oficial de seguridad de la información cada mes verifica el listado de las personas que no han asistido a las charlas de sensibilización en seguridad, con el fin de convocarlas para la siguiente charla. En caso que las personas no asistan remite correo al personal , elnace de seguridad y jefe de dependencia para que se promueva la asistencia del mismo. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	ALTO	FUERTE	MODERADO	REDUCIR	Verificar las actas de entrega del personal que finalice sus labores en el equipo de comunicaciones.	Meta: 100% de las actas verificaciones Indicador Actas verificadas / Actas presentadas	Recursos Humano	Asesor de Comunicaciones	30/06/2022

13. PROVISIÓN Y SOPORTE DE SERVICIOS TI

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital).	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-13-1	**PROVISIÓN Y SOPORTE DE SERVICIOS TI**	Mantener la infraestructura tecnológica mínimo en un 95% de disponibilidad y atender satisfactoriamente, mínimo el 90% de las solicitudes registradas durante la vigencia en la mesa de servicios de TI.	1.Base de Datos de Infodoc 2.MDB_CA 3.prowinbdcat02 4.MISPROD - Producción 5.HISPROD - Producción 6. WCCPROD - Producción 7.MAPASPRO 8.MAPASBD 9.MISDES-Desarrollo 10.PREPOS-Preproduccion 11.MISPROD-Pruebas 12.MISPROD - DRP 13.Base de datos de Sicapital - DRP 14.IDECAPRU (Base de Datos)	Pérdida de Confidencialidad e Integridad Bases de Datos Automatizadas	Seguridad Digital	1. Asignación errada de los derechos de acceso a nivel de administración de la base de datos. 2. Información Sensible sin cifrado a nivel de base de datos 3. Gestión deficiente de las contrasellas de administración en la base de datos. 4. Desconocimiento de la configuración de la base de datos 5. Desconocimiento de las politicas de seguridad de la información	El sistema de administración de la base de datos cada vez que un administrador de bases de datos se identifica con las credenciales, valida contra la información registrada en la base de usuarios autorizados, con el fin de verificar los permisos y accesos permitidos al mismo. En caso de que las credenciales ingresadas no correspondan con las registradas en la base de usuarios autorizados, el sistema no permite el ingreso. La evidencia del control queda registrada en la base de datos del sistema. – DETECTIVO EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario designado de RRHH y/o OAI cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado los deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no esté firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (SRH o OAJ) Los administradores de bases de datos una vez identificada por parte del equipo de seguridad de la información la información definida como clasificada o reservada a nivel de bases de datos (datos personales), implementan herramientas de control para evitar que se pueda acceder a nivel de bases de datos a esta información. Lo anterior con el fin de garantizar la confidencialidad e integridad de la información. La evidencia del control queda registrada en la mesa de servicios de TI y en la base de datos donde se implemento. Los administradores de bases de datos cada vez que se requiere realizan revisión de los logs de auditoria de la base de datos con el fin de detectar irregularidades o eventos sospechosos que puedan afectar la seguridad de la información. En caso que se presente alguna alguna anomalia, realizan el tratamiento correspondiente. La evidencia del control queda registrado en correo electrónico o mesa de servicios de TI Los administradores de bases de datos mensualmente realizan revisión de los logs de auditoria de las bases de datos con el fin de verificar el registro de los eventos en estos logs de auditoria . En caso que se presente alguna alguna anomalia, entrar a solucionarla. La evidencia del control queda registrado en correo electrónico o mesa de servicios de TI. No queda registrada evidencia del control en caso que todo este funcionando correctamente, pero en caso de que se presente una incidencia la evidencia queda soportada en la mesa de servcios de TI.	ALTO	MODERADO	MODERADO	REDUCIR	Continuar con el proceso de ofuscamiento a nivel de bases de datos (Go Catastral)	Meta. Datos personales ofuscados en GoCatastral	Recursos Humanos, Recursos Tecnológicos	Administradores de plataforma (bases de datos)	30/06/2022
RS-13-2	**PROVISIÓN Y SOPORTE DE SERVICIOS TI**	Mantener la infraestructura tecnológica mínimo en un 95% de disponibilidad y atender satisfactoriamente, mínimo el 90% de las solicitudes registradas durante la vigencia en la mesa de servicios de TI.	1.Base de Datos de Infodoc 2.MDB_CA 3.prowinbdcat02 4.MISPROD - Producción 5.HISPROD - Producción 6. WCCPROD - Producción 7.MAPASPRO 8.MAPASBD 9.MISDES-Desarrollo 10.PREPOS-Preproduccion 11.MISPROD-Pruebas 12.MISPROD - DRP 13.Base de datos de Sicapital - DRP 14.IDECAPRU (Base de Datos)	Pérdida de Disponibilidad Bases de Datos Automatizadas	Seguridad Digital	1. Ausencia de copias de respaldo 1a. Ausencia de mecanismos de monitoreo 2. Ausencia de documentación 2a.Configuración incorrecta de parámetros 3. Ausencia de planes de continuidad 4. Desconocimiento de politicas de seguridad de la información	Los administradores de plataformas (bases de datos) revisan cada año la matriz de programación de copias de respaldo y recuperación, remitida por el gestor de accesos, con el fin de verificar que se realice el respaldo correspondiente a la información vital del proceso. El jefe de dependencia revisa la matriz y en caso de ser necesario solicita realizar las modificaciones pertinentes. La evidencia queda registrada en una mesa de servicios de TI. – DETECTIVO El grupo de operadores apoyado por los administradores de plataforma (bases de datos), semestralmente o cuando se requiera, ejecuta las pruebas de respaldo, inicialmente verificando las cintas y validando el contenido de esta, con el fin de dar el punto de partida a la prueba de restauración. En caso, que la cinta y/o su contenido presenten problemas se busca la cinta con la fecha más cerca al punto de restauración acordado. La evidencia del control queda registrado en documento donde se indican todos los pasos que se ejecutan o en la Mesa de Servicios de TI.. - CORRECTIVO Y DETECTIVO El grupo de operadores apoyado por los administradores de plataforma (bases de datos), semestralmente o cuando se requiera, ejecuta las pruebas de respaldo, inicialmente verificando las cintas y validando el contenido de esta, con el fin de dar el punto de partida a la prueba de restauración. En caso, que la cinta y/o su contenido presenten problemas se busca la cinta con la fecha más cerca al punto de restauración acordado. La evidencia del control queda registrado en documento donde se indican todos los pasos que se ejecutan o en la Mesa de Servicios de TI.. - CORRECTIVO Y DETECTIVO EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. La herramienta SIEM monitorea los servicios de la infraestructura tecnológica (incluido urls) y una vez se evidencia indisponibilidad del servicio, alertas de seguridad notifica mediante correo electrónico a los administradores de plataforma o a los ingenieros de que realizan monitoreo de la herramienta en la Subgerencia de Infraestructura Tecnológica, con el fin que se verifique y atienda la indisponibilidad del servicio o incidente presentado. La evidencia del control queda registrada en la herramienta SIEM y /o monitoreo realizado por el personal de infraestructura.	ALTO	MODERADO	MODERADO	REDUCIR	1. Reforzar el control de revisión de la matriz de copias de respaldo por parte de los administradores de bases de datos	Indicador. Matriz de programación verificada	Recursos Humanos, Recursos Tecnológicos	Administradores de plataforma (bases de datos)	30/06/2022
RS-13-8	**PROVISIÓN Y SOPORTE DE SERVICIOS TI**	Mantener la infraestructura tecnológica mínimo en un 95% de disponibilidad y atender satisfactoriamente, mínimo el 90% de las solicitudes registradas durante la vigencia en la mesa de servicios de TI.	ANTIVIRUS (Software)	Pérdida de Disponibilidad ANTIVIRUS	Seguridad Digital	1. Ausencia de copias de respaldo 2. Ubicación de los archivos de configuración. 3. Ausencia de planes de continuidad	El administrador de la plataforma de antivirus mensualmente verifica que se están generando los respaldos automáticos. De no generarse los respaldos, revisa la configuración de la herramienta. Las evidencias del seguimiento a la generación de backups queda registrada en el equipo del administrador de la plataforma La herramienta SIEM monitorea los servicios de la infraestructura tecnológica (incluido urls) y una vez se evidencia indisponibilidad del servicio, alertas de seguridad notifica mediante correo electrónico a los administradores de plataforma o a los ingenieros de que realizan monitoreo de la herramienta en la Subgerencia de Infraestructura Tecnológica, con el fin que se verifique y atienda la indisponibilidad del servicio o incidente presentado. La evidencia del control queda registrada en la herramienta SIEM y /o monitoreo realizado por el personal de infraestructura. Los ingenieros asignados para realizar monitoreo a la plataforma del SIEM, una vez evidencian indisponibilidad del servicio, alertas de seguridad notifican mediante correo electrónico a los administradores de las plataformas, con el fin que se verifique y atienda la indisponibilidad del servicio o incidente presentado. La evidencia del control queda registrada en el correo remitido a los administradores de plataforma.	MODERADO	MODERADO	MODERADO	REDUCIR	Realizar los mantenimientos preventivos de la plataforma	Meta: 3 # mantenimientos realizados / numero de mantenimientos programados	Recursos Humanos del proveedor , Recursos Tecnológicos	Subgerente de Infraestructura Tecnológica	30/06/2022
RS-13-27	**PROVISIÓN Y SOPORTE DE SERVICIOS TI**	Mantener la infraestructura tecnológica mínimo en un 95% de disponibilidad y atender satisfactoriamente, mínimo el 90% de las solicitudes registradas durante la vigencia en la mesa de servicios de TI.	1. Gerentes / Subgerentes 2. Administradores de Seguridad Perimetral	Pérdida de Confidencialidad del recurso humano	Seguridad Digital	Desconocimiento de politicas de seguridad de la información	El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario designado de RRHH y/o OAI cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado los deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no esté firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (SRH o OAJ)	MODERADO	FUERTE	MODERADO	REDUCIR	Sensibilizar a los funcionarios / contratistas (Gerentes, Subgerentes y Administradores de seguridad perimetral) sobre la importancia de su rol y respecto a los controles de seguridad y privacidad de la información que se deben tener en cuenta con el fin que no se materialicen riesgos de seguridad.	Meta1. 2 administradores de seguridad perimetral Indicador Numero de administradores de seguridad perimetral sensibilizados / # de administradores de seguridad perimetral de la Unidad	Recursos Humanos y Recursos Físicos	Gerente de Tecnología y Subgerentes	30/06/2022
RS-13-28	**PROVISIÓN Y SOPORTE DE SERVICIOS TI**	Mantener la infraestructura tecnológica mínimo en un 95% de disponibilidad y atender satisfactoriamente, mínimo el 90% de las solicitudes registradas durante la vigencia en la mesa de servicios de TI.	1. Gerentes / Subgerentes 2. Administradores de Seguridad Perimetral	Pérdida de Disponibilidad del recurso humano	Seguridad Digital	1. Ausencia del personal 2. Desconocimiento de politicas	El oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. La persona designadada por el jefe de la dependencia cada vez que se retira un funcionario o un contratista revisa el formato de entrega de cargo y/o informe final respectivamente con el fin de verificar que todo lo que manejaba quede registrado en el formato correspondiente y en una carpeta sus evidencia. En caso que no este diligenciado de acuerdo a lo requerido este no es firmado por el jefe de la depencia hasta que se lleve a feliz término. El formato y/o informe final debe estar diligenciado y firmado por el profesional de retiro y el jefe de la dependencia. La secretaria debe radicar este en SRH o en la Subgerencia de Contratación para que sea adjuntado en el expediente correspondiente.	MODERADO	FUERTE	MODERADO	REDUCIR	Definir plan de documentación a desarrollar sobre el manejo de la plataforma perimetral de la Unidad.	Meta. Cronograma para la documentación de seguridad perimetral	Recursos Humanos y Recursos Físicos	Gerente de Tecnología y Subgerentes	30/06/2022

15. CONTROL DISCIPLINARIO INTERNO

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital).	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN

RS-15-1	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Proceso disciplinario verbal 2. Proceso disciplinario segunda instancia 3. Proceso Discipinario Ordinario 4. Actas de reparto 5. Actas de seguimiento (Información Análoga)	Pérdida de Confidencialidad e Integridad Procesos Disciplinarios-Actas (Información Análoga)	Seguridad Digital	1. Ausencia de controles de acceso a la información. 2. Desconocimiento o no aplicación de las politicas de seguridad y privacidad de la información	El jefe de dependencia asigna a un funcionario de la OCD para que controle y sea responsable de la información que se almacena en el archivo de gestion. Esta asignación se realiza cada vez que se requiera de acuerdo a las necesidades del proceso con el propósito que solo se pueda tener control de la informacion de la dependencia y evitar el acceso por parte de personal no autorizado. En caso que no exista la asignación de la persona responsable del archivo cualquier funcionario de la OCD puede acceder a los documentos del mismo. La evidencias de la asignación de personal quedan registradas en las actas de reunión de seguimiento. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – PREVENTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	1. Designar a un servidor de la Dependencia como responsable y custodio del archivo de gestión, con el fin de controlar el acceso al mismo . 2.Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras	1. Meta 1: 1 Indicador: 1 Servidor designado 2.Meta 2: 100% funcionarios/contratistas de OCD sensibilizados Indicador 2 # personas sensibilizadas / # personas convocadas*100	Recursos Humanos Recurso Físico (Llave)	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2022
RS-15-3	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Proceso disciplinario verbal 2. Proceso disciplinario segunda instancia 3. Proceso Discipinario ordinario 4. Actas de reparto 5. Actas de seguimiento (Información Digital/Electrónica)	Pérdida de Confidencialidad e Integridad Procesos Disciplinarios-Actas ((Información Digital/Electrónica))	Seguridad Digital	Deficiencia en la autorización de permisos de la información Acceso intencionado por parte de personal no autorizado Errores en los procesos de recopilación y captura de información Ausencia de control de acceso Borrado de información / datos personales por error humano Desconocimiento de politicas de seguridad de la información	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia cada vez que se requiera, con el propósito que se otorguen los permisos correspondientes al funcionario y poder evitar el acceso no autorizado a la información. El jefe de dependencia registra la solicitud en la mesa de servicios de TI. En caso que se realice la asignación por parte de personal diferente al jefe de dependencia, esta solicitud es cerrada y no resuelta por la mesa de servicios de TI. La evidencia de la solicitud queda registrada en la mesa de servicios de TI. El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos o por mesa de servicios, indicando los ajustes requeridos. La evidencia queda registrada en la mesa de servicios TI o en correo electronico EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – PREVENTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	1. Continuar la revisión del reporte de cuentas de usuario 2.Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras	Meta1 = 3 Indicador1 Revisiones realizadas / revisiones programadas*100 2.Meta 2: 100% funcionarios/contratistas de OCD sensibilizados Indicador 2 # personas sensibilizadas / # personas convocadas*100	Recursos Humanos, Tecnológicos	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2022
RS-15-5	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Archivo de gestion de la OCD (Instalaciones)	Pérdida de Confidencialidad e Integridad (Archivo de Gestión OCD)	Seguridad Digital	Ausencia de control de acceso Desconocimiento de politicas de seguridad de la información	El jefe de dependencia asigna a un funcionario de la OCD para que controle y sea responsable de la información que se almacena en el archivo de gestion. Esta asignación se realiza cada vez que se requiera de acuerdo a las necesidades del proceso con el propósito que solo se pueda tener control de la informacion de la dependencia y evitar el acceso por parte de personal no autorizado. En caso que no exista la asignación de la persona responsable del archivo cualquier funcionario de la OCD puede acceder a los documentos del mismo. La evidencias de la asignacion de personal quedan registradas en las actas de reunión de seguimiento. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos o por mesa de servicios, indicando los ajustes requeridos. La evidencia queda registrada en la mesa de servicios TI o en correo electronico	MODERADO	FUERTE	MODERADO	REDUCIR	1. Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras 2. Continuar la revisión del reporte de cuentas de usuario	Meta 1 : 100% funcionarios/contratistas de OCD sensibilizados # personas que participan / # personas convocadas*100 Meta 2 = 3 Indicador1 Revisiones realizadas / revisiones programadas*100	Recursos Humanos Recurso Físico (Llave)	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2022
RS-15-7	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Sistema de grabación 2.Correo electronico OCD 3.Sistema de Informacion Disciplinario Distrital (Servicio)	Pérdida de Confidencialidad e Integridad (Sistema de Grabación - Correo electronico OCD -Sistema de Informacion Disciplinario Distrital)	Seguridad Digital	Ausencia de control de acceso Desconocimiento de politicas de control de acceso	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia cada vez que se requiera, para hacer uso del sistema de grabación entregado por la Subgerencia de Infraestructura Tecnologica (teams). Asi como el acceso (usuario y/o contraseñas) al correo de la Dependencia y el Sistema de Información Disciplinaria SID, con el propósito que unicamente accedan a estos servicios (audiencias, diligencias, correo electronico, y SID) el personal autorizado. La evidencia de la asignación queda registrada en la herramienta de teams, correo electronico o mesa de servicios de ser el caso. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO	MODERADO	FUERTE	MODERADO	ASUMIR	1. Designar al servidor de la dependencia responsable y custodio del correo electronico de la Oficina , de actualizaciones en el Sistema SID Y los profesionales encargados de realizar las diligencias 2. Solicitar - Cuando se requiera - por correo electronico a al administrador del Sistema de Información Disciplinario el usuario y clave de acceso para el servidor designado para diligenciar la informacio en el sistema SID. 3.Designacion de servidor de la Oficina responsable y custodio del correo electronico, con el fin de controlar el acceso al mismo y la información . 3.Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras	1.Meta 1 : 1 Indicador: 1 Servidor designado para cada tarea Meta2: 1 Indicador: 1 Servidor designado 2. Meta 2: 1 correo electronico. Indicador:1 correo electronico enviado 3.Meta 3: 100% funcionarios/contratistas de OCD sensibilizados Indicador 3 # personas sensibilizadas / # personas convocadas*100	Recursos Humanos Recurso Físico (Llave)	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2023
RS-15-11	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Profesional especializado y universitario 2. cargos secretariales 3.Contratistas (Recurso Humano)	Pérdida de Confidencialidad (Profesionales - cargos secretariales - contratistas)	Seguridad Digital	Ausencia del personal Entrenamiento insuficiente en seguridad Falla de conciencia acerca de la seguridad	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO Cada vez que se va a vincular un funcionario o contratista de la dependencia desde la Subgerencia de recursos Humanos / Oficina Asesora Jurídica revisan que se encuentre firmado el acuerdo de confidencialidad para el manejo de la información de la Unidad. La evidencia es el documento firmado por cada funcionario / contratista , el cual queda anexo al expediente laboral/contractual correspondiente. En caso que el documento no se encuentre firmado, se debe actualizar y hacer firmar al funcionario o contratista.	MODERADO	FUERTE	MODERADO	REDUCIR	1. Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras 2.Implementar firma de acuerdo de confidencialidad con el fin de asegurar la información de la dependencia	1. Meta: 100% funcionarios/contratistas de OCD sensibilizados Indicador 2 # personas sensibilizadas / # personas convocadas*100 2.Meta:2 : 1 Indicador 1 firma digital implementada	Recursos Humanos Recurso Físico (Llave)	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2024
RS-15-13	CONTROL DISCIPLINARIO INTERNO	Gestionar durante la vigencia, el 100% de los procesos disciplinarios en curso, cumpliendo los principios constitucionales y legales del debido proceso y ejecutar trimestralmente las actividades de prevención programadas para mitigar la ocurrencia de faltas disciplinarias en salvaguarda de la función pública	1. Base de datos de los procesos disciplinarios 2. Bases de datos con información relacionada con los procesos judiciales 3. Base de datos cuadro de términos de los procesos disciplinarios (Bases de Datos)	Pérdida de Confidencialidad e Integridad Procesos Disciplinarios- Bases de Datos en excel ((Información Digital/Electrónica))	Seguridad Digital	Deficiencia en la autorización de permisos de la información Acceso intencionado por parte de personal no autorizado Errores en los procesos de recopilación y captura de información Ausencia de control de acceso Borrado de información / datos personales por error humano Desconocimiento de politicas de seguridad de la información	El jefe de dependencia realiza la asignación de accesos de los funcionarios y contratistas de la dependencia cada vez que se requiera, con el propósito que se otorguen los permisos correspondientes al funcionario y poder evitar el acceso no autorizado a la información. El jefe de dependencia registra la solicitud en la mesa de servicios de TI. En caso que se realice la asignación por parte de personal diferente al jefe de dependencia, esta solicitud es cerrada y no resuelta por la mesa de servicios de TI. La evidencia de la solicitud queda registrada en la mesa de servicios de TI. El jefe de dependencia revisa cada 4 meses el reporte de cuentas de usuario remitido por el gestor de accesos, con el fin de validar que los permisos o privilegios asignados al funcionario o contratista esten acordes a las funciones y/o actividades actuales. El jefe de dependencia revisa los permisos solicitados contra los permisos asignados a los funcionarios y contratistas y en caso de ser necesario solicita realizar las modificaciones respondiendo el correo electrónico inicialmente enviado por el gestor de accesos o por mesa de servicios, indicando los ajustes requeridos. La evidencia queda registrada en la mesa de servicios TI o en correo electronico EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – PREVENTIVO	MODERADO	FUERTE	MODERADO	REDUCIR	1. Continuar la revisión del reporte de cuentas de usuario 2.Solicitar sensibilizaciones de seguridad de la información para el personal de la OCD referente al manejo de información física y acceso a áreas seguras	Meta1 = 3 Indicador1 Revisiones realizadas / revisiones programadas*100 2.Meta 2: 100% funcionarios/contratistas de OCD sensibilizados Indicador 2 # personas sensibilizadas / # personas convocadas*100	Recursos Humanos, Tecnológicos	Jefe de Dependencia de la Oficina de Control Disciplinario	30/06/2025

16. GESTIÓN CATASTRAL TERRITORIAL

No	PROCESO	OBJETIVO	ACTIVO (Solo aplica para la formulación de riesgos de seguridad digital)	RIESGO	TIPOLOGÍA DEL RIESGO	CAUSAS	CONTROLES	RIESGO INHERENTE	SOLIDEZ DEL CONJUNTO DE CONTROLES	RIESGO RESIDUAL	TRATAMIENTO - OPCIONES DE MANEJO	ACTIVIDADES PROGRAMADAS	META/INDICADOR	RECURSOS	RESPONSABLES	FECHA LÍMITE DE IMPLEMENTACIÓN
RS-16-1	GESTIÓN CATASTRAL TERRITORIAL	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	1. Tramites Inmediatos 2. Tramites no inmediatos	Perdida de confidencialidad e integridad de la información análoga	Seguridad Digital	1. Desconocimiento de las politicas de seguridad de la informacion 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizaciones de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario (a) designado para manejar los documentos físicos del territorio es el/la encargado (a) de asegurar que se mantenga la integridad y confidencialidad de la información física. Si se requiere un documento, se debe solicitar a este funcionario(a) quien accederá al área exclusiva designada para el archivo (cuando aplique) para la búsqueda de la información solicitada. En algunos territorios (Santaforia, Palmira, Dosquebradas, Pereira) se maneja bitacora de prestamo de documentos para llevar el control correspondiente. El funcionario designado de RRHH y/o OAI cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado los deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no este firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (SRH o OAI)	ALTO	MODERADO	ALTO	REDUCIR	1. Asignación formal (memorando y/o correo electrónico) de persona encargada de manejar la información física del territorio. 2. Continuar con la verificación semanal del aseguramiento de la información análoga.	1. # de trámites asignados / total de trámites 2. # de trámites verificados semanal/ total de trámites	Recursos Humanos	Lider de proceso	30/06/2022

RS-16-2	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	1. Tramites Inmediatos 2. Tramites no inmediatos	Perdida de disponibilidad de la información análoga	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	El funcionario (a) designado para manejar los documentos físicos del territorio es el/la encargado (a) de asegurar que se mantenga la integridad y confidencialidad de la información física. Si se requiere un documento, se debe solicitar a este funcionario(a) quien accederá al área exclusiva designada para el archivo (cuando aplique) para la búsqueda de la información solicitada. En algunos territorios (SantaRosa, Palmira, Dosquebradas, Pereira) se maneja bitacora de prestamo de documentos para llevar el control correspondiente. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El encargado de gestión documental cada vez que se requiere realiza la digitalización de documentos del territorio. Esta información es almacenada en Cordis. Semanalmente se remite consolidado de la información recibida al lider del subproceso de gestión documental.	ALTO	FUERTE	MODERADO	REDUCIR	1. Continuar con el proceso de digitalización de la información análoga semanalmente con el fin de generar copias de soporte.	# de trámites digitalizados / total de trámites	Recursos Humanos	Lider de proceso	30/06/2022
RS-16-7	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	1. Base de Datos Santa Rosa, Pereira, Palmira y Dosquebradas. 2. Base de datos.	Perdida de confidencialidad e integridad de las bases de Datos	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO La persona encargada de asignar permisos en la plataforma de sharepoint en cada territorio, realiza el proceso de asignación cada vez que se requiera dando los permisos al usuario de acuerdo al rol correspondiente. La evidencia de la asignación queda registrada en la plataforma.	ALTO	MODERADO	MODERADO	REDUCIR	Realizar proceso de Revisión de gestion de acceso a los usuarios	# de revisiones / total de accesos	Tecnologia	Encargado de la plataforma de sharepoint en cada territorio	30/06/2022
RS-16-9	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	1. Resoluciones. 2. Actas. 3. PQRS. 4. Trámites Inmediatos 5. Trámites No Inmediatos (Información electrónica)	Perdida de confidencialidad e integridad de información electrónica	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO La persona encargada de asignar permisos en la plataforma de sharepoint en cada territorio, realiza el proceso de asignación cada vez que se requiera dando los permisos al usuario de acuerdo al rol correspondiente. La evidencia de la asignación queda registrada en la plataforma.	ALTO	MODERADO	ALTO	REDUCIR	Sensibilizar al equipo de los territorios en el manejo de la información digital - controles de seguridad que se deben tener en cuenta para mitigar la materialización de los riesgos	Meta1. Capacitar al 50% de los funcionarios y contratistas de cada territorio Indicador # personas sensibilizadas / # personas en el territorio	Recursos Humanos y Tecnológicos	Lider del Proceso	30/06/2022
RS-16-10	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	1. Resoluciones. 2. Actas. 3. PQRS. 4. Trámites Inmediatos 5. Trámites No Inmediatos (Información electrónica)	Perdida de disponibilidad de la información electrónica	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO La información es respaldada automaticamente en la plataforma de Sharepoint El encargado de la plataforma de sharepoint de cada territorio cada vez que se requiera realiza procesos de restauración de la información con el fin de que esta se encuentre disponible. En caso de no poder realizar el proceso de restauración debe colocar una mesa de servicios de TI para que se solicite apoyo al proveedor de Microsoft para la respectiva recuperación. La evidencia de control queda en la mesa de servicios de TI.	ALTO	FUERTE	MODERADO	REDUCIR	Sensibilizar al equipo de los territorios en el manejo de la información digital - controles de seguridad que se deben tener en cuenta para mitigar la materialización de los riesgos	Meta1. Capacitar al 100% de los funcionarios y contratistas de cada territorio	Recursos Humanos y Tecnológicos	Lider del Proceso	30/06/2022
RS-16-11	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	Archivos de gestión para Santa Rosa, Pereira, Palmira y Dosquebradas	Perdida de confidencialidad e integridad de archivos de gestión	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO En cada territorio existe un area donde se maneja la información física, el lugar es accedido unicamente por el personal de apoyo de gestión documental. En algunos casos el área cuenta con cerradura.	ALTO	FUERTE	ALTO	REDUCIR	Sensibilizar al equipo de los territorios en el los controles de seguridad que se deben tener en cuenta en los archivos de gestión con el fin mitigar la materialización de los riesgos	Meta1. Capacitar al 100% de los funcionarios y contratistas de cada territorio	Recursos Humanos y Tecnológicos	Lider del Proceso	30/06/2022
RS-16-12	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	Archivos de gestión para Santa Rosa, Pereira, Palmira y Dosquebradas	Perdida de disponibilidad de archivos de gestión	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. – DETECTIVO En cada territorio existe un area donde se maneja la información física, el lugar es accedido unicamente por el personal de apoyo de gestión documental. En algunos casos el área cuenta con cerradura.	MODERADO	FUERTE	MODERADO	REDUCIR	Sensibilizar al equipo de los territorios en el los controles de seguridad que se deben tener en cuenta en los archivos de gestión con el fin mitigar la materialización de los riesgos	Meta1. Capacitar al 100% de los funcionarios y contratistas de cada territorio	Recursos Humanos y Tecnológicos	Lider del Proceso	30/06/2022
RS-16-13	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	Funcionarios y contratistas de Santa Rosa, Pereira, Palmira y Dosquebradas	Perdida de confidencialidad de funcionarios y contratistas de los territorios	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados. El funcionario designado de RRHH y/o OAJ cada vez que ingresa un funcionario y/o contratista a la Unidad verifica que el formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de a Unidad Administrativa Especial De Catastro Distrital, se encuentre debidamente firmado; con el fin que el funcionario y/o contratista haya aceptado los deberes y derechos en las cláusulas allí descritas. En caso de que, el formato no esté firmado se remite nuevamente al funcionario y/o contratista para llevar a feliz término el proceso de contratación. La evidencia queda en el expediente del funcionario y/o contratista manejado por correspondiente (SRH o OAJ)	ALTO	FUERTE	ALTO	REDUCIR	Realizar sensibilizaciones para que el personal conozca sobre los contr	Meta1. Capacitar al 100% de los f	Recursos Humanos	Lider del Proceso	30/06/2022
RS-16-14	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	Funcionarios y contratistas de Santa Rosa, Pereira, Palmira y Dosquebradas	Perdida de disponibilidad de funcionarios y contratistas de los territorios	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Generar las actas de entrega (contratistas) y verificar formato de entre	Meta1. 100% documentos factas	Recursos Humanos	Lider del Proceso	30/06/2022
RS-16-15	**GESTIÓN CATASTRAL TERRITORIAL**	Prestar el servicio como gestor u operador catastral a entidades territoriales de acuerdo con la capacidad institucional y en ejecución al 100% de los contratos suscritos.	Equipos de Cómputo	Perdida de confidencialidad e integridad de equipos de cómputo en los territorios	Seguridad Digital	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia o insuficiencia de pruebas de software 3. Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo 4. Asignación errada de los derechos de acceso 5. Falla en la producción de informes de gestión	El personal de la mesa de servicios cada vez que se va a entregar un equipo de cómputo, configura que el equipo cuente con usuario de administrador para realizar procesos de administración del equipo. Lo anterior se realiza con el fin que el usuario normal no pueda realizar instalaciones sobre el equipo asignado. En caso de no poder configurar el usuario administrador en el equipo, se debe reinstalar el mismo hasta que se pueda realizar la configuración. La evidencia del proceso queda registrado en la mesa de servicios de TI y en el acta de entrega del equipo. EL oficial de seguridad de la información cada mes revisa el listado de las personas a convocar a las sensibilizacionES de seguridad de la información, con el fin que todo el personal de las dependencias asista al proceso programado. Verifica las personas que asistieron y las que no asistieron. Si existen personas que no asistieron remite correo al enlace de cada dependencia para que se programen a los funcionarios y contratistas. De igual manera programa a los funcionarios y contratistas a la siguiente sensibilización de seguridad de la información. La evidencia del control queda registrada en el correo remitido a los enlaces de cada dependencia y a los funcionarios o contratistas convocados.	MODERADO	FUERTE	MODERADO	REDUCIR	Realizar sensibilizaciones para que el personal conozca sobre los controles y lineamientos de seguridad de la información, con el fin de evitar la materialización del riesgo de perdida de confidencialidad en el recurso humano	Meta1. Capacitar al 100% de los funcionarios y contratistas de cada territorio	Recursos Humanos y Tecnológicos	Lider del Proceso	30/06/2022