1 OBJETIVO

Evaluar constantemente el modelo de seguridad y privacidad de la información de la ADRES, mediante la verificación de la situación actual de la Entidad y su entorno, el entendimiento de la dinámica de los procesos de la Entidad y los agentes externos que intervienen directa e indirectamente, con el propósito de mantener actualizados, alineados, socializados y publicados los lineamientos de Seguridad y Privacidad de la ADRES, los cuales se encuentran definidos dentro de las políticas general y específicas de Seguridad y Privacidad de la información, así como el plan de Seguridad y Privacidad de la información que la Entidad ha adoptado.

2 ALCANCE

Inicia con la definición de los planes de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información, continua con la aprobación de estos, seguido con la definición del plan de Sensibilización en Seguridad de la Información y la ejecución de los diferentes planes; finaliza con el reporte de hitos alcanzados dentro del Plan de Acción de la Entidad

3 LÍDER DEL PROCEDIMIENTO

Director de Gestión de Tecnologías de Información y Comunicaciones.

4 POLÍTICAS DE OPERACIÓN

- El presente procedimiento se encuentra alineado con el Modelo de Arquitectura Empresarial que el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC ha definido.
- La Dirección de Gestión de Tecnologías de Información y Comunicaciones lidera el ejercicio del presente procedimiento, sin embargo, de ser necesario se requiere el apoyo de las otras direcciones y oficinas con el fin de llevar oportunamente la ejecución de las actividades que se planteen.
- La gestión de riesgos de seguridad y privacidad de la información se llevará a cabo de acuerdo con lo definido por el manual operativo de administración de riesgos de la Entidad.
- Las políticas de operación del presente procedimiento se encuentran alineadas con las directrices de la política Gestión de los Requisitos Legales que se encuentran dentro del marco de las Políticas Específicas de Seguridad y Privacidad de la Información que la Entidad ha definido.
- El Gestor de operaciones DGTIC, constantemente está verificando diferentes fuentes de información que apliquen directa o indirectamente a la entidad en los temas relacionados a su cargo. Para esto debe tomar como referencia:

FUENTE	PROVEEDOR
Plan de Seguridad y Privacidad de la Información de periodos anteriores.	Dirección de Gestión de Tecnologías de Información y Comunicaciones
Plan de Acción Integrado Anual.	Oficina Asesora de Planeación y Control de Riesgos

Resultados del Cuadro de Mando Integral	Oficina Asesora de Planeación y Control de Riesgos
Normatividad vigente aplicable	Diferentes entes del Gobierno Nacional
Marcos metodológicos vigentes	Diferentes entidades y empresas a nivel mundial
Matriz de Valoración de Activos de Información, la cual se encuentra dentro del formato OSTI-FR02.	Todos los procesos de la ADRES
Documentación de los sistemas de información	Dirección de Gestión de Tecnologías de Información y Comunicaciones
Documentación de incidentes de seguridad ocurridos al interior de la ADRES como en otras entidades	Dirección de Gestión de Tecnologías de Información y Comunicaciones Otras Entidades
Informes de control interno	Oficina de Control Interno
Informes generados por Entes de control	Entes de control
Informes de análisis de vulnerabilidades o Ethical Hacking realizados a la infraestructura tecnológica	Dirección de Gestión de Tecnologías de Información y Comunicaciones
Decisiones y/o requerimientos a nivel TI o que impacten la seguridad de la Información por parte de las dependencias de la ADRES	Todos los procesos de la ADRES
Políticas: general y específicas de Seguridad y Privacidad de la información	Dirección de Gestión de Tecnologías de Información y Comunicaciones
Plan Estratégico Institucional	Oficina Asesora de Planeación y Control de Riesgos
Plan Estratégico de la dirección de Gestión de Tecnologías de Información y Comunicaciones y de seguridad de la información	Dirección de Gestión de Tecnologías de Información y Comunicaciones

- Dentro de las actividades que se definan en el Plan de Seguridad y Privacidad de la Información se deben desarrollar acciones como:
  - (i) Revisar, actualizar, aprobar y socializar tanto las políticas generales y específicas de Seguridad y Privacidad de la información.
  - (ii) Ejercicios de análisis de vulnerabilidades o Ethical Hacking realizados a la infraestructura tecnológica.
  - (iii) Requerimientos legales relacionados con el alcance del Modelo de Seguridad y Privacidad de la Información.
  - (iv) Proyectos relacionados con Seguridad y Privacidad de la Información.

- El presente procedimiento está alineado con los siguientes controles ISO 27000:
  - i. A. 5.1.1 Conjunto de políticas para la seguridad de la información. la gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes
  - ii. A.5.1.2 Revisión de las políticas para la seguridad de la información. La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continuidad idónea, eficiencia y efectividad.

iii. A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

iv. A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

5 **REQUISITOS LEGALES:** Ver normograma del proceso.

6 DEFINICIONES: Ver glosario general.

7 DESARROLLO DEL PROCEDIMIENTO

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Elaborar Planes de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Anualmente conforme a las fechas que defina la Oficina Asesora de Planeación y Control de Riesgos - OAPCR, con el propósito de dar cumplimiento al decreto 612 de 2018, se estructuran los planes: de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para lo cual se apoya en las fuentes de información definidas dentro de las políticas del presente procedimiento. Dicho plan será diligenciado en el formato DIES-FR07 PLAN DE ACCIÓN ANUAL ADRES y una vez finalizado se le comunicará al director de Gestión de Tecnologías de Información y Comunicaciones.	Gestor de operaciones DGTIC	DIES-FR07 Plan de acción integrado anual ADRES elaborado
2 **PC**	Validar y aprobar Planes de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información	El director de Gestión de Tecnologías de Información y Comunicaciones, una vez se le haya informado sobre la definición del plan de Seguridad y Privacidad de la Información y con el propósito de validar si este se encuentra alineado con los objetivos definidos para la dependencia para la vigencia y las fuentes de información aplicables, valida las diferentes actividades que se hayan incluido dentro de este.	Director de Gestión de Tecnologías de Información y Comunicaciones	DIES-FR07 Plan de acción integrado anual ADRES aprobado

No	Actividad	Descripción de la Actividad	Responsable	Registro
		¿Las actividades se encuentran alineadas a los objetivos y fuentes de información aplicables? **SI**: remite a la OAPCR este plan junto con los demás planes de la dependencia que deben estar consolidados en el formato DIES-F07 PLAN DE ACCIÓN ANUAL ADRES y, por lo tanto, el procedimiento continúa con el Procedimiento de Formulación del Plan de Acción Integrado Anual y con la actividad siguiente. En el caso de ajustes, si éstos son aprobados por el Director de Tecnologías de la Información y las Comunicaciones, se remite el plan al procedimiento Seguimiento a la Ejecución del Plan de Acción Integrado Anual y Estratégico Institucional, para someter los ajustes a aprobación del Comité Institucional de Gestión y Desempeño y reflejarlos dentro del Plan de Acción Integrado Anual, en caso de aprobación. **NO**: Retorna a la actividad anterior, informándole al Gestor de operaciones DGTIC para que lleve a cabo los cambios respectivos.		
3	Definir plan de Sensibilización en Seguridad de la Información	Anualmente, con el propósito de buscar mecanismos para generar conciencia frente a la Seguridad y Privacidad de la Información, se define el plan de Sensibilización en Seguridad de la Información que se llevará a cabo dentro de la vigencia, previa aprobación del Plan de Acción Integrado Anual por parte de la Junta Directiva de la ADRES, el cual viene del Procedimiento de Formulación del Plan de Acción Integrado Anual, o de los cambios por parte del Comité Institucional de Gestión y Desempeño, que viene del Procedimiento de Seguimiento a la Ejecución del Plan de Acción Integrado Anual y Estratégico Institucional	Gestor de operaciones DGTIC	Plan de Sensibilización en Seguridad de la Información elaborado

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Una vez el plan de sensibilización se encuentre definido, se le remitirá al director de Gestión de Tecnologías de Información y Comunicaciones.		
4 **PC**	Validar plan de Sensibilización en Seguridad de la Información	El director de Gestión de Tecnologías de Información y Comunicaciones, una vez se le haya informado sobre la definición del plan de Sensibilización en Seguridad de la Información y con el propósito de validar si este se encuentra alineado con los objetivos definidos para la dependencia para la vigencia, valida las diferentes actividades que se hayan incluido dentro de este. ¿Las actividades se encuentran alineadas a los objetivos? **SI:** Informa a la OAPCR sobre el plan para que en la próxima sesión del Comité Institucional de Gestión y Desempeño sea validado y aprobado, continuando así con la actividad siguiente del presente procedimiento. **NO**: Informa al Gestor de operaciones DGTIC para que lleve a cabo los cambios respectivos y por consiguiente el procedimiento retorna a la actividad anterior.	Director de Gestión de Tecnologías de Información y Comunicaciones	Plan de Sensibilización en Seguridad de la Información aprobado
5	Desarrollar actividades definidas dentro de los planes	El Gestor de operaciones DGTIC y de ser necesario el personal requerido, conforme con el cronograma definido dentro de los planes de Seguridad y Privacidad de la Información, Sensibilización en Seguridad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el propósito de dar cumplimiento a los compromisos definidos, desarrolla las actividades correspondientes dejando evidencia de los avances o inconvenientes de las mismas. Dichas evidencias podrán ser entre otras: • Listados de asistencia • Actas • Material utilizado • Correos electrónicos	Gestor de operaciones DGTIC	Evidencia de actividades

No	Actividad	Descripción de la Actividad	Responsable	Registro
		• Publicaciones en página Web y/o Intranet		
6 **PC**	Validar ajustes a los planes	El Gestor de operaciones DGTIC una vez se desarrollen las actividades planeadas; con el propósito de revisar desviaciones de lo planeado versus lo ejecutado, realiza validaciones frente a las actividades definidas, dentro de estas validaciones podrá: (i) Replantear alcance de las actividades producto de limitantes en el tiempo, recurso o presupuesto que eventualmente se tenga planteado. (ii) Incluir nuevas actividades producto de necesidades emergentes de la Entidad, de la dirección o del entorno. ¿Se requiere ajustes? **SI**: Se deberá modificar según corresponda el Plan de Seguridad y Privacidad de la Información o el Plan de Sensibilización en Seguridad de la Información o el plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información retornado así a la actividad: Validar y aprobar Planes de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información **NO:** Se continuará (retornará) a la actividad Desarrollar actividades definidas dentro de los planes. O en caso de que corresponda fecha de reporte de los diferentes planes se continuará con la actividad Reportar los resultados de ejecución de los planes.	Gestor de operaciones DGTIC	Plan de Seguridad y Privacidad de la Información ajustado Plan de Sensibilización en Seguridad de la Información ajustado Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ajustado
7	Reportar los resultados de ejecución de los planes	El Gestor de operaciones DGTIC, teniendo en cuenta las fechas establecidas por la Oficina Asesora de Planeación y Control de Riesgos, con el propósito de informar los alcances y limitantes frente a los planes de Seguridad y Privacidad de la Información, Sensibilización en	Gestor de operaciones DGTIC	DIES-FR07 Plan de acción integrado anual ADRES

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Seguridad de la Información y Tratamiento de Riesgos de Seguridad y Privacidad de la Información; reporta los Hitos alcanzados que han sido definidos dentro de dichos planes y que se encuentran relacionados en DIES-F07 PLAN DE ACCIÓN INTEGRADO ANUAL ADRES. **FIN DEL PROCEDIMIENTO.**		

8 CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Asesor del proceso
01	29 de junio de 2018	Emisión y Publicación inicial	Johanna Bejarano Heredia Gestor de Operaciones OAPCR
02	08 de noviembre de 2019	Actualización del procedimiento de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 del Departamento Administrativo de la Función Pública – DAFP. Se redefinen las actividades del procedimiento en general teniendo en cuenta la inclusión de la Mesa de Servicios de la Dirección de Gestión de Tecnologías de Información y Comunicaciones.	Ricardo Andrés Varón Villareal Gestor de Operaciones OAPCR
03	*18 de marzo de 2020*	Actualización de las políticas de operación teniendo en cuenta el cambio de versión del Modelo de Arquitectura Empresarial definido por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.	Olga Marcela Vargas Asesor OAPCR
03	*9 de julio de 2020*	Actualización código por cambio de nombre del proceso de GSTE a OSTI. No se genera nueva versión debido a que no se modifica contenido del procedimiento y por lo tanto no requiere aprobación por parte del líder del proceso.	Olga Marcela Vargas Asesor OAPCR

9 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Juan Carlos Escobar Baquero Gestor de Operaciones - Dirección de Gestión de Tecnologías de Información y Comunicaciones	**Carlos Andrés Ruiz Romero** Gestor de Operaciones – Grupo Gestión Soporte a las Tecnologías	**Sergio Andrés Soler Rosas.** Director de Gestión de Tecnologías de Información y Comunicaciones