PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso: Gestión de TICS

2022

Versión	Fecha Versión	Observación
1	2021-01-20	Versión año 2021
2	2022-01-27	Actualización 2022

Tabla 1. Control de cambios

Tabla de contenido

Tablas de Informe

Tabla de ilustraciones

Introducción

El IPSE en su proceso de actualización y adaptación al marco legal en temas de seguridad digital, toma como referencia 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 .”

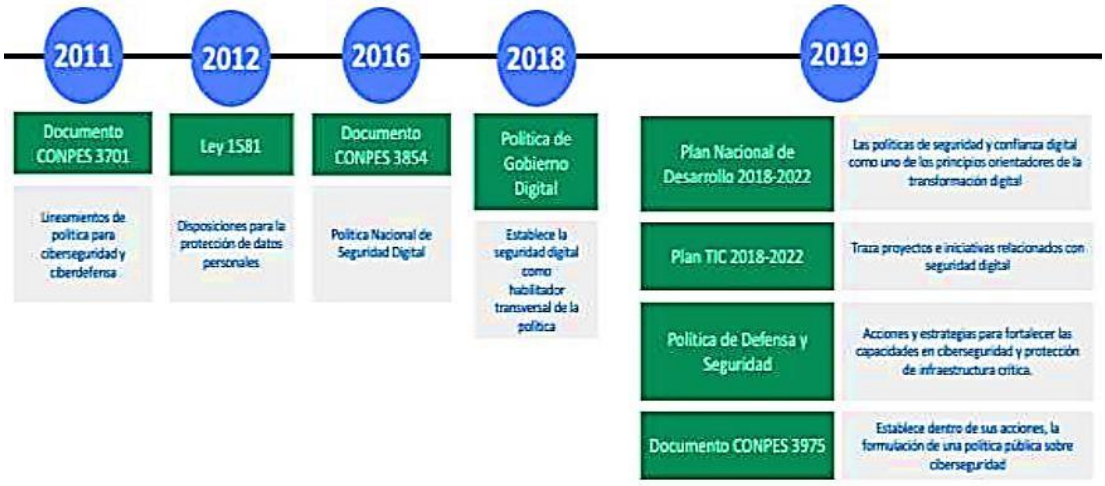

Ilustración 1. Implementación de Políticas y estrategias desde el Gobierno Nacional para brindar seguridad y defensa en el ciberespacio Fuente: Elaboración DNP, 2020

Sobre ese marco de trabajo El Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas - IPSE presenta su plan de tratamiento de riesgos de seguridad digital para la vigencia 2022.

Objetivo

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

a. 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.

b. 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
Resolución 512 de 2019	2021	Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
Decreto 103 de 2015,	2021	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	2021	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2021	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2021	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	2021	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	2021	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.	2021	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2021	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2021	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2021	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,	2021	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la lucha contra la corrupción y se dictan otras disposiciones

Marco Normativo	Año	Descripción
Ley 527 de 1999	2021	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	2021	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	2021	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	2021	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2021	Por la cual se dictan disposiciones generales para la protección de datos personales.

Tabla 2. Marco normativo

3. Tratamiento de riesgos

a. Factores de riesgo

Para la vigencia 2022 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

b. 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.

Para evaluar el riesgo aplicaremos la metodología de la ISO 27001

c. Evaluación de riesgos cualitativa

La evaluación de riesgos cualitativa destaca los mayores riesgos, lo que permite respaldar las decisiones de asignación de recursos. Pero también hace posible que los directores de área y los propietarios de riesgos se pregunten “que pasaría si…” con respecto a las consecuencias de varias acciones de gestión potenciales.

Este tipo de evaluación, dentro del análisis de riesgos en ISO 27001, se puede llevar a cabo de dos formas diferentes:

d. Evaluación simple

En una evaluación de riesgos simple, se evalúan las consecuencias y las probabilidades directamente. Una vez que identificamos los riesgos, simplemente utilizamos una escala para evaluar por separado las consecuencias y las probabilidades de cada uno de ellos.

Por ejemplo, se puede utilizar una escala de 0 a 4, en donde 0 es una probabilidad muy baja, 1 baja, 2 media, 3 muy probable y 4 extremadamente alta. Igualmente se podría utilizar una escala de 1 a 10. Cuanto mayor sea la escala, más precisos son los resultados, pero también más tiempo requerirá la evaluación.

e. Evaluación detallada de riesgos

En la evaluación detallada de riesgos, además de evaluar esos dos elementos –probabilidad y consecuencia– se evalúa otro adicional: el valor del activo. Para esto, se considera qué tipo de daño podría sucederle si su confidencialidad, integridad o disponibilidad estuviesen en peligro.

Como es lógico, tanto las amenazas como las vulnerabilidades influyen directamente en la probabilidad. Cuanto mayor es la amenaza y mayor es la vulnerabilidad, es más probable que ocurra el riesgo y viceversa.

Por ello, una vez se cuenta con los valores, calcular el riesgo es muy fácil. Es cuestión de realizar una operación matemática a elegir, o bien sumar o bien multiplicar los valores. Después de este cálculo es preciso determinar si los valores obtenidos son aceptables o no, y luego entrar en la etapa de gestión y tratamiento de riesgos.

f. Evaluación de riesgos cuantitativa

La evaluación cuantitativa en un análisis de riesgos en ISO 27001 considera datos puntuales, precisos y medibles, utilizando fórmulas matemáticas y recursos computacionales. De ese modo se calculan los valores de probabilidad e impacto usualmente expresados en cifras monetarias.

De acuerdo a estas dos evaluaciones utilizaremos la simple.

4. 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 2022, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

I lustración 2. Estrategias de Gestión de Riesgos 2021

a. 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

b. Estrategias Orientadas al Conocimiento

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, la Entidad adelantará en la vigencia 2022, 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

c. 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 2022 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

d. 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
- Renovación de la infraestructura tecnológica

5. Hoja de ruta

Producto	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

6. Acciones específicas

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
Planeación	Perdida 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 buen clima organizacional	El área de GABYS Y TICS 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 SGI. 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.
		Contraseñas genéricas	Imposibilidad de determinar los responsables de divulgación	El área de GABYS Y TICS 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 SGI. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución través de la documentación en Intranet.	3. Solicitar el cambio inmediato de la contraseña o en caso extremo la inhabilitación de la contraseña.
		Divulgación no autorizada de Contraseñas	Imposibilidad de determinar los responsables de divulgación	El Oficial de Seguridad de la Información durante la vigencia, implementará la estrategia de sensibilización y documentación	4. Activar el procedimiento de gestión de incidentes y reportar en el plan de mejoramiento.

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
				para el uso de contraseñas seguras. En caso 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.	
Planeación	Pérdida de Disponibilidad	Severidad para la gestión de cambios	Acciones de entes de control	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 a GABYS Y TICS quien activa acciones para agilizar el trámite respectivo.
		Falta de Capacitación y documentación	Producción de información inexacta y/o incompleta	**GABYS Y TICS** trimestralmente 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. **GABYS Y TICS** 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	**GABYS Y TICS** con el apoyo de comunicaciones 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 para el mejoramiento	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 actualizada.
		Falla tecnológica	Toma de decisiones inadecuada	El Jefe de TICS cuando se presente una incidencia no atendida dentro del acuerdo de nivel de servicio, notificará directamente al Jefe de tics, 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 tics para tomar medidas oportunas para su restablecimiento.
Planeación	Perdida de Integridad	Contraseñas genéricas	Pérdida de imagen y confianza institucional	GABYS Y TICS durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a t través de la documentación de las políticas de operación y del SGI. 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.

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
		Falla tecnológica	Reprocesos	El Jefe de TICS cuando se presente una incidencia no atendida dentro del acuerdo de nivel de servicio, notificará directamente al jefe de TICS y a la tercera línea de defensa el impacto de la incidencia, mediante comunicado oficial. Si aun así el incidente no es resuelto, se l levará 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 TICS para tomar medidas oportunas para su restablecimiento
		Inadecuado versiona miento de los documentos	Inadecuada toma de decisiones	El personal de Planeación 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 t través de TRD y correos electrónicos	3. Notificar al autor de las inconsistencias para su rectificación.
Gestión documental	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 l levando según l 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 del SIGIPSE	No aplica	Coordinar con el administrador de SIGIPSE para aplicar las medidas correctivas
		Fallas tecnológicas en el SIGIPSE	Reprocesos y demoras en la ejecución de actividades	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	El administrador del SIGIPSE socializara con los usuarios de la plataforma, los roles y caracterización de los usuarios, los cuales se comprometen a dar buen uso de ellos	1 . Retirar el rol inmediatamente
		Ausencia de acuerdos de confidencialidad	Pérdida de la imagen institucional y del proceso	El administrador 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	2. Oficiar el acuerdo de confidencialidad con copia a GABYS Y TICS.

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
				electrónicos, contratos o actas de posesión.	
		Incumplimiento de políticas de contraseñas seguras	Acceso de la información por parte de personal no autorizado	El administrador socializará la importancia del manejo de contraseñas seguras para el SIGIPSE, 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 al área de comunicaciones que todos los servidores y contratistas cambien la contraseña del SIGIPSE 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 notificación la plataforma estará disponible. Como evidencia se dejan correos de TICS	2. Corregir la información y volver a publicar
Grupo contractual	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.
Grupo contractual	Pérdida de Confidencialidad	Desconocimiento de las normas asociados a protección de datos personales.	Demandas por ley habeas data	El coordinador del área de TICS 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. 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

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
		Errores en almacenamiento de la información	Pérdida de credibilidad institucional	El coordinador del área de TICS 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 TICS, 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 en GLPI	digitalizado en el servidor de carpeta compartidas, se recurre al aplicativo ORFEO.
Grupo contractual	Pérdida de Confidencialidad	Desconocimiento de las normas asociados a protección de datos personales	Demandas por ley habeas data	El coordinador del área de TICS 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 de Comunicaciones. Se deja evidencia en el plan de sensibilización de seguridad.	1. Cuando se reciba una denuncia o demanda por habeas data, se coordina las acciones de respuesta con el área 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 TICS a partir de la vigencia 2019 documentara las responsabilidades sobre el correcto uso de las cuentas de usuarios en las plataformas del IPSE 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 oficial de seguridad y/o coordinador de TICS 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 profesional asignado por el área de TICS a partir de la vigencia 2019 documentara las responsabilidades sobre el correcto uso de las plataformas tecnológicas 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 oficial de seguridad y/o coordinador de TICS enviará comunicación formal de la cuenta de usuario reiterando la importancia del manejo de la misma
Tecnologías de la Información	Pérdida de Confidencialidad	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 TICS, cada vez que lo solicita el líder funcional, asigna los roles y privilegios, verificando el LDAP 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 formatos de solicitud de roles	1. El líder funcional identifica la debilidad en los roles y privilegios y notifica a TICS. 2. Realizar las correcciones solicitadas.
		Debilidades en la clasificación de los activos de información	Investigaciones disciplinarias	Los responsables de los activos de información de GABYS Y TICS, semestralmente, con el propósito de mantener actualizada la calificación de la información y prevenir accesos no autorizados a la misma, realizan la revisión del índice de información. Cuando se identifique un nuevo activo se informará a Gestión Documental. Como evidencia se tienen el índice y correos electrónicos.	1. Notificar a Gestión Documental del nuevo activo o cambio de clasificación del existente. 2. Enviar listado de activos actualizado a Gestión Documental.

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
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 del IPSE. 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 GLPI 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 GLPI 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 GLPI.	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

Proceso/ Subproceso	Nombre del Riesgo	Causas	Consecuencias	Acciones preventivas	Acción de contingencia ante posible materialización
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 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 o en la plataforma dispuesta por el proveedor	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, GLTI, Intranet, Orfeo, Vmware, bases de datos, 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 GLTI 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.

Tabla 4 Matriz de riesgos de seguridad de la información

FIN DEL DOCUMENTO