El servicio público es de todos

Función Pública

FUNCIÓN PUBLICA

Plan de tratamiento de riesgos de seguridad de la información vigencia 2020-2022

Enero de 2021

VERSIÓN 3

Versión	Fecha Versión	Observación
1	2020-10-31	Versión año 2020
2	2021-01-19	Primera versión año 2021
3	2021-01-30	Actualización 2021

Tabla 1. Control de cambios

Tabla de contenido

Tablas del Informe

Tabla de ilustraciones

Introducción

Durante el segundo semestre del año 2020, el Consejo Nacional de Política Económica y Social, publico el Documento CONPES 3995 sobre POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, el cual resalta que "*El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías*."

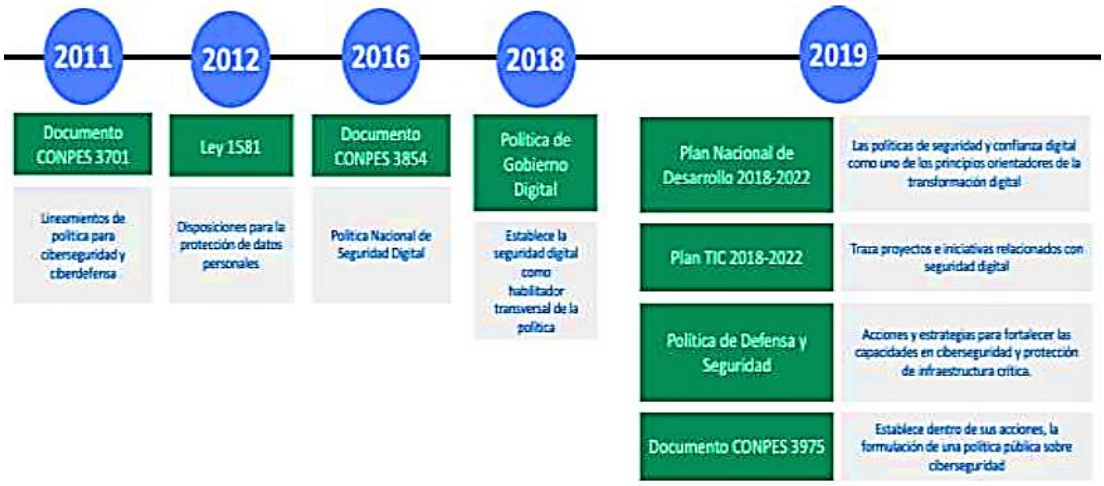

Ilustración 1. Implementación de Políticas y estrategias desde el Gobierno Nacional para brindar seguridad y defensa en el ciberespacio. Fuente: Elaboración DNP, 2020

Sobre ese marco de trabajo el Departamento Administrativo de la Función Pública presenta su plan de tratamiento de riesgos de seguridad digital para la vigencia 2021.

1. Objetivo

1.1. Objetivo General

Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional

1.2. Propósitos

- Mejorar continuamente los conocimientos del equipo de trabajo en materia de seguridad digital y prevención de riesgos.

- Preparar a todos los colaboradores para responder ante incidentes de seguridad que afecten los activos de información.

- Mejorar la confianza de los grupos de valor en nuestra capacidad institucional para preservar la seguridad de la información.

1.3. Indicador

- La Efectividad en el tratamiento de los riesgos de seguridad digital.

- Medición: Porcentaje de riesgos de seguridad digital adecuadamente gestionados de acuerdo al plan de tratamiento

.

2. Marco normativo

La actualización del plan estratégico se define teniendo en cuenta el siguiente marco normativo:

Marco Normativo	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública	2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto 103 de 2015,	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	2018	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009,	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para

Marco Normativo	Año	Descripción
		la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia1991 - Artículo 15	2015	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Tabla 2. Marco normativo

3. Tratamiento de riesgos

3.1. Factores de riesgo

Para la vigencia 2021 se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura
- Identificación y protección de los datos de carácter personal
- Adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente
- Entorno global digital inseguro
- Aislamiento forzoso del personal en sus residencias
- Segregación apropiada de roles y privilegios en todos los sistemas de información

3.2. Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad). La siguiente tabla describe la valoración de los riesgos definidos por el Departamento Administrativo de la Función Pública.

3.3. Estrategia de tratamiento de riesgo

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

- Transferir: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.

- Mitigar: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

- Evitar: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.
- Aceptar: consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2021, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

Ilustración 2.Estrategias de Gestión de Riesgos 2021

3.3.1 Estrategias Orientadas al Conocimiento

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los servidores, contratistas y pasantes apropien conocimientos en materia de:

- Ley de protección de datos personales
- Ley de transparencia y acceso a la información
- Políticas institucionales de seguridad digital
- Modalidades y control de ataques informáticos
- Uso seguro de los recursos informáticos

3.3.2 Estrategias Orientadas al Conocimiento

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, la Entidad adelantará en la vigencia 2021, acciones específicas en materia de:

- Fortalecimiento de su infraestructura de servicios básicos de energía
- Actualización de planes alternos de operación por dependencias en caso de: pérdida de continuidad de servicios informáticos, imposibilidad de accesos a sedes y aislamiento obligatorio por emergencia sanitaria

- Mejoramiento de sus capacidades de detección oportuna de eventos adversos de seguridad de la información

3.3.3 Estrategias orientadas al conocimiento

Con el fin de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados la Entidad emprenderá en la vigencia 2021 acciones específicas para:

- Actualizar los instrumentos de acceso a la información pública
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información

3.3.4 Estrategias de fortalecimiento de controles técnicos

Ante el aumento del tipo y complejidad de amenazas informáticas la entidad implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos
- Reforzamiento de controles de acceso a servicios en la nube
- Verificación y control de copias de respaldo
- Control de cambios en plataformas tecnológicas
- Aplicación de parches de seguridad y actualización de equipos de procesamiento de datos

3.4. Hoja de ruta

Producto	2021											
	E	F	M	A	M	J	J	A	S	O	N	D
Estrategias orientadas al conocimiento												
Estrategias orientadas a la continuidad del servicio												
Estrategias orientadas al control de acceso												
Estrategias de fortalecimiento de controles técnicos												

Tabla 3. Hoja de ruta

3.5. Acciones específicas

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones Preventivas	Acción de contingencia ante posible materialización
Direccionamiento Estratégico	Pérdida de Confidencialidad	Cultura de inseguridad (desconocimiento de buenas prácticas)	Procesos disciplinarios	El jefe de la Oficina Asesora de Planeación cada dos meses vela por el cumplimiento y la efectividad de la campaña de sensibilización en seguridad de la información. En caso de desviación se revalúa la estrategia de la campaña. Se evidencia su implementación mediante piezas, actas de reunión y reportes.	**1.** Activar el procedimiento de gestión de incidentes.
		Colaboradores que divulgan la información	Deterioro del clima laboral de la Entidad	La Coordinadora del Grupo de Mejoramiento durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a través de la documentación de las políticas de operación y del SIG. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución a través de la documentación en Intranet.	**2.** Reportar a las instancias pertinentes el caso.
		Claves genéricas	Imposibilidad de determinar el responsable de la divulgación	La Coordinadora del Grupo de Mejoramiento durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a través de la documentación de las políticas de operación y del SIG. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución a través de la documentación en Intranet.	**3.** Solicitar el cambio inmediato de la contraseña o en caso extremo la inhabilitación de la contraseña.
		Divulgaciones no autorizadas de claves	Imposibilidad de determinar el responsable de la divulgación	El Oficial de Seguridad de la Información durante la vigencia, implementará la estrategia de sensibilización y documentación para el uso de contraseñas seguras. En caso	**4.** Activar el procedimiento de gestión de incidentes y

				de resistencia al cambio y baja participación en la sensibilización, desde la alta dirección se emitirá una directriz de obligatorio cumplimiento. Se evidencia a través del plan de trabajo, estrategia documentada, actas de reunión.	reportar en el plan de mejoramiento.
Direccionamiento Estratégico	Pérdida de Disponibilidad	Inflexibilidad para la gestión de cambios	Acciones de entes de control	El personal de la Oficina Asesora de Planeación cada vez que se requiera, acompañará la apropiación e interiorización de los cambios, mediante sesiones de trabajo. Cuando se continúa presentando desconocimiento de los lineamientos, se recomendará el uso de herramientas automatizadas. Se evidencia su implementación mediante registros de reunión y recomendaciones documentadas.	**1.** El responsable del documento notifica las demoras en la revisión y aprobación de cambios al Coordinador del Grupo de Mejoramiento quien activa acciones para agilizar el trámite respectivo.
		Ausencia de capacitación y manuales	Producción de información inexacta	El Grupo de Mejoramiento mensualmente y de manera selectiva revisará la actualización de los procesos a cargo, asegurando que se encuentren las versiones vigentes publicadas en la Intranet. Si se encuentra información desactualizada en la Intranet, se ajusta el documento de manera inmediata y se reportará el incumplimiento en la matriz de seguimiento. Se evidencia su implementación a través de las versiones de Intranet y comunicados internos.	**2.** El Coordinador del Grupo de Mejoramiento Institucional asigna de manera oportuna a la persona con conocimiento específico en el tema que requiere el usuario para atender el soporte y apoyo a las inquietudes.
		Desactualización de la información	Pérdida de credibilidad	El Grupo de Mejoramiento mensualmente enviará las alertas y comunicados a las dependencias para fortalecer el uso y la consulta de la información descrita en los procesos y procedimientos. En caso de detectar el uso de información desactualizada se documentará en el plan de mejoramiento y se informará a la tercera línea de defensa. Se evidencia a través del plan de mejoramiento y comunicados.	**3.** Tomar la última versión identificada del documento y reconstruirlo a través de fuentes como correos electrónicos, copias almacenadas por otros colaboradores y participación de los autores. Someter a aprobación y posterior publicación de la versión reconstruida.

		Falla tecnológica	Toma de decisiones inadecuada	El Jefe de la OAP cuando se presente una incidencia no atendida dentro del acuerdo de nivel de servicio, notificará directamente al Jefe de OTIC y a la tercera línea de defensa el impacto de la incidencia, mediante comunicado oficial. Si aun así el incidente no es resuelto, se llevará ante Comité para su análisis y toma de decisiones. Se evidencia mediante comunicados oficiales y actas de comité.	**4.** Se establece comunicación directa con el jefe de OTIC para tomar medidas oportunas para su restablecimiento.
Direccionamiento Estratégico	Pérdida de la Integridad	Claves genéricas	Pérdida de imagen y confianza institucional	La Coordinadora del Grupo de Mejoramiento durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a través de la documentación de las políticas de operación y del SIG. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución a través de la documentación en Intranet.	**1.** Solicitar el cambio inmediato de la contraseña o en caso extremo la inhabilitación de la contraseña.
		Falla tecnológica	Reprocesos	El Jefe de la OAP cuando se presente una incidencia no atendida dentro del acuerdo de nivel de servicio, notificará directamente al jefe de OTIC y a la tercera línea de defensa el impacto de la incidencia, mediante comunicado oficial. Si aun así el incidente no es resuelto, se llevará ante Comité para su análisis y toma de decisiones. Se evidencia mediante comunicados oficiales y actas de comité.	**2.** Se establece comunicación directa con el jefe de OTIC para tomar medidas oportunas para su restablecimiento.
		Inadecuado versionamiento de los documentos	Inadecuada toma de decisiones	El personal de OAP al momento de crear nuevas versiones de los documentos identifica los archivos con un estándar de nombre aplicando la guía para la organización de documentos electrónicos. Cuando se nombran incorrectamente los archivos, el encargado de la TRD notifica al autor las inconsistencias para su rectificación. Se evidencia a través de TRD y correos electrónicos.	**3.** Notificar al autor de las inconsistencias para su rectificación.

Gestión del Conocimiento	Pérdida de Confidencialidad	Errores en almacenamiento de documentos físicos	Hallazgos de entes de control	No aplica	El profesional de la dependencia se reúne con el profesional del Grupo de Gestión Documental para verificar que la gestión del archivo se esté llevando según lineamientos emitidos.
		Incorrecta clasificación de nivel de acceso de los datos de la PQRSD	Incumplimiento ley habeas data	No aplica	Actualizar la versión del documento publicado sin el dato semiprivado.
		Debilidades en los recursos físicos para almacenamiento y custodia de PQRSD en papel	Incumplimiento ley habeas data	No aplica	El profesional de la dependencia se reúne con el profesional del Grupo de Gestión Documental para verificar que la gestión del archivo se esté llevando según lineamientos emitidos.
Generación de Productos y Servicios	Pérdida de Disponibilidad	Incompatibilidad en los servicios de interoperabilidad para intercambio de información	Inconsistencias o vacíos en el producto de caracterización de empleo público	No aplica	Coordinar con el supervisor del convenio de la Registraduría Nacional la recolección de la información a través de almacenamiento externo.
		Fallas tecnológicas en el sistema de información o canales de comunicación en Función Pública	Reprocesos y demoras en la ejecución de actividades	No aplica	
		Fallas tecnológicas en el sistema de información o canales de comunicación en Registraduría Nacional	Generación de información inconsistente por procesos manuales	No aplica	

Generación de Productos y Servicios	Pérdida de Confidencialidad	Inadecuado manejo de roles y privilegios del personal con acceso a la información	Acceso de la información por parte de personal no autorizado	Los coordinadores de la Dirección de Empleo Público cada vez que se vincule un servidor o contratista, socializará la ruta en donde se encuentra los documentos asociados a los roles del SIGEP, con el fin de conocer y validar los requisitos para cada uno de los mismos. En caso que el documento se encuentre desactualizado se deberá ajustar a la normativa vigente. Se evidencia en los documentos, presentaciones en power point o videos.	**1.** Retirar el rol inmediatamente
		Ausencia de acuerdos de confidencialidad	Pérdida de la imagen institucional y del proceso	Los coordinadores de la Dirección de Empleo Público cada vez que se vincule un servidor o contratista socializara a los funcionarios y contratistas las obligaciones de los acuerdos de confidencialidad, para cumplir con la normatividad de tratamiento de los datos personales. En caso de incumplimiento se procede administrativa o disciplinariamente. Se evidencia en correos electrónicos, contratos o actas de posesión.	**2.** Oficiar el acuerdo de confidencialidad con copia a la Secretaria General.
		Incumplimiento de políticas de contraseñas seguras	Acceso de la información por parte de personal no autorizado	El director de la Dirección de Empleo Público mensualmente socializará la importancia del manejo de contraseñas seguras para el sistema SIGEP, con el fin de mantener un nivel de seguridad adecuado para el acceso al sistema de información. En caso de no efectuar la socialización se enviará a través de correo electrónico. Se evidencia en registro de reunión interna o correo electrónico.	**3.** Solicitar a la Oficina de Tecnologías de la información que todos los servidores y contratistas cambien la contraseña del sistema SIGEP en el próximo inicio de sesión.
Generación de Productos y Servicios	Pérdida de Integridad	Fallas tecnológicas en la plataforma	Pérdida de credibilidad	Los integrantes del gestor normativo cuando realizan la revisión de la información publicada remiten un correo con los resultados de la inspección al supervisor del contrato y al líder del gestor normativo, con el fin de dejar registro de la verificación ejecutada. En caso de identificar errores de digitación se solicita la corrección al responsable. Se deja evidencia en correos electrónicos.	**1.** Cuando vuelva a activarse la plataforma se carga la información que quedo pendiente
		Errores de digitación	Toma de decisiones erróneas	La responsable de digitación cuando recibe notificación de que plataforma estará en mantenimiento reprograma sus actividades de cargue de información, con el fin de evitar perdida de datos. En caso de no recibir	**2.** Corregir la información y volver a publicar.

				notificación la plataforma estará disponible. Como evidencia se dejan correos de la Oficina de Tecnologías de la Información.	
Acción Integral	Pérdida de Integridad	Scripts o códigos fuente que no contemplan todos los casos cuando se hacen actualizaciones en las bases de datos.	Demoras o paralización de las actividades por necesidad de reconstrucción de los datos registrados a partir de la documentación física.	No aplica	**1.** Ubicar la copia de seguridad más reciente **2.** Restaurar la información que haya sido modificada o borrada. **3.** Verifica que la restauración haya sido exitosa.
		Malos procedimientos durante la restauración de copias de respaldo o reconstrucción de índices en el motor de bases de datos.	Demora en la toma de decisiones.	No aplica	**1.** Ubicar la copia de seguridad más reciente **2.** Restaurar la información que haya sido modificada o borrada. **3.** Verifica que la restauración haya sido exitosa.
		Diligenciamiento de fecha diferente a la registrada en los documentos físicos.	Reprocesos en las actividades operativas.	No aplica	**1.** Verificar contra las evidencias físicas. **2.** Informar sobre la inconsistencia encontrada al responsable. **3.** Corregir la información.
Acción Integral	Pérdida de Disponibilidad	Acceso no autorizado al archivo físico de la dependencia.	Procesos disciplinarios y administrativos	El Coordinador del Grupo de Apoyo a la Gestión Meritocrática semestralmente, con el fin de verificar la lista de personal de la dependencia que ingresa al área de archivo, valida el registro de entradas y salidas. En caso de no realizarse el diligenciamiento de ingreso imparte instrucciones para que se cumpla el control. Como evidencia se tienen los registros de entrada y registros de reunión.	**1.** En caso de pérdida del documento físico, se recurre al documento digitalizado en el servidor de carpeta compartidas. **2.** En caso de pérdida de los documentos digitales, se tiene el documento en el archivo en físico. **3.** En caso de pérdida del documento del archivo en físico y del documento digitalizado
		Errores en almacenamiento de la información	Pérdida de credibilidad institucional	El coordinador del Grupo de Apoyo a la Gestión Meritocrática semestralmente, con el fin de verificar los roles y privilegios del personal asociado a la Dependencia, valida los permisos de acceso a las carpetas en el servidor de carpeta compartidas, solicitando	

				un reporte a la OTIC (Oficina de Tecnologías de la Información y las Comunicaciones) en donde se evidencien las personas que tienen acceso a las carpetas y el tipo de permiso. Si se detectan usuarios o permisos que no corresponden, solicita el ajuste. Como evidencia se tienen correos electrónicos y el reporte de la OTIC.	en el servidor de carpeta compartidas, se recurre al aplicativo PSIGMA.
		Acceso no autorizado a los archivadores del área de Meritocracia.	Pérdida patrimonial	El profesional designado diariamente, con el fin de prevenir el acceso a las llaves de los archivadores de la Dependencia, las mantiene en un lugar seguro, bajo llave. En caso de que el profesional se encuentre ausente el coordinador tiene acceso al lugar de almacenamiento. Como evidencia se tienen los lugares de almacenamiento bajo llave.	
Acción Integral	Pérdida de Confidencialidad	Desconocimiento de las normas asociados a protección de datos personales	Demandas por ley habeas data	El coordinador de Asesoría y Gestión a partir de la vigencia 2019 documentara las propuestas de mensajes sobre protección de datos personales, para ser incluidas en el plan de sensibilización de seguridad. En caso de requerir ajustes de diseño se coordinará con la Oficina Asesora de Comunicaciones. Se deja evidencia en el plan de sensibilización de seguridad.	**1.** El Director de la Dirección de Empleo Público cuando se reciba una denuncia o demanda por habeas data coordina las acciones de respuesta con el Grupo de Defensa Jurídica.
		Debilidades en la administración de claves y contraseñas por parte de administradores delegados	Sanciones o llamados de atención por incumplimiento de ley habeas data	El coordinador de Asesoría y Gestión a partir de la vigencia 2019 documentara las responsabilidades sobre el correcto uso de la cuenta de usuario SIGEP para incluirlo en el protocolo de uso seguro. Los ajustes y recomendaciones serán coordinados con el responsable de seguridad de la información. Se deja evidencia en el protocolo.	**2.** El Director de Empleo Público enviará comunicación formal de la cuenta de usuario reiterando la importancia del manejo de la misma.
		Préstamo no controlado de cuentas de usuario	Pérdida de confianza Institucional	El coordinador de Asesoría y Gestión a partir de la vigencia 2019 documentara las responsabilidades sobre el correcto uso de la cuenta de usuario SIGEP en el protocolo de uso seguro. Los ajustes y recomendaciones serán coordinados con el responsable de seguridad de la información. Se deja evidencia en el protocolo.	**3.** El Director de Empleo Público enviará comunicación formal de la cuenta de usuario reiterando la importancia del manejo de la misma.
Acción Integral	Pérdida de Confidencialidad	Errores en las asignaciones de permisos de	Pérdida de credibilidad institucional	El coordinador del Grupo de Apoyo a la Gestión Meritocrática semestralmente, con el fin de verificar los roles y privilegios del	**1.** El coordinador y su equipo de trabajo determinan el alcance

		acceso a las carpetas del servidor de carpeta compartidas.		personal asociado a la Dependencia, valida los permisos de acceso a las carpetas en el servidor de carpeta compartidas, solicitando un reporte a la OTIC (Oficina de Tecnologías de la Información y las Comunicaciones) en donde se evidencien las personas que tienen acceso a las carpetas y el tipo de permiso. Si se detectan usuarios o permisos que no corresponden, solicita el ajuste. Como evidencia se tienen correos electrónicos y el reporte de la OTIC.	de la información divulgada o con pérdida de confidencialidad. **2.** Convocar al comité de crisis para evaluar la estrategia de respuesta ante la pérdida de confidencialidad. **3.** Determinar si se debe solicitar el apoyo de organizamos de seguridad en caso de delito informático. **4.** Paralelamente a las acciones anteriormente descritas, se solicita el acompañamiento de Defensa Jurídica.
		Uso de contraseñas con niveles bajos de seguridad.	Procesos disciplinarios y administrativos.	El coordinador del Grupo de Apoyo de Gestión Meritocrática trimestralmente, con el fin de mantener y preservar la confidencialidad de la información, solicita a la Oficina de Tecnologías de la Información y las comunicaciones que configure el cambio de contraseñas de la Dependencia. En caso de que no se tramite la solicitud, se comunicará con el jefe de la OTIC. Como evidencia se tienen correos electrónicos.	
Acción Integral	Pérdida de Integridad	Scripts o códigos fuente que no contemplan todos los casos cuando se hacen actualizaciones en las bases de datos.	Demoras o paralización de las actividades por necesidad de reconstrucción de los datos registrados a partir de la documentación física.	No aplica	**1.** Ubicar la copia de seguridad más reciente **2.** Restaurar la información que haya sido modificada o borrada. **3.** Verifica que la restauración haya sido exitosa.
		Malos procedimientos durante la restauración de copias de respaldo o reconstrucción de índices en el motor de bases de datos.	Demora en la toma de decisiones.	No aplica	**1.** Ubicar la copia de seguridad más reciente **2.** Restaurar la información que haya sido modificada o borrada. **3.** Verifica que la restauración haya sido exitosa.
		Diligenciamiento de fecha diferente a la registrada en los documentos físicos.	Reprocesos en las actividades operativas.	No aplica	**1.** Verificar contra las evidencias físicas. **2.** Informar sobre la inconsistencia encontrada al

					responsable. **3.** Corregir la información.
Acción Integral	Pérdida de Confidencialidad	Desconocimiento de las normas asociados a protección de datos personales	Demandas por ley habeas data	El coordinador de Asesoría y Gestión semestralmente coordinará con las otras dependencias de la entidad las propuestas de mensajes sobre protección de datos personales, para ser incluidas en el plan de sensibilización de seguridad. En caso de requerir ajustes de diseño se coordinará con la Oficina Asesora de Comunicaciones. Se deja evidencia en el plan de sensibilización de seguridad.	**1.** El Director de DPTSC cuando se reciba una denuncia o demanda por habeas data coordina las acciones de respuesta con el Grupo de Defensa Jurídica.
		Debilidades en la administración de claves y contraseñas por parte de administradores delegados	Sanciones o llamados de atención por incumplimiento de ley habeas data	El coordinador de Asesoría y Gestión semestralmente verificará que se esté cumpliendo con a Guía de usuario en el Sistema Único de Información de Trámites-SUIT 3 sobre el correcto uso de la cuenta de usuario. Los ajustes y recomendaciones serán coordinados con el responsable de seguridad de la información. Se deja evidencia en la guía del usuario SUIT.	**2.** El coordinador de asesoría y gestión de la DPTSC enviará correo electrónico reiterando la importancia del manejo adecuado de la cuenta del usuario.
		Préstamo no controlado de cuentas de usuario	Pérdida de confianza Institucional	El coordinador de Asesoría y Gestión semestralmente verificará que se esté cumpliendo con a Guía de usuario en el Sistema Único de Información de Trámites-SUIT 3 sobre el correcto uso de la cuenta de usuario. Los ajustes y recomendaciones serán coordinados con el responsable de seguridad de la información. Se deja evidencia en la guía del usuario SUIT.	**2.** El coordinador de asesoría y gestión de la DPTSC enviará correo electrónico reiterando la importancia del manejo adecuado de la cuenta del usuario.
Gestión de Recursos	Pérdida de Confidencialidad	Manipulación inadecuada de los controles de confidencialidad en el SECOP II	Investigaciones disciplinarias	El líder del subproceso de Gestión Contractual durante la vigencia con el fin de sensibilizar a su equipo sobre la seguridad en SECOP II, socializa mediante comunicado los controles de seguridad. que se deben aplicar. En caso de no surtir los resultados del comunicado se reitera en las reuniones internas de seguimiento. Se evidencia su gestión mediante correo electrónico y actas de reunión.	**1.** Informar al ordenador del gasto **2.** Desactivar la vista pública del documento en la plataforma **3.** Evaluar el impacto legal
		Debilidades en los controles de la ley habeas data	Demandas	El líder del subproceso de Gestión Contractual durante la vigencia, con el fin de dar precisión a la cláusula de confidencialidad en los	**1.** Notificar al titular de la información y al responsable de

				procesos de contratación, actualizará la cláusula en la minuta para próximos contratos. Si se presentan demoras ante el ordenador del gasto en su aprobación alerta sobre los riesgos identificados. Se evidencia su gestión con el modelo de la cláusula y correos electrónicos.	seguridad de la información. **2.** Evaluar los impactos legales de la fuga de información **3.** Informar a la Superintendencia de Industria y Comercio a través del aplicativo web **4.** Definir con el comité de emergencia el tratamiento respectivo.
		Debilidad en los controles de seguridad para contraseñas	Reprocesos	El administrador de los sistemas de información institucionales, anualmente, con el fin de fortalecer la seguridad, configurará las opciones de seguridad de cambio obligatorio de claves y contraseñas en el directorio activo. En el caso de incidencias reconfirma las opciones de seguridad. Registro de configuración en el directorio activo.	**1.** Bloquear provisionalmente la cuenta **2.** Retroalimentación de la Política de Seguridad de la Información **3.** Evaluar la respectiva notificación al ente de control respectivo
Servicio al Ciudadano	Pérdida de Confidencialidad	Asignación errónea de roles y privilegios	Quejas y reclamos de los usuarios	No aplica	**1.** Identificar la causa de raíz de la pérdida de confidencialidad de los activos asociados al proceso.
		Incumplimiento de acuerdo de confidencialidad de proveedores	Procesos legales contra administradores externos de las bases de datos	No aplica	**2.** Definir e implementar las acciones de corrección.
		Desconocimiento políticas de seguridad digital	Sanciones por incumplimiento de habeas data	No aplica	**3.** Realizar seguimiento a la efectividad de las acciones definidas.
Gestión Documental	Pérdida de Confidencialidad	Permisos no autorizados de acceso a la información, o incumplimiento de los controles definidos en el proceso.	Procesos disciplinarios	No aplica	**1.** Reportar el incidente a la mesa de ayuda y aplicar el procedimiento de gestión de incidencias de seguridad

		Desconocimiento del nivel de clasificación o reserva de la información.	Investigaciones y posibles sanciones de los Entes de control internos y externos	No aplica	**2.** Identificar e implementar las acciones de corrección
		Fallas en los controles de acceso físico a la información.	Pérdida de Credibilidad	No aplica	**3.** Realizar seguimiento a la efectividad de las acciones.
Defensa Jurídica	Pérdida de Integridad	Falta de intervenciones necesarias por el Departamento	Reprocesos	No aplica	El profesional notificará de inmediato al Coordinador del Grupo de Defensa Judicial, quien a su vez informará al Director Jurídico, para implementar las medidas correctivas a que haya lugar.
		Archivo en un expediente diferente al correcto	Reprocesos	No aplica	
		Error en el archivo de folios	Reprocesos	No aplica	
Tecnologías de la Información	Pérdida de Confidencialidad	Debilidades en la gestión de contraseñas	Demandas	El líder del proceso y el responsable de seguridad de la información, semestralmente, con el fin de asegurar el manejo adecuado de las políticas de control de acceso, realizan campañas de sensibilización. De no cumplirse con las políticas se presenta el caso en el Comité de Gestión y Desempeño Institucional. Como evidencia se tienen las campañas, correos electrónicos o actas de comité.	**1.** Notificar al comité de Gestión y Desempeño la falta de aplicación de la Política y acciones para construir contraseñas seguras. **2.** Aplicar los correctivos.
		Debilidades en la gestión de roles y privilegios a servicios	Pérdida de la imagen institucional y del proceso	El responsable del servicio de información donde la administración de los usuarios este a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, cada vez que lo solicita el líder funcional, asigna los roles y privilegios, verificando el Proactivanet se apliquen los Checklist con parámetros de seguridad establecidos. En caso de no cumplir con la aplicación de los parámetros se devuelve. Como evidencia se tienen los ProactivaNet.	**1.** El líder funcional identifica la debilidad en los roles y privilegios y notifica a la Oficina de Tecnologías. **2.** Realizar las correcciones solicitadas.
		Debilidades en la clasificación de los activos de información	Investigaciones disciplinarias	Los responsables de los activos de información de la Oficina de Tecnologías de la Información y las Comunicaciones, semestralmente, con el propósito de mantener actualizada la calificación de la información y	**1.** Notificar a Gestión Documental del nuevo activo o cambio de clasificación del existente.

				prevenir accesos no autorizados a la misma, realizan la revisión del índice de información. Cuando se identifique un nuevo activo se informará al grupo de Gestión Documental. Como evidencia se tienen el índice y correos electrónicos.	**2.** Enviar listado de activos actualizado a Gestión Documental.
Tecnologías de la Información	Pérdida de Disponibilidad	Restricciones presupuestales para contar con infraestructura de alta disponibilidad.	Incumplimiento de objetivos y metas del proceso.	El líder del proceso mensualmente realiza seguimiento al proyecto de actualización de la arquitectura empresarial. Cuando sesione el comité institucional de gestión y desempeño reporta el avance. Como evidencia se tienen actas del comité y los informes de supervisión.	**1.** Activar planes de contingencias asociados a las dependencias afectadas. **2.** Revisar anualmente la actualización de los planes de contingencia.
		Obsolescencias tecnológicas.	Demoras en los procesos institucionales para el desarrollo de su gestión.	El responsable del activo de información cada vez que el fabricante libere versiones de software base para corregir vulnerabilidades, debe realizar el análisis de su impacto y si es viable apicararlas. Los coordinadores realizan seguimiento a la estrategia. Como evidencia se tiene el registro en ProactivaNet de la respectiva actualización	Reemplazar o actualizar los servicios tecnológicos de acuerdo con las disponibilidades de presupuesto y restricciones tecnológicas.
		Pérdida de servicios esenciales.	Afectación en la credibilidad de la entidad.	El profesional asignado diariamente con el fin de detectar variaciones en el desempeño de las plataformas monitoriza los eventos y mensajes generados por los dispositivos. En caso de presentarse el incidente se comunica con el proveedor o realiza las acciones pertinentes. Como evidencia se tienen las alertas generadas o correos electrónicos.	Activar planes de contingencias asociados a las dependencias afectadas.
		Entorno digital inseguro	Afectación en la reputación de la entidad.	El responsable de seguridad de la información e informática y el líder del proceso mensualmente, con el fin de verificar reportes y alertas de seguridad e identificar amenazas potenciales, realiza diagnósticos internos y externos de las plataformas o verifica reportes de entes externos. Cuando se identifican amenazas se realizan las acciones correspondientes. Como evidencia se tienen los reportes de comunicaciones por mensajes instantáneos o correos electrónicos de proveedores o reportes de grupos de interés o registro de pruebas de vulnerabilidades realizados.	Se activa protocolo de seguridad, donde se notifica al centro de respuesta de incidentes informáticos del MINTIC (C-SIRT).

		Incumplimiento en los acuerdos de nivel de servicio en el soporte por parte de los proveedores.	Afectación en la imagen de la entidad.	El supervisor del contrato cada vez que se presente una indisponibilidad del servicio con el fin de llevar un control de cada caso, registra en proactivaNet la indisponibilidad, la causa y su solución. En caso de presentarse incumplimiento se validarán las cláusulas del contrato. Como evidencia se tienen los informes mensuales de seguimiento y el registro en ProactivaNet.	**1.** Ejecutar clausulas presentes en el contrato. **2.** Activar planes de contingencia manual de las diferentes dependencias que se vean afectadas por la falta del servicio.
Tecnologías de la Información	Pérdida de Integridad	Ataques informáticos	Retrasos y reprocesos en los servicios de información	El profesional responsable de los servicios de información, cada vez que se actualiza el software base o se aprueban cambios en caso de que apliquen, con el fin de garantizar que el sistema permanezca actualizado y seguro, realiza la aplicación de parches de software y aplicativo. Cuando falla en la aplicación de parches se restaura la versión estable del servicio y se tramita un nuevo cambio de configuración. Como evidencia se tienen los controles de cambio registrados en ProactivaNet o correos electrónicos.	**1.** Aplicar el procedimiento de incidentes de seguridad de la información. **2.** Notificar al comité de emergencias de la incidencia. **3.** Si no se logra controlar el incidente, solicitar el apoyo de Csirt gobierno o Colcert de Mindefensa.
		Fallas tecnológicas	Demoras en la prestación de los servicios tecnológicos	El supervisor de acuerdo con la programación definida en el contrato, con el fin de garantizar el correcto funcionamiento y estabilidad del hardware, coordina el cumplimiento del mantenimiento preventivo. En caso de presentarse incidencias sobre el hardware se reporta al contratista para su respectiva solución. Como evidencia se tienen los correos electrónicos y registro de ProactivaNet.	**1.** Llamar al proveedor para notificar la ocurrencia de una falla. **2.** Aplicar el plan de contingencia.
		Error humano	Pérdida de credibilidad e imagen institucional	El profesional a cargo de los servicios del servidor de carpeta compartidas, ProactivaNet, Intranet, Orfeo, Portales Web y micrositios, anualmente, con el fin de prevenir la pérdida de información debido a errores humanos, generará un reporte de roles y privilegios y se remite al área para su revisión y formulación de ajustes. De acuerdo a la respuesta del área se realizan las modificaciones pertinentes. Como evidencia se tienen el Proactivanet y el informe de roles generado.	**1.** Notificar al administrador del servicio, sobre el error cometido en la plataforma. **2.** El administrador en caso de ser posible realiza la corrección respectiva. **3.** Si no es viable la corrección se solicita el apoyo interno o externo.

Comunicación	Pérdida de Integridad	Uso simultáneo de cuentas personales y cuentas institucionales en el mismo dispositivo	PQRSD por parte de los grupos de valor	El jefe del área de Comunicaciones en el último trimestre del año, con el fin de realizar el manejo de las redes sociales institucionales de manera segura, solicita la asignación de un dispositivo móvil (smartphone), propiedad de la entidad. En caso de no recibir el activo, el profesional asignado deberá continuar realizando las buenas prácticas sobre su dispositivo personal. Como evidencia se tiene el correo electrónico.	**1.** Eliminar las publicaciones. **2.** Responder, rectificar y generar comunicaciones aclaratorias a los grupos de valor. **3.** Comunicarse con el administrador directo de la red social para recuperar las cuentas en caso de vulneración.
		Acceso a las redes sociales desde computadores que no son seguros	Investigaciones disciplinarias y administrativas	El profesional asignado, cada vez que se requiera, con el fin de mantener la integridad de la información, da preferencia al uso de datos personales, frente al uso de redes inseguras externas. En caso de no tener acceso a las redes institucionales o de datos personales, se ingresa a redes externas verificando la seguridad de la misma. Como evidencia se tienen las publicaciones realizadas.	
		Uso de contraseñas débiles para acceso a las redes institucionales	Afectación de la imagen institucional	El profesional asignado, trimestralmente, con el fin de evitar la pérdida de integridad en el manejo de las redes sociales, modifica las contraseñas de acuerdo a la política y acciones para construir contraseñas seguras. En caso de que no se realice el cambio de claves en los tiempos previstos, el supervisor reitera la necesidad de cumplir la política de seguridad. Como evidencia se dejan los correos electrónicos en los que se informa al Jefe de la OAC sobre el cambio de contraseñas.	
Gestión Talento Humano	Pérdida de Confidencialidad	Errores en el otorgamiento de permisos de acceso a las carpetas de almacenamiento de información reservada	Incumplimiento de la ley Habeas Data	El coordinador del Grupo de Gestión Humana semestralmente solicitará a la Oficina de Tecnologías de la Información un reporte de usuarios con los permisos de acceso a la carpeta de historias laborales digitalizadas, para verificar que solo el personal debidamente autorizado tenga acceso En caso que se detecte permisos asignados incorrectamente se solicitará el ajuste. Se evidencia a través de correos electrónicos.	**1.** El coordinador del Grupo de Gestión Humana y su equipo de trabajo determinará el alcance de la divulgación no autorizada o perdida de confidencialidad. **2.** En caso de ser necesario se convocará

		Acceso no autorizado a las copias de respaldo de historias laborales digitalizadas	Pérdida de confianza	El coordinador del Grupo de Gestión Humana semestralmente solicitará a la Oficina de Tecnologías de la Información un reporte de los usuarios con los permisos de acceso a las copias de respaldo de la carpeta de historias laborales digitalizadas, ubicación y controles de seguridad que se aplican a las mismas, para verificar que solamente el personal autorizado tenga acceso y las copias estén salvaguardadas. En caso que se detecte permisos asignados incorrectamente u oportunidades de mejora se solicitará el ajuste. Se evidencia a través de correos electrónicos.	al comité de crisis para evaluar la estrategia de respuesta al incidente. **3.** Preparar notificaciones a los titulares de los datos afectados y a los entes de control correspondientes. **4.** Ordenar el reforzamiento de los controles de acceso a los activos de información. **5.** Paralelamente a las acciones mencionadas solicitar el acompañamiento al Grupo de Defensa Jurídica.
Evaluación Independiente	Pérdida de Confidencialidad	Ausencia de protocolo de seguridad de la Información para preservar las evidencias de auditorias	Especulaciones sobre resultados no oficialmente entregados y publicados	El Equipo de la Oficina de Control Interno durante la vigencia, elaborará el protocolo de seguridad de la información para protección de las evidencias. En el caso que la oficina no elabore este protocolo se acogerá a las políticas de operación establecidas por el departamento en esta materia. Se evidenciará mediante el documento de protocolo elaborado.	**1.** Restringir el acceso inmediato a la información que fue vulnerada.
		Desconocimiento en la identificación de la información clasificada y reservada	Pérdida de credibilidad en el proceso	El Jefe de la Oficina de Control Interno durante la vigencia, solicitará capacitación en materia de Seguridad de la Información y Protección de datos, con el fin de fortalecer los conocimientos y habilidades en el tema. En el caso que no se interioricen los conceptos se generaran nuevas estrategias. Se evidenciará su gestión mediante las actas de reuniones y material didáctico.	**2.** Notificar al líder del proceso afectado
		Debilidades en el establecimiento de roles y privilegios de las carpetas compartidas	Procesos disciplinarios	El Jefe de la Oficina de Control Interno durante la vigencia, solicitará mediante Proactivanet la aplicación de las restricciones a la información, con el fin de proteger la confidencialidad de las evidencias. En el caso de no aplicar la restricción se deberá acoger	**3.** Emprender la acción administrativa a que haya lugar.

				a las políticas de operación definidas por el Departamento. Se evidenciará mediante registro de Proactivanet.	
Evaluación Independiente	Pérdida de Integridad	Contraseñas fáciles de adivinar	Reprocesos	El Equipo de la Oficina de Control Interno esporádicamente, aplica las políticas de creación de contraseñas, con el fin de asegurar el control de acceso a la información. En el caso de no aplicación, cada integrante asume la responsabilidad de integridad de la información. Se evidencia su gestión mediante el registro de cambios de contraseña.	**1.** Recuperar la última versión y volver a aplicar los cambios aprobados
		Uso de información compartida	Pérdida de credibilidad de los informes presentados por el proceso	El responsable cada vez que requiera consolidar un informe, verifica que la información esté completa y corresponda a la versión final, con el fin de preservar la integridad del mismo. En el caso de identificar inconsistencias o modificaciones no autorizadas, corrobora con los profesionales de la oficina. Se evidencia su gestión mediante las diferentes versiones y la aprobación del documento final.	**2.** El jefe del proceso valida y aprueba la reconstrucción del documento.
		No utilización de herramientas de control de cambios en los documentos	Inadecuada toma de decisiones	Los profesionales que tienen conocimiento de la opción de control de cambios, cada vez que ajustan documentos, con el fin de conservar la trazabilidad de las modificaciones realizadas, aplican el control de cambios. En caso de no aplicación, justifica las modificaciones con la persona que consolida. Se evidencia su gestión mediante correos electrónicos y versiones del documento.	**3.** Publicación del documento.
Seguimiento y Evaluación	Pérdida de Integridad	Cambios no controlados o supervisados durante la publicación de la información	sanciones e incumplimientos	El líder o coordinador del proceso, semestralmente, con el fin de contar con copias de respaldo, revisa que la periodicidad de ejecución de las mismas, corresponda a la frecuencia con que se actualiza la información. Si se presentan cambios en el esquema de producción de datos, coordina con la OTIC los ajustes. Se evidenciará su gestión mediante Proactivanet y correos electrónicos.	**1.** Una vez identificado la modificación se solicita a la OTIC, se solicita la restauración del último Backup **2.** Con la copia restaurada, se valida si se requieren actualizar o afectar ajustes.
		Inadecuada segregación de	Demoras y retrabajos	El personal designado para la gestión de los archivos en la TRD, trimestralmente, con el fin	**1.** Hacer copias de respaldo de la

		roles para acceso a la información		de detectar de acceso no autorizado a la información, revisará de derechos de acceso de los usuarios. En caso de falla notifica al líder o coordinador del proceso para su ajuste. Evidencia de su gestión mediante correos electrónicos y Proactivanet.	información. **2.** Solicitar ajuste de roles a OTIC.
		Fallas tecnológicas que generen daño o alteración de la información	Toma errónea de decisiones	El líder o coordinador del proceso, semestralmente, con el fin de contar con copias de respaldo, revisa que la periodicidad de ejecución de las mismas, corresponda a la frecuencia con que se actualiza la información. Si se presentan cambios en el esquema de producción de datos, coordina con la OTIC los ajustes. Se evidenciará su gestión mediante Proactivanet y correos electrónicos.	**1.** Una vez identificado la modificación se solicita a la OTIC, se solicita la restauración del último Backup **2.** Con la copia restaurada, se valida si se requieren actualizar o afectar ajustes.
Seguimiento y Evaluación	Pérdida de la Disponibilidad de Activos	Inadecuado manejo de roles y privilegios para acceso a la información.	Incumplimiento de metas y compromisos	El líder y coordinador del proceso semestralmente, revisaran los privilegios asignados para acceso a la información mediante una matriz de roles y responsabilidades. En caso de inconsistencias gestionan los ajustes ante TI. Se evidenciará su gestión mediante matriz y tiquetes de Proactivanet.	**1.** Efectuar procesos manuales de tratamiento de información usando las copias de respaldo disponibles.
		Falla de servicios esenciales (correo, internet, intranet, servidor de carpeta compartidas)	Pérdida de confianza en el proceso	El Grupo de Mejoramiento semestralmente revisará y actualizará los planes de contingencia institucionales, para incluir acciones específicas que permitan reaccionar oportunamente. Si la acción específica no es efectiva se ajustará la estrategia. Se evidenciará su gestión mediante el plan de contingencia.	**2.** Realizar el tratamiento de la información usando copias de información disponibles en el computador de cada colaborador del proceso.
		Fallas en la plataforma tecnológica	Re-trabajos	El Grupo de Mejoramiento semestralmente revisará y actualizará los planes de contingencia institucionales, para incluir acciones específicas que permitan reaccionar oportunamente. Si la acción específica no es efectiva se ajustará la estrategia. Se evidenciará su gestión mediante el plan de contingencia.	**3.** Aplicar el plan de contingencia definido

Tabla 4. Matriz de riesgos de seguridad de la información

Plan de tratamiento de riesgos de seguridad de la información 2021

VERSIÓN 3

Proceso de Tecnologías de la información

Enero de 2021

Departamento Administrativo de la Función Pública

Carrera 6 n.º 12-62, Bogotá, D.C., Colombia

Conmutador: 7395656 Fax: 7395657

Web: www.funcionpublica.gov.co

eva@funcionpublica.gov.co

Línea gratuita de atención al usuario: 018000 917770

Bogotá, D.C., Colombia.